

AWS Academy Lab Project - Cloud Security Builder

Welcome, Rowan

Congratulations on your most recent badge 🎉



AWS Academy Graduate - AWS Academy Cloud Security Foundations

[Amazon Web Services Training and Certification](#)

Share



Phase 1: Securing data in Amazon S3

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

🔔 Successfully created bucket "data-bucket-0ea04e7ecc0d51eb9"

To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Account snapshot - updated every 24 hours [All AWS Regions](#) [View Storage Lens dashboard](#)

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

General purpose buckets | Directory buckets

General purpose buckets (5) [Info](#) [All AWS Regions](#)

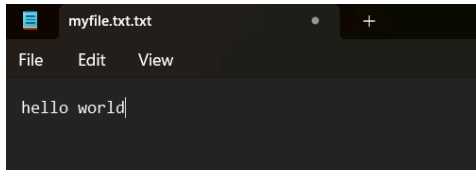
Buckets are containers for data stored in S3.

Find buckets by name

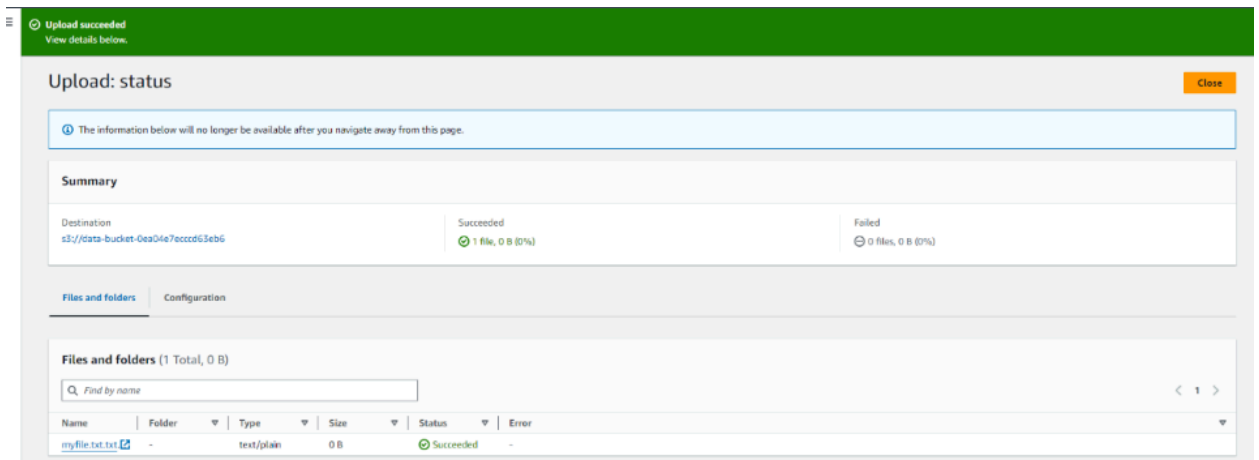
Copy ARN Empty Delete Create bucket

Name	AWS Region	IAM Access Analyzer	Creation date
aws-config-0ea04e7ecc0d51eb9	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 7, 2024, 23:35:54 (UTC+03:00)
cloudtrail-logs-0ea04e7ecc0d51eb9	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 7, 2024, 23:35:53 (UTC+03:00)
data-bucket-0ea04e7ecc0d51eb9	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 7, 2024, 23:47:32 (UTC+03:00)
s3-inventory-0ea04e7ecc0d51eb9	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 7, 2024, 23:35:53 (UTC+03:00)
s3-objects-access-log-0ea04e7ecc0d51eb9	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 7, 2024, 23:35:53 (UTC+03:00)

Creating a text file contain "Hello World"



Uploading text file contains hello world



change policies



Verify 1 Paolo see our S3

Amazon S3

Buckets

Access Grants

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight

► AWS Marketplace for S3

CloudShell

Feedback

Account snapshot - updated every 24 hours

Storage lens provides visibility into storage usage and activity trends.

General purpose buckets

Directory buckets

General purpose buckets (5)

Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	IAM Access Analyzer	Creation date
aws-config-0ea04e7ecccd63eb6	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 7, 2024, 23:35:54 (UTC+03:00)
cloudtrail-logs-0ea04e7ecccd63eb6	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 7, 2024, 23:35:53 (UTC+03:00)
data-bucket-0ea04e7ecccd63eb6	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 7, 2024, 23:47:32 (UTC+03:00)
s3-inventory-0ea04e7ecccd63eb6	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 7, 2024, 23:35:53 (UTC+03:00)
s3-objects-access-log-0ea04e7ecccd63eb6	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 7, 2024, 23:35:53 (UTC+03:00)

Copy ARN

Empty

Delete

Create bucket

New: AWS User Notifications quick setup

Enable common notifications for CloudWatch, EC2, and Health using the new quick setup feature in AWS User Notifications.

Done

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

- Verification 2 Mary Denies

✖

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

Edit the bucket to be enabled

Successfully edited Bucket Versioning

To transition, archive, or delete older object versions, [configure lifecycle rules](#) for this bucket.

data-bucket-0ea04e7ecccd63eb6

Objects

Properties

Permissions

Metrics

Management

Access Points

Bucket overview

AWS Region

US East (N. Virginia) us-east-1

Amazon Resource Name (ARN)

arn:aws:s3:::data-bucket-0ea04e7ecccd63eb6

Creation date

October 7, 2024, 23:47:32 (UTC+03:00)

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

Task 1.3: Implement the S3 Inventory feature on a bucket

Creating Inventory

Inventory successfully created.

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

Bucket policy successfully created

Amazon S3 created a policy on the destination bucket to allow it to place data in that bucket. [Learn more](#)

View policy

Amazon S3 > Buckets > data-bucket-0ea04e7ecccd63eb6 > Management > Inventory configurations

Inventory configurations (1)

Info

View details

Edit

Delete

Create job from manifest

Create inventory configuration


You can create Inventory configurations on a bucket to generate a flat file list of your objects and metadata. These scheduled reports can include all objects in the bucket or be limited to a shared prefix. [Learn more](#)

< 1 > ⚙



	Name	Status	Scope	Destination	Frequency	Last export	Format
<input type="radio"/>	Inventory	Enabled	Entire bucket	s3://s3-inventory...	Daily	-	Apache Parquet

Task 1.4: Confirm that versioning works as intended

Upload Excel file update in the bucket from Paolo's account

 Upload succeeded
View details below.

Summary


Destination s3://data-bucket-0ea04e7eccd63eb6	Succeeded  1 file, 8.5 KB (100.00%)	Failed  0 files, 0 B (0%)
--	---	---

Files and folders

Configuration









Files and folders (1 Total, 8.5 KB)



< 1 >




Name	Folder	Type	Size	Status	Error
customers.csv...	-	application/v...	8.5 KB	 Succeeded	-

Testing the versioning working

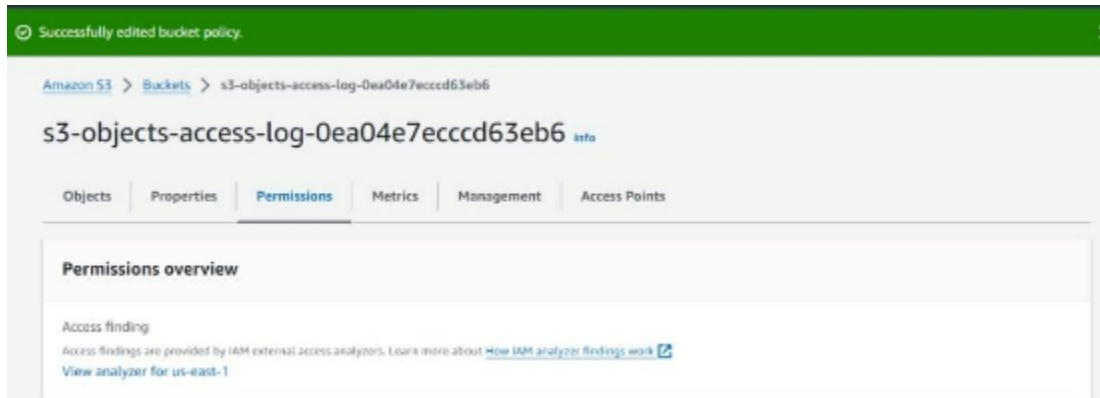
Objects (3) [info](#)

  Copy S3 URI  Copy URL  Download  Open  Delete **Actions**  Create folder  Upload

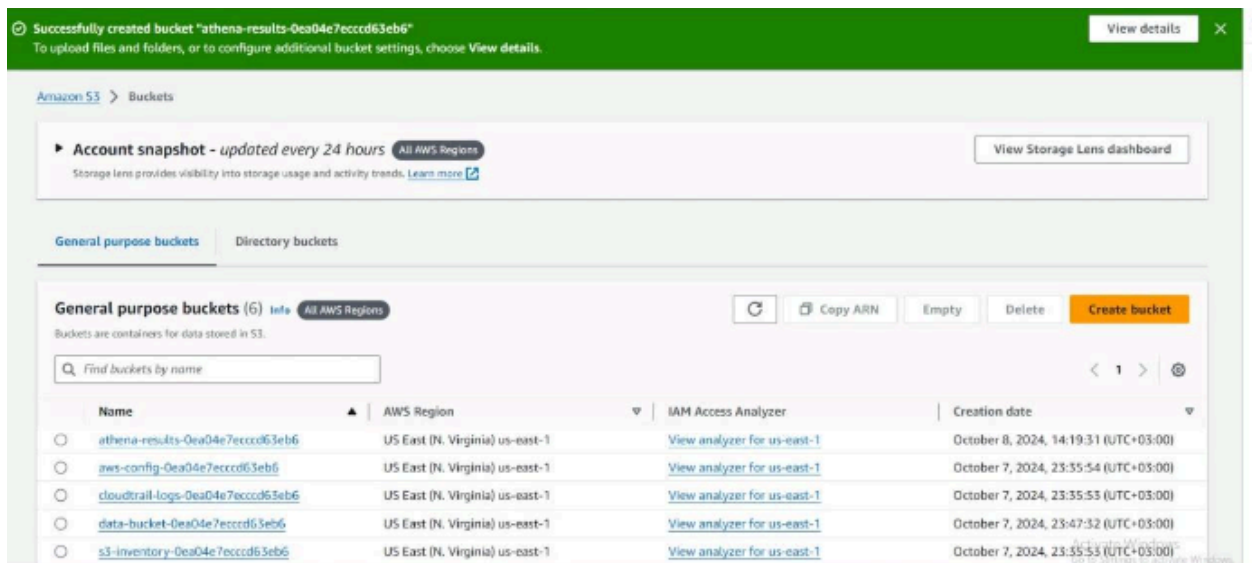
 Show versions < 1 > 

<input type="checkbox"/>	Name	Type	Version ID	Last modified	Size	Storage class
<input type="checkbox"/>	 customers.csv.xlsx	xlsx	2bINbWM4xVlnA_Nvu6q6e qvG6Xu5bYNP	October 8, 2024, 12:44:29 (UTC+03:00)	8.5 KB	Standard
<input type="checkbox"/>	 customers.csv.xlsx	xlsx	JpjslpRSKHZ3KJ0HLcMzhcEA kcmQJMYT	October 8, 2024, 12:35:30 (UTC+03:00)	8.5 KB	Standard
<input type="checkbox"/>	 myfile.txt.txt	txt	null	October 7, 2024, 23:53:08 (UTC+03:00)	0 B	Standard

Added access within the access bucket



Create Athena bucket



Task 1.4: Confirm that versioning works as intended

Creating new working group

Workgroup created
project2 was created successfully.

Amazon Athena > Workgroups > project2

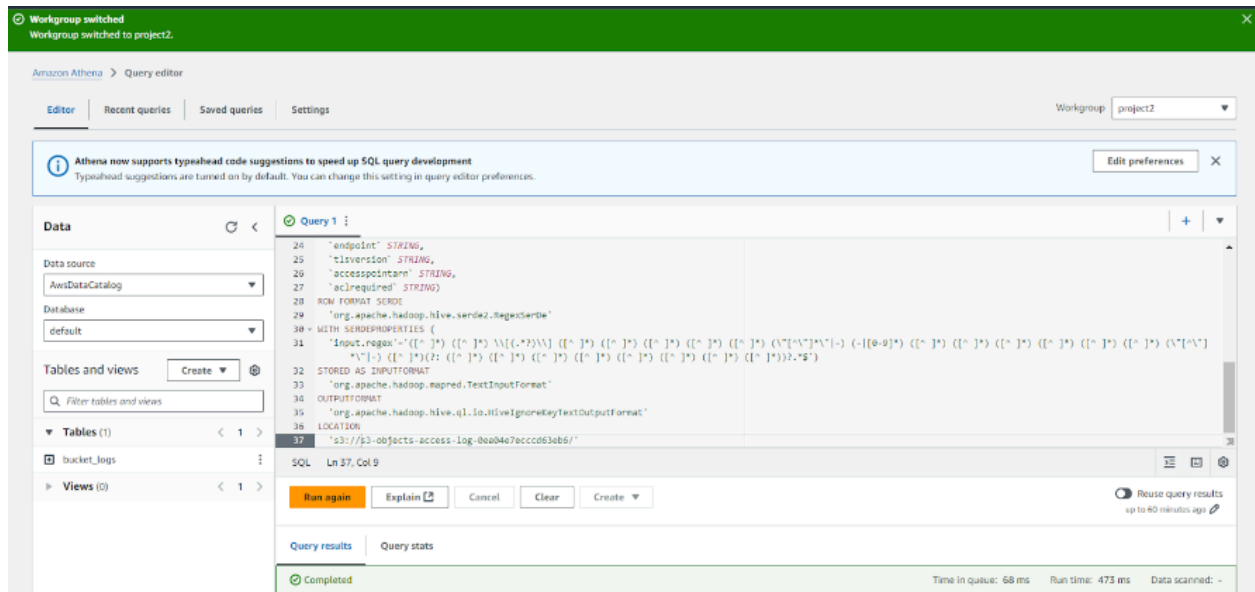
project2

EditTurn off workgroupDelete

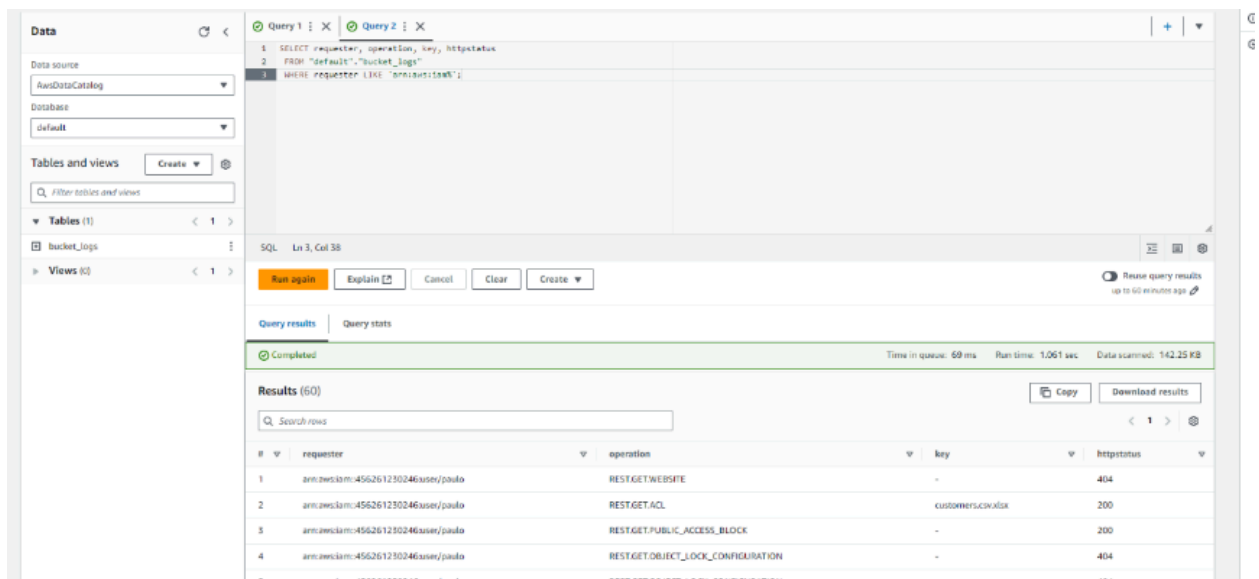
Overview details

Workgroup name project2	Query engine version status Automatic	Query result location s3://athena-results-0ea04e7ecccd63eb6/
Description -	Override client side settings Turned off	Encrypt query results -
Created on 2024-10-09T06:51:35.429+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-1:456261230246: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)		

Table query created in the project 2 workgroup



Running different queries



Phase 2: Securing VPCs

Task 2.1: Review LabVPC and its associated resources

VPC FlowLogs Role script IAM role 1

The screenshot shows the AWS IAM console's 'Permissions policies' page. The left sidebar displays the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Roles, Policies, and Access reports. The main content area shows a list of permissions policies, with 'VPCFlowLogPolicy' selected. Below the list, the policy's JSON definition is displayed, showing actions like 'logs:CreateLogGroup', 'logs:CreateLogStream', 'logs:Describe*', and 'logs:PutLogEvents'. The policy is of type 'Customer inline' and has 0 attached entities. A 'Permissions boundary' section at the bottom indicates it is not set.

```
1- {
2-   "statement": [
3-     {
4-       "action": [
5-         "logs:CreateLogGroup",
6-         "logs:CreateLogStream",
7-         "logs:Describe*",
8-         "logs:PutLogEvents"
9-       ],
10-      "resource": "*",
11-      "effect": "Allow"
12-    }
13-   ]
14- }
```

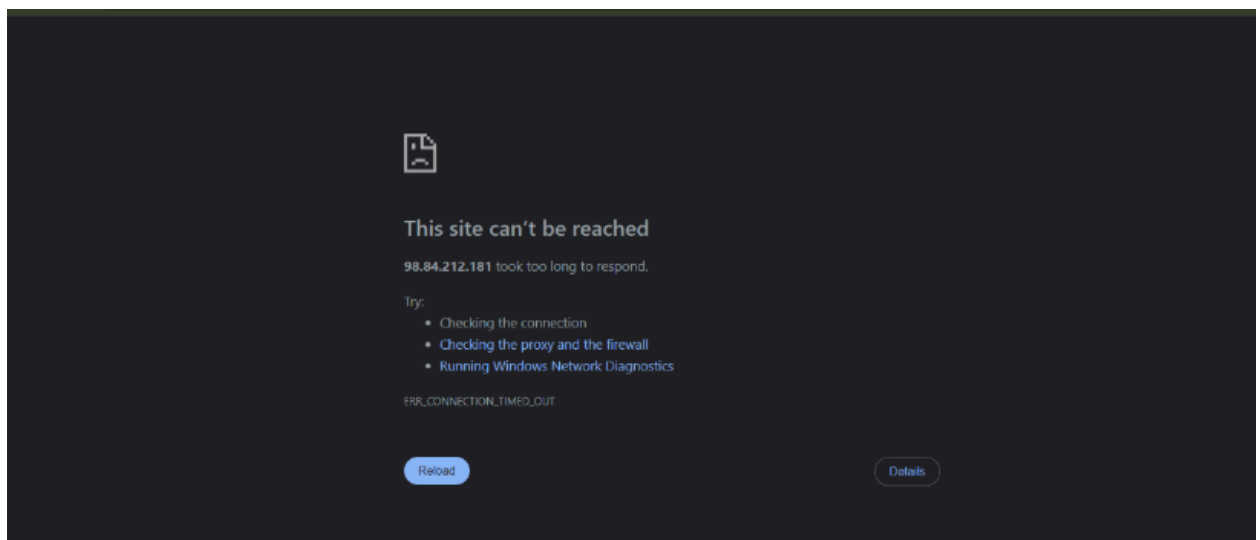
Task 2.2: Create a VPC flow log

Our VPC 1

The screenshot shows the AWS VPC console's 'vpc-077bdf50418dc8c21 / LabVPC' page. The left sidebar shows the 'VPC dashboard' menu with options like Virtual private cloud, Your VPCs, Subnets, Route tables, and Security. The main content area displays the VPC's details, including its ID, state (Available), DNS hostnames (Enabled), and DNS resolution (Enabled). Below the details, the 'Resource map' section shows a diagram of the VPC's resources, including subnets (us-east-1a), route tables (rtb-013653038108c613a), and network connections (LabVPCIG).

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

It's failed



testing and can't access this instance on this port

```
bash - "p-172.31.52.170" x Immediate x ⓘ
Installing : 1:openssl11-libs-1.1.1za-1.amzn2.0.1.x86_64
Installing : openssl11-pkcs11-0.4.10-6.amzn2.0.1.x86_64
Installing : libretls-3.8.1-1.el7.x86_64
Installing : libbsd-1.1.0-1.el7.x86_64
Installing : libbsd-0.12.2-1.el7.x86_64
Installing : netcat-1.226-1.el7.x86_64
Verifying : netcat-1.226-1.el7.x86_64
Verifying : libbsd-0.12.2-1.el7.x86_64
Verifying : openssl11-pkcs11-0.4.10-6.amzn2.0.1.x86_64
Verifying : libbsd-1.1.0-1.el7.x86_64
Verifying : 1:openssl11-libs-1.1.1za-1.amzn2.0.1.x86_64
Verifying : libretls-3.8.1-1.el7.x86_64

Installed:
  netcat.x86_64 0:1.226-1.el7

Dependency Installed:
  libbsd.x86_64 0:0.12.2-1.el7  libbsd.x86_64 0:1.1.0-1.el7  libretls.x86_64 0:3.8.1-1.el7  openssl11-libs.x86_64 1:1.1.1za-1.amzn2.0.1  openssl11-pkcs11.x86_64 0:0.4.10-6.amzn2.0.1

Complete!
voclabs:~/environment $ nc -vz 98.84.212.181 80
```

Task 2.4: Configure route table and security group settings

Logs in LabVPCFlowLogs

CloudWatch > Log groups > LabVPCFlowLogs > All events

Log events

Actions

Start tailing

Create metric filter

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](#)

Filter events - press enter to search

Clear

1m

30m

1h

12h

Custom

UTC timezone

Display

	Timestamp	Message	Log stream name
	2024-10-09T15:34:28.000Z	2 456261230246 eni-0dfa8a8e9cee57db1 103.56.61.138 10.1.3...	eni-0dfa8a8e9cee57db1-all
	2024-10-09T15:34:29.000Z	2 456261230246 eni-0dfa8a8e9cee57db1 45.84.89.3 10.1.3.4 6...	eni-0dfa8a8e9cee57db1-all
	2024-10-09T15:34:29.000Z	2 456261230246 eni-0dfa8a8e9cee57db1 117.195.71.37 10.1.3...	eni-0dfa8a8e9cee57db1-all
	2024-10-09T15:34:29.000Z	2 456261230246 eni-0dfa8a8e9cee57db1 118.123.105.93 10.1.3...	eni-0dfa8a8e9cee57db1-all
	2024-10-09T15:34:29.000Z	2 456261230246 eni-0dfa8a8e9cee57db1 141.98.11.79 10.1.3.4...	eni-0dfa8a8e9cee57db1-all
	2024-10-09T15:34:29.000Z	2 456261230246 eni-0dfa8a8e9cee57db1 185.196.220.81 10.1.3...	eni-0dfa8a8e9cee57db1-all
	2024-10-09T15:34:29.000Z	2 456261230246 eni-0dfa8a8e9cee57db1 167.94.145.29 10.1.3...	eni-0dfa8a8e9cee57db1-all
	2024-10-09T15:34:29.000Z	2 456261230246 eni-0dfa8a8e9cee57db1 172.206.141.247 10.1...	eni-0dfa8a8e9cee57db1-all
	2024-10-09T15:34:29.000Z	2 456261230246 eni-0dfa8a8e9cee57db1 199.45.134.184 10.1.3...	eni-0dfa8a8e9cee57db1-all
	2024-10-09T15:34:29.000Z	2 456261230246 eni-0dfa8a8e9cee57db1 80.66.83.47 10.1.3.4 ...	eni-0dfa8a8e9cee57db1-all
	2024-10-09T15:35:29.000Z	2 456261230246 eni-0dfa8a8e9cee57db1 103.203.57.17 10.1.3...	eni-0dfa8a8e9cee57db1-all
	2024-10-09T15:35:29.000Z	2 456261230246 eni-0dfa8a8e9cee57db1 79.110.62.183 10.1.3...	eni-0dfa8a8e9cee57db1-all

Searching about rejected logs

Log events

Actions

Start tailing

Create metric filter

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](#)

54.157.190.120

Clear

1m

30m

1h

12h

Custom

UTC timezone

Display

	Timestamp	Message	Log stream name
▼	2024-10-09T20:03:21.000Z	2 456261230246 eni-0dfa8a8e9cee57db1 54.157.190.120 10.1.3...	eni-0dfa8a8e9cee57db1-all
		2 456261230246 eni-0dfa8a8e9cee57db1 54.157.190.120 10.1.3.4 39026 80 6 6 360 1728504201 1728504242 REJECT OK	
▼	2024-10-09T20:04:21.000Z	2 456261230246 eni-0dfa8a8e9cee57db1 54.157.190.120 10.1.3...	eni-0dfa8a8e9cee57db1-all
		2 456261230246 eni-0dfa8a8e9cee57db1 54.157.190.120 10.1.3.4 39026 80 6 1 60 1728504261 1728504295 REJECT OK	

Add security group rules with ports

Inbound security group rules successfully modified on security group (sg-024bb6e65420e9fe1 | WebServer2SecurityGroup)

Details

EC2 > Security Groups > sg-024bb6e65420e9fe1 - WebServer2SecurityGroup

sg-024bb6e65420e9fe1 - WebServer2SecurityGroup

Actions

Details

Security group name WebServer2SecurityGroup	Security group ID sg-024bb6e65420e9fe1	Description WebServer2SecurityGroup	VPC ID vpc-01219418cd7294374
Owner 456261230246	Inbound rules count 5 Permission entries	Outbound rules count 1 Permission entry	

Edit Inbound

Inbound security group rules successfully modified on security group (sg-042dd672880de8f7d | WebServerSecurityGroup)

Details

EC2 > Security Groups > sg-042dd672880de8f7d - WebServerSecurityGroup

sg-042dd672880de8f7d - WebServerSecurityGroup

Actions

Details

Security group name WebServerSecurityGroup	Security group ID sg-042dd672880de8f7d	Description WebServerSecurityGroup	VPC ID vpc-077bdf50418dc8c21
Owner 456261230246	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

The routsin Web server

Edit routes

Route 1
Destination
10.1.0.0/16

Propagated
No

Target
local

Status
✔ Active

Route 2
Destination

Propagated
No

Target
Internet Gateway

Status
-

Remove

Add route

Cancel Preview Save changes

The port is successfully accessed

Hello world from WebServer!

Task 2.5: Secure the WebServerSubnet with a network ACL

If we change the network access control It will fail (access control list is denied)

Inbound rule 1

Rule number [Info](#)

100

Type [Info](#)

SSH (22) ▼

Protocol [Info](#)

TCP (6) ▼

Port range [Info](#)

22

Source [Info](#)

0.0.0.0/0

Allow/Deny [Info](#)

Deny ▼

Remove

Task 2.6: Review NetworkFirewallVPC and its associated resources

The NetworkFirewallVPC

The resource map displays the following components and their relationships:

- VPC** (NetworkFirewallVPC): The central virtual private cloud.
- Subnets (2)**:
 - us-east-1a**: Contains **WebServer2Subnet** and **FirewallSubnet**.
- Route tables (1)**: **rtb-01b1465c6b1c79d8a**, which is associated with the subnets.
- Network connections (1)**: **NetworkFirewallG**, which connects the VPC to other networks.

Task 2.7: Create a network firewall

Creating Firewall

[VPC](#) > [Network Firewall: Firewalls](#) > Create firewall

Step 1

Describe firewall

Step 2

Configure VPC and subnets

Step 3 - optional

Configure advanced settings

Step 4

Associate firewall policy

Step 5 - optional

Add tags

Describe firewall [Info](#)

Name and describe your firewall so you can easily identify it and distinguish it from other resources.

Firewall details

Firewall name

Enter a unique name for the firewall. You can't change the name of the firewall after creation.

NetworkFirewall

The name must have 1-128 characters. Valid characters: a-z, A-Z, 0-9 and - (hyphen). The name can't start or end with a hyphen, and it can't contain two consecutive hyphens.

Task 2.8: Create route tables

Creating Route table

Step 1
[Describe firewall](#)

Step 2
Configure VPC and subnets

Step 3 - optional
Configure advanced settings

Step 4
Associate firewall policy

Step 5 - optional
Add tags

Step 6
Review and create

Configure VPC and subnets [Info](#)

The firewall protects the subnets within an Amazon Virtual Private Cloud (VPC) by filtering traffic going between the subnets and locations outside of your VPC. After you create the firewall and its associated firewall policy, configure your VPC to route traffic through the endpoints created by the firewall.

VPC

For each Availability Zone where you want protection, provide Network Firewall with a public subnet that's dedicated to the firewall endpoint. Only use the firewall subnets that you specify here for the firewall. Don't use them for any other purpose.

VPC

Choose the VPC where you want to create this firewall.

NetworkFirewallVPC

Firewall subnets

Each subnet must have one available IP address. You can't change the subnet's IP address type after creation.

Availability Zone

us-east-1a

Subnet

Choose a subnet

IP address type

Choose an IP address type

Remove subnet

Add new subnet

Adding new destination and change it in the route table

Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional

Create a tag with a key of 'Name' and a value that you specify.

IGW-Ingress-Route-Table

VPC

The VPC to use for this route table.

vpc-08111cbcff722abd5 (NetworkFirewallVPC)

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Q Name X

Value - optional

Q IGW-Ingress-Route-Table X Remove

Add new tag

You can add 49 more tags.

Task 2.9: Configure logging for the network firewall

Creating log group

CloudWatch > Log groups > Create log group

Create log group

Log group details [Info](#)

CloudWatch Logs offers two log classes: Standard and Infrequent Access. [Learn more about the features offered by each log class.](#)

Log group name

Retention setting

Log class [Info](#)

KMS key ARN - optional

Tags

A tag is a label that you assign to an Amazon Web Services resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your Amazon Web Services costs.

No tags are associated with this log group.

[Add new tag](#)

You can add up to 50 more tag(s).

Editing the logging of NetworkFireWall

VPC > Network Firewall: Firewalls > NetworkFirewall > Edit firewall logging configuration

Edit firewall logging configuration [Info](#)

Configure the log type and the log destination. Logs are generated only for stateful rule groups.

Logging configuration

Log type
You can choose to emit alert logs, flow logs, or both.

☒ Alert
☒ Flow
☐ TLS

Alert log destination

Log destination
You can send each log type to a S3 bucket, a CloudWatch log group, or a Kinesis Data Firehose delivery stream.

☐ S3
☒ CloudWatch log group
☐ Kinesis data firehose

CloudWatch log group
Send the logs to a CloudWatch log group.

Flow log destination

Log destination
You can send each log type to a S3 bucket, a CloudWatch log group, or a Kinesis Data Firehose delivery stream.

☐ S3
☒ CloudWatch log group
☐ Kinesis data firehose

CloudWatch log group
Send the logs to a CloudWatch log group.

Task 2.10: Configure the firewall policy and test access

Creating NetworkFirewall

You've successfully created rule group NetworkFirewallVPCRuleGroup

VPC > Network Firewall: Firewalls > NetworkFirewall

NetworkFirewall Info

Delete

Overview Info

Firewall status 🟢 Ready	Associated firewall policy FirewallPolicy	Associated VPC vpc-08111cbcff722abd5
----------------------------	--	---

Firewall details | Firewall policy settings | Monitoring

Firewall details Edit

Name NetworkFirewall	Description -
-------------------------	------------------

VPC Edit

Associated VPC vpc-08111cbcff722abd5	Firewall subnets subnet-0932d5c501c96e796 (IPv4)
---	---

Phase 3: Securing AWS resources by using AWS KMS

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

Creating Key

Review

Key configuration

Key type Symmetric	Key spec SYMMETRIC_DEFAULT	Key usage Encrypt and decrypt
Origin AWS KMS	Regionality Single-Region key	

You cannot change the key configuration after the key is created.

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

Adding Sofia Policy

Key policy

Switch to policy view

Key administrators (2)

AddRemove

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](#)

Q Search Key administrators

< 1 >

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

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

Editing the S3 bucket and add KMS for the encryption

Edit default encryption [Info](#)

Default encryption

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

Encryption type [Info](#)

- ☐ Server-side encryption with Amazon S3 managed keys (SSE-S3)
- ☒ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- ☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the [Storage](#) tab of the [Amazon S3 pricing page](#).

AWS KMS key [Info](#)

- ☒ Choose from your AWS KMS keys
- ☐ Enter AWS KMS key ARN

Available AWS KMS keys

arn:aws:kms:us-east-1:495000172139:key/b224...



[Create a KMS key](#)

Bucket Key

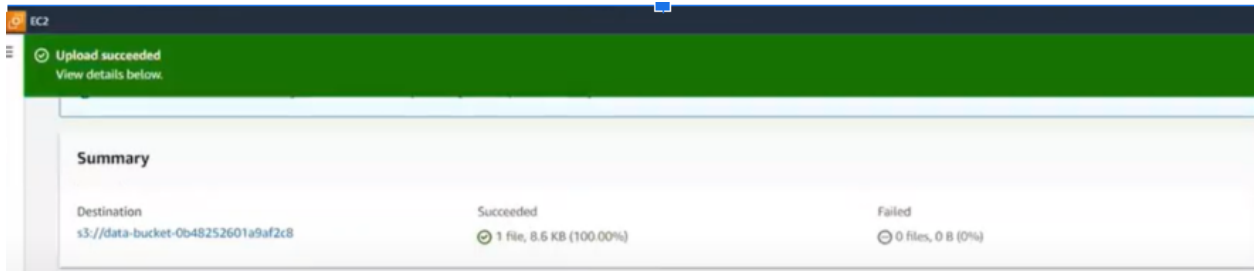
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

- ☐ Disable
- ☒ Enable

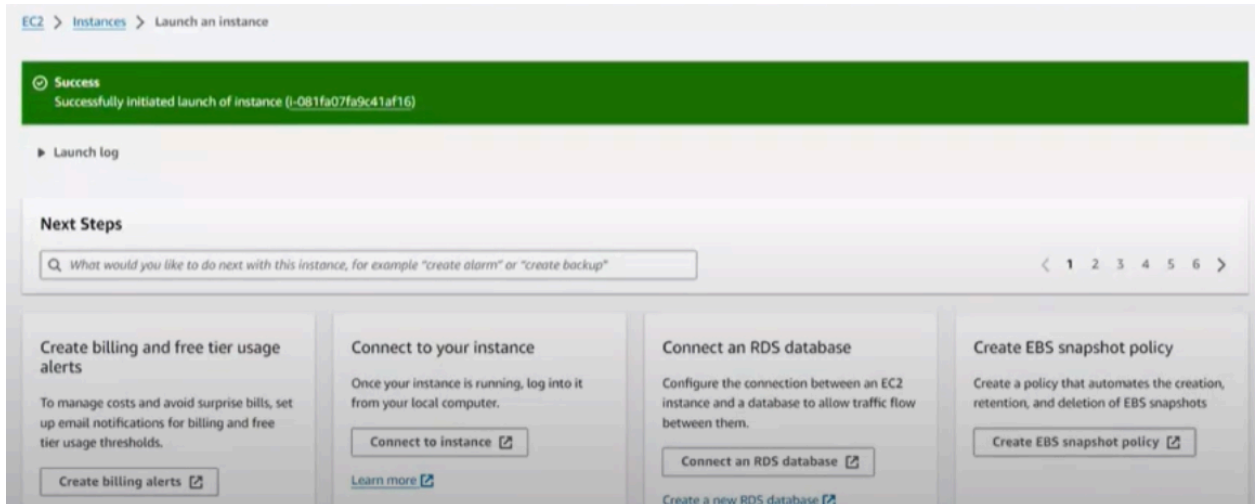
The uploaded Excel

	A	B	C	D	E	F	G	H	I	J	K
1	xxxxxxxxxx										
2											
3	date,description,amount,principal,interest										
4											
5	2023-01-14	payment	1000.00	845.52	154.48						
6											
7	2022-12-22	payment	1021.52	742.80	278.72						
8											
9	2022-11-15	payment	1000.00	855.27	144.73						
10											

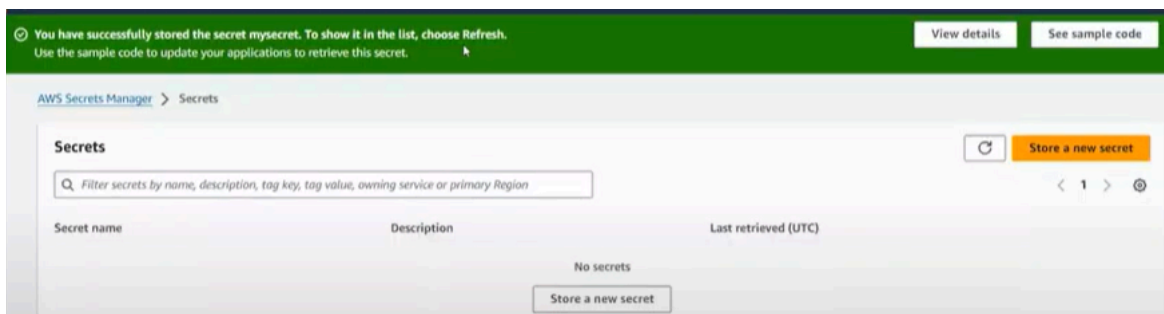
Success



Lunch Instance



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

My Estimate

Edit

Export

Share

Estimate summary

Info

Upfront cost
0.00 USD

Monthly cost
24.38 USD

Total 12 months cost
292.56 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

Find resources

< 1 > ⚙

<input type="checkbox"/>	Service Name	Status	Upfront cost	Monthly cost	Description	Region	Config Summary
<input type="checkbox"/>	Amazon EC2	-	0.00 USD	24.38 USD	-	Oman (Muscat)	Tenancy (Shared Instances), Operating system (L...
<input type="checkbox"/>	Amazon Virtual Priva...	-	0.00 USD	0.00 USD	-	Oman (Muscat)	