

# AWS Academy lab: Securing and Monitoring Resources with AWS

---

This project is part of the [Cloud Infrastructure Security Course](#) in the [Cybersecurity Specialization](#) at [CESAR School](#).

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

Student: [Pedro Coelho](#)

Instructor: [Ioram Sette](#)

## Table of Contents

- [AWS Academy lab: 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](#)
    - [Task 1.2: Enable versioning and object-level logging on a bucket](#)
    - [Task 1.3: Implement the S3 Inventory feature on a bucket](#)
    - [Task 1.4: Confirm that versioning works as intended](#)
    - [Task 1.5: Confirm object-level logging and query the access logs by using Athena](#)
  - [Phase 2: Securing VPCs](#)
    - [Task 2.1: Review LabVPC and its associated resources](#)
    - [Task 2.2: Create a VPC flow log](#)
    - [Task 2.3: Access the WebServer instance from the internet and review VPC flow logs in CloudWatch](#)
    - [Task 2.4: Configure route table and security group settings](#)
    - [Task 2.5: Secure the WebServerSubnet with a network ACL](#)
    - [Task 2.6: Review NetworkFirewallVPC and its associated resources](#)
    - [Task 2.7: Create a network firewall](#)
    - [Task 2.8: Create route tables](#)
    - [Task 2.9: Configure logging for the network firewall](#)
    - [Task 2.10: Configure the firewall policy and test access](#)
  - [Phase 3: Securing AWS resources by using AWS KMS](#)
    - [Task 3.1: Create a customer managed key and configure key rotation](#)
    - [Task 3.2: Update the AWS KMS key policy and analyze an IAM policy](#)
    - [Task 3.3: Use AWS KMS to encrypt data in Amazon S3](#)
    - [Task 3.4: Use AWS KMS to encrypt the root volume of an EC2 instance](#)
    - [Task 3.5: Use AWS KMS envelope encryption to encrypt data in place](#)
    - [Task 3.6: Use AWS KMS to encrypt a Secrets Manager secret](#)
  - [Phase 4: Monitoring and logging](#)
    - [Task 4.1: Use CloudTrail to record Amazon S3 API calls](#)
    - [Task 4.2: Use CloudWatch Logs to monitor secure logs](#)
    - [Task 4.3: Create a CloudWatch alarm to send notifications for security incidents](#)

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

## Phase 1: Securing Data in Amazon S3

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

data-bucket-01f5a3e8ab0aef64d [Info](#)

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

### Objects (2) [Info](#)

[Delete](#) [Actions ▾](#)

[Create folder](#)

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

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	<a href="#"></a> <a href="#">costumers.csv</a>	csv	September 28, 2024, 12:19:19 (UTC-03:00)	326.0 B	Standard
<input type="checkbox"/>	<a href="#"></a> <a href="#">myfile.txt</a>	txt	September 28, 2024, 10:25:36 (UTC-03:00)	11.0 B	Standard

## Bucket policy

[Edit](#) [Delete](#)

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



**Public access is blocked because Block Public Access settings are turned on for this bucket**

To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about [using Amazon S3 Block Public Access](#)

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

[Copy](#)

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

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

[Alt+S] | N. Virginia ▾ | paulo @ 5183-3738-6052

[Amazon S3](#) > [Buckets](#) > data-bucket-01f5a3e8ab0aef64d

## data-bucket-01f5a3e8ab0aef64d [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](#)

	Name	Type	Last modified	Size	Storage class
	<a href="#">costumers.csv</a>	csv	September 28, 2024, 12:19:19 (UTC-03:00)	326.0 B	Standard
	<a href="#">myfile.txt</a>	txt	September 28, 2024, 10:25:36 (UTC-03:00)	11.0 B	Standard

[Alt+S] | N. Virginia ▾ | mary @ 5183-3738-6052

[Amazon S3](#) > [Buckets](#) > data-bucket-01f5a3e8ab0aef64d

## data-bucket-01f5a3e8ab0aef64d [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](#)

	Name	Type	Last modified	Size	Storage class
--	------	------	---------------	------	---------------

**Insufficient permissions to list objects**

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

[Diagnose with Amazon Q](#)

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

## Bucket Versioning

[Edit](#)

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

Bucket Versioning

Enabled

Multi-factor authentication (MFA) delete

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

Disabled

## Server access logging

[Edit](#)

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

Server access logging

Enabled

Log object key format

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

Destination bucket

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

## Bucket policy

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

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

```
{
  "Version": "2012-10-17",
  "Id": "S3-Console-Auto-Gen-Policy-1727532601272",
  "Statement": [
    {
      "Sid": "S3PolicyStmt-DO-NOT-MODIFY-1727532601032",
      "Effect": "Allow",
      "Principal": {
        "Service": "logging.s3.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::s3-objects-access-log-01f5a3e8ab0aef64d/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "518337386052"
        }
      }
    }
  ]
}
```

[Copy](#)

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

Amazon S3 > Buckets > data-bucket-01f5a3e8ab0aef64d > Management > Inventory configurations

Inventory configurations (1)		Info	<a href="#">View details</a>	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Create job from manifest</a>	<a href="#">Create inventory configuration</a>														
You can create inventory configurations on a bucket to generate a flat file list of your objects and metadata. These scheduled reports can include all objects in the bucket or be limited to a shared prefix. <a href="#">Learn more</a>																					
<table border="1"> <thead> <tr> <th>Name</th> <th>Status</th> <th>Scope</th> <th>Destination</th> <th>Frequency</th> <th>Last export</th> <th>Format</th> </tr> </thead> <tbody> <tr> <td>Inventory</td> <td>Enabled</td> <td>Entire bucket</td> <td>s3://s3-inventory-01...</td> <td>Daily</td> <td>-</td> <td>Apache Parquet</td> </tr> </tbody> </table>								Name	Status	Scope	Destination	Frequency	Last export	Format	Inventory	Enabled	Entire bucket	s3://s3-inventory-01...	Daily	-	Apache Parquet
Name	Status	Scope	Destination	Frequency	Last export	Format															
Inventory	Enabled	Entire bucket	s3://s3-inventory-01...	Daily	-	Apache Parquet															

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

costumers.csv [Info](#)

[Copy S3 URI](#) [Download](#) [Open](#) [Object actions](#)

Properties Permissions Versions

Versions (2)

Version ID	Type	Last modified	Size	Storage class
<a href="#">oZ4wNmbDqQ33br5vKYh4y_LHkYliApv8</a> (Current version)	csv	September 28, 2024, 12:19:19 (UTC-03:00)	326.0 B	Standard
<a href="#">REG_2iXWDSMw.qt5x5.juxEEFKxr95wv</a>	csv	September 28, 2024, 12:17:35 (UTC-03:00)	204.0 B	Standard

Amazon S3 > Buckets > data-bucket-01f5a3e8ab0aef64d

[data-bucket-01f5a3e8ab0aef64d](#) [Info](#)

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

Objects [Info](#)

[Create folder](#) [Upload](#)

[Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#)

Find objects by prefix [Show versions](#)

[Diagnose with Amazon Q](#)

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>				

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

## s3-objects-access-log-01f5a3e8ab0aef64d [Info](#)

Objects Properties Permissions Metrics Management Access Points

### Objects (22) [Info](#)

[Create folder](#)  [Upload](#)

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

Find objects by prefix < 1 >

<input type="checkbox"/>	Name	Type	Last modified	Size
<input type="checkbox"/>	<a href="#"> data-bucket2024-09-28-14-40-31-4AE1B5152A0C479D</a>	-	September 28, 2024, 11:40:32 (UTC-03:00)	
<input type="checkbox"/>	<a href="#"> data-bucket2024-09-28-15-15-15-01808A9474A36B55</a>	-	September 28, 2024, 12:15:16 (UTC-03:00)	
<input type="checkbox"/>	<a href="#"> data-bucket2024-09-28-15-17-59-76C1C081FDEF98EA</a>	-	September 28, 2024, 12:18:00 (UTC-03:00)	
<input type="checkbox"/>	<a href="#"> data-bucket2024-09-28-15-18-18-CDD88C6D4879B8CA</a>	-	September 28, 2024, 12:18:19 (UTC-03:00)	

**Data**

Data source: AwsDataCatalog

Database: default

Tables and views: Create ▾

Filter tables and views

Tables (1) < 1 >

+ bucket\_logs :

Views (0) < 1 >

**Query 5 :**

```
1 CREATE EXTERNAL TABLE `default.bucket_logs`  
2   `bucketowner` STRING,  
3   `bucket_name` STRING,  
4   `requestdatetime` STRING,  
5   `remoteip` STRING,  
6   `requester` STRING,  
7   `requestid` STRING,  
8   `operation` STRING,  
9   `key` STRING,  
10  `request_uri` STRING,  
11  `httpstatus` STRING,  
12  `errorcode` STRING,  
13  `bytesent` BIGINT,  
14  `objectsize` BIGINT,  
15  `totaltime` STRING,
```

SQL Ln 37, Col 48

Run again Explain Cancel Clear

**Query results** | **Query stats**

Completed

Query successful.

**Query 6 :** X | **Query 5 :** X

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

SQL Ln 3, Col 38

**Run again** **Explain ↗** **Cancel** **Clear** **Create ▾**

**Query results** **Query stats**

🕒 Completed

## Results (22)

🔍 Search rows

#	▲ requester
1	arn:aws:iam::518337386052:user/paulo
2	arn:aws:iam::518337386052:user/paulo
3	arn:aws:iam::518337386052:user/paulo
4	arn:aws:iam::518337386052:user/paulo
5	arn:aws:iam::518337386052:user/paulo
6	arn:aws:iam::518337386052:user/paulo
7	arn:aws:iam::518337386052:user/paulo
8	arn:aws:iam::518337386052:user/paulo

## Phase 2: Securing VPCs

Task 2.1: Review LabVPC and its associated resources

VPC > Your VPCs > vpc-0c5491f25cd9300b1 / LabVPC

**Details** [Info](#)

VPC ID <a href="#">vpc-0c5491f25cd9300b1</a>	State <span>Available</span>	DNS hostnames Enabled
Tenancy Default	DHCP option set <a href="#">dopt-0e07fcbe09fcfc793a</a>	Main route table <a href="#">rtb-0240fd1f797fdc9cb</a>
Default VPC No	IPv4 CIDR 10.1.0.0/16	IPv6 pool -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID <a href="#">518337386052</a>

[Resource map](#) | [CIDRs](#) | [Flow logs](#) | [Tags](#) | [Integrations](#)

**Resource map** [Info](#)

```
graph LR; V[VPC] --- S[Subnets]; V --- RT[Route tables]; V --- NC[Network connections]; S --- RT; S --- NC;
```

The diagram illustrates the relationships between the VPC, Subnets, Route tables, and Network connections. The VPC is connected to Subnets, Route tables, and Network connections. Subnets are connected to Route tables.

**VPC** [Show details](#)  
Your AWS virtual network  
[LabVPC](#)

**Subnets (1)**  
Subnets within this VPC  
**us-east-1a**  
[WebServerSubnet](#)

**Route tables (1)**  
Route network traffic to resources  
[rtb-0240fd1f797fdc9cb](#)

**Network connections (1)**  
Connections to other networks  
[LabVPCIG](#)

## Roles (22) [Info](#)

An IAM role is an identity you can create and manage.

[Search](#)

<input type="checkbox"/>	Role name
<input type="checkbox"/>	<a href="#"><u>VPCFlowLogsRole</u></a>
<input type="checkbox"/>	<a href="#"><u>WebServerRole</u></a>

[IAM](#) > [Roles](#) > [VPCFlowLogsRole](#)

# VPCFlowLogsRole [Info](#)

## Summary

Creation date

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

Last activity

-

[Permissions](#)

[Trust relationships](#)

[Tags \(1\)](#)

[Last Accessed](#)

## Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

 *Search*



**Policy name** 



[VPCFlowLogPolicy](#)

**Instances (1/3) Info**

All states												
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitoring	Security group name
aws-cloud9-Cl...	i-0ddaaef5de964e6340	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	<span>View alarms</span>	us-east-1a	ec2-35-172-187-250.co...	35.172.187.250	35.172.187.250	-	disabled	aws-cloud9-CloudInst...
<b>WebServer</b>	<b>i-09e257fb839c1ea</b>	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	<span>View alarms</span>	us-east-1a	ec2-50-19-156-90.com...	50.19.156.90	50.19.156.90	-	disabled	WebServerSecurityGroup
WebServer2	i-0774fae6376088697	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	<span>View alarms</span>	us-east-1a	ec2-34-193-5-254.com...	34.193.5.254	34.193.5.254	-	disabled	WebServer2SecurityGroup

**i-09e257fb839c1ea (WebServer)**

**Details** | Status and alarms | Monitoring | Security | Networking | Storage | Tags

**Instance summary** Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-09e257fb839c1ea (WebServer)	50.19.156.90   open address	10.1.3.4
IPv6 address	Instance state	Public IPv4 DNS
-	<span>Running</span>	ec2-50-19-156-90.compute-1.amazonaws.com   open address
Hostname type	Private IP DNS name (IPv4 only)	Elastic IP addresses
IP name: ip-10-1-3-4.ec2.internal	ip-10-1-3-4.ec2.internal	50.19.156.90 (WebServerEIP) [Public IP]
Answer private resource DNS name	Instance type	AWS Compute Optimizer finding
-	t2.micro	<span>Opt-in to AWS Compute Optimizer for recommendations.</span>   Learn more
Auto-assigned IP address	VPC ID	Auto Scaling Group name
-	vpc-0c5491f25cd9300b1 (LabVPC)	-
IAM Role	Subnet ID	
WebServerRole	subnet-02947d525beaa6185 (WebServerSubnet)	

## Task 2.2: Create a VPC flow log

[VPC](#) > [Your VPCs](#) > vpc-0c5491f25cd9300b1 / LabVPC

**Details** Info

VPC ID	State	DNS hostnames	DNS resolution
vpc-0c5491f25cd9300b1	<span>Available</span>	Enabled	Enabled
Tenancy	DHCP option set	Main route table	Main network ACL
Default	dopt-0e07fcceb09fcf793a	rtb-0240fd1f797fd9cb	act-05aa62e2e5673f030d
Default VPC No	IPv4 CIDR	IPv6 pool	IPv6 CIDR (Network border group)
No	10.1.0.0/16	-	-
Network Address Usage metrics	Route 53 Resolver DNS Firewall rule groups	Owner ID	
Disabled	-	518337386052	

[Resource map](#) | [CIDRs](#) | [Flow logs](#) | [Tags](#) | [Integrations](#)

**Flow logs (1) Info**

Name	Flow log ID	Filter	Destination type	Destination name	IAM role ARN	Cross account IAM role	Maximum aggregation interval
LabVPCFlowLogs	fl-05e2bfe14954ff7f5	ALL	cloud-watch-logs	LabVPCFlowLogs	arn:aws:iam::518337386052:role/vpcfl...	-	1 minute

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

```
voclabs:~/environment $ nc -vz 50.19.156.90 80
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connection timed out.

voclabs:~/environment $ nc -vz 50.19.156.90 22
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connection timed out.
```

[CloudWatch](#) > [Log groups](#) > [LabVPCFlowLogs](#) > eni-00b4de5af5738678d-all

**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
2024-09-29T11:46:52.000Z	2 518337386052 eni-00b4de5af5738678d 35.172.187.250 10.1.3.4 37768 80 6 4 240 1727610412 1727610472 REJECT OK
2 518337386052 eni-00b4de5af5738678d 35.172.187.250 10.1.3.4 37768 80 6 4 240 1727610412 1727610472 REJECT OK	
2024-09-29T11:46:52.000Z	2 518337386052 eni-00b4de5af5738678d 35.172.187.250 10.1.3.4 53150 22 6 4 240 1727610412 1727610472 REJECT OK
2 518337386052 eni-00b4de5af5738678d 35.172.187.250 10.1.3.4 53150 22 6 4 240 1727610412 1727610472 REJECT OK	

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

Details								
Security group name <a href="#">WebServerSecurityGroup</a>	Security group ID <a href="#">sg-0099b6b85d2b5052d</a>	Description <a href="#">WebServerSecurityGroup</a>						
Owner <a href="#">518337386052</a>	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry						
<a href="#">Inbound rules</a>	<a href="#">Outbound rules</a>	<a href="#">Tags</a>						
<b>Inbound rules (3)</b>  <input type="text" value="Search"/>								
<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	
<input type="checkbox"/>	-	sgr-05538fd817df7c264	IPv4	SSH	TCP	22	18.206.107.24/29	
<input type="checkbox"/>	-	sgr-066269d462c1d5...	IPv4	SSH	TCP	22	35.172.187.250/32	
<input type="checkbox"/>	-	sgr-038b9a55ecb4cc8b8	IPv4	HTTP	TCP	80	0.0.0.0/0	

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

```
aws Services Search [Alt+S]
,
~\ ##
~~ \###\ Amazon Linux 2023
~~ \###|
~~ \#/ https://aws.amazon.com/linux/amazon-linux-2023
~~ V~,'->
~~ /'
~~-. / /
~/m/
[ec2-user@webserver ~]$ ping -c 3 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (3.162.95.220) 56(84) bytes of data.
64 bytes from server-3-162-95-220.iad61.r.cloudfront.net (3.162.95.220): icmp_seq=1 ttl=246 time=1.59 ms
64 bytes from server-3-162-95-220.iad61.r.cloudfront.net (3.162.95.220): icmp_seq=2 ttl=246 time=2.18 ms
64 bytes from server-3-162-95-220.iad61.r.cloudfront.net (3.162.95.220): icmp_seq=3 ttl=246 time=1.90 ms
--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.589/1.890/2.179/0.241 ms
[ec2-user@webserver ~]$
```

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

Inbound rules (3)						
Filter inbound rules						
Rule number	Type	Protocol	Port range	Source	Allow/Deny	
90	HTTP (80)	TCP (6)	80	0.0.0.0/0	<span>Allow</span>	
100	SSH (22)	TCP (6)	22	0.0.0.0/0	<span>Allow</span>	
^	All traffic	All	All	0.0.0.0/0	<span>Deny</span>	

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

## Task 2.6: Review NetworkFirewallVPC and its associated resources

i-0774fae6376088697 (WebServer2)

Details | Status and alarms | Monitoring | **Security** | Networking | Storage | Tags

▼ Security details

IAM Role [WebServerRole](#)

Owner ID [518337386052](#)

Security groups

[sg-0bface695daa9298f \(WebServer2SecurityGroup\)](#)

▼ Inbound rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups
-	sgr-0584715ebb4249f4e	8080	TCP	0.0.0.0/0	<a href="#">WebServer2SecurityGroup</a>
-	sgr-00bb5f3152f129797	80	TCP	0.0.0.0/0	<a href="#">WebServer2SecurityGroup</a>
-	sgr-059499d8f4c0f083d	22	TCP	0.0.0.0/0	<a href="#">WebServer2SecurityGroup</a>

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

```

      #
~\ _###_          Amazon Linux 2023
~~ \###\_
~~ \|##|
~~   \#/ ___
~~     V~' '-->
~~~   /
~~. / /
~/m/,'

[ec2-user@webserver2 ~]$ python3 -m http.server 8080 &
[1] 7247
[ec2-user@webserver2 ~]$ Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
35.172.187.250 - - [29/Sep/2024 12:41:04] "GET / HTTP/1.1" 200 -

```

## Task 2.7: Create a network firewall

VPC > Network Firewall: Firewalls > NetworkFirewall

### NetworkFirewall

**Overview**

<p>Firewall status</p> <span style="color: green;">Ready</span>	<p>Associated firewall policy</p> <a href="#">FirewallPolicy</a>
---	--

## Task 2.8: Create route tables

VPC > Route tables > rtb-03fa3a9b36e4c05be / IGW-Ingress-Route-Table

<p><b>Details</b> <a href="#">Info</a></p> <table border="0" style="width: 100%;"> <tr> <td style="width: 30%;">Route table ID</td> <td style="width: 30%;"><a href="#">rtb-03fa3a9b36e4c05be</a></td> <td style="width: 30%;">Main</td> </tr> <tr> <td> </td> <td><input type="checkbox"/> No</td> <td><input type="checkbox"/> Explicit subnet associations</td> </tr> <tr> <td>VPC</td> <td><a href="#">vpc-03fb5f5a8c2805eb3</a>   NetworkFirewallVPC</td> <td>Owner ID</td> </tr> <tr> <td></td> <td></td> <td><a href="#">518337386052</a></td> </tr> </table>	Route table ID	<a href="#">rtb-03fa3a9b36e4c05be</a>	Main		<input type="checkbox"/> No	<input type="checkbox"/> Explicit subnet associations	VPC	<a href="#">vpc-03fb5f5a8c2805eb3</a>   NetworkFirewallVPC	Owner ID			<a href="#">518337386052</a>	<p>Edge associations</p> <a href="#">igw-080d41ec5e542bcb0</a> / NetworkFirewallIG
Route table ID	<a href="#">rtb-03fa3a9b36e4c05be</a>	Main											
	<input type="checkbox"/> No	<input type="checkbox"/> Explicit subnet associations											
VPC	<a href="#">vpc-03fb5f5a8c2805eb3</a>   NetworkFirewallVPC	Owner ID											
		<a href="#">518337386052</a>											

[Routes](#) [Subnet associations](#) [Edge associations](#) [Route propagation](#) [Tags](#)

**Routes (2)**

Destination	Target	Status	Propagated
10.1.0.0/16	local	<input checked="" type="radio"/> Active	No
10.1.3.0/28	<a href="#">vpce-052c1b6ba247f7a54</a>	<input checked="" type="radio"/> Active	No

rtb-0fd32d2679d39aae3 / Firewall-Route-Table

<p><b>Details</b> <a href="#">Info</a></p> <table border="0" style="width: 100%;"> <tr> <td style="width: 30%;">Route table ID</td> <td style="width: 30%;"><a href="#">rtb-0fd32d2679d39aae3</a></td> <td style="width: 30%;">Main</td> </tr> <tr> <td> </td> <td><input type="checkbox"/> No</td> <td><input type="checkbox"/> Explicit subnet associations</td> </tr> <tr> <td>VPC</td> <td><a href="#">vpc-03fb5f5a8c2805eb3</a>   NetworkFirewallVPC</td> <td>Owner ID</td> </tr> <tr> <td></td> <td></td> <td><a href="#">518337386052</a></td> </tr> </table>	Route table ID	<a href="#">rtb-0fd32d2679d39aae3</a>	Main		<input type="checkbox"/> No	<input type="checkbox"/> Explicit subnet associations	VPC	<a href="#">vpc-03fb5f5a8c2805eb3</a>   NetworkFirewallVPC	Owner ID			<a href="#">518337386052</a>	<p>Explicit subnet associations</p> <a href="#">subnet-0817412e9879898bf</a> / FirewallSubnet
Route table ID	<a href="#">rtb-0fd32d2679d39aae3</a>	Main											
	<input type="checkbox"/> No	<input type="checkbox"/> Explicit subnet associations											
VPC	<a href="#">vpc-03fb5f5a8c2805eb3</a>   NetworkFirewallVPC	Owner ID											
		<a href="#">518337386052</a>											

[Routes](#) [Subnet associations](#) [Edge associations](#) [Route propagation](#) [Tags](#)

**Routes (2)**

Destination	Target	Status	Propagated
0.0.0.0/0	<a href="#">igw-080d41ec5e542bcb0</a>	<input checked="" type="radio"/> Active	No
10.1.0.0/16	local	<input checked="" type="radio"/> Active	No

rtb-051dbbce25bbdf429 / WebServer2-Route-Table

Details		Info
Route table ID <a href="#">rtb-051dbbce25bbdf429</a>	Main	Explicit subnet associations
VPC <a href="#">vpc-03fb5f5a8c2805eb3</a>   NetworkFirewallVPC	No	<a href="#">subnet-070adb973424bad13</a> / WebServer2Subnet
Owner ID <a href="#">518337386052</a>		

[Routes](#) | [Subnet associations](#) | [Edge associations](#) | [Route propagation](#) | [Tags](#)

---

Routes (2)		
<input type="text"/> Filter routes		
Destination	Target	Status
0.0.0.0/0	<a href="#">vpce-052c1b6ba247f7a54</a>	<span>Active</span>
10.1.0.0/16	local	<span>Active</span>

## Task 2.9: Configure logging for the network firewall

Logging				Edit
Network Firewall generates logs for stateful rule groups. You can configure different destinations for different log types.				
Log type	Alert log destination	Flow log destination	TLS log destination	
Flow, Alert	CloudWatch log group - NetworkFirewallVPCLogs	CloudWatch log group - NetworkFirewallVPCLogs	Not configured	

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

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

Rules (5)								
<input type="text"/> Find resources by name or value								
Description	Geo IP	Protocol	Source	Destination	Destination port	Direction	Action	
-	-	TCP	ANY	ANY	8080	Forward	Drop	
-	-	TCP	ANY	ANY	80	Forward	Pass	
-	-	TCP	ANY	ANY	22	Forward	Pass	
-	-	TCP	ANY	ANY	443	Forward	Pass	
-	-	ICMP	ANY	ANY	ANY	Forward	Pass	

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

```
      #_
  ~\  #####      Amazon Linux 2023
  ~~ \#####\
  ~~  \###|
  ~~   \#/   https://aws.amazon.com/linux/amazon-linux-2023
  ~~    V~, /_>
  ~~~   /_/
  ~~_. /_/
  _/m/,'

Last login: Sun Sep 29 12:39:55 2024 from 18.206.107.28
[ec2-user@webserver2 ~]$ ping -c 3 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.154.236.231) 56(84) bytes of data.
64 bytes from server-18-154-236-231.iad55.r.cloudfront.net (18.154.236.231): icmp_seq=1 ttl=244 time=3.77 ms
64 bytes from server-18-154-236-231.iad55.r.cloudfront.net (18.154.236.231): icmp_seq=2 ttl=244 time=2.42 ms
64 bytes from server-18-154-236-231.iad55.r.cloudfront.net (18.154.236.231): icmp_seq=3 ttl=244 time=2.22 ms

--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 2.220/2.806/3.774/0.689 ms
[ec2-user@webserver2 ~]$ sudo netstat -tulpn | grep -i listen
tcp        0      0 0.0.0.0:22          0.0.0.0:*          LISTEN      2331/sshd: /usr/sbi
tcp        0      0 0.0.0.0:8080        0.0.0.0:*          LISTEN      7247/python3
tcp6       0      0 ::1:22             ::*:*              LISTEN      2331/sshd: /usr/sbi
tcp6       0      0 ::1:80             ::*:*              LISTEN      1998/httpd
[ec2-user@webserver2 ~]$
```

## Phase 3: Securing AWS resources by using AWS KMS

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

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

## ec6e4c68-5c3f-456f-b6d8-df77f09a2202

### General configuration

Alias	Status
MyKMSKey	Enabled
ARN	Description
<input type="checkbox"/> arn:aws:kms:us-east-1:518337386052:key/ec6e4c68-5c3f-456f-b6d8-df77f09a2202	-

### Key policy

### Key administrators (1)

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

Search Key administrators

Name

Path

voclabs

/

### Key deletion

Allow key administrators to delete this key

### Key users (1)

The following IAM users and roles can use this key for cryptographic operations. They can also allow AWS services that are integrated with KMS to us

Search Key users

Name

Path

voclabs

/

<b>Automatic key rotation</b> <small>Info</small>	
AWS KMS automatically rotates the key based on the rotation period that you define.	
Status	Rotation period
<input checked="" type="checkbox"/> Enabled	365

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

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

# ec6e4c68-5c3f-456f-b6d8-df77f09a2202

## General configuration

Alias

MyKMSKey

ARN

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

Key policy

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

# FinancialAdvisorGroup [Info](#)

## Summary

User group name

FinancialAdvisorGroup

Users (1)

**Permissions**

Last Accessed

## Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.



*Search*



Policy name



PolicyForFinancialAdvisors

# PolicyForFinancialAdvisors [Info](#)

## Policy details

Type

Customer managed

Creation time

September 28, 2024, 10:

[Permissions](#)

[Entities attached](#)

[Tags](#)

[Policy versions \(1\)](#)

[Last Accessed](#)

i This policy defines some actions, resources, or conditions that do not provide permissions. To grant access to a service or resource, define a condition or action that includes the service or resource.

## Permissions defined in this policy [Info](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity, attach a policy document to the identity.

 [Search](#)

### Allow (2 of 421 services)

Service	▲	Access level	▼	Resource
<a href="#">KMS</a>		Limited: Read, Write		All resources
<a href="#">S3</a>		Limited: List, Read, Write		BucketName  string like  All

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

The screenshot shows the AWS Lambda console with a success message: "Upload succeeded". Below it, the "Upload: status" page displays a summary of the upload results. The destination was "s3://data-bucket-01f5a3e8ab0aef64d". The status shows 1 file (loan-data.csv) succeeded at 168.0 B (100.00%) and 0 files failed at 0 B (0%). The "Files and folders" tab is selected, showing a table with one item: "loan-data.csv" which is a text/csv file of size 168.0 B and status Succeeded.

The screenshot shows the "Server-side encryption settings" page. It indicates that server-side encryption protects data at rest. Under "Encryption type", it says "Server-side encryption with AWS Key Management Service keys (SSE-KMS)". The "Encryption key ARN" is listed as "arn:aws:kms:us-east-1:518337386052:key/ec6e4c68-5c3f-456f-b6d8-df77f09a2202". Under "Bucket Key", it says "When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS." A link to "Learn more" is provided. The "Enabled" setting is checked.

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::518337386052:user/paulo is not authorized to perform: kms:Decrypt on resource: arn:aws:kms:us-east-1:518337386052:key/ec6e4c68-5c3f-456f-b6d8-df77f09a2202 because no identity-based policy allows the kms:Decrypt action</Message>
  <RequestId>8JS7FARVN2E8PNCE</RequestId>
  <HostId>9i46fNzBe4nf/UV4mhJF6focXUf1ZZdLikp9qvdlCRN0ynJygfP4T8xBt3xvYBao5nd20kzQKIY=</HostId>
</Error>

```

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

Instances (1/4) [Info](#)

Find Instance by attribute or tag (case-sensitive)			All states								
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Pub		
<input type="checkbox"/>	aws-cloud9-Cl...	i-0ddaeaf5de964e6340	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	<a href="#">View alarms</a>	us-east-1a	ec2-35-172-187-250.co...	35.1		
<input checked="" type="checkbox"/>	EncryptedInst...	i-0f05ad44565e48aea	<span>Running</span>	t2.micro	<span>Initializing</span>	<a href="#">View alarms</a>	us-east-1a	ec2-3-93-70-56.comput...	3.93		
<input type="checkbox"/>	WebServer	i-09e257fbbed839c1ea	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	<a href="#">View alarms</a>	us-east-1a	ec2-50-19-156-90.com...	50.1		
<input type="checkbox"/>	WebServer?	i-0774fa63376088697	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	<a href="#">View alarms</a>	us-east-1a	ec2-3-192-5-254.com	34.1		

i-0f05ad44565e48aea (EncryptedInstance)

Details	Status and alarms	Monitoring	Security	Networking	<b>Storage</b>	Tags	
<b>▼ Root device details</b>							
Root device name					Root device type		
 /dev/xvda					EBS		
<b>▼ Block devices</b>							
<input data-bbox="152 507 166 512" type="text"/> Filter block devices							
✓	Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID
<input checked="" type="checkbox"/>	vol-08901071224b259bc	/dev/xvda	8	 Attached	2024/09/29 12:54 GMT-3	Yes	ec6e4c68-5c3f-456f-b6d8-df77f09a2202

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

```
'`#_
~\_####`      Amazon Linux 2023
~~\_####\_
~~ \###|
~~  \#/ _-_
~~   V~' _-'>
~~~ /
~~.-. / \
~~-/`/ \
/_m/`/ \
Last login: Sun Sep 29 13:51:50 2024 from 18.206.107.27
[ec2-user@webserver2 ~]$ echo "Let's encrypt these file contents. Sensitive data here." > data_unencrypted.txt
[ec2-user@webserver2 ~]$ cat data_unencrypted.txt
Let's encrypt these file contents. Sensitive data here.
[ec2-user@webserver2 ~]$ aws kms list-keys
{
  "Keys": [
    {
      "KeyId": "2325c571-f352-4aa8-8da9-3271d070d7df",
      "KeyArn": "arn:aws:kms:us-east-1:518337386052:key/2325c571-f352-4aa8-8da9-3271d070d7df"
    },
    {
      "KeyId": "b99b66cb-bf3e-4e07-b459-48a8135f6533",
      "KeyArn": "arn:aws:kms:us-east-1:518337386052:key/b99b66cb-bf3e-4e07-b459-48a8135f6533"
    },
    {
      "KeyId": "ec6e4c68-5c3f-456f-b6d8-df77f09a2202",
      "KeyArn": "arn:aws:kms:us-east-1:518337386052:key/ec6e4c68-5c3f-456f-b6d8-df77f09a2202"
    }
  ]
}
[ec2-user@webserver2 ~]$ result=$(aws kms generate-data-key --key-id alias/MyKMSKey --key-spec AES_256)
echo $result | python3 -m json.tool
{
  "CiphertextBlob": "AQIDAHhEpCW7g3QGgj+PiTiImuyJdxXrkS8l2f7zcEPDgiJ/VQHqhBHo8aaGq3Lt7SLRhBpvAAAAAfjb8BgkqhkiG9w0
  "Plaintext": "pzY+3UIVDHoSdm/4bbWgZpVwtv35tRpWYZRTDUmcyFI=",
  "KeyId": "arn:aws:kms:us-east-1:518337386052:key/ec6e4c68-5c3f-456f-b6d8-df77f09a2202"
}
[ec2-user@webserver2 ~]$ █
```

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

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

```
[ec2-user@webserver2 ~]$ aws secretsmanager list-secrets
{
    "SecretList": [
        {
            "ARN": "arn:aws:secretsmanager:us-east-1:518337386052:secret:mysecret-M3j0wd",
            "Name": "mysecret",
            "KmsKeyId": "arn:aws:kms:us-east-1:518337386052:key/ec6e4c68-5c3f-456f-b6d8-df77f09a2202",
            "LastChangedDate": "2024-09-29T16:06:50.152000+00:00",
            "Tags": [],
            "SecretVersionsToStages": {
                "2d6b815e-04d9-475d-875e-f86976acdelf": [
                    "AWSCURRENT"
                ]
            },
            "CreatedDate": "2024-09-29T16:06:50.087000+00:00"
        }
    ]
}
[ec2-user@webserver2 ~]$ aws secretsmanager get-secret-value --secret-id mysecret
{
    "ARN": "arn:aws:secretsmanager:us-east-1:518337386052:secret:mysecret-M3j0wd",
    "Name": "mysecret",
    "VersionId": "2d6b815e-04d9-475d-875e-f86976acdelf",
    "SecretString": "{\"secret\":\"my secret data\"}",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": "2024-09-29T16:06:50.146000+00:00"
}
[ec2-user@webserver2 ~]$ █
```

## Phase 4: Monitoring and logging

#### Task 4.1: Use CloudTrail to record Amazon S3 API calls

Trails										
<span style="float: right;">Copy events to Lake</span> <span style="float: right;"></span> <span style="float: right;">Delete</span> <span style="float: right; background-color: orange; color: white; padding: 2px 5px;">Create trail</span>										
Name	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status		
<a href="#">data-bucket-reads-writes</a>	US East (N. Virginia)	Yes	Disabled	No	<a href="#">cloudtrail-logs-01f5a3e8ab0aeaf64d</a>	-	-		Logging	

⌚ Successfully created Athena table: [cloudtrail\\_logs\\_cloudtrail\\_logs\\_01f5a3e8ab0aef64d](#)  
To view this table and run a query, open the Amazon Athena console. Athena charges for running queries. [Learn more](#)

CloudTrail > Event history

Query 6 : X | Query 5 : X | [Query 7](#) : X

```
1 SELECT eventtime, useridentity.principalid, requestparameters, eventname
2 FROM cloudtrail_logs_cloudtrail_logs_01f5a3e8ab0aef64d
3 WHERE
4     eventname in ('PutObject') AND
5     requestparameters LIKE '%customer-data.csv%'
6 limit 10;
```

SQL Ln 6, Col 10

Run again Explain Cancel Clear Create ▾

Query results | Query stats

Completed

Results (1)

Search rows

#	eventtime	principalid	requestparameters
1	2024-09-29T19:45:06Z	AROAXRL2Q2ZCLGCVVCB33:user3535650=Pedro_Coelho_Duarte_Ribeiro	{"X-Amz-Date":"20240929T194505Z","bucketName":"data-bucket-0"}

The screenshot shows the AWS Lambda SQL interface. At the top, there are three tabs: 'Query 6 : X', 'Query 5 : X', and 'Query 7 : Query 7 : X'. The third tab is underlined, indicating it is active. Below the tabs is a code editor containing the following SQL query:

```
1 SELECT eventTime, userIdentity.principalId, sourceIPAddress, userAgent, eventName
2 FROM cloudtrail_logs_clouptrail_logs_01f5a3e8ab0aef64d
3 WHERE eventName IN ('GetObject')
4 AND requestParameters LIKE '%customer-data.csv%'
5 LIMIT 10;
```

Below the code editor, it says 'SQL Ln 1, Col 1'. Underneath are several buttons: 'Run again' (orange), 'Explain', 'Cancel', 'Clear', and 'Create ▾'. The 'Query results' tab is selected, showing a green bar with 'Completed'. The 'Results (3)' section contains a search bar and a table with the following data:

#	eventTime	principalId	sourceIPAddress
1	2024-09-29T19:45:26Z	AROAXRL2Q2ZCLGCVVCB33:user3535650=Pedro_Coelho_Duarte_Ribeiro	187.21.13.24
2	2024-09-29T19:45:28Z	AROAXRL2Q2ZCLGCVVCB33:user3535650=Pedro_Coelho_Duarte_Ribeiro	187.21.13.24
3	2024-09-29T19:45:44Z	AROAXRL2Q2ZCLGCVVCB33:user3535650=Pedro_Coelho_Duarte_Ribeiro	187.21.13.24

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

[CloudWatch](#) > Log groups

## Log groups (1/4)

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



Filter log groups or try prefix search



### Log group



[/aws/lambda/c131607a3337212l7762512t1-AdjustA...](#)



[/aws/lambda/c131607a3337212l7762512t1-AdjustB...](#)



[EncryptedInstanceSecureLogs](#)



[LabVPCFlowLogs](#)

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

```
2024-09-29T20:28:08Z I! Started the Statsd service on 40125
2024-09-29T20:28:08Z I! [inputs.socket_listener] Listening on udp://127.0.0.1:25826
2024-09-29T20:28:08Z I! {"caller":"service@v0.103.0/service.go:208","msg":"Everything is ready. Begin running and processing data."}
2024-09-29T20:28:08Z W! {"caller":"localhostgate/featuregate.go:63","msg":"The default endpoints for all servers in components will change to use localhost instead of LocalHostAsDefaultHost"}
2024-09-29T20:28:08Z I! Statsd listener listening on: [::]:8125
2024-09-29T20:28:08Z I! {"caller":"ec2tagger/ec2tagger.go:480","msg":"ec2tagger: Initial retrieval of tags succeeded","kind":"processor","name":"ec2tagger","pipe":true}
2024-09-29T20:28:08Z I! {"caller":"ec2tagger/ec2tagger.go:391","msg":"ec2tagger: EC2 tagger has started, finished initial retrieval of tags and Volumes","kind":"processor","name":"ec2tagger","pipe":true}
2024-09-29T20:28:09Z I! First time setting retention for log group EncryptedInstanceSecureLogs, update map to avoid setting twice
2024-09-29T20:28:09Z I! [outputs.cloudwatchlogs] Configured middleware on AWS client
2024-09-29T20:28:09Z I! [logagent] piping log from EncryptedInstanceSecureLogs/EncryptedInstanceSecureLogs-i-0f05ad44565e48aea(/var/log/secure) to cloudwatchlogs
```

```
voclabs:~/environment $ ssh -i labsuser.pem ec2-user@54.224.234.4
The authenticity of host '54.224.234.4 (54.224.234.4)' can't be established.
ECDSA key fingerprint is SHA256:HaCgM1xwBjF7bhBli+X85NX1IP0N91V7yx2nLvZddyQ.
ECDSA key fingerprint is MD5:c9:29:8e:75:b5:ff:0f:b5:d9:39:06:bf:7c:f3:f0:4f.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '54.224.234.4' (ECDSA) to the list of known hosts.
Last login: Sun Sep 29 20:24:41 2024 from ec2-18-206-107-29.compute-1.amazonaws.com
      ,      #
 ~\_ #####_      Amazon Linux 2
 ~~ \#####\
 ~~  \###|      AL2 End of Life is 2025-06-30.
 ~~   \#/ __
 ~~    V~' '-'>
 ~~     /      A newer version of Amazon Linux is available!
 ~~ ._. _/
 ~~  _/ _/      Amazon Linux 2023, GA and supported until 2028-03-15.
 _/m'          https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-10-1-3-13 ~]$ exit
logout
Connection to 54.224.234.4 closed.
voclabs:~/environment $ ssh -i labsuser.pem ubuntu@54.224.234.4
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
```

▶ 2024-09-29T20:40:43.025Z Sep 29 20:39:56 ip-10-1-3-13 sshd[3910]: pam\_unix(sshd:session): session opened for user ec2-user by (uid=0)

▶ 2024-09-29T20:40:43.025Z Sep 29 20:40:42 ip-10-1-3-13 sshd[4101]: Received disconnect from 35.172.187.250 port 51240:11: disconnected by user

▶ 2024-09-29T20:40:43.025Z Sep 29 20:40:42 ip-10-1-3-13 sshd[4101]: Disconnected from 35.172.187.250 port 51240

▶ 2024-09-29T20:40:47.158Z Sep 29 20:40:42 ip-10-1-3-13 sshd[3910]: pam\_unix(sshd:session): session closed for user ec2-user

▶ 2024-09-29T20:41:09.838Z Sep 29 20:41:09 ip-10-1-3-13 sshd[4133]: Invalid user ubuntu from 35.172.187.250 port 56392

▶ 2024-09-29T20:41:09.838Z Sep 29 20:41:09 ip-10-1-3-13 sshd[4133]: input\_userauth\_request: invalid user ubuntu [preauth]

▶ 2024-09-29T20:41:14.158Z Sep 29 20:41:09 ip-10-1-3-13 sshd[4133]: Connection closed by 35.172.187.250 port 56392 [preauth]

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

CloudWatch > Alarms

**Alarms (1)**

Hide Auto Scaling alarms

Name	State	Last state update (UTC)	Conditions
<a href="#">Not_valid_users_exceeding_limit</a>	Insufficient data	2024-09-29 20:55:00	NotValidUsers >= 5 for 1 datapoints within 1 day



## Subscription confirmed!

You have successfully subscribed.

Your subscription's id is:

arn:aws:sns:us-east-

1:518337386052:Not\_valid\_users\_exceeding\_limit:4e2a5b8e-c3e9-4ec0-93a1-dd16d8e96036

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

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

### Log events

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

Invalid user

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

### Alarms (1)

Search

Alarm state: In alarm

Name

▼ | State

[Not\\_valid\\_users\\_exceeding\\_limit](#)

In alarm

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

to me ▾

You are receiving this email because your Amazon CloudWatch Alarm "Not\_valid\_users\_exceeding\_limit" in the US East (N. Virginia) region triggered on 29 September, 2024 20:57:06 UTC".

View this alarm in the AWS Management Console:

[https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/Not\\_valid\\_users\\_exceeding\\_limit](https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/Not_valid_users_exceeding_limit)

Alarm Details:

- Name: Not\_valid\_users\_exceeding\_limit
- Description: Not valid access attempts over SSH to the EncryptedInstance server have exceeded 4 in the last 24 hours.
- State Change: INSUFFICIENT\_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [8.0 (28/09/24 20:57:00)] was greater than or equal to the threshold of 4.0.
- Timestamp: Sunday 29 September, 2024 20:57:06 UTC
- AWS Account: 518337386052
- Alarm Arn: arn:aws:cloudwatch:us-east-1:518337386052:alarm:Not\_valid\_users\_exceeding\_limit

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

Name	AWS Region
<a href="#">athena-results-666</a>	US East (N. Virginia) us-east-1
<a href="#">aws-athena-query-results-518337386052-us-east-1</a>	US East (N. Virginia) us-east-1
<a href="#">aws-config-01f5a3e8ab0aef64d</a>	US East (N. Virginia) us-east-1
<a href="#">cloudtrail-logs-01f5a3e8ab0aef64d</a>	US East (N. Virginia) us-east-1
<a href="#">compliance-bucket-01f5a3e8ab0aef64d</a>	US East (N. Virginia) us-east-1
<a href="#">data-bucket-01f5a3e8ab0aef64d</a>	US East (N. Virginia) us-east-1
<a href="#">s3-inventory-01f5a3e8ab0aef64d</a>	US East (N. Virginia) us-east-1
<a href="#">s3-objects-access-log-01f5a3e8ab0aef64d</a>	US East (N. Virginia) us-east-1

# Rules

A rule is a compliance check that helps you manage your AWS resources.

## Rules

Filter by compliance status

All



Name



s3-bucket-logging-enabled

### Remediation action

Remediation action	Description
AWS-ConfigureS3BucketLogging	Enables Logging on S3 Bucket

### Parameters

Key	Value	Description
AutomationAssumeRole	arn:aws:iam::518337386052:role/SSMAutomationRole	(Optional) The ARN of the role that allows Automation to perform the actions on your behalf.
TargetPrefix	-	(Optional) Specifies a prefix for the keys under which the log files will be stored.
GranteeEmailAddress	-	(Optional) Email address of the grantee.
GranteeType	CanonicalUser	(Optional) Type of grantee
BucketName	RESOURCE_ID	(Required) The name of the Amazon S3 Bucket for which you want to configure logging.
GranteeId	d4bdae1ddc96f96d97d09f060f24770b6db937ed9ae76b810e47402ab7537738	(Optional) The canonical user ID of the grantee.
GranteeUri	-	(Optional) URI of the grantee group.
TargetObjectKeyPartitionDataSource	-	(Optional) Specifies the partition date source for the partitioned prefix.
GrantedPermission	FULL_CONTROL	(Optional) Logging permissions assigned to the Grantee for the bucket.
TargetBucket	s3-objects-access-log-01f5a3e8ab0aef64d	(Required) Specifies the bucket where you want Amazon S3 to store server access logs. You can have
TargetObjectKeyPrefix	-	(Optional) Amazon S3 key format for log objects.

Resources in scope				
	ID	Type	Status	Annotation
○	athena-results-666	S3 Bucket	-	
○	aws-athena-query-results-518337386052-us-east-1	S3 Bucket	-	
○	aws-config-01f5a3e8ab0aef64d	S3 Bucket	-	
○	cloudtrail-logs-01f5a3e8ab0aef64d	S3 Bucket	-	
○	compliance-bucket-01f5a3e8ab0aef64d	S3 Bucket	<span style="color: green;">●</span> Action executed successfully	
○	s3-inventory-01f5a3e8ab0aef64d	S3 Bucket	-	
○	s3-objects-access-log-01f5a3e8ab0aef64d	S3 Bucket	-	

## Server access logging

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

Server access logging

Enabled

Destination bucket

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