

Digital Egypt Pioneers Initiative - DEPI

New Horizon Alex.

AWS Academy - AWS Cloud Architect

Project report

By: Hamza Shokry Warda

# 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

The screenshot shows the AWS S3 Bucket Properties page. The left sidebar has 'Buckets' selected under 'Amazon S3'. The main content area shows the bucket 'data-bucket-0d8eba3afba87e395' with the 'Properties' tab selected. The 'Bucket overview' section displays the ARN as 'arn:aws:s3:::data-bucket-0d8eba3afba87e395' and the creation date as 'September 24, 2024, 19:07:35 (UTC+03:00)'. The 'Bucket Versioning' section shows it is 'Enabled'. The 'Tags (0)' section indicates there are no tags applied to the bucket.

Amazon S3 > Buckets > data-bucket-0d8eba3afba87e395

**Objects (4) Info**

Name	Type	Last modified	Size	Storage class
customer-data.csv	csv	October 5, 2024, 10:20:31 (UTC+03:00)	350.0 B	Standard
customers.csv	csv	September 27, 2024, 11:24:11 (UTC+03:00)	328.0 B	Standard
loan-data.csv	csv	October 4, 2024, 10:52:58 (UTC+03:00)	172.0 B	Standard
myfile.txt	txt	September 24, 2024, 19:14:20 (UTC+03:00)	11.0 B	Standard

Amazon S3 > Bucket policy

```

{
    "Effect": "Allow",
    "Principal": "*",
    "AWS": [
        "arn:aws:iam::768826479868:user/sofia",
        "arn:aws:iam::768826479868:user/paulo",
        "arn:aws:iam::768826479868:role/voclabs"
    ],
    "Action": "s3:*",
    "Resource": [
        "arn:aws:s3:::data-bucket-0d8eba3afba87e395",
        "arn:aws:s3:::data-bucket-0d8eba3afba87e395/*"
    ]
},
{
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:*",
    "Resource": [
        "arn:aws:s3:::data-bucket-0d8eba3afba87e395"
    ]
}
  
```

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

Screenshot of the AWS S3 Bucket Properties page for 'data-bucket-0d8eba3afba87e395'.

**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

**Bucket overview**

AWS Region US East (N. Virginia) us-east-1	Amazon Resource Name (ARN) arn:aws:s3:::data-bucket-0d8eba3afba87e395	Creation date September 24, 2024, 19:07:35 (UTC+03:00)
---	--	---

**Bucket Versioning**

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

Bucket Versioning  
Enabled

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

**Tags (0)**

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Screenshot of the AWS S3 Bucket Configuration page for 'data-bucket-0d8eba3afba87e395'.

**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

**Name** Status Scope Days until transition to Archive ... Days until transition to Deep ...

No archive configurations  
No configurations to display.

**Create configuration**

**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-0d8eba3afba87e395

Log object key format  
data-bucket{[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]}

**AWS CloudTrail data events (1)** [Info](#) [Configure in CloudTrail](#)

Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. [Learn more](#)

Name Access

[data-bucket-reads-writes](#) Read, Write

**Create event notification**

**Event notifications (0)**

Send a notification when specific events occur in your bucket. [Learn more](#)

Name Event types Filters Destination type Destination

No event notifications

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

```

{
  "Version": "2012-10-17",
  "Id": "S3-Console-Auto-Gen-Policy-1727418945836",
  "Statement": [
    {
      "Sid": "S3PolicyStmt-DO-NOT-MODIFY-1727418945593",
      "Effect": "Allow",
      "Principal": "*",
      "Service": "logging.s3.amazonaws.com"
    },
    {
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::s3-objects-access-log-0d8eba3afba87e395/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "768826479868"
        }
      }
    }
  ]
}

```

**Object Ownership** [Info](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

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

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

Successfully modified a destination bucket policy  
Amazon S3 modified the existing bucket policy to add the required permissions. [Learn more](#)

**Inventory configurations (1) [Info](#)**

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

Name	Status	Scope	Destination	Frequency	Last export	Format
Inventory	Enabled	Entire bucket	s3://s3-inventory-0d8eba3...	Daily	-	Apache Parquet

## Task 1.4: Confirm that versioning works as intended

The screenshot shows the AWS S3 console with the path `Amazon S3 > Buckets > data-bucket-0d8eba3afba87e595 > customers.csv`. The file `customers.csv` has two versions:

Version ID	Type	Last modified	Size	Storage class
4F86Vi1qV9sgCegxVU5YIM4oAb.1xp5 (Current version)	csv	September 27, 2024, 11:24:11 (UTC+03:00)	328.0 B	Standard
NozXX3uNPGbCtj5135Qivpa.M8i6.x7	csv	September 27, 2024, 11:21:54 (UTC+03:00)	204.0 B	Standard

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

The screenshot shows the Amazon Athena Query editor with the path `Amazon Athena > Query editor`. The query `Query 1` is running:

```
1 CREATE EXTERNAL TABLE `default.bucket_logs`(`bucketowner` STRING,  
2 `bucket_name` STRING,  
3 `requester` STRING,  
4 `remoteip` STRING,  
5 `requester` STRING,  
6 `requestid` STRING,  
7 `operation` STRING,  
8 `key` STRING,  
9 `request_url` STRING,  
10 `httpstatus` STRING,  
11 `errortype` STRING,  
12 `bytessent` BIGINT,  
13 `objectsize` BIGINT,  
14 `totaltime` STRING,
```

The results show a successful execution:

Completed	Time in queue: 45 ms	Run time: 457 ms	Data scanned: -
Query successful.			

```

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

```

SQL Ln 1, Col 1

Run again Explain Cancel Clear Create

Query results Completed Time in queue: 110 ms Run time: 707 ms Data scanned: 105.18 KB

Results (95) Copy Download results

#	requester	operation	key	httpstatus
1	arn:aws:iam::768826479868:user/paulo	REST.GET.BUCKETVERSIONS	-	200

## Cost assessment to secure Amazon S3

Successfully added Amazon Athena estimate.

AWS Pricing Calculator > My Estimate Edit

My Estimate

Service Name	Status	Upfront cost	Monthly cost	Description	Region	Config Summary
Amazon Simple Storage Service	-	0.02 USD	5.65 USD	-	US East (N. Virginia)	S3 Standard storage (50 GB p...)
Amazon Athena	-	0.00 USD	1,159.42 USD	-	US East (N. Virginia)	Total number of queries (5 per...

Acknowledgement

AWS Pricing Calculator provides only an estimate of your AWS fees and doesn't include any taxes that might apply. Your actual fees depend on a variety of factors, including your actual usage of AWS services. Learn more

## Phase 2: Securing VPCs

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

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways
- Peering connections

Security

- Network ACLs
- Security groups

DNS firewall

CloudShell Feedback

VPC > Your VPCs > vpc-0a8351ccc4178a59e

### vpc-0a8351ccc4178a59e / LabVPC

**Details**

VPC ID	vpc-0a8351ccc4178a59e	State	Available	DNS hostnames	Enabled	DNS resolution	Enabled
Tenancy	Default	DHCP option set	dopt-0de0aa5b9e1fde46e	Main route table	rtb-062223e6372ef4570	Main network ACL	acl-0a0effd12a466fc92
Default VPC	No	IPv4 CIDR	10.1.0.0/16	IPv6 pool	-	IPv6 CIDR (Network border group)	-
Network Address Usage metrics	Disabled	Route 53 Resolver DNS Firewall rule groups	-	Owner ID	768826479868		

**Resource map**

Resource map

VPC Show details

Subnets (1)

Route tables (1)

Network connections (1)

us-east-1a

WebServerSubnet

rtb-062223e6372ef4570

LabVPCIG

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## Task 2.2: Create a VPC flow log

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways
- Peering connections

Security

- Network ACLs
- Security groups

DNS firewall

CloudShell Feedback

VPC > Your VPCs > vpc-0a8351ccc4178a59e

### vpc-0a8351ccc4178a59e / LabVPC

**Details**

VPC ID	vpc-0a8351ccc4178a59e	State	Available	DNS hostnames	Enabled	DNS resolution	Enabled
Tenancy	Default	DHCP option set	dopt-0de0aa5b9e1fde46e	Main route table	rtb-062223e6372ef4570	Main network ACL	acl-0a0effd12a466fc92
Default VPC	No	IPv4 CIDR	10.1.0.0/16	IPv6 pool	-	IPv6 CIDR (Network border group)	-
Network Address Usage metrics	Disabled	Route 53 Resolver DNS Firewall rule groups	-	Owner ID	768826479868		

**Flow logs**

Flow logs (1)

Name	Flow log ID	Filter	Destination type	Destination name	IAM role ARN
LabVPCFlowLogs	fl-0026ab9735aeafaf1b	ALL	cloud-watch-logs	LabVPCFlowLogs	arn:aws:iam::76

Actions

Create flow log

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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

The screenshot shows the AWS CloudWatch Log Groups interface. On the left, a navigation sidebar includes sections for Billing, Logs (Log groups, Log Anomalies, Live Tail, Logs Insights, Contributor Insights), Metrics (All metrics, Explorer, Streams), X-Ray traces, Events (Rules, Event Buses), Application Signals, Network monitoring, and Insights (Settings, Getting Started, What's new). The main content area displays the 'LabVPCFlowLogs' log group details. Key information shown includes:

- Log class:** Standard
- ARN:** arn:aws:logs:us-east-1:768826479868:log-group:LabVPCFlowLogs:\*
- Creation time:** 13 days ago
- Retention:** Never expire
- Stored bytes:** 600.15 KB
- Metric filters:** 0
- Subscription filters:** 0
- Contributor Insights rules:** -
- KMS key ID:** -
- Anomaly detection:** Configure
- Data protection:** -
- Sensitive data count:** -

Below the details, there are tabs for Log streams, Tags, Anomaly detection, Metric filters, Subscription filters, Contributor Insights (selected), and Data protection. The Log streams tab lists one stream: eni-08c8646cc1d6a8631-all, with its last event time being 2024-10-10 03:31:55 (UTC).

The screenshot shows the AWS CloudWatch Log Events interface for the eni-08c8646cc1d6a8631-all stream. The left sidebar is identical to the first screenshot. The main content area displays log events with a timestamp and message column. The messages show various network traffic logs, such as:

- 2024-10-10T03:36:13.000Z 2 768826479868 eni-08c8646cc1d6a8631 162.216.150.118 10.1.3.4 51469 2098 6 1 44 1728531373 1728531429 REJECT OK
- 2024-10-10T03:36:13.000Z 2 768826479868 eni-08c8646cc1d6a8631 205.210.31.243 10.1.3.4 56125 10010 6 1 44 1728531373 1728531429 REJECT OK
- 2024-10-10T03:36:13.000Z 2 768826479868 eni-08c8646cc1d6a8631 139.144.239.74 10.1.3.4 48984 443 6 1 44 1728531373 1728531429 REJECT OK
- 2024-10-10T03:36:13.000Z 2 768826479868 eni-08c8646cc1d6a8631 162.216.149.248 10.1.3.4 53139 46989 6 1 44 1728531373 1728531429 REJECT OK
- 2024-10-10T03:36:13.000Z 2 768826479868 eni-08c8646cc1d6a8631 147.185.132.235 10.1.3.4 50233 58008 6 1 44 1728531373 1728531429 REJECT OK
- 2024-10-10T03:36:13.000Z 2 768826479868 eni-08c8646cc1d6a8631 79.110.62.63 10.1.3.4 57237 16220 6 1 40 1728531373 1728531429 REJECT OK
- 2024-10-10T03:36:13.000Z 2 768826479868 eni-08c8646cc1d6a8631 94.102.49.190 10.1.3.4 23320 4443 6 1 44 1728531373 1728531429 REJECT OK
- 2024-10-10T03:36:13.000Z 2 768826479868 eni-08c8646cc1d6a8631 35.203.211.131 10.1.3.4 55639 8116 6 1 44 1728531373 1728531429 REJECT OK
- 2024-10-10T03:36:13.000Z 2 768826479868 eni-08c8646cc1d6a8631 35.203.211.186 10.1.3.4 49534 2122 6 1 44 1728531373 1728531429 REJECT OK
- 2024-10-10T03:36:13.000Z 2 768826479868 eni-08c8646cc1d6a8631 162.216.150.96 10.1.3.4 51935 2012 6 1 44 1728531373 1728531429 REJECT OK
- 2024-10-10T03:37:03.000Z 2 768826479868 eni-08c8646cc1d6a8631 35.203.211.182 10.1.3.4 52089 55022 6 1 44 1728531423 1728531433 REJECT OK
- 2024-10-10T03:37:03.000Z 2 768826479868 eni-08c8646cc1d6a8631 193.41.206.142 10.1.3.4 48461 8728 6 1 40 1728531423 1728531433 REJECT OK
- 2024-10-10T03:37:14.000Z 2 768826479868 eni-08c8646cc1d6a8631 162.216.150.83 10.1.3.4 50253 49456 6 1 44 1728531434 1728531486 REJECT OK
- 2024-10-10T03:37:14.000Z 2 768826479868 eni-08c8646cc1d6a8631 80.82.65.99 10.1.3.4 51315 8443 6 1 40 1728531434 1728531486 REJECT OK

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

AWS Services Search [Alt+S]

N. Virginia vocabs/user3362557-Hamza\_Shokry\_Warda @ 7688-2647-9868

VPC > Subnets > subnet-0842e04b858ca0f27

### subnet-0842e04b858ca0f27 / WebServerSubnet

**Actions**

**Details**

Subnet ID	subnet-0842e04b858ca0f27	Subnet ARN	arn:aws:ec2:us-east-1:768826479868:subnet/subnet-0842e04b858ca0f27	State	Available	IP4 CIDR	10.1.3.0/28
Available IPv4 addresses	10	IPv6 CIDR	-	IPv6 CIDR association ID	-	Availability Zone	us-east-1a
Availability Zone ID	use1-2z6	Network border group	us-east-1	VPC	vpc-0a8351ccc4178a59e   LabVPC	Route table	rtb-062223e6372ef4570
Network ACL	acl-0a0effd12a466fc92	Default subnet	No	Auto-assign public IPv4 address	Yes	Auto-assign IPv6 address	No
Auto-assign customer-owned IPv4 address	No	Customer-owned IPv4 pool	-	Outpost ID	-	IPv4 CIDR reservations	-
IPv6 CIDR reservations	-	IPv6-only	No	Hostname type	IP name	Resource name DNS A record	Disabled
Resource name DNS AAAA record	Disabled	DNS64	Disabled	Owner	768826479868	Owner	Disabled

Flow logs | Route table | Network ACL | CIDR reservations | Sharing | Tags

Route table: rtb-062223e6372ef4570 Edit route table association

Routes (2)

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search [Alt+S]

N. Virginia vocabs/user3362557-Hamza\_Shokry\_Warda @ 7688-2647-9868

VPC dashboard

EC2 Global View Filter by VPC

Virtual private cloud Your VPCs Subnets

Route tables Internet gateways Egress-only internet gateways Carrier gateways DHCP option sets Elastic IPs Managed prefix lists Endpoints Endpoint services NAT gateways Peering connections

Security Network ACLs Security groups

DNS firewall

CloudShell Feedback

Route tables (1/1) Info

Last updated 1 minute ago Actions Create route table

Route table ID: rtb-062223e6372ef4570 Clear filters

Name	Route table ID	Explicit subnet assoc...	Edge associations	Main	VPC
-	rtb-062223e6372ef4570	-	-	Yes	vpc-0a8351ccc4178a59e   LabVPC

rtb-062223e6372ef4570

Routes (2) Both Edit routes

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0d8eba3afba87e395	Active	No
10.1.0.0/16	local	Active	No

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

```

Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

[ec2-user@webserver ~]$ ping -c 3 www.amazon.com
PING diag4hukkh62yn.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=249 time=1.61 ms
64 bytes from server-3-162-95-220.iad61.r.cloudfront.net (3.162.95.220): icmp_seq=2 ttl=249 time=1.82 ms
64 bytes from server-3-162-95-220.iad61.r.cloudfront.net (3.162.95.220): icmp_seq=3 ttl=249 time=1.60 ms
--- diag4hukkh62yn.cloudfront.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.604/1.679/1.824/0.102 ms
[ec2-user@webserver ~]$ 
[ec2-user@webserver ~]$ 

```

i-0a34ddf809325c09b (WebServer)  
PublicIPs: 18.213.135.204 PrivateIPs: 10.1.3.4

[CloudShell](#) [Feedback](#)

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

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

```

File Edit Find View Go Run Tools Window Support Preview Run
Go Anything (Ctrl+P)
CloudInstance
README.md
aws

bash -"ip-172-31-31-87 e x Immediate +"
voclabs:~/environment $ nc -vz 35.168.41.4 22
Ncat: Version 7.90 ( https://nmap.org/ncat )
Ncat: Connected to 35.168.41.4:22.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
voclabs:~/environment $ nc -vz 35.168.41.4 21
Ncat: Version 7.90 ( https://nmap.org/ncat )
Ncat: Connecting timed out.
voclabs:~/environment $ nc -vz 35.168.41.4 22
Ncat: Version 7.90 ( https://nmap.org/ncat )
Ncat: Connected to 35.168.41.4:22.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
voclabs:~/environment $ 

```

CodeWhisperer AWS profile default

Network ACL: `acl-0a0efdd12a466fc92`

**Inbound rules (3)**

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

**Outbound rules (2)**

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

## Task 2.6: Review NetworkFirewallVPC and its associated resources

Your VPCs (1/3) Info

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route
<input checked="" type="checkbox"/> NetworkFirewallVPC	vpc-0584290e63bf6bcb6	Available	10.1.0.0/16	-	dopt-0de0aa5b9e1fde46e	rtb-0362c14
<input type="checkbox"/> LabVPC	vpc-0a8351cc4178a59e	Available	10.1.0.0/16	-	dopt-0de0aa5b9e1fde46e	rtb-062223
-	vpc-0eb118ce7f66c76af	Available	172.31.0.0/16	-	dopt-0de0aa5b9e1fde46e	rtb-0ba6d9

**vpc-0584290e63bf6bcb6 / NetworkFirewallVPC**

**Resource map** Info

- VPC Show details**: Your AWS virtual network. Subnets: NetworkFirewallVPC.
- Subnets (2)**: Subnets within this VPC. us-east-1a: FirewallSubnet, WebServer2Subnet.
- Route tables (4)**: Route network traffic to resources. rtb-0362c14: Firewall-Route-Table, IGW-Ingress-Route-Table, WebServer2-Route-Table.
- Network connections (1)**: Connections to other networks. NetworkFirewallIG.

## Task 2.7: Create a network firewall

The screenshot shows the AWS Network Firewall NetworkFirewall details page. The left sidebar includes sections for NAT gateways, Peering connections, Security (Network ACLs, Security groups), DNS firewall (Rule groups, Domain lists), Network Firewall (Firewalls, Firewall policies, Network Firewall rule groups, TLS inspection configurations, Network Firewall resource groups), Virtual private network (VPN) (Customer gateways, Virtual private gateways, Site-to-Site VPN connections, Client VPN endpoints), and AWS Verified Access. The main content area displays the NetworkFirewall details for 'NetworkFirewall'. It shows the Firewall status as 'Ready', the Associated firewall policy as 'FirewallPolicy', and the Associated VPC as 'vpc-0584290e63bf6bc6'. Below this, tabs for Firewall details, Firewall policy settings, and Monitoring are visible. Under Firewall details, there are sections for Firewall details (Name: NetworkFirewall, Description: -), VPC (Associated VPC: vpc-0584290e63bf6bc6, Firewall subnets: subnet-0959f044a80adb4ba (IPv4)), and Firewall endpoints.

## Task 2.8: Create route tables

The screenshot shows the AWS VPC dashboard Route tables page. The left sidebar includes sections for EC2 Global View, Virtual private cloud (Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, Peering connections), Security (Network ACLs, Security groups), and DNS firewall. The main content area displays the route table 'rtb-0741ac2d3e542aed6 / IGW-Ingress-Route-Table'. It shows the Details (Route table ID: rtb-0741ac2d3e542aed6, Main: No, Owner ID: 768826479868, Explicit subnet associations: -, Edge associations: igw-062a5cc69967e026e / NetworkFirewallIG). Below this, tabs for Routes, Subnet associations, Edge associations, Route propagation, and Tags are visible. The Routes section shows two entries: Destination 10.1.0.0/16 Target local Status Active Propagated No, and Destination 10.1.3.0/28 Target vpce-06ff1b97a1fc30c47 Status Active Propagated No.

VPC dashboard > Route tables > rtb-024bfbbbe3a33579c4 / Firewall-Route-Table

**Details**

Route table ID rtb-024bfbbbe3a33579c4	Main No	Explicit subnet associations subnet-0959f044a80adb4ba / FirewallSubnet	Edge associations -
VPC vpc-0584290e63bf6ccb6   NetworkFirewallVPC	Owner ID 768826479868		

**Routes (2)**

Destination	Target	Status	Propagated
0.0.0.0/0	igw-06f1b97a1fc30c47	Active	No
10.1.0.0/16	local	Active	No

VPC dashboard > Route tables > rtb-08baee344753da88a / WebServer2-Route-Table

**Details**

Route table ID rtb-08baee344753da88a	Main No	Explicit subnet associations subnet-0c6f8361da934b0f8 / WebServer2Subnet	Edge associations -
VPC vpc-0584290e63bf6ccb6   NetworkFirewallVPC	Owner ID 768826479868		

**Routes (2)**

Destination	Target	Status	Propagated
0.0.0.0/0	vpc-06f1b97a1fc30c47	Active	No
10.1.0.0/16	local	Active	No

## Task 2.9: Configure logging for the network firewall

**Log group details**

**Log streams (36)**

Last event time	Log stream
2024-10-10 04:01:45 (UTC)	/aws/network-firewall/flow/NetworkFirewall_2024-10-10-04
2024-10-10 04:01:26 (UTC)	/aws/network-firewall/alert/NetworkFirewall_2024-10-10-04
2024-10-10 03:41:01 (UTC)	/aws/network-firewall/flow/NetworkFirewall_2024-10-10-03
2024-10-10 03:36:26 (UTC)	/aws/network-firewall/alert/NetworkFirewall_2024-10-10-03
2024-10-09 19:33:39 (UTC)	/aws/network-firewall/flow/NetworkFirewall_2024-10-09-19
2024-10-09 19:14:11 (UTC)	/aws/network-firewall/alert/NetworkFirewall_2024-10-09-19
2024-10-09 18:59:59 (UTC)	/aws/network-firewall/flow/NetworkFirewall_2024-10-09-18
2024-10-09 18:58:00 (UTC)	/aws/network-firewall/alert/NetworkFirewall_2024-10-09-18

**Log events**

Timestamp	Message
2024-10-04T02:29:24.000Z	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "1728008964", "event": {"tcp": {"tcp_flags": "1e", "syn": true, "rst": true, "p...}}
2024-10-04T02:29:24.000Z	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "1728008964", "event": {"tcp": {"tcp_flags": "12", "syn": true, "ack": true}, "...}}
2024-10-04T02:29:27.000Z	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "1728008967", "event": {"tcp": {"tcp_flags": "1e", "syn": true, "rst": true, "p...}}
2024-10-04T02:29:27.000Z	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "1728008967", "event": {"tcp": {"tcp_flags": "12", "syn": true, "ack": true}, "...}}
2024-10-04T02:30:13.000Z	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "1728009013", "event": {"tcp": {"tcp_flags": "1f", "syn": true, "fin": true, "r...}}
2024-10-04T02:30:13.000Z	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "1728009013", "event": {"tcp": {"tcp_flags": "12", "syn": true, "ack": true}, "...}}

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

A newer release of "Amazon Linux" is available.  
 Version 2023.5.20241001:  
 Run "/usr/bin/dnf check-release-update" for full release and version update info

```

  _\###_
 /###\  Amazon Linux 2023
  \###/
   \###/
    \###/
     \###/
      \###/
       \###/
        \###/
         \###/
          \###/
           \###/
            \###/
             \###/
              \###/
               \###/
                \###/
                 \###/
                  \###/
                   \###/
                    \###/
                     \###/
                      \###/
                       \###/
                        \###/
                         \###/
                          \###/
                           \###/
                            \###/
                             \###/
                              \###/
                               \###/
                                \###/
                                 \###/
                                  \###/
                                   \###/
                                    \###/
                                     \###/
                                      \###/
                                       \###/
                                        \###/
                                         \###/
                                          \###/
                                           \###/
                                            \###/
                                             \###/
                                              \###/
                                               \###/
                                                \###/
                                                 \###/
                                                  \###/
                                                   \###/
                                                    \###/
                                                     \###/
                                                      \###/
                                                       \###/
                                                        \###/
                                                         \###/
                                                          \###/
                                                           \###/
                                                            \###/
                                                             \###/
                                                              \###/
                                                               \###/
                                                                \###/
                                                                 \###/
                                                                \###/
                                                               \###/
                                                                \###/
                                                               \###/
                                                                \###/
                                                               \###/>

```

root@i-0fff64e6587bcf527:~# ping -c 3 www.amazon.com  
 PING diag4hukkh62yn.cloudfront.net (3.167.40.181) 56(84) bytes of data.  
 64 bytes from server-3-167-40-181.iad61.r.cloudfront.net (3.167.40.181): icmp\_seq=1 ttl=245 time=2.94 ms  
 64 bytes from server-3-167-40-181.iad61.r.cloudfront.net (3.167.40.181): icmp\_seq=2 ttl=245 time=2.05 ms  
 64 bytes from server-3-167-40-181.iad61.r.cloudfront.net (3.167.40.181): icmp\_seq=3 ttl=245 time=2.06 ms

```

--- diag4hukkh62yn.cloudfront.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 2.048/2.350/2.342/0.419 ms
[ec2-user@webserver2 ~]$ sudo netstat -alnlp | grep -i listen
tcp        0      0 0.0.0.0:22          0.0.0.0:*          LISTEN      2338/sshd: /usr/sbin
tcp        0      0 0.0.0.0:8080        0.0.0.0:*          LISTEN      3455/python3
tcp6       0      0 ::1:22             ::*               LISTEN      2338/sshd: /usr/sbin
tcp6       0      0 ::1:80             ::*               LISTEN      2005/httpd
[ec2-user@webserver2 ~]$ 

```

i-0fff64e6587bcf527 (WebServer2)  
 PublicIPs: 35.168.41.4 PrivateIPs: 10.1.3.4

VPC dashboard X

EC2 Global View

Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways
- Peering connections

Security

- Network ACLs
- Security groups

DNS firewall

CloudShell Feedback

**NetworkFirewall** Delete

**Overview**

Firewall status	Associated firewall policy	Associated VPC
Ready	<a href="#">FirewallPolicy</a>	<a href="#">vpc-0584290e63bf6bcb6</a>

**Firewall details**

Name	Description
NetworkFirewall	-

**VPC**

Associated VPC	Firewall subnets
<a href="#">vpc-0584290e63bf6bcb6</a>	<a href="#">subnet-0959f044a80adb4ba</a> (IPv4)

**Firewall endpoints**

Screenshot of the AWS CloudShell interface showing the AWS DNS Firewall configuration.

The sidebar navigation includes:

- DNS firewall
- Rule groups
- Domain lists
- Network Firewall
- Firewalls
- Firewall policies
- Network Firewall rule groups
- TLS inspection configurations
- Network Firewall resource groups
- Virtual private network (VPN)
- Customer gateways
- Virtual private gateways
- Site-to-Site VPN connections
- Client VPN endpoints
- AWS Verified Access
- Verified Access instances [New](#)
- Verified Access trust providers [New](#)
- Verified Access groups [New](#)

The main content area shows the "No IP set reference" section with the message: "There are no IP set reference to display." Below it is the "Rules (5)" table:

Description	Geo IP	Protocol	Source	Destination	Destination port	Direction	Action	Keyword
-	-	TCP	ANY	ANY	8080	Forward	Drop	sid:1
-	-	TCP	ANY	ANY	80	Forward	Pass	sid:2
-	-	TCP	ANY	ANY	22	Forward	Pass	sid:3
-	-	TCP	ANY	ANY	443	Forward	Pass	sid:4
-	-	ICMP	ANY	ANY	ANY	Forward	Pass	sid:5

Below the table is the "Customer managed key" section with the message: "Key type AWS owned key".

CloudShell status bar: CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Screenshot of the AWS CloudShell interface showing terminal output for a ping test and a CloudWatch Log Stream.

The terminal output shows a ping test from an EC2 instance to the Amazon Linux 2023 website:

```
[ec2-user@webserver ~]$ ping -c 3 www.amazon.com
PING diag4hukkh62yn.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=249 time=1.61 ms
64 bytes from server-3-162-95-220.iad61.r.cloudfront.net (3.162.95.220): icmp_seq=2 ttl=249 time=1.62 ms
64 bytes from server-3-162-95-220.iad61.r.cloudfront.net (3.162.95.220): icmp_seq=3 ttl=249 time=1.60 ms
--- diag4hukkh62yn.cloudfront.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.604/1.679/1.824/0.102 ms
[ec2-user@webserver ~]$
```

A CloudWatch Log Stream window is open, showing log entries for instance i-0a54ddf809323c09b (WebServer). The log entries show the public and private IP addresses of the instance:

```
i-0a54ddf809323c09b (WebServer)
PublicIPs: 18.213.155.204 PrivateIPs: 10.1.3.4
```

CloudShell status bar: CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS CloudWatch Log Groups interface. The left sidebar includes sections for Billing, Logs (Log groups, Log Anomalies, Live Tail, Logs Insights, Contributor Insights), Metrics (All metrics, Explorer, Streams), X-Ray traces, Events (Rules, Event Buses), Application Signals, Network monitoring, and Insights (Settings, Getting Started, What's new). The main pane is titled "NetworkFirewallVPCLogs" and shows "Log group details". It has tabs for Log streams, Tags, Anomaly detection, Metric filters, Subscription filters, Contributor Insights, and Data protection. Under "Log streams (36)", there is a search bar and filters for "Exact match" and "Show expired". A table lists 36 log streams with their last event times, such as "/aws/network-firewall/flow/NetworkFirewall\_2024-10-10-04" (2024-10-10 04:01:45 UTC) and "/aws/network-firewall/alert/NetworkFirewall\_2024-10-10-04" (2024-10-10 04:01:26 UTC).

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

The screenshot shows the AWS Pricing Calculator interface. At the top, a green banner says "Successfully added AWS Network Firewall estimate." The main area is titled "My Estimate" and shows an "Edit" link. It includes a "Estimate summary" section with "Upfront cost: 0.00 USD", "Monthly cost: 452.23 USD", and "Total 12 months cost: 5,426.76 USD" (Includes upfront cost). To the right, there is a "Getting Started with AWS" section with "Get started for free" and "Contact Sales" buttons. Below this is a table titled "My Estimate" with columns for Service Name, Status, Upfront cost, Monthly cost, Description, Region, and Config Summary. It lists three resources: Amazon EC2, Amazon Virtual Private Cloud, and AWS Network Firewall. At the bottom, there is a footer with links for Privacy, Site terms, and Cookie preferences, along with a copyright notice: "© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved." A yellow support icon is in the bottom right corner.

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

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

The screenshot shows the AWS KMS console for a specific key. The left sidebar lists 'Customer managed keys' under 'Key Management Service (KMS)'. The main area shows the 'General configuration' tab, which includes fields for Alias (MyKMSkey), Status (Enabled), ARN (arn:aws:kms:us-east-1:768826479868:key/83431716-daf3-4a49-9f19-a207a41b8259), Description ('-'), Creation date (Oct 04, 2024 10:32 GMT+3), and Regionality (Single Region). Below this is the 'Key policy' tab, which contains a JSON policy document:

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:768826479868:alias/MyKMSkey",
                "arn:aws:iam::768826479868:role/voclabs",
                "arn:aws:iam::768826479868:user/sofia"
            ]
        }
    ]
}

```

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

This screenshot shows the same AWS KMS key configuration as the previous one, but with a modified key policy. The JSON document now includes an additional statement:

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:768826479868:alias/MyKMSkey",
                "arn:aws:iam::768826479868:role/voclabs",
                "arn:aws:iam::768826479868:user/sofia"
            ]
        },
        {
            "Sid": "Deny unauthorized access",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:768826479868:alias/MyKMSkey"
            ]
        }
    ]
}

```

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

Screenshot of the AWS S3 Object Overview page for the file "loan-data.csv".

The left sidebar shows the navigation menu for Amazon S3, including Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Storage Lens settings, Dashboards, Storage Lens groups, AWS Organizations settings, Feature spotlight, and AWS Marketplace for S3.

The main content area displays the following details for "loan-data.csv":

- Properties:** Owner (avslabscw6686770169925341), AWS Region (US East (N. Virginia) us-east-1), Last modified (October 4, 2024, 10:52:58 (UTC+03:00)), Size (172.0 B), Type (csv), Key (loan-data.csv).
- S3 URI:** s3://data-bucket-0d8eba3afba87e395/loan-data.csv
- Amazon Resource Name (ARN):** arnaws3::data-bucket-0d8eba3afba87e395/loan-data.csv
- Entity tag (Etag):** 1275abebe657d67b63abad93167e298b
- Object URL:** https://data-bucket-0d8eba3afba87e395.s3.amazonaws.com/loan-data.csv

At the bottom, there is a success message: "Successfully edited default encryption. Objects uploaded, modified, or copied into this bucket will inherit this encryption configuration unless otherwise specified." Other tabs include Permissions and Versions.

Screenshot of the AWS S3 Bucket Configuration page.

The left sidebar shows the navigation menu for Amazon S3, including Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Storage Lens settings, Dashboards, Storage Lens groups, AWS Organizations settings, Feature spotlight, and AWS Marketplace for S3.

The main content area displays the following configuration details:

- Tags (0):** You can use bucket tags to track storage costs and organize buckets. [Learn more](#).
- Default encryption:** Server-side encryption is automatically applied to new objects stored in this bucket.
  - Encryption type:** Info (Server-side encryption with AWS Key Management Service keys (SSE-KMS))
  - Encryption key ARN:** arnawskmsus-east-1:768826479868:key/83431716-daf3-4a49-9f19-a207a41b8259
  - Bucket Key:** When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#).
- Intelligent-Tiering Archive configurations (0):** Enable objects stored in the Intelligent-Tiering storage class to tier-down to the Archive tier or the Deep Archive Access tier which are optimized for objects that will be rarely accessed for long periods of time. [Learn more](#).

At the bottom, there is a success message: "Successfully edited default encryption. Objects uploaded, modified, or copied into this bucket will inherit this encryption configuration unless otherwise specified." Other tabs include View details, Edit, Delete, and Create configuration.

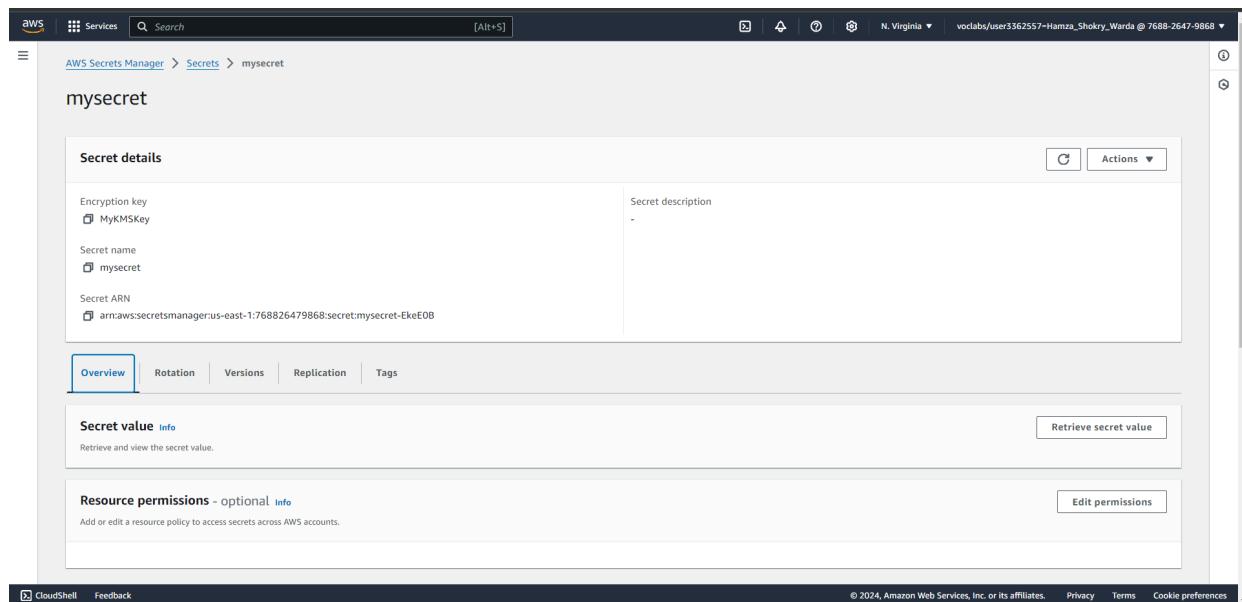
The screenshot shows the AWS S3 console. On the left, there's a sidebar with various options like Buckets, Access Grants, and Storage Lens. The main area is titled 'Storage class' and shows 'Standard' selected. It also includes sections for 'Server-side encryption settings' (using SSE-KMS) and 'Additional checksums'. At the top right, there's a note about generating a delete marker.

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

The screenshot shows the AWS EC2 instance details page. The instance configuration includes fields like IPv6 address, Instance state (Running), Hostname type, Private IP DNS name, Instance type (t2.micro), VPC ID, Subnet ID, and Instance ARN. In the 'Storage' tab, it shows a single volume attached: 'yol-oabc7b739697edda' with device name '/dev/xvda', size 8 GiB, and an attachment status of 'Attached'. The 'Encrypted' column is marked as 'Yes' and the 'KMS key ID' is listed as 'arn:aws:kms:us-east-1:768826479868:key/85431716-daf3-4a49-9f19-a207a41b8259'.

## 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



```

aws | Services | Search | [Alt+S]
① Keyboard shortcut
To tab out of the terminal window and select the next button element, press the left and right Shift keys together.
[ec2-user@webserver2 ~]$ aws secretsmanager list-secrets
{
  "SecretList": [
    {
      "ARN": "arn:aws:secretsmanager:us-east-1:768826479868:secret:mysecret-EkeE0B",
      "Name": "mysecret",
      "LastModified": "2024-10-04T08:39:56.940000+00:00",
      "LastAccessedDate": "2024-10-04T00:00:00+00:00",
      "Tags": [],
      "SecretVersionsToStages": {
        "a9eb303b-38a3-402b-b91f-13719fa064fc": [
          "AWS CURRENT"
        ]
      },
      "CreatedDate": "2024-10-04T08:39:56.870000+00:00"
    }
  ]
}
[ec2-user@webserver2 ~]$ aws secretsmanager get-secret-value
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:
  aws help
  aws <command> help
  aws <command> <subcommand> help
aws: error: the following arguments are required: --secret-id
[ec2-user@webserver2 ~]$ aws secretsmanager get-secret-value --secret-id mysecret
{
  "ARN": "arn:aws:secretsmanager:us-east-1:768826479868:secret:mysecret-EkeE0B",
  "Name": "mysecret",
  "VersionId": "a9eb303b-38a3-402b-b91f-13719fa064fc",
  "SecretString": "i-0fff64e6587bcf527 (WebServer2)
  PublicIPs: 35.168.4.14  PrivateIPs: 10.1.3.4"
}
CloudShell Feedback
© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

```

## Cost assessment for using AWS KMS

Successfully added Amazon EC2 estimate.

[AWS Pricing Calculator](#) > My Estimate

**My Estimate** [Edit](#)

Estimate summary		Info		Getting Started with AWS	
Upfront cost 0.00 USD	Monthly cost 6.73 USD	Total 12 months cost <b>80.76 USD</b>	Includes upfront cost	<a href="#">Get started for free</a>	<a href="#">Contact Sales</a>

**My Estimate**

<a href="#">Find resources</a>									
<input type="checkbox"/>	Service Name	Status	Upfront cost	Monthly cost	Description	Region	Config Summary	Add service	
<input type="checkbox"/>	AWS Key Management Service	-	0.00 USD	1.06 USD	-	US East (N. Virginia)	Number of customer manage...		
<input type="checkbox"/>	Amazon Simple Storage Servi...	-	0.00 USD	0.41 USD	-	US East (N. Virginia)	S3 Standard storage (10 GB p...		
<input type="checkbox"/>	Amazon EC2	-	0.00 USD	5.26 USD	-	US East (N. Virginia)	Tenancy (Shared Instances), O...		

Privacy | Site terms | Cookie preferences | © 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

## Phase 4: Monitoring and logging

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

AWS Services Search [Alt+S] N. Virginia v oclabs/user3362557=Hamza\_Shokry\_Warda @ 7688-2647-9868 ▾

CloudTrail > Trails > arn:aws:cloudtrail:us-east-1:768826479868:trail/data-bucket-reads-writes

### data-bucket-reads-writes

Delete Stop logging

**General details**

Trail logging	Logging	Trail log location	cloudtrail-logs-0d8eba3afba87e395/AWSLogs/76826479868	Log file validation	Enabled	SNS notification delivery	Disabled
Trail name	data-bucket-reads-writes			Last file validation delivered	-	Last SNS notification	-
Multi-region trail	Yes	Last log file delivered	-				
Apply trail to my organization	Not enabled	Log file SSE-KMS encryption	Not enabled				

**CloudWatch Logs**

No CloudWatch Logs log groups  
CloudWatch Logs is not configured for this trail

**Tags**

Manage tags

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search [Alt+S] N. Virginia v oclabs/user3362557=Hamza\_Shokry\_Warda @ 7688-2647-9868 ▾

Amazon Athena > Query editor

Editor Recent queries Saved queries Settings Workgroup primary

**Data**

Data source: AwsDataCatalog Database: default

Tables and views: Create

Tables (2): bucket\_logs, cloudtrail\_logs\_cloudtrail\_logs\_0d8eba3afba87e395

Views (0)

SQL: SELECT \* FROM "default"."cloudtrail\_logs\_cloudtrail\_logs\_0d8eba3afba87e395" limit 10;

Run again Explain Cancel Clear Create

Reuse query results up to 60 minutes ago

**Query results**

Completed Time in queue: 66 ms Run time: 927 ms Data scanned: 10.51 KB

Results (10)

Copy Download results

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS CloudWatch Logs Insights interface. In the top navigation bar, there are tabs for Services, Search, and a dropdown for N. Virginia. Below the navigation is a search bar and a toolbar with icons for copy, paste, and refresh.

The main area has a sidebar titled "Data" with sections for Data source (AwsDataCatalog) and Database (default). Under "Tables and views", there are two tables listed: eventname and awsregion. The eventname table has columns for eventname, awsregion, sourceipaddress, useragent, errorcode, errormessage, requestparameters, responseelements, additionaleventdata, requestid, eventid, resources, and array-struct<arn:string,accountid:string>. The awsregion table has columns for region and accountid.

The central workspace contains a SQL editor with the following query:

```

1 SELECT eventtime, useridentity.principalId, "sourceipaddress", "useragent", requestparameters, eventname
2 FROM cloudtrail_logs_cloudtrail_logs_0d8eba3afba87e395
3 WHERE
4   eventname in ('GetObject') AND
5   requestparameters LIKE '%customer-data.csv%'
6 limit 10;

```

Below the SQL editor is a "Run again" button and a "Re-execute" button. The "Query results" tab is selected, showing a table with one row of data. The row details are:

	sourcelpaddress	useragent
RFR: user3362557=Hamza_Shokry_Warda	197.48.57.66	[Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36]

At the bottom of the interface, there are links for CloudShell, Feedback, and a copyright notice: © 2024, Amazon Web Services, Inc. or its affiliates.

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

The screenshot shows the AWS CloudWatch Terminal interface. The terminal window displays a log message from an EC2 instance. The log message is as follows:

```

2024-10-05T08:00:27Z I! ["caller": "service@0.100.0/service.go:200", "msg": "Everything is ready. Begin running and processing data."]
2024-10-05T08:00:27Z W! ["caller": "localhostgate/featuresgate.go:63", "msg": "The default endpoints for all servers in components will change to use localhost instead of 0.0.0.0 in a future version. Use the feature gate to preview the new default.", "component": "UseLocalHostAsDefaultHost"]
2024-10-05T08:00:27Z I! Statsd listener listening on: [::]:18125
2024-10-05T08:00:27Z I! ["caller": "ec2tagger/ec2tagger.go:480", "msg": "ec2tagger: Initial retrieval of tags succeeded", "kind": "processor", "name": "ec2tagger", "pipeline": "metrics/host"}
2024-10-05T08:00:27Z I! ["caller": "ec2tagger/ec2tagger.go:391", "msg": "ec2tagger: EC2 tagger has started, finished initial retrieval of tags and Volumes", "kind": "processor", "name": "ec2tagger", "pipeline": "metrics/host"}
2024-10-05T08:00:28Z I! First time setting retention for log group EncryptedInstanceSecureLogs, update map to avoid setting twice
2024-10-05T08:00:28Z I! [logagent] piping log from EncryptedInstanceSecureLogs/EncryptedInstanceSecureLogs-1-0e825c37662f43673(/var/log/secure) to cloudwatchlogs with retention 180
2024-10-05T08:00:28Z I! [outputs.cloudwatchlogs] Retrieved 0 time, going to sleep 10.091766ms before retrying.
[ec2-user@ip-10-1-3-12 ~]$ sudo tail -f /var/log/secure
Oct 5 08:00:24 ip-10-1-3-12 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Oct 5 08:00:26 ip-10-1-3-12 sudo: pam_unix(sudo:session): session closed for user root
Oct 5 08:00:31 ip-10-1-3-12 sudo: ec2-user : TTY=tty0 / : PWD=/home/ec2-user : USER=root : COMMAND=/sbin/service#040amazon-cloudwatch-agent#040status
Oct 5 08:00:35 ip-10-1-3-12 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Oct 5 08:01:32 ip-10-1-3-12 sudo: ec2-user : TTY=tty0 / : PWD=/home/ec2-user : USER=root : COMMAND=/bin/cat#040/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
Oct 5 08:01:32 ip-10-1-3-12 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Oct 5 08:01:32 ip-10-1-3-12 sudo: pam_unix(sudo:session): session closed for user root
Oct 5 08:03:12 ip-10-1-3-12 sudo: ec2-user : TTY=tty0 / : PWD=/home/ec2-user : USER=root : COMMAND=/bin/tail#040/f1040/var/log/secure
Oct 5 08:03:12 ip-10-1-3-12 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Oct 5 08:07:17 ip-10-1-3-12 ec2-instance-connect[4279]: Querying EC2 Instance Connect keys for matching fingerprint: SHA256:fqWZ+EKpMlR0+IxuVg9/VuE+FWRtGZFB0wQr/lxek
Oct 5 08:07:17 ip-10-1-3-12 sshd[4123]: error: failed to load keys from /opt/aws/lambda/etc/run-authorized-keys: ec2-user SHA256:fqWZ+EKpMlR0+IxuVg9/VuE+FWRtGZFB0wQr/lxek failed, status 255
Oct 5 08:07:17 ip-10-1-3-12 sshd[4123]: Accepted publickey for ec2-user from 3.226.75.73 port 48094 ssh2: RSA SHA256:fqWZ+EKpMlR0+IxuVg9/VuE+FWRtGZFB0wQr/lxek
Oct 5 08:07:17 ip-10-1-3-12 sshd[4123]: Accepted publickey for ec2-user from 3.226.75.73 port 48094 ssh2: RSA SHA256:fqWZ+EKpMlR0+IxuVg9/VuE+FWRtGZFB0wQr/lxek
Oct 5 08:07:17 ip-10-1-3-12 sshd[4123]: pam_unix(sshd:session): session opened for user ec2-user by (uid=0)
Oct 5 08:08:04 ip-10-1-3-12 sshd[4131]: Received disconnect from 3.226.75.73 port 48094:11: disconnected by user
Oct 5 08:08:39 ip-10-1-3-12 sshd[4123]: pam_unix(sshd:session): session closed for user ec2-user
Oct 5 08:08:29 ip-10-1-3-12 sshd[4339]: Invalid user ubuntu from 3.226.75.73 port 52928
Oct 5 08:08:29 ip-10-1-3-12 sshd[4339]: input.userauth.request: invalid user ubuntu [preauth]
Oct 5 08:08:29 ip-10-1-3-12 sshd[4339]: Connection closed by 3.226.75.73 port 52928 [preauth]

```

At the bottom of the terminal window, it says "i-0e825c37662f43673 (EncryptedInstance)". Below that, it shows PublicIPs: 98.82.163.40 and PrivateIPs: 10.1.3.12. The bottom right corner includes links for CloudShell, Feedback, and a copyright notice: © 2024, Amazon Web Services, Inc. or its affiliates.

The screenshot shows the AWS CloudWatch Logs interface. On the left, a sidebar navigation includes CloudWatch, Favorites and recents, Dashboards, Alarms, Logs (Log groups, Log Anomalies, Live Tail, Logs Insights, Contributor Insights), Metrics (All metrics, Explorer, Streams), X-Ray traces, Events (Rules, Event Buses), and CloudShell/Feedback. The main area displays a list of log entries. A specific entry is highlighted:

```

2024-10-05T08:00:33.390Z Oct 5 08:00:26 ip-10-1-3-12 sudo: pam_unix(sudo:session): session closed for user root
2024-10-05T08:00:58.946Z Oct 5 08:00:58 ip-10-1-3-12 sudo: ec2-user : TTY:pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/sbin/service@#0@amazon-cloudwatch-agent@#0@status
2024-10-05T08:00:58.946Z Oct 5 08:00:58 ip-10-1-3-12 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
2024-10-05T08:01:03.163Z Oct 5 08:00:58 ip-10-1-3-12 sudo: pam_unix(sudo:session): session closed for user root
2024-10-05T08:01:32.528Z Oct 5 08:01:32 ip-10-1-3-12 sudo: ec2-user : TTY:pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/cat@#0@opt/aws/amazon-cloudwatch-agent/logs/amazon...
2024-10-05T08:01:32.528Z Oct 5 08:01:32 ip-10-1-3-12 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
2024-10-05T08:01:37.163Z Oct 5 08:01:32 ip-10-1-3-12 sudo: pam_unix(sudo:session): session closed for user root
2024-10-05T08:03:12.555Z Oct 5 08:03:12 ip-10-1-3-12 sudo: ec2-user : TTY:pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/tail@#0@#0@var/log/secure
2024-10-05T08:03:12.555Z Oct 5 08:03:12 ip-10-1-3-12 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
2024-10-05T08:03:17.163Z Oct 5 08:03:17 ip-10-1-3-12 sudo: pam_unix(sudo:session): session closed for user root
2024-10-05T08:07:17.137Z Oct 5 08:07:17 ip-10-1-3-12 ec2-instance-connect[4279]: Querying EC2 Instance Connect keys for matching fingerprints: SHA256:fqwuZEkp1lR0+IxuVg8/Vu+FhRTG...
2024-10-05T08:07:17.137Z Oct 5 08:07:17 ip-10-1-3-12 sshd[4123]: error: AuthorizedKeysCommand /opt/aw...
2024-10-05T08:07:17.137Z Oct 5 08:07:17 ip-10-1-3-12 sshd[4123]: Accepted publickey for ec2-user from 3.226.75.73 port 48094 ssh2: RSA SHA256:fqwuZEkp1lR0+IxuVg8/Vu+FhRTG...
2024-10-05T08:07:21.164Z Oct 5 08:07:17 ip-10-1-3-12 sshd[4123]: pam_unix(sshd:session): session opened for user ec2-user by (uid=0)
2024-10-05T08:08:04.500Z Oct 5 08:07:17 ip-10-1-3-12 sshd[4123]: Accepted publickey for ec2-user from 3.226.75.73 port 48094 ssh2: RSA SHA256:fqwuZEkp1lR0+IxuVg8/Vu+FhRTG...
2024-10-05T08:08:04.500Z Oct 5 08:07:17 ip-10-1-3-12 sshd[4123]: pam_unix(sshd:session): session opened for user ec2-user by (uid=0)
2024-10-05T08:08:04.500Z Oct 5 08:08:04 ip-10-1-3-12 sshd[4313]: Received disconnect from 3.226.75.73 port 48094:11: disconnected by user
2024-10-05T08:08:04.500Z Oct 5 08:08:04 ip-10-1-3-12 sshd[4313]: Disconnected from 3.226.75.73 port 48094
2024-10-05T08:08:09.163Z Oct 5 08:08:04 ip-10-1-3-12 sshd[4123]: pam_unix(sshd:session): session closed for user ec2-user
2024-10-05T08:08:30.056Z Oct 5 08:08:29 ip-10-1-3-12 sshd[4339]: Invalid user ubuntu from 3.226.75.73 port 52928
2024-10-05T08:08:30.056Z Oct 5 08:08:29 ip-10-1-3-12 sshd[4339]: input_userauth_request: invalid user ubuntu [preauth]
2024-10-05T08:08:34.164Z Oct 5 08:08:29 ip-10-1-3-12 sshd[4339]: Connection closed by 3.226.75.73 port 52928 [preauth]

```

No newer events at this moment. Auto retry paused. [Resume](#)

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

The screenshot shows the AWS CloudWatch Metrics Filter interface. On the left, a sidebar navigation includes CloudWatch, Favorites and recents, Dashboards, Alarms, Logs (Log groups, Log Anomalies, Live Tail, Logs Insights, Contributor Insights), Metrics (All metrics, Explorer, Streams), X-Ray traces, Events (Rules, Event Buses), and CloudShell/Feedback. The main area displays a 'Metric filters (1)' section. A single filter is listed:

**Not valid users**

- Filter pattern: "Invalid user"
- Metric: **secure** / **NotValidUsers**
- Metric value: 1
- Default value: 0
- Unit: Count
- Dimensions: -
- Alarms: None.

The screenshot shows the AWS CloudWatch Alarms interface. On the left, there's a navigation sidebar with sections like Favorites and recent, Dashboards, Alarms (with 1 active), All alarms, Billing, Logs, Metrics, X-Ray traces, Events, Rules, and Event Buses. The main area is titled 'Alarms (1)' and lists one alarm: 'Not valid users exceeding limit on EncryptedInstance'. The alarm is in an 'In alarm' state, last updated on 2024-10-05 09:27:44. The condition is 'NotValidUsers >= 5 for 1 datapoints within 1 day'. Actions are enabled.

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

The screenshot shows the AWS S3 Access Control List (ACL) configuration page. The left sidebar includes Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, and Block Public Access settings for this account. Under Storage Lens, there are options for Dashboards, Storage Lens groups, and AWS Organizations settings. A Feature spotlight section is also present. The main content area displays the ACL for the object writer. Two informational messages are shown: 'Public access is blocked because Block Public Access settings are turned on for this bucket' and 'The console displays combined access grants for duplicate grantees'. The grantee table lists the Bucket owner (your AWS account) and other groups like Everyone (public access) and Authenticated users group (anyone with an AWS account).

**AWS Config**

The rule: s3-bucket-logging-enabled has been added to your account.

**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.

Name	Remediation action	Type	Enabled evaluation mode	Detect
s3-bucket-logging-enabled	Not set	AWS managed	DETECTIVE	-

**Documentation** [Partners](#) [FAQs](#) [Pricing](#)

CloudShell Feedback

**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

No archive configurations  
No configurations to display.

Create configuration

**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  
Disabled

**AWS CloudTrail data events (1)** [Info](#)

Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. [Learn more](#)

Name	Access
data-bucket-reads-writes	Read, Write

**Event notifications (0)**

Send a notification when specific events occur in your bucket. [Learn more](#)

Name	Event types	Filters	Destination type	Destination
No event notifications Choose Create event notification to be notified when a specific event occurs.				

CloudShell Feedback

**AWS Config**

**Remediation action**

Remediation action	Description
AWS-ConfigureS3BucketLogging	Enables Logging on S3 Bucket

**Parameters**

Key	Value	Description
AutomationAssumeRole	arn:awsiam::768826479868: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	289a5b4ce8ad6dc19f5e8b028ea9c22ecf46d7f41f590587aeb76191b1d4f0b5	(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-0d8eba3afba87e395	(Required) Specifies the bucket where you want Amazon S3 to store server access logs.
TargetObjectKeyPrefix	-	(Optional) Amazon S3 key format for log objects.

**CloudShell** **Feedback** © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

**AWS Config**

**Resources in scope**

ID	Type	Status	Annotation	Compliance
athena-results-0d8eba3afba87e395	S3 Bucket	-	-	⚠ Noncompliant
aws-athena-query-results-768826479868-us-east-1	S3 Bucket	-	-	⚠ Noncompliant
aws-config-0d8eba3afba87e395	S3 Bucket	-	-	⚠ Noncompliant
cloudtrail-logs-0d8eba3afba87e395	S3 Bucket	-	-	⚠ Noncompliant
s3-inventory-0d8eba3afba87e395	S3 Bucket	-	-	⚠ Noncompliant
s3-objects-access-log-0d8eba3afba87e395	S3 Bucket	-	-	⚠ Noncompliant

**View details** **Remediate** **CloudShell** **Feedback** © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS Amazon S3 console. On the left, there's a navigation sidebar with links like 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, and AWS Marketplace for S3.

The main content area displays monitoring and logging configurations:

- Server access logging:** A configuration panel with "No configurations to display." and a "Create configuration" button. It includes a section for "AWS CloudTrail data events (1)" and "Event notifications (0)".
- AWS CloudTrail data events (1):** Shows one event named "data-bucket-reads-writes" with "Access" set to "Read, Write". A "Configure in CloudTrail" button is available.
- Event notifications (0):** A table with columns for Name, Event types, Filters, Destination type, and Destination. It shows "No event notifications" and a "Create event notification" button.

At the bottom, there are links for CloudShell, Feedback, © 2024, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

## Cost assessment for monitoring and logging

The screenshot shows the AWS Pricing Calculator. At the top, it says "Successfully added Amazon CloudWatch estimate." and has links for Feedback, Language: English, Contact Sales, and Create an AWS Account.

The main area is titled "My Estimate" and shows an "Estimate summary" table:

Upfront cost	Monthly cost	Total 12 months cost
0.00 USD	6.00 USD	<b>72.00 USD</b> Includes upfront cost

To the right, there's a "Getting Started with AWS" section with "Get started for free" and "Contact Sales" buttons.

The "My Estimate" table lists resources:

Service Name	Status	Upfront cost	Monthly cost	Description	Region	Config Summary
AWS CloudTrail	-	0.00 USD	0.00 USD	-	US East (N. Virginia)	Management events units (millions)
Amazon CloudWatch	-	0.00 USD	6.00 USD	-	US East (N. Virginia)	Number of Metrics (includes d...)

At the bottom, there's an "Acknowledgement" note about the estimate being non-binding, and links for Privacy, Site terms, Cookie preferences, and © 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.