

# Securing and Monitoring Resources with AWS

Salma Mohamed Mohamed Kassem

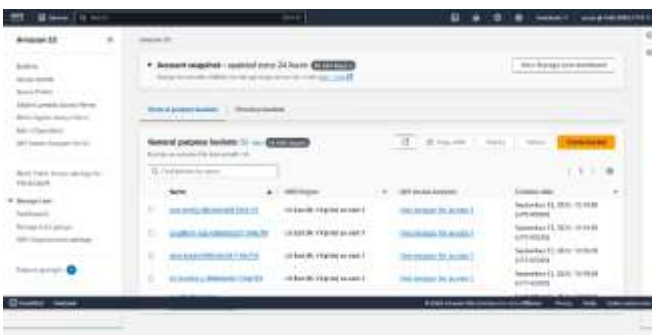
AWS Solution Architect and Admin Track



## Week1 : Securing data in Amazon S3

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

- ✓ Create a new S3 bucket.
- ✓ Apply a bucket policy that restricts access.
- ✓ Upload myfile.txt



### Test access

Paulo

- Has access to data-bucket object and can download the file

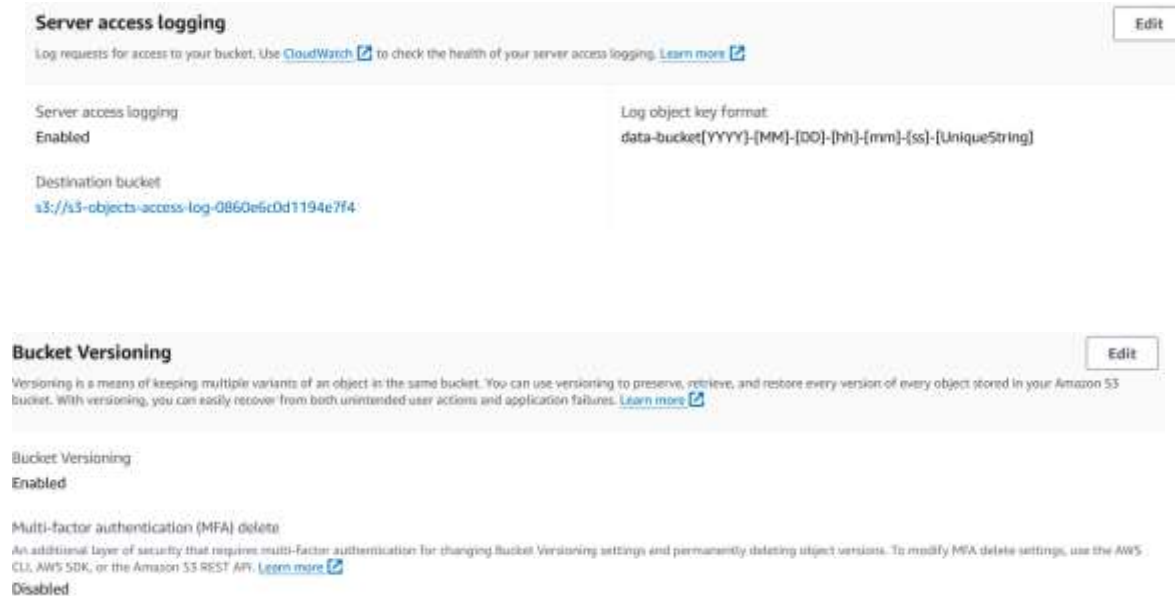


Mary

- Don't have access to the data-bucket objects

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

- ✓ Enable versioning on the data-bucket
- ✓ Enable server access logging on the data-bucket



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

- ✓ Enable the S3 Inventory feature on the data-bucket

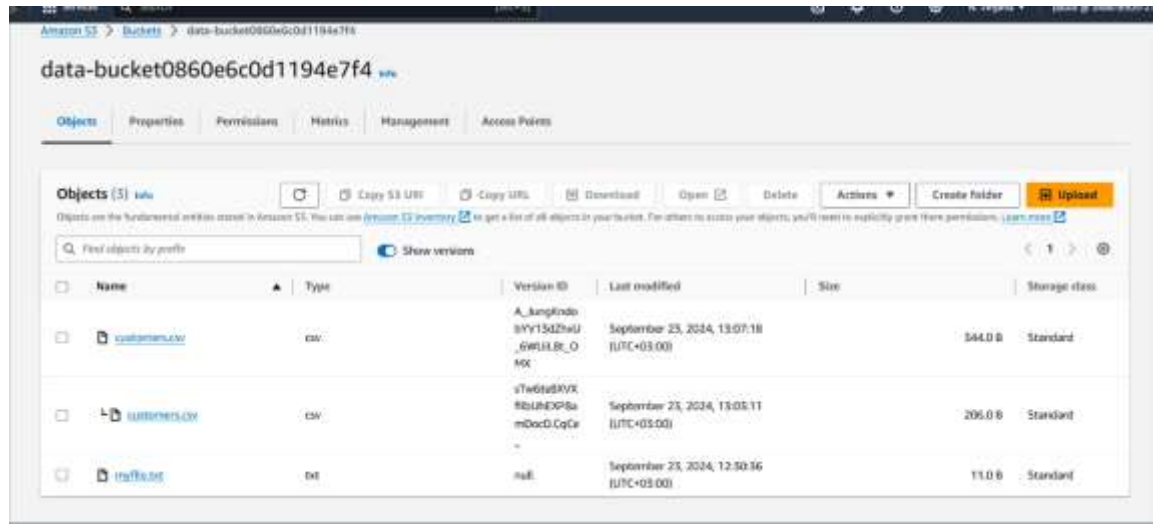


## Task 1.4: Confirm that versioning works as intended

- ✓ On your computer, create a new file named customers.csv. Then, copy the following text to the file and save the changes
- ✓ Log in to the AWS account as the paulo user and upload the customers.csv file to the data-bucket
- ✓ Analyze how many versions of customer.csv exist by navigating to the customers.csv details page and choosing the Versions tab
- ✓ On your computer, edit the customers.csv file and add more data to it. For example, add the following two rows of data at the bottom of the file
- ✓ Login as Paulo : Paulo can access files

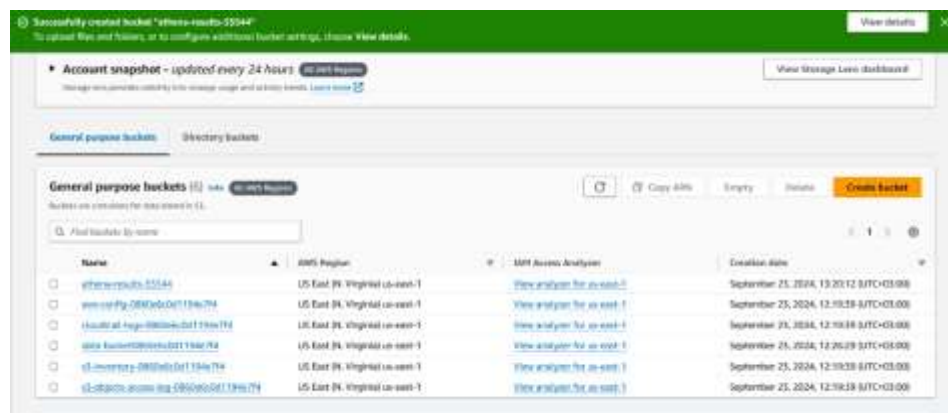
## DEPI

- Login as Mary : Mary cant access files

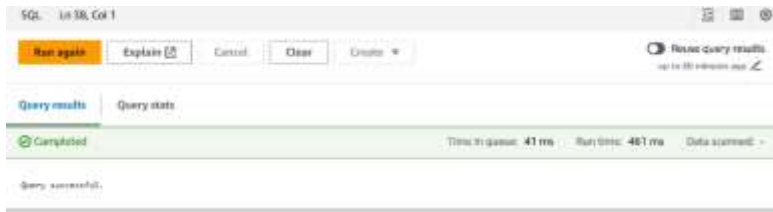


## Task 1.5: Confirm object-level logging and query the access logs by using Athena

- ✓ Create an Athena table from the access logs
- ✓ In the Editor tab paste the following query into the query area
- ✓ Query the table to discover access details



## DEPI



## Cost assessment to secure Amazon S3:-

Includes upfront cost

Upfront cost	Monthly cost	Total 12 months cost
0.01 USD	21.42 USD	257.05 USD

## Week 2 : Securing VPCs

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



### Task 2.2: Create a VPC flow log

Name	Flow log ID	Filter	Destination type	Destination name	IAM role
LabVPCFlowLogs	fl-06659a0e33b0d417c	ALL	cloud-watch-logs	/aws/lambda/c133601a538297217688...	arn:aws:iam::...

10 minutes

Monday, September 23, 2024 at 14:10:...

1 minute

Monday, September 23, 2024 at 14:14:...

## Task 3.2: Access the WebServer instance from the internet and review VPC flow logs in CloudWatch

```

Verifying : 2:nmap-ncat-6.40-19.amzn2.0.1.x86_64

Installed:
  nmap-ncat.x86_64 2:6.40-19.amzn2.0.1

Complete!
voclabs:~/environment $ nc -vz 100.27.126.214 80
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 100.27.126.214:80.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
voclabs:~/environment $ curl -s http://169.254.169.254/latest/meta-
3.216.191.98voclabs:~/environment $

```



The connection has timed out

The server at 100.27.126.214 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few minutes.
- Proxy or firewall could block your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try again

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



## DEPI

VPC > Route tables > rftb-0d57d6c17746a2748 > Edit routes

### Edit routes

Destination	Target	Status	Propagated
10.1.0.0/16	local	Active	No
0.0.0.0/0	local	Active	No
	Internet Gateway	Active	No
	igw-0950e6c0d01194e7fa	Active	No

[Add route](#) [Remove](#) [Cancel](#) [Preview](#) [Save changes](#)

```
ncat: Version 7.50 ( https://nmap.org/ncat )
ncat: Connected to 100.27.120.214:80.
ncat: 0 bytes sent, 0 bytes received in 0.03 seconds.
voclabs:~/environment $ nc -vs 100.27.120.214 22
ncat: Version 7.50 ( https://nmap.org/ncat )
ncat: Connected to 100.27.120.214:22.
ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
voclabs:~/environment $ curl http://100.254.160.254/latest/meta-data/public-ipv4
3.216.191.98voclabs:~/environment $ sudo yum install -y jq
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amazon1-core
237 packages excluded due to repository priority protections
Package jq-1.5-1.amzn2.0.2.x86_64 already installed and latest version
Nothing to do
voclabs:~/environment $
voclabs:~/environment $ curl https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '._prefixes[] | select(.region=="us-east-1") | select(.service=="EC2_INSTANCE_CONNECT")'
$ total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             %             %              %              %              %
100 100% 100 100%    0     0  22.0M    0     0    0     0      0      0     0    0
100.254.160.254/20
voclabs:~/environment $ ping -c 3 www.amazon.com
PING d3ag4ukkkh2yn.cloudfront.net (3.162.95.220) 56(84) bytes of data:
64 bytes from server: 3.162.95.220: icmp_seq=1 ttl=249 time=1.22 ms
64 bytes from server: 3.162.95.220: icmp_seq=2 ttl=249 time=1.51 ms
64 bytes from server: 3.162.95.220: icmp_seq=3 ttl=249 time=1.64 ms

--- d3ag4ukkkh2yn.cloudfront.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 1.225/1.435/1.547/0.154 ms
```

Hello world from WebServer!

## Task 2.5: Secure the Webserver Subnet with a network ACL

Inbound rules (4)

Filter inbound rules

< 1 >

Rule number	Type	Protocol	Port ranges	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
101	SSH (22)	TCP (6)	22	0.0.0.0/0	Allow
102	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
+	All traffic	All	All	0.0.0.0/0	Deny

Hello world from WebServer!

Hello world from WebServer2 port 8080!

## Task 2.6: Review NetworkFirewallVPC and its associated resources

- ✓ Observe the existing NetworkFirewallVPC resources and configurations.
- ✓ Confirm access to the WebServer2 instance on ports 80 and 22
- ✓ Start an additional website that runs on WebServer2 port 8080 and test access.

[illegible]

## Task 2.7: Create a network firewall

- ✓ In the Amazon VPC console, create a firewall named `NetworkFirewall`
- ✓ Create route tables
- ✓ Add an edge association to the `IGW-Ingress-Route-Table` so that the `NetworkFirewallIG` internet gateway is associated with the route table.
- ✓ Create another route table in `NetworkFirewallVPC` for the `FirewallSubnet`



The image shows three screenshots from the AWS Management Console:

**Top Screenshot: NetworkFirewall Overview**

- Green banners: "You've successfully created firewall NetworkFirewall" and "You've successfully created firewall policy FirewallPolicy".
- Breadcrumbs: VPC > Network Firewall: Firewalls > NetworkFirewall
- Header: NetworkFirewall [info](#) [Delete](#)
- Overview [info](#)
  - Firewall status: Provisioning
  - Associated firewall policy: [FirewallPolicy](#)
  - Associated VPC: [vpc-0b0aa52fbb9b6e05c](#)
- Tabs: Firewall details (selected), Firewall policy settings, Monitoring

**Middle Screenshot: Edit subnet associations**

Change which subnets are associated with this route table.

Available subnets (1/2)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input type="checkbox"/> WebServer2Subnet	subnet-03a8e5c27c6b179ac	10.1.1.0/28	-	Main [rtb-0795d95001eb70fa4]
<input checked="" type="checkbox"/> FirewallSubnet	subnet-012805151fb81310f	10.1.1.0/28	-	Main [rtb-0795d95001eb70fa4]

Selected subnets

subnet-012805151fb81310f / FirewallSubnet X

[Cancel](#) [Save associations](#)

**Bottom Screenshot: Routes**

Routes (2)

[Filter routes](#)

[Both](#) [Edit routes](#)

Destination	Target	Status	Propagated
0.0.0.0/0	<a href="#">vpc-0795d95001eb70fa4</a>	Active	No
10.1.0.0/16	local	Active	No

## Task 2.8 Create all the route tables that are needed to route traffic to and from the internet through the firewall endpoint

- ✓ Created IGW-Ingress-Route-Table in the *NetworkFirewallVPC*
- ✓ Edit the route table to add a new route
- ✓ Add an edge association to the *IGW-Ingress-Route-Table* so that the *NetworkFirewallIG* internet gateway is associated with the route table
- ✓ Created a *Firewall-Route-Table* route table in *NetworkFirewallVPC* for the *FirewallSubnet*
- Created a *WebServer2-Route-Table*



## DEPI

- ✓ At the end of task we were asked to delete all resources related to task

VPC > Route tables > rtb-0d2d176656aad8c92

### rtb-0d2d176656aad8c92 / WebServer2-Route-Table

Actions

**Details** Info

Route table ID rtb-0d2d176656aad8c92	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-0b0aa52fbb9b6e05c   NetworkFirewallVPC	Owner ID 548689092770		

Routes Subnet associations Edge associations Route propagation Tags

**Routes (2)** Both Edit routes

Filter routes

Destination	Target	Status	Propagated
0.0.0.0/0	vpc-0753a115601dk3ac4	Active	No
10.1.0.0/16	local	Active	No

### Edit subnet associations

Change which subnets are associated with this route table

**Available subnets (1/2)**

Filter subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
WebServer2Subnet	subnet-03d8e5c27f6b179ac	10.1.3.0/28	-	Main (rtb-075a098821eb70fa4)
FirewallSubnet	subnet-012005151f8d1110f	10.1.1.0/28	-	rtb-0760b3bd4e7ed5639 / Firewall-Bo...

**Selected subnets**

subnet-03d8e5c27f6b179ac / WebServer2Subnet X

Cancel Save associations

VPC > Route tables > rtb-0d07dec3774ca25a8 > Edit routes

### Edit routes

Destination	Target	Status	Propagated
10.1.0.0/16	local	Active	No
0.0.0.0/0	local	X	
	Internet Gateway	Active	No
	igw-096defc0d1194e7fa	X	

Add route

Cancel Preview Save changes

## Task 2.9: Configure logging for the network firewall

- ✓ Create a CloudWatch log group named NetworkFirewallVPCLogs with a retention setting of 6 months
- ✓ In the settings for the NetworkFirewall that you created, browse to the Firewall details area, and configure both Alert and Flow type logging. Set the log destination for both types of logging to use the NetworkFirewallVPCLogs CloudWatch log group.

The screenshot shows the AWS CloudWatch console. The top section, 'Log groups (5)', lists several log groups. The bottom section, 'Logging', shows the configuration for the Network Firewall.

Log group	Log class	Anomaly d...	Data prot...	Sensitive ...	Retention	Metric filters
/aws/lambda/c131601a33829726768870111-Adju...	Standard	Configure	-	-	Never expires	-
/aws/lambda/c131601a33829726768870111-Adju...	Standard	Configure	-	-	Never expires	-
EncryptedInstanceSecureLogs	Standard	Configure	-	-	6 months	1 filter
EncryptedInstanceSecureLogs	Standard	Configure	-	-	Never expires	-
NetworkFirewallVPCLogs	Standard	Configure	-	-	6 months	-

**Logging**

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

- ✓ Navigate to the details page for the NetworkFirewall and begin to create the rule group
- ✓ Configure the stateful rule group with the name NetworkFirewallVPCRuleGroup and a capacity of 100. Use the other default settings
- ✓ Test the firewall rules
- ✓ In the CloudWatch console, observe the network firewall log entries that were created by your tests in the previous step

The screenshot shows the 'Stateful rule groups (1)' section in the AWS CloudWatch console. It displays a single rule group with the following details:

Priority	Name	Capacity	Is managed?	Run in alert mode?
1	NetworkFirewall-VPC-RuleGroup1	100	No	Not available

Rules (5)						
<div> Delete Move up Move down </div> <div> Find rules </div> <div> &lt; 1 &gt; </div>						
Protocol	Source	Source port	Destination	Destination port	Action	Keyword
TCP	ANY	ANY	ANY	8080	Drop	sid:2
TCP	ANY	ANY	ANY	80	Pass	sid:3
TCP	ANY	ANY	ANY	22	Pass	sid:4
TCP	ANY	ANY	ANY	443	Pass	sid:5
IP	ANY	ANY	ANY	ANY	Pass	sid:6

Protocol	Port	Action	
TCP	80	Pass	
TCP	22	Pass	
TCP	8080	Drop	
ICMP	Any	Pass	
TCP	443	Pass	

#### IGW-Ingress-Route-Table

0.0.0.0/0	Gateway load balancer Endpoint	All	All	Allow
10.0.1.0/24	Local	All	All	Allow

#### Firewall-Route-Table

0.0.0.0/0	NetworkFirewallIG	All	All	Allow
10.0.2.0/24	Local	All	All	Allow

#### Webserver2-Route-Table

0.0.0.0/0	Gateway load balancer Endpoint	All	All	Allow
10.0.3.0/24	Local	All	All	Allow

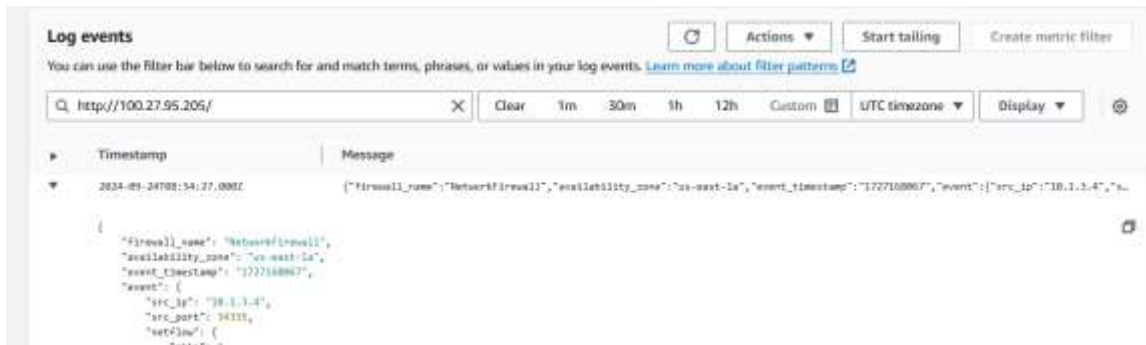
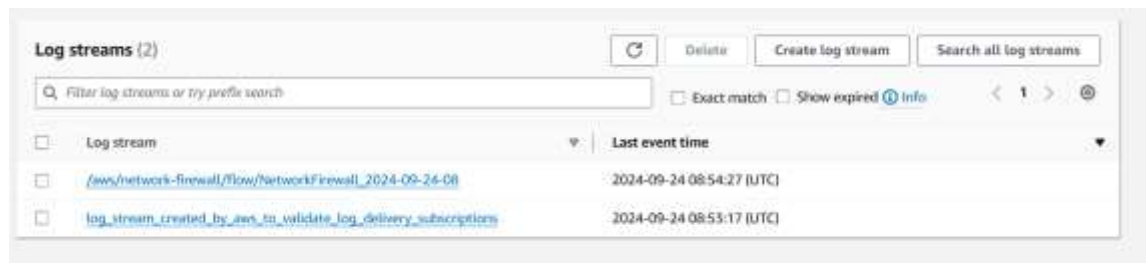
```

Last login: Tue Sep 24 12:29:33 2024 from 3.216.191.98
[ec2-user@webserver2 ~]$ ping -c 3 www.amazon.com

sudo netstat -tulnp | grep -i listen
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=1.76 ms
64 bytes from 162.219.225.118 (162.219.225.118): icmp_seq=2 ttl=56 time=1.81 ms
64 bytes from 162.219.225.118 (162.219.225.118): icmp_seq=3 ttl=56 time=1.63 ms

--- www-amazon-com.customer.fastly.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.633/1.734/1.811/0.074 ms
tcp        0      0 0.0.0.0:22          0.0.0.0:*           LISTEN      2344/sshd: /usr/sbi
tcp6       0      0 :::22              :::*                 LISTEN      2344/sshd: /usr/sbi
tcp6       0      0 :::80              :::*                 LISTEN      1998/httpd

```

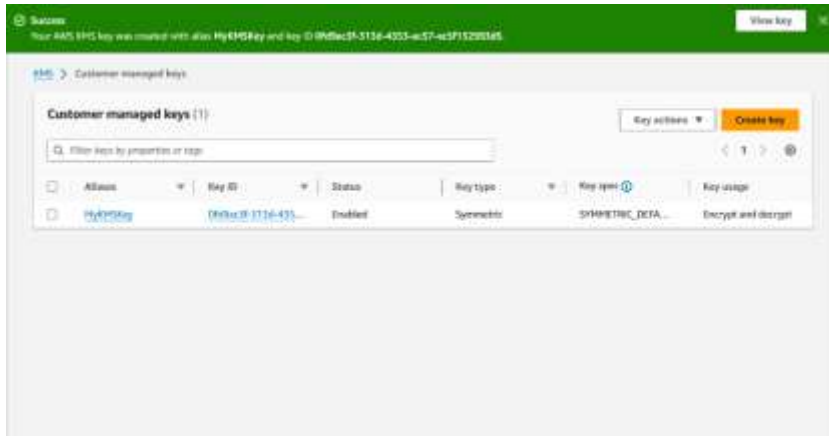


## Cost estimate to secure a VPC with a network firewall

Upfront cost	Monthly cost	Total 12 months cost
0.00 USD	161.90 USD	1,942.80 USD
		Includes upfront cost

## Week33 :Securing AWS resources by using AWS KMS

### Task 3.1: Create a customer managed key and configure key rotation3



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

- ✓ Sofia can access bucket containing loan-data.csv
- ✓ Paulo can't access



## DEPI

Amazon S3 > Buckets > data-bucket0860e6c0d1194e7f4

### data-bucket0860e6c0d1194e7f4 [info](#)

Objects Properties Permissions Metrics Management Access Points

Objects (4) [info](#) [Copy S3 URL](#) [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](#)

[Show versions](#) < 1 >

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	<a href="#">customer-data.csv</a>	CSV	September 24, 2024, 15:09:17 (UTC+03:00)	328.0 B	Standard
<input type="checkbox"/>	<a href="#">customers.csv</a>	CSV	September 25, 2024, 15:07:18 (UTC+03:00)	344.0 B	Standard
<input type="checkbox"/>	<a href="#">loan-data.csv</a>	CSV	September 24, 2024, 14:25:54 (UTC+03:00)	170.0 B	Standard
<input type="checkbox"/>	<a href="#">myfile.txt</a>	Text	September 25, 2024, 12:30:38 (UTC+03:00)	11.0 B	Standard

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

```
<?xml version="1.0"?>
<Error>
  <Code>AccessDenied</Code>
  <Message>User: arn:aws:iam::54888992779:user/paula is not authorized to perform: aws:Decrypt on resource: arn:aws:kms:us-east-1:94888992779:key/0f9ac3f-313d-4353-ac57-ac3f152993d5 because no policy allows the aws:Decrypt action/Message
  <Type>AccessDeniedException</Type>
  <Detail>{"message": "User: arn:aws:iam::54888992779:user/paula is not authorized to perform: aws:Decrypt on resource: arn:aws:kms:us-east-1:94888992779:key/0f9ac3f-313d-4353-ac57-ac3f152993d5 because no policy allows the aws:Decrypt action/Message"}</Detail>
</Error>
```

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

- ✓ While logged in with the *voclabs* role, create a new EC2 instance. Keep the default settings except for the following
- ✓ On the details page for *EncryptedInstance*, choose the **Storage** tab and verify that the instance root volume is encrypted.

Instances (4) [info](#) [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

[All states](#) < 1 >

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
<input type="checkbox"/>	WebServer-2	i-00ea8b9e60efda2d2	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-100-27-
<input type="checkbox"/>	WebServer	i-0210bf6b7700474056	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-100-27-
<input type="checkbox"/>	EncryptedInst...	i-0726a7750a22f89a8	Pending	t2.micro	-	View alarms +	us-east-1a	ec2-3-237-1
<input type="checkbox"/>	aws-cloud9-CL...	i-045db36858afbc3	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1f	ec2-3-216-1

Select an instance:

Block devices

<input checked="" type="checkbox"/>	Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID
<input checked="" type="checkbox"/>	vol-f09f2a08b35e6325c	/dev/xvda	8	Attached	2024/09/24 14:52 GMT+3	Yes	0f9ac3f-313d-4353-ac5







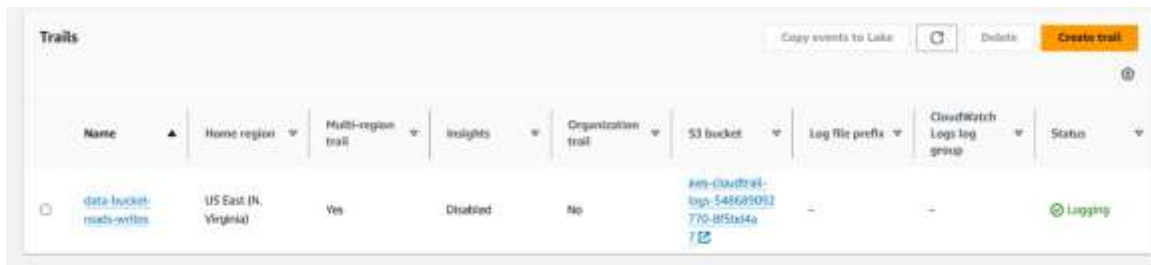
## Cost estimate

Upfront cost	Monthly cost	12 months cost
0.00 USD	7.00 USD	84.00 USD

## Phase 4: Monitoring and logging

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

- ✓ Create a CloudTrail trail
- ✓ On your computer, create a file named `customer-data.csv`. Then, in a text editor, paste the following data into the file and save the changes.
- ✓ Use the CloudTrail console to create an Athena table that describes the format of the data in the cloudtrail-logs S3 bucket.



## DEPI

Amazon S3 > Buckets > data-bucket0860e6c0d1194e7f4

### data-bucket0860e6c0d1194e7f4 [info](#)

Objects Properties Permissions Metrics Management Access Points

**Objects (4)** [info](#) [Copy S3 URL](#) [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](#)

[Show versions](#) < 1 >

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	<a href="#">customer-data.csv</a>	CSV	September 24, 2024, 15:09:17 (UTC+03:00)	328.0 B	Standard
<input type="checkbox"/>	<a href="#">customers.csv</a>	CSV	September 25, 2024, 15:07:18 (UTC+03:00)	344.0 B	Standard
<input type="checkbox"/>	<a href="#">loan-data.csv</a>	CSV	September 24, 2024, 14:25:54 (UTC+03:00)	170.0 B	Standard
<input type="checkbox"/>	<a href="#">myfile.txt</a>	Text	September 25, 2024, 12:50:38 (UTC+03:00)	11.0 B	Standard

**Services**

**Data**

Data source

Database

Tables and views [Create](#) [Settings](#)

**Tables (2)** < 1 >

- ☐ bucket\_logs
- ☐ cloudtrail\_logs

**Views (0)** < 1 >

<input type="checkbox"/>	bucket_logs	...
<input type="checkbox"/>	cloudtrail_logs	...
	eventversion	string
	useridentity	struct<type:string,principalid:string,arn:string,accountid:string,userName:string,sessionContext:struct<attributes:struct<mfaAuthenticated:string,creationDate:string>,sessionIssuer:struct<type:string,principalid:string,arn:string,accountId:string,userName:string>>>
	eventtime	string
	eventsources	string
	eventname	string
	awsregion	string
<b>Views (0)</b>	<span>&lt; 1 &gt;</span>	

```

48 )
49 ROW FORMAT SERDE 'org.openx.data.jsonserde.JsonSerDe'
50 WITH SERDEPROPERTIES (
51     'ignore.malformed.json' = 'true'
52 )
53 LOCATION 's3://cloudtrail-logs/'
54 TBLPROPERTIES ('has_encrypted_data'='false');
55

```

## DEPI

```
Query 1 : X Query 2 : X Query 3 : X Query 4 : X Query 5 : X
1 SELECT eventtime, useridentity.principalid, requestparameters, eventname
2 FROM cloudtrail_logs
3 WHERE
4     eventname IN ('PutObject') AND
5     requestparameters LIKE '%customer-data.csv%'
6 LIMIT 10;
7
```

## Task 4 . 2: Use CloudWatch Logs to monitor secure logs

**Log groups (5)**

By default, we only load up to 1000 log groups.

Filter log groups or try prefix search

Exact match

Log group	Log class	Anomaly d...	Data prot...	Sensitive ...	Retention	Metric filters
<a href="#">/aws/lambda/i33601a3382972f768870111-AdjustA...</a>	Standard	<a href="#">Configure</a>	-	-	Never expire	-
<a href="#">/aws/lambda/i33601a3382972f768870111-AdjustB...</a>	Standard	<a href="#">Configure</a>	-	-	Never expire	-
<a href="#">EncryptedInstanceSecureLogs</a>	Standard	<a href="#">Configure</a>	-	-	6 months	1 filter
<a href="#">/aws/lambda/i33601a3382972f768870111-AdjustC...</a>	Standard	<a href="#">Configure</a>	-	-	Never expire	-
<a href="#">/aws/lambda/i33601a3382972f768870111-AdjustD...</a>	Standard	<a href="#">Configure</a>	-	-	6 months	-

```
ec2-user@webserver2 ~ % ssh -i labuser.pem ec2-user@encryptedinstance-public-1P
ssh: Could not resolve hostname encryptedinstance-public-1P: Name or service not known
ec2-user@webserver2 ~ % ssh -i labuser.pem ec2-user@encryptedinstance-100.27.95.205
ssh: Could not resolve hostname encryptedinstance-100.27.95.205: Name or service not known
ec2-user@webserver2 ~ % ssh -i labuser.pem ec2-user@100.27.95.205
The authenticity of host '100.27.95.205 (100.27.95.205)' can't be established.
ECDSA key fingerprint is SHA256:1ab8000000000000000000000000000000000000000000000000000000000000.
ECDSA key fingerprint is MD5:6a:7a:fe:c3:72:c3:43:95:da:71:af:22:3e:d8:9a:bc.
Are you sure you want to continue connecting (yes/no)? no
Host key verification failed.
ec2-user@webserver2 ~ % ssh -i labuser.pem ec2-user@100.27.95.205
The authenticity of host '100.27.95.205 (100.27.95.205)' can't be established.
ECDSA key fingerprint is SHA256:1ab8000000000000000000000000000000000000000000000000000000000000.
ECDSA key fingerprint is MD5:6a:7a:fe:c3:72:c3:43:95:da:71:af:22:3e:d8:9a:bc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '100.27.95.205' (ECDSA) to the list of known hosts.
ec2-user@encryptedinstance-100.27.95.205 ~ %
Last login: Tue Sep 24 12:03:10 2024 from 10.206.107.30
ec2-user@webserver2 ~ % cat /etc/passwd
ec2-user:x:1000:1000::/home/ec2-user:/bin/bash
ec2-user@webserver2 ~ %
```

```
bin/systemctl enable rsyslog
or (id=1000)

bin/systemctl start rsyslog
or (id=1000)

bin/tail -f /var/log/auth.log
or (id=1000)

bin/tail -f /var/log/secure
or (id=1000)
```

## DEPI

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
#	2024-09-24T12:11:10.826Z	Sep 24 12:11:10 webserver2 sudo[9990]: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/secure
#	2024-09-24T12:12:10.850Z	Sep 24 12:12:10 webserver2 sudo[9128]: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/secure
#	2024-09-24T12:20:04.674Z	Sep 24 12:20:04 webserver2 sudo[9351]: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/secure

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

**Metric filters [1]**

---

[Not valid users](#) ☐

Filter pattern

Metric value 1

Metric

[secure](#) / [type-DB606c0d1194e7f4](#)

Metric value

1

Default value

0

Unit

Count

Dimensions

-

Alarms

None

CloudWatch > Alarms

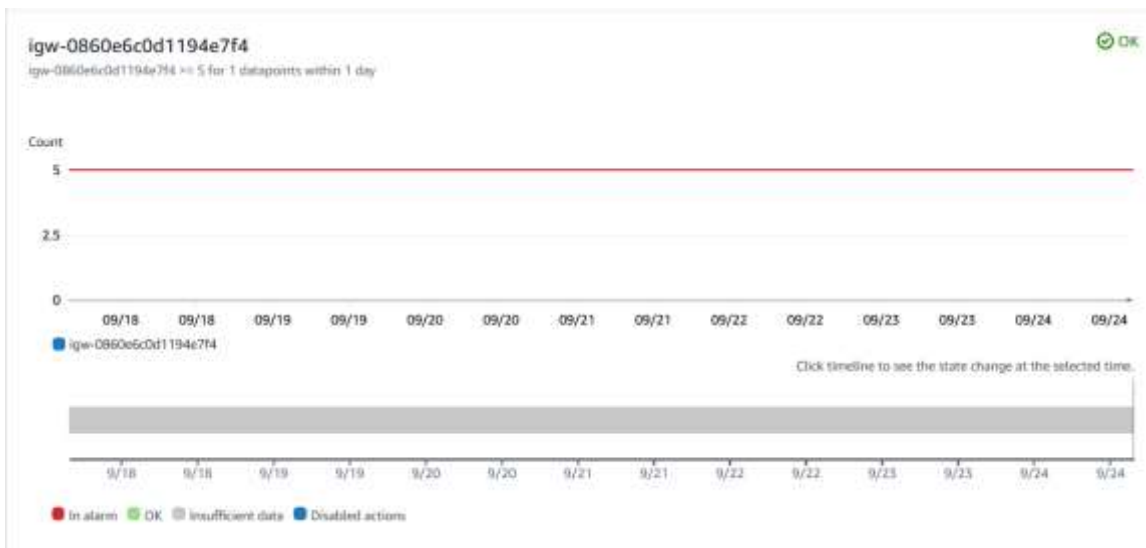
**Alarms [1]** ☐ Hide Auto Scaling alarms

<input type="checkbox"/>	Name	State	Last state update (UTC)	Conditions	Actions
<input type="checkbox"/>	<a href="#">Not valid users exceeding limit on</a> <a href="#">SecurityIncidents</a>	<input checked="" type="radio"/> Insufficient data	2024-09-24 12:42:06	<a href="#">type-DB606c0d1194e7f4</a> >= 5 for 1 datapoints within 1 day	<input checked="" type="radio"/> Actions enabled <b>Warning</b>

```

    /m/
Last login: Tue Sep 24 12:03:30 2024 from 18.206.107.28
[ec2-user@webserver2 ~]$ exit
logout
Connection to 100.27.95.205 closed.
voclabs:~/environment $ ssh -i labsuser.pem ubuntu@EncryptedInstance-100.27.95.205
ssh: Could not resolve hostname encryptedinstance-100.27.95.205: Name or service not known
voclabs:~/environment $ ssh invalid-user@<EncryptedInstance-public-IP>
bash: syntax error near unexpected token `newline'
voclabs:~/environment $ ssh invalid-user@100.27.95.205
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh invalid-user@100.27.95.205
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh invalid-user@100.27.95.205
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh invalid-user@100.27.95.205
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh invalid-user@100.27.95.205
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh invalid-user@100.27.95.205
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $

```



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

Parameters		
Key	Value	Description
AutomationAssumeRole	arn:aws:iam::548689092770: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.
GrantEmailAddress	-	(Optional) Email address of the grantee.
GranteeType	igw-0860e6cd1194e7f41	(Optional) Type of grantee.
BucketName	RESOURCE_ID	(Required) The name of the Amazon S3 Bucket for which you want to configure logging.
GranteeId	548689092770	(Optional) The canonical user ID of the grantee.
GranteeUri	-	(Optional) URI of the grantee group.
TargetObjectKeyPartitionDateSource	-	(Optional) Specifies the partition date source for the partitioned prefix.
GrantedPermission	FULL_CONTROL	(Optional) Logging permissions assigned to the Grantee for the bucket.
TargetBucket	s3-objects-access-log-0860e6cd1194e7f41	(Required) Specifies the bucket where you want Amazon S3 to store server access logs. You can have only one bucket per Amazon S3 account.
TargetObjectKeyPrefix	-	(Optional) Amazon S3 key format for log objects.

### Rules

A rule is a compliance check that helps you manage your ideal configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and displays the compliance results.

Rules

Filter by compliance status

All

View details

Edit rule

Actions

Add rule

Name	Remediation action	Type	Enabled evaluation mode	Detective compliance
<input type="checkbox"/> s3-bucket-logging-enabled	AWS-ConfigureS3BucketLogging	AWS managed	DETECTIVE	<div>7 Noncompliant resources</div>

### Rule details

Get

Description

Checks if logging is enabled for your S3 buckets. The rule is NON\_COMPLIANT if logging is not enabled.

Config rule ARN

arn:aws:config::us-east-1:548689092770:config-rules/config-rule-425n4

Enabled evaluation mode

DETECTIVE

Last successful detective evaluation

September 24, 2024 3:59 PM

Detective evaluation trigger type

Overized configuration changes

Configuration changes

Scope of changes

Resources

Resource type

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.

Cost Estimate

Upfront cost	Monthly cost	12 Months cost
0.00 USD	13.71 USD	164.52 USD Includes upfront costs