

Name:AbdelRahman Moustafa Mohamed Abdallah

Group name: AWS Cloud Specialist (ALX1\_SWD8\_M1e)

Student ID: 1110242719

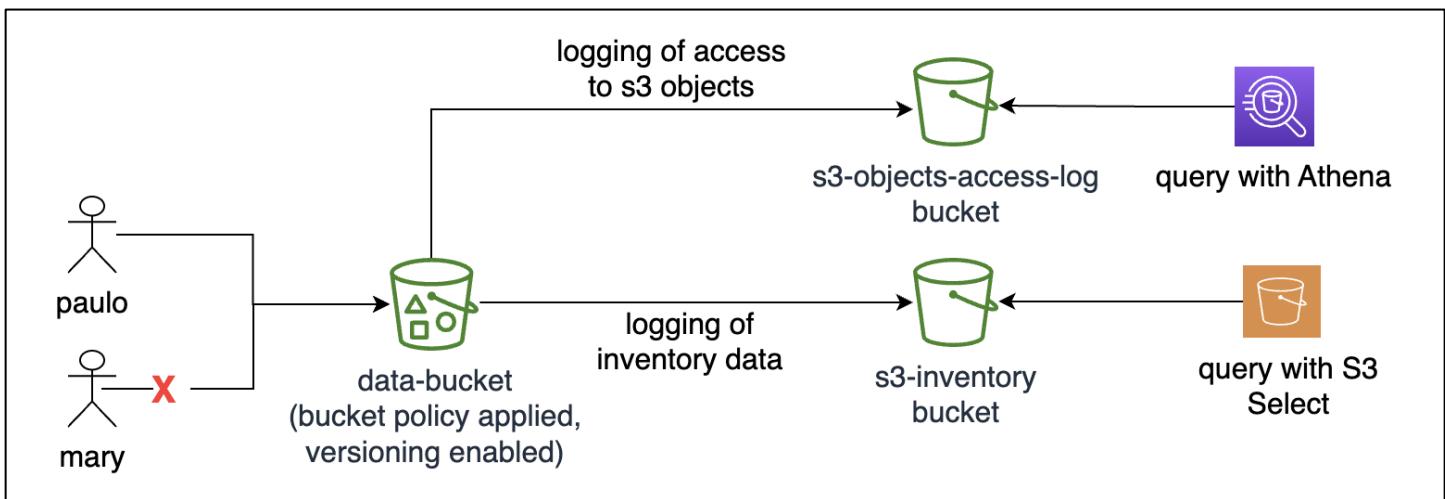
AWS Academy Cloud Security Foundations  
Securing and Monitoring Resources with AWS

Supervise by: Eng. Merhan Adel

## Badge Link



# Phase 1: Securing data in Amazon S3



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

Screenshot of the AWS S3 console showing the contents of the **data-bucket-0153b53120bc83bce**. The bucket contains the following objects:

Name	Type	Last modified	Size	Storage class
aws-academy-graduate-aws-academy-cloud-web-applicat.png	png	September 28, 2024, 14:42:21 (UTC+03:00)	64.8 KB	Standard
customer-data.csv	csv	September 30, 2024, 16:07:04 (UTC+03:00)	346.0 B	Standard
customers.csv	csv	September 27, 2024, 18:11:56 (UTC+03:00)	357.0 B	Standard
loan-data.csv	csv	September 30, 2024, 15:17:06 (UTC+03:00)	184.0 B	Standard
myfile.txt	txt	September 27, 2024, 00:50:05 (UTC+03:00)	11.0 B	Standard

Screenshot of the AWS S3 console showing the **Bucket policy** editor for the **data-bucket-0153b53120bc83bce**.

The policy JSON is as follows:

```
4  {
5   "Effect": "Allow",
6   "Principal": [
7     "AWS": []
8     "arn:aws:iam::654812467323:user/sofia",
9     "arn:aws:iam::654812467323:role/voclabs",
10    "arn:aws:iam::654812467323:user/paulo"
11  ],
12 },
13 "Action": "s3:*",
14 "Resource": [
15   "arn:aws:s3:::data-bucket-0153b53120bc83bce",
16   "arn:aws:s3:::data-bucket-0153b53120bc83bce/*"
17 ],
18 },
19 {
20   "Effect": "Deny",
21   "Principal": "*",
22   "Action": "s3:*",
23   "Resource": [
24     "arn:aws:s3:::data-bucket-0153b53120bc83bce",
25     "arn:aws:s3:::data-bucket-0153b53120bc83bce/*"
26   ],
27   "Condition": {
28     "StringNotEquals": {
29       "aws:PrincipalArn": [
30         "arn:aws:iam::654812467323:role/voclabs",
31         "arn:aws:iam::654812467323:user/paulo",
32       ]
33     }
34   }
35 }
```

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

The screenshot shows the 'Edit Bucket Versioning' page for an S3 bucket named 'data-bucket-0153b53120bc83bce'. The 'Bucket Versioning' section is open, showing two options: 'Suspend' (unchecked) and 'Enable' (checked). A note below explains that enabling versioning preserves existing objects and allows recovery from failures. Another note about Multi-factor authentication (MFA) delete is present. The 'Save changes' button is highlighted in orange at the bottom right.

The screenshot shows the 'Edit server access logging' page for the same S3 bucket. The 'Server access logging' section is open, with 'Enable' selected. A yellow warning box states that enabling server access logging will update the bucket policy to include access to the S3 log delivery group. Below this, the 'Destination' section is filled with the path 's3://s3-objects-access-log-0153b53120bc83bce/data-bucket/'. Other fields like 'Destination Region' (US East (N. Virginia) us-east-1), 'Destination bucket name' (s3-objects-access-log-0153b53120bc83bce), and 'Destination prefix' (data-bucket/) are also visible. The 'Log object key format' section contains two radio button options, with the first one selected. The 'Log object key example' field shows the path 'data-bucket/2024-07-01-10-12-56-[UniqueString]'. The 'Save changes' button is located at the bottom right.

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

The screenshot shows the AWS S3 console with the path: Amazon S3 > Buckets > data-bucket-0153b53120bc83bce > Management > Inventory configurations > Inventory.

**Inventory report source:**

- Filter: Entire bucket
- Object versions: All versions

**Inventory configuration details:**

Destination: <a href="#">s3://s3-inventory-0153b53120bc83bce</a>	Format: Apache Parquet
Destination account ID: 654812467323	Last export: 2024-09-30
Status: Enabled	Frequency: Daily

**Inventory report encryption:** Server-side encryption protects data at rest. No encryption key specified. The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.

**Additional metadata fields:** Fields for bucket name, key name, version id, isLatest, and delete marker are automatically included in your report. [Learn more](#)

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

The screenshot shows the AWS S3 console with the path: Amazon S3 > Buckets > data-bucket-0153b53120bc83bce > Management > Inventory configurations > Inventory.

**Inventory configuration details:**

Destination: <a href="#">s3://s3-inventory-0153b53120bc83bce</a>	Format: Apache Parquet
Destination account ID: 654812467323	Last export: 2024-09-30
Status: Enabled	Frequency: Daily

**Inventory report encryption:** Server-side encryption protects data at rest. No encryption key specified. The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.

**Additional metadata fields:** Fields for bucket name, key name, version id, isLatest, and delete marker are automatically included in your report. [Learn more](#)

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

## Task 1.4: Confirm that versioning works as intended

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with links like 'Console Home', 'Billing and Cost Management', 'EC2', 'S3', 'Elastic Beanstalk', and 'VPC'. Below the navigation bar, the path 'Amazon S3 > Buckets > data-bucket-0153b53120bc83bce' is displayed. The main area is titled 'data-bucket-0153b53120bc83bce Info'. Under the 'Objects' tab, there are six items listed:

Name	Type	Version ID	Last modified	Size	Storage class
aws-academy-graduate-aws-academy-cloud-web-applicat.png	png	tyHaka_CV_t2EejLz1o4gwi fa.zj4VZw	September 28, 2024, 14:42:21 (UTC+03:00)	64.8 KB	Standard
customer-data.csv	csv	wT3oMC17i3.LifdDfTYkng KoUJ_IhbXd	September 30, 2024, 16:07:04 (UTC+03:00)	346.0 B	Standard
customers.csv	csv	IHEBsmzbN3Sin4JY8LAAH78GTGWCKCyp	September 27, 2024, 18:11:56 (UTC+03:00)	357.0 B	Standard
customers.csv	csv	GNdMlnwtJL23V6fTYGkd vj85BduRipA	September 27, 2024, 17:56:47 (UTC+03:00)	215.0 B	Standard
loan-data.csv	csv	gNAGVZdOYz5psxoBihen k3IKp566ABW	September 30, 2024, 15:17:06 (UTC+03:00)	184.0 B	Standard
myfile.txt	txt	null	September 27, 2024, 00:50:05 (UTC+03:00)	11.0 B	Standard

A red box highlights the second and third 'customers.csv' entries, which are versions of the same file. The 'Actions' dropdown menu at the top right includes options like 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'.

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

The screenshot shows the Amazon Athena Query Editor interface. In the top navigation bar, the user is in the 'N. Virginia' region and has a workgroup named 'project'. The main area displays three queries:

- Query 1:** A failed query with the error message: "Error: [AmazonAthena] Error: Failed to execute statement: com.amazonaws.services.athena.AthenaException: The provided AWS IAM ARN is not valid." It includes the SQL command: `SELECT requester, operation, key, httpstatus FROM "default"."bucket_logs" WHERE requester LIKE 'arn:aws:iam%';`
- Query 2:** A failed query with the error message: "Error: [AmazonAthena] Error: Failed to execute statement: com.amazonaws.services.athena.AthenaException: The provided AWS IAM ARN is not valid." It includes the SQL command: `SELECT requester, operation, key, httpstatus FROM "default"."bucket_logs" WHERE requester LIKE 'arn:aws:iam%';`
- Query 3:** A completed query with the status 'Completed' and 17 results. The results table has columns: #, requester, operation, key, and httpstatus. One visible row is: # 1, requester: arn:aws:iam::654812467323:user/paulo, operation: REST.PUT.OBJECT, key: aws-academy-graduate-aws-academy-cloud-web-applicat.png, httpstatus: 200.

The sidebar on the left shows the data source is 'AwsDataCatalog' and the database is 'default'. Under 'Tables and views', there are two tables: 'bucket\_logs' and 'cloudtrail\_logs\_cloudtrail\_logs\_0153b53'. The 'Views' section is empty.

This screenshot shows the same Amazon Athena Query Editor interface, but the completed query now has 17 results. The results table is identical to the one in the previous screenshot, listing 17 rows of access log data. The columns are: #, requester, operation, key, and httpstatus. The last few rows show operations like REST.GET.BUCKET, REST.GET.VERSIONING, and REST.GET.OWNERSHIP\_CONTROLS.

**Cost assessment to secure Amazon S3**

## Estimate Cost CSV File

# Phase 2: Securing VPCs

## Task 2.1: Review LabVPC and its associated resources

Screenshot of the AWS VPC Dashboard showing the details and resource map for the LabVPC.

**VPC Details:**

- VPC ID: `vpc-0a4453958694c371e`
- State: Available
- Tenancy: Default
- Default VPC: No
- IPv4 CIDR: `10.1.0.0/16`
- Network Address Usage metrics: Disabled
- DNS hostnames: Enabled
- Main route table: `rtb-0c4e75cbdecf2a213`
- IPv6 pool: -
- Route 53 Resolver DNS Firewall rule groups: -
- Owner ID: `654812467323`
- DNS resolution: Enabled
- Main network ACL: `acl-0e13ed77a8f356f50`
- IPv6 CIDR (Network border group): -

**Resource Map:**

- VPC: `LabVPC`
- Subnets (1): `us-east-1a` (WebServerSubnet)
- Route tables (1): `rtb-0c4e75cbdecf2a213`
- Network connections (1): `LabVPCIG`

Screenshot of the AWS EC2 Instances page showing the details for the WebServer instance.

**Instance Summary:**

- Instance ID: `i-0ef8a3f1b94afdf49` (WebServer)
- Public IPv4 address: `34.231.120.100` [open address]
- Private IP4 address: `10.1.3.4`
- IPv6 address: -
- Instance state: Running
- Public IPv4 DNS: `ec2-34-231-120-100.compute-1.amazonaws.com` [open address]
- Hostname type: IP name: `ip-10-1-3-4.ec2.internal`
- Private IP DNS name (IPv4 only): `ip-10-1-3-4.ec2.internal`
- Instance type: `t2.micro`
- Elastic IP addresses: `34.231.120.100 (WebServerEIP) [Public IP]`
- IP name: `ip-10-1-3-4.ec2.internal`
- VPC ID: `vpc-0a4453958694c371e (LabVPC)`
- AWS Compute Optimizer finding: `Opt-in to AWS Compute Optimizer for recommendations. | Learn more`
- Subnet ID: `subnet-0ce346cf0a9d8366f (WebServerSubnet)`
- Auto Scaling Group name: -
- Answer private resource DNS name: -
- Auto-assigned IP address: -
- IAM Role: `WebServerRole`
- IMDSv2 Required
- Instance ARN: `arn:aws:ec2:us-east-1:654812467323:instance/i-0ef8a3f1b94afdf49`

**Details Tab:**

- Platform: Amazon Linux (Inferred)
- Platform details: Linux/UNIX
- Stop protection: Disabled
- AMI ID: `ami-0ebfd941bbafe70c6`
- AMI name: `al2023-ami-2023.5.20240916.0-kernel-6.1-x86_64`
- Launch time: Tue Oct 01 2024 18:14:23 GMT+0300 (Eastern European Summer Time) (about 1 hour)
- Monitoring: disabled
- Termination protection: Disabled
- AMI location: `amazon/al2023-ami-2023.5.20240916.0-kernel-6.1-x86_64`

## Task 2.2: Create a VPC flow log

The screenshot shows the AWS VPC dashboard for a VPC named 'vpc-0a4453958694c371e / LabVPC'. In the 'Flow logs' tab, a single flow log named 'LabVPCFlowLogs' is listed. It has a flow log ID of 'fl-02fad3364047022c1' and is associated with the destination type 'cloud-watch-logs' and destination name 'LabVPCFlowLogs'. The IAM role ARN is 'arn:aws:iam::654812467323:role/'. Other tabs like 'Resource map', 'CIDRs', and 'Tags' are also visible.

The screenshot shows the AWS CloudWatch Log Groups interface for the 'LabVPCFlowLogs' group. Under the 'Log streams' tab, there is one entry: 'eni-0d048c3a09c3b731e-all'. The details page for this stream shows it was created 3 days ago and has a retention period of 'Never expire'. Metrics and subscription filters are listed as well.

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

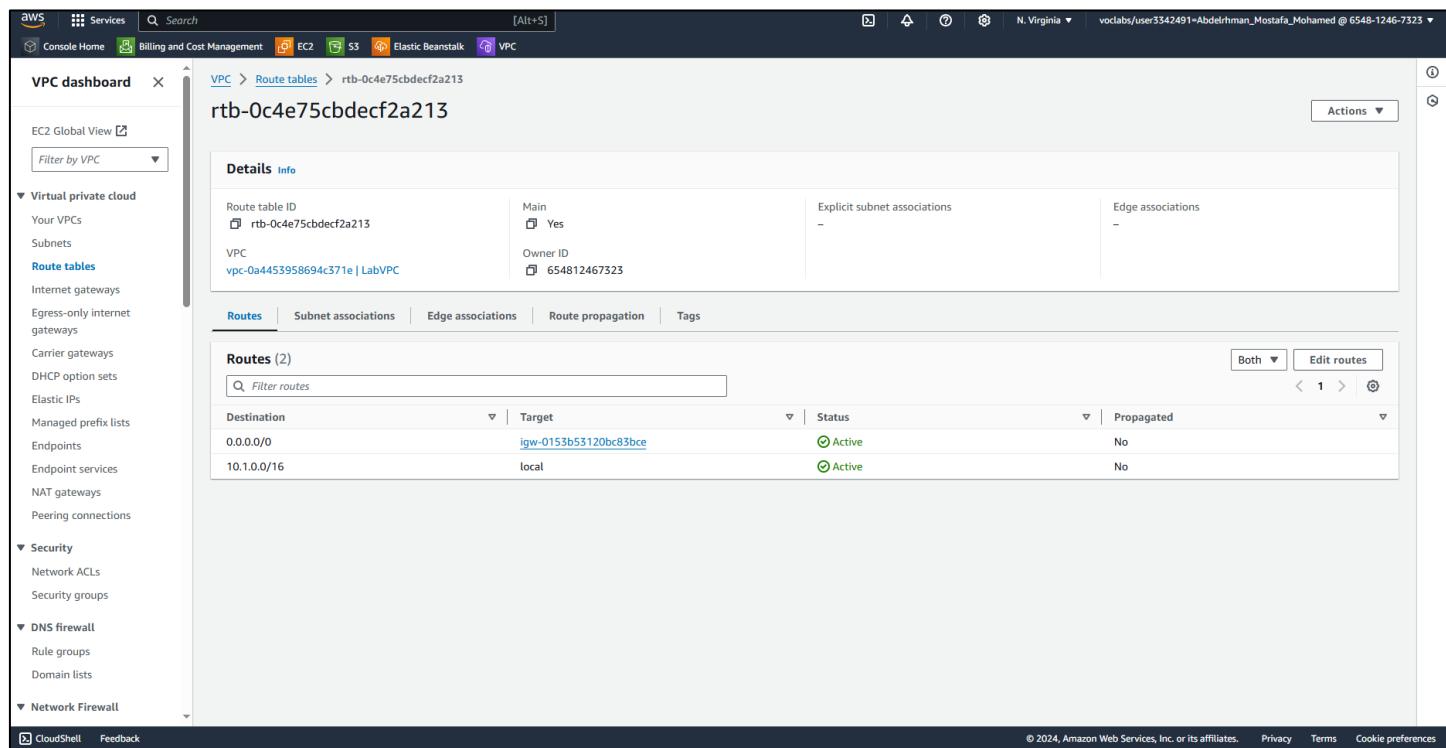
The screenshot shows the AWS CloudWatch Log Groups interface. The left sidebar navigation includes: Services, CloudWatch (selected), Billing and Cost Management, EC2, S3, Elastic Beanstalk, VPC, CloudWatch (selected), Favorites and recent, Dashboards, Alarms, Logs (selected), Log groups (selected), Log Anomalies, Live Tail, Logs Insights, Contributor Insights, Metrics, All metrics, Explorer, Streams, X-Ray traces, Events, Application Signals, Network monitoring, Insights, Settings, Getting Started, CloudShell, and Feedback.

The main content area displays the "LabVPCFlowLogs" log group details. Key information shown includes:

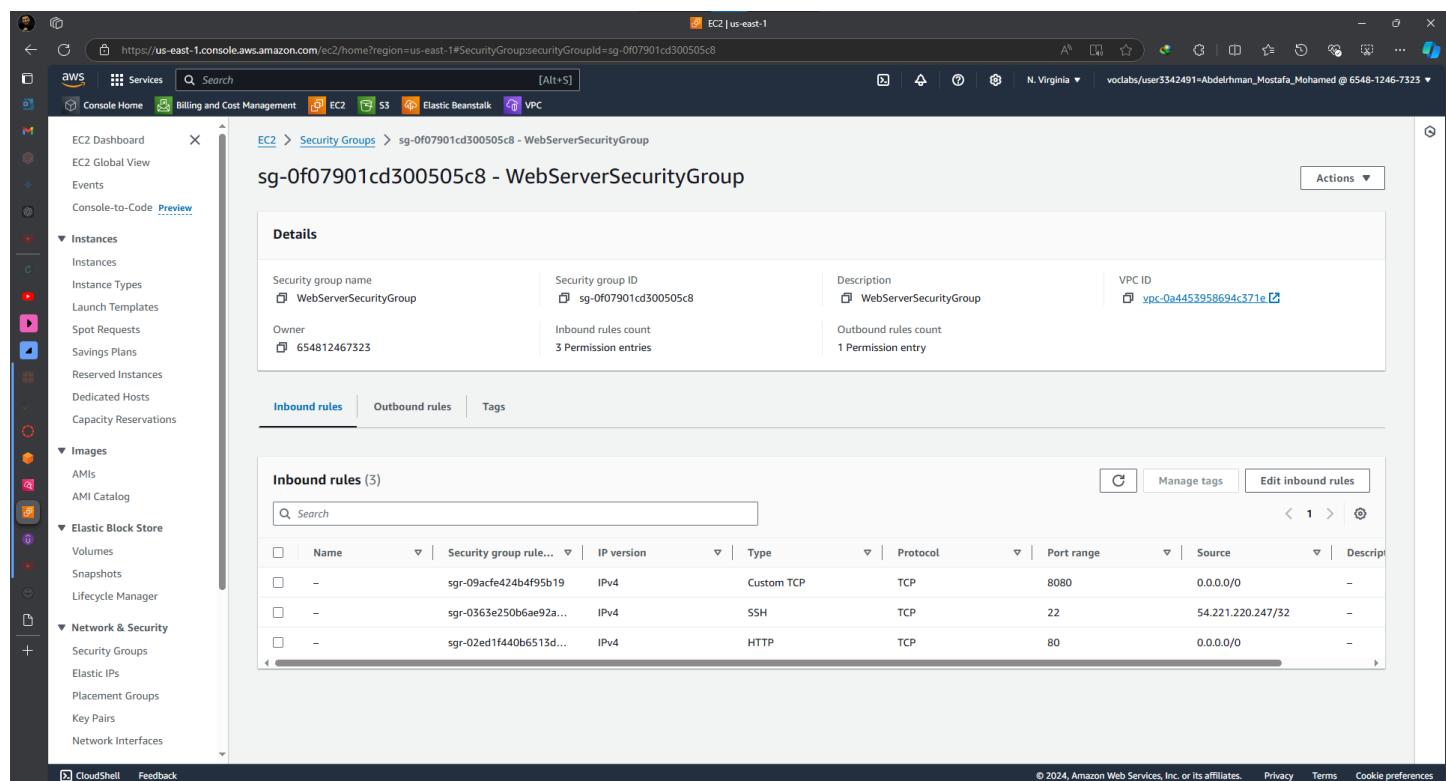
- Log class: Standard
- ARN: arn:aws:logs:us-east-1:654812467323:log-group:LabVPCFlowLogs:\*
- Creation time: 3 days ago
- Retention: Never expire
- Stored bytes: 138.07 KB
- Metric filters: 0
- Subscription filters: 0
- Contributor Insights rules: -
- KMS key ID: -
- Anomaly detection: Configure
- Data protection: -
- Sensitive data count: -

Below the details, the "Log streams" tab is selected, showing one log stream named "eni-0d048c3a09c3b731e-all". The stream's last event time is listed as 2024-10-01 18:50:47 (UTC+03:00). Other tabs include Tags, Anomaly detection, Metric filters, Subscription filters, Contributor Insights, and Data protection.

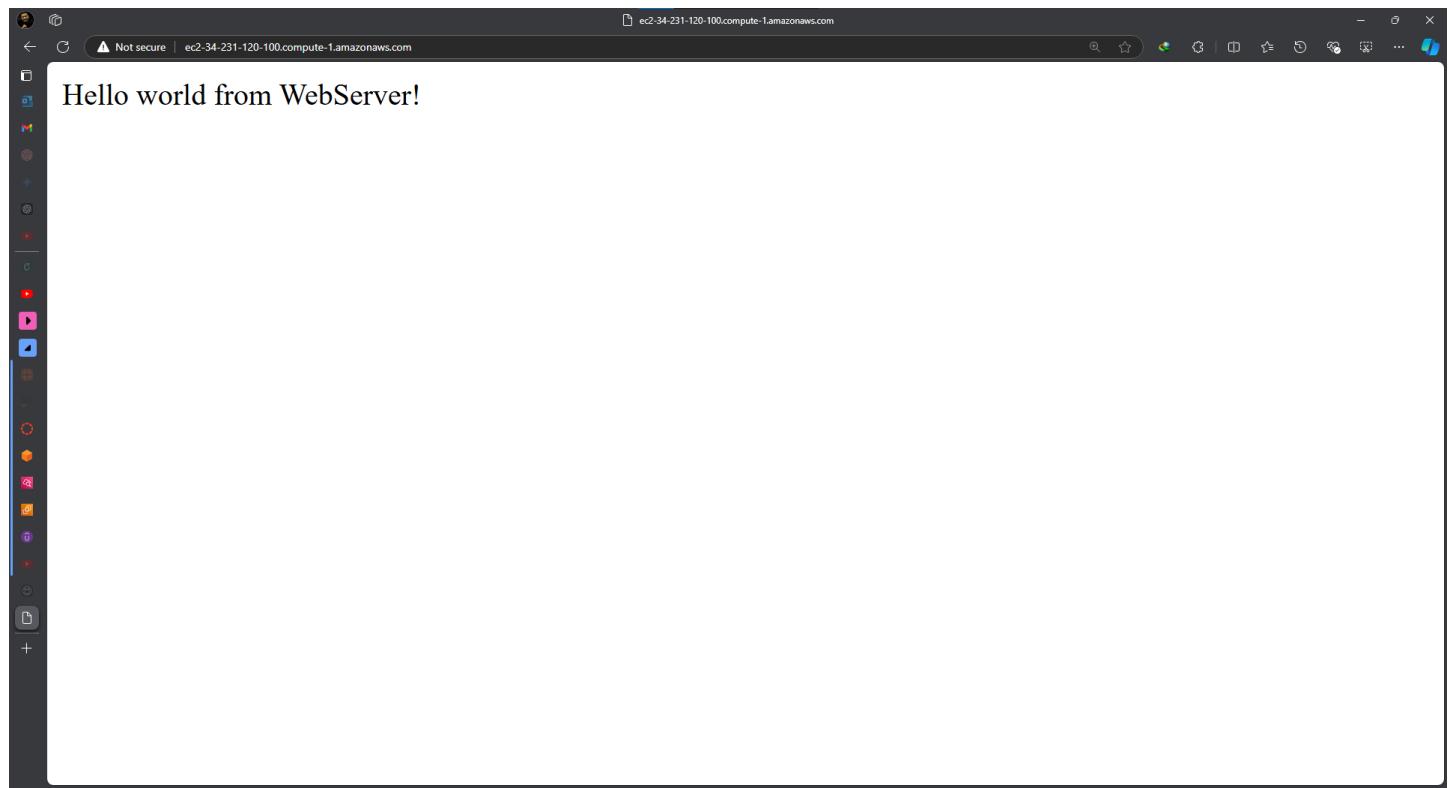
## Task 2.4: Configure route table and security group settings



The screenshot shows the AWS VPC dashboard with the route table configuration for 'rtb-0c4e75cbdecf2a213'. The 'Details' tab is selected, showing the route table ID, VPC, and owner information. The 'Routes' tab displays two routes: one to the internet gateway (igw-0153b53120bc83bce) and one to the local subnet (10.1.0.0/16). The 'Subnet associations' tab indicates that the main subnet is associated.



The screenshot shows the AWS EC2 Dashboard with the security group configuration for 'sg-0f07901cd300505c8 - WebServerSecurityGroup'. The 'Details' tab is selected, showing the security group name, owner, and VPC information. The 'Inbound rules' tab displays three rules: one for port 8080 (Custom TCP), one for port 22 (TCP), and one for port 80 (TCP).



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

The screenshot shows the AWS VPC Network ACL Details page. The Network ACL ID is acl-0e13ed77a8f356f50. It is associated with subnet-Oce346cf0a9d8366f / WebServerSubnet, owned by user 654812467323, and is the Default Yes. The VPC ID is vpc-0a4453958694c371e / LabVPC. The Inbound rules section lists three rules:

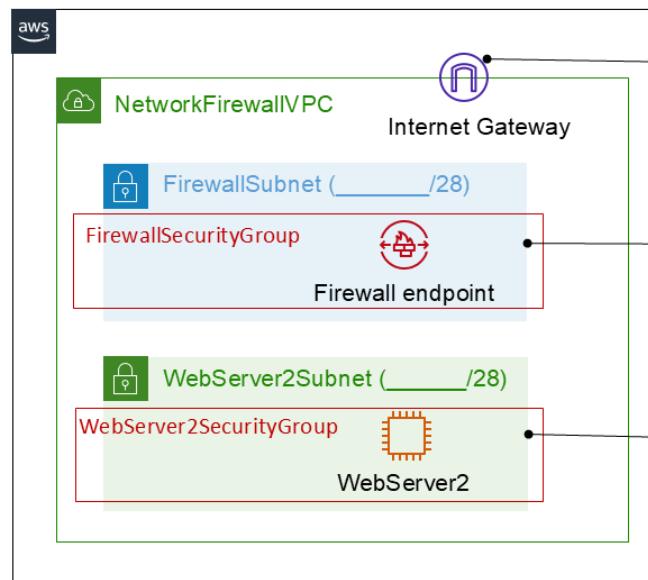
Rule number	Type	Protocol	Port range	Source	Allow/Deny
90	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
100	SSH (22)	TCP (6)	22	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

The screenshot shows a web browser window with the URL ec2-34-231-120-100.compute-1.amazonaws.com. The page content is "Hello world from WebServer!".

## Task 2.6: Review NetworkFirewallVPC and its associated resources

The screenshot shows the AWS VPC Console interface. On the left, there's a sidebar with various navigation options under 'Virtual private cloud' and 'Network Firewall'. The main area displays the 'Details' tab for a VPC with ID `vpc-07a19f79164561498`, which is named 'NetworkFirewallVPC'. The 'Details' table includes information like State (Available), DHCP option set (dopt-023796eaa12deae9e), and Route tables (rtb-0fb874aed0360a49a). Below the table, the 'Resource map' tab is selected, showing a diagram of the VPC architecture. The diagram includes nodes for 'VPC' (with 'Show details' and 'NetworkFirewallVPC' sub-options), 'Subnets (2)' (listing 'us-east-1a' and 'FirewallSubnet', 'WebServer2Subnet'), 'Route tables (4)' (listing 'rtb-0fb874aed0360a49a', 'WebServer2-Route-Table', 'IGW-Ingress-Route-Table', and 'Firewall-Route-Table'), and 'Network connections (1)' (listing 'NetworkFirewallIG').

The screenshot shows a web browser window with the URL `44.208.224.35`. The page content is 'Hello world from WebServer2!'. This indicates that traffic is successfully reaching the second web server within the VPC.



IGW-Ingress-Route-Table	
Destination	Target
10.1.0.0/16	local
10.1.3.0/28	<a href="#">vpce-0ee5aaaf4208bc1d15</a>
Firewall-Route-Table	
Destination	Target
0.0.0.0/0	<a href="#">igw-05afa5bee40c5a0cb</a>
10.1.0.0/16	local
WebServer2-Route-Table	
Destination	Target
0.0.0.0/0	<a href="#">vpce-0ee5aaaf4208bc1d15</a>
10.1.0.0/16	local

Network Firewall Rules		
Protocol	Port	Action
TCP	80	Pass
TCP	22	Pass
TCP	443	Pass
ICMP	ANY	Pass

aws

## Task 2.7: Create a network firewall

The screenshot shows the AWS VPC Management Console with the URL [https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#NetworkFirewallDetails;arn=arn:aws:network-firewall:us-east-1:654812467323\\_firewall-NetworkFirewall](https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#NetworkFirewallDetails;arn=arn:aws:network-firewall:us-east-1:654812467323_firewall-NetworkFirewall). The left sidebar is expanded to show the 'Network Firewall' section under 'Firewalls'. The main content area displays the 'NetworkFirewall' details for a firewall named 'NetworkFirewall'. The 'Overview' tab is selected, showing the firewall status as 'Ready', associated with a 'FirewallPolicy' and a specific VPC ('vpc-07a19f79164561498'). The 'Firewall details' tab shows the VPC association ('Associated VPC: vpc-07a19f79164561498') and its subnets ('subnet-03a6ae5e7bf67bec (IPv4)'). The 'Firewall endpoints' tab lists one endpoint in the 'us-east-1a' availability zone, which is also marked as 'Ready'.

Availability Zone	Firewall subnet	Endpoint ID	Firewall endpoint status
us-east-1a	subnet-03a6ae5e7bf67bec	vpc-07a19f79164561498-0005a44209b1d1f	Ready

## Task 2.8: Create route tables

The screenshot shows the AWS VPC Route Tables page. On the left, a sidebar lists various VPC-related services. The main content area displays the details for a route table named "rtb-05f531bec6b95b37c". The "Details" tab is selected, showing the route table ID, VPC, and subnet associations. The "Routes" tab is also selected, displaying two routes:

Destination	Target	Status	Propagated
0.0.0.0/0	igw-05afa5bee40c5a0cb	Active	No
10.1.0.0/16	local	Active	No

The screenshot shows the AWS VPC Route Tables page. The sidebar and route table details are identical to the previous screenshot, but the route table ID is now "rtb-03ef495c1873848db". The "Routes" tab is selected, displaying two routes:

Destination	Target	Status	Propagated
0.0.0.0/0	vpce-0ee5aaaf4208bc1d15	Active	No
10.1.0.0/16	local	Active	No

AWS Services Network Firewall Rules N. Virginia vodabs/user3342491=Abdelrhman\_Mostafa @ 6548-1246-7323

Console Home Billing and Cost Management EC2 S3 Elastic Beanstalk VPC

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 Rule groups Domain lists Network Firewall Firewalls Firewall policies Network Firewall rule groups CloudShell Feedback

VPC > Route tables > rtb-0bb7a79d391215da9 / IGW-Ingress-Route-Table Actions

Details Info

Route table ID rtb-0bb7a79d391215da9	Main No	Explicit subnet associations -	Edge associations igw-05afa5bee40c5a0cb / NetworkFirewallIG
VPC vpc-07a19f79164561498   NetworkFirewallVPC	Owner ID 654812467323		

Routes Subnet associations Edge associations Route propagation Tags

Routes (2) Both Edit routes < 1 >

Destination	Target	Status	Propagated
10.1.0.0/16	local	Active	No
10.1.3.0/28	vpc-e0ee5aaaf4208bc1d15	Active	No

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

## Task 2.9: Configure logging for the network firewall

The screenshot shows the AWS CloudWatch Log Groups interface. The left sidebar navigation includes: Services, CloudWatch (selected), Favorites and recent, Dashboards, Alarms (0), Logs (selected), Log groups (selected), Log Anomalies, Live Tail, Logs Insights, Contributor Insights, Metrics, All metrics, Explorer, Streams, X-Ray traces, Events, Application Signals, Network monitoring, Insights, Settings, and Getting Started.

The main content area displays the "NetworkFirewallVPCLogs" log group details. The ARN is arn:aws:logs:us-east-1:654812467323:log-group:NetworkFirewallVPCLogs:. The log group has 372.62 KB stored bytes, 0 metric filters, 0 subscription filters, and 0 contributor insights rules. It was created 3 days ago and has a retention of 6 months. There is no KMS key ID, anomaly detection, data protection, or sensitive data count.

The "Log streams" tab is selected, showing 21 log streams. The streams listed are:

Log stream	Last event time
/aws/network-firewall/flow/NetworkFirewall_2024-10-01-16	2024-10-01 19:40:01 (UTC+03:00)
/aws/network-firewall/alert/NetworkFirewall_2024-10-01-16	2024-10-01 19:20:14 (UTC+03:00)
/aws/network-firewall/flow/NetworkFirewall_2024-10-01-15	2024-10-01 18:59:51 (UTC+03:00)

Actions, View in Logs Insights, Start tailing, and Search log group buttons are available at the top right of the log group details section.

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

The screenshot shows the AWS Network Firewall Rule Group configuration page. The left sidebar navigation includes: 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 (Rule groups, Domain lists), Network Firewall (Firewalls, Firewall policies, Network Firewall rule groups, TLS inspection configurations, Network Firewall resource groups). The main content area displays the 'NetworkFirewallVPCRuleGroup' rule group details, showing it is Stateful with a capacity of 100 and is Active. It also shows sections for Rule variables (empty) and IP set references (empty).

The screenshot shows the AWS Network Firewall Rules configuration page. The left sidebar navigation includes: 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 (Rule groups, Domain lists), Network Firewall (Firewalls, Firewall policies, Network Firewall rule groups, TLS inspection configurations, Network Firewall resource groups). The main content area displays the 'Rules (5)' section, which lists five rules with descriptions like 'sid:1' through 'sid:5'. It also shows a 'Customer managed key' section with an AWS owned key.

Cost estimate to secure a VPC with a network firewall : [CSV File](#)

# 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 interface. A key named "MyKMSKey" has been created with the following details:

- General configuration:**
  - Alias: MyKMSKey
  - Status: Enabled
  - ARN: arn:aws:kms:us-east-1:654812467323:key/99b4b0f1-f94f-49dc-b51b-5ccf5e0c8d1e
  - Description: -
  - Creation date: Sep 30, 2024 15:06 GMT+3
  - Regionality: Single Region
- Key policy:** This tab is selected, showing the current key administrators.
- Cryptographic configuration:** Shows the key rotation settings.
- Tags:** No tags are present.
- Key rotation:** No rotation has been configured yet.
- Aliases:** No aliases are present.

The "Key policy" section lists three IAM users or roles as key administrators:

Name	Path	Type
voclabs	/	Role
sofia	/	User

The screenshot shows the AWS KMS console interface with the "Key rotation" tab selected for the "MyKMSKey" key.

**Automatic key rotation:** Status is Enabled, with a rotation period of 365 days. The next rotation date is set for Sep 30, 2025.

**On-demand key rotation:** A "Rotate Now" button is available to immediately initiate key material rotation.

**Key rotation history:** No history is present.

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

**Key policy**

[Edit](#) [Switch to default view](#)

```
{  
    "Sid": "Allow access for Key Administrators",  
    "Effect": "Allow",  
    "Principal": {  
        "AWS": [  
            "arn:aws:iam::654812467323:role/voclabs",  
            "arn:aws:iam::654812467323:user/sofia"  
        ]  
    },  
    "Action": [  
        "kms>Create*",  
        "kms:Describe*",  
        "kms:Enable*"  
    ]  
}
```

The screenshot shows the AWS Amazon S3 console. The left sidebar is titled 'Amazon S3' and includes sections for 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. It also features a 'Storage Lens' section with sub-options like Dashboards, Storage Lens groups, and AWS Organizations settings. A 'Feature spotlight' section is present with 7 items. At the bottom, there's a link to the AWS Marketplace for S3.

The main content area shows the 'Edit default encryption' page for a bucket named 'data-bucket-0153b53120bc83bce'. The top navigation bar includes 'Search [Alt+S]', a refresh icon, a question mark icon, a gear icon, 'N. Virginia', and a user ID 'vodlabs/user3342491=Abdelrhman\_Mostafa @ 6548-1246-7323'.

The 'Default encryption' section is active, showing that server-side encryption is automatically applied to new objects stored in the bucket. It provides three options:

- 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](#).

The 'AWS KMS key' section is also visible, with the 'Enter AWS KMS key ARN' option selected. A search bar contains the ARN 'arn:aws:kms:us-east-1:654812467323:key/99b4bf0f1-f94f-49dc-b51' and a 'Create a KMS key' button.

The 'Bucket Key' section notes that using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. It states that S3 Bucket Keys aren't supported for DSSE-KMS. A 'Learn more' link is provided.

The 'Encryption type' section has a note: "Changing the default encryption settings might cause in-progress replication and Batch Replication jobs to fail. These jobs might fail because of missing AWS KMS permissions on the IAM role that's specified in the replication configuration. If you change the default encryption settings, make sure that this IAM role has the necessary AWS KMS permissions." A 'Learn more' link is included.

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

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

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>XB57ZZEYHPI6R20</RequestId>
<HostId>CkC689W#01ukrc4qgB#dyIwFmVonM4C/cKIsLy8aynhlarNzp9qb4KywA5664yPc6YvEcE</HostId>
</Error>
```

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

The screenshot shows the AWS EC2 Instance Details page for an instance named i-0db95d8d3db212bb5. The Storage tab is selected. In the Block Devices table, the first row (Volume ID: vol-003b38467e29680d4, Device name: /dev/xvda) has its 'Encrypted' column highlighted with a red box. The 'Encrypted' value is Yes, and the 'KMS key ID' is 99b4b0f1-f94f-49dc-b51b-5ccf5e0c8d1e.

Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID	Delete on term
vol-003b38467e29680d4	/dev/xvda	8	Attached	2024/09/30 15:29 GMT+3	Yes	99b4b0f1-f94f-49dc-b51b-5ccf5e0c8d1e	Yes

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

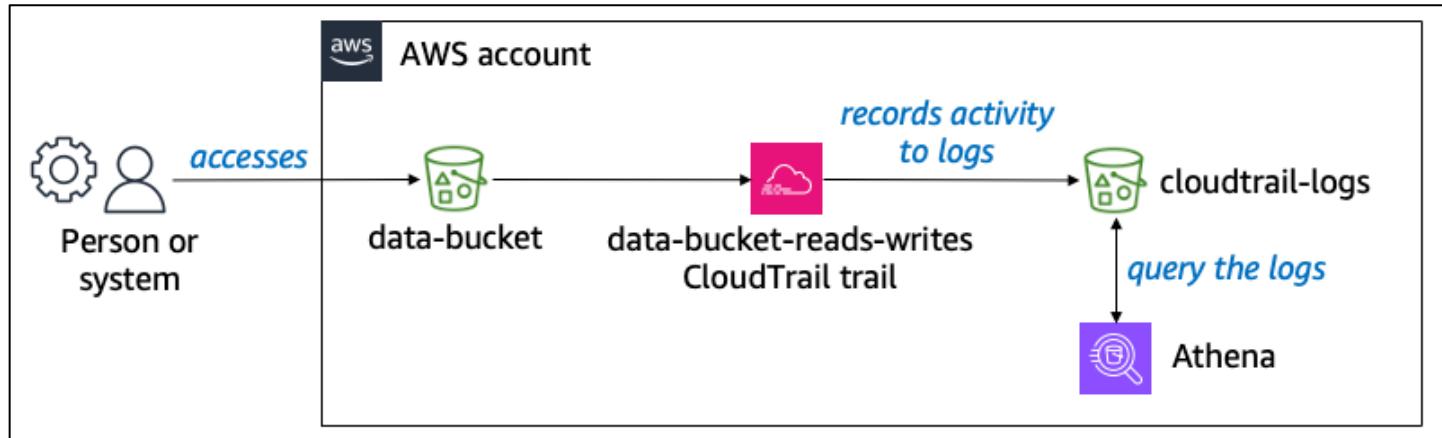
Task 3.6: Use AWS KMS to encrypt a Secrets Manager secret

```
[ec2-user@webserver2 ~]$ aws secretsmanager list-secrets
{
    "SecretList": [
        {
            "ARN": "arn:aws:secretsmanager:us-east-1:654812467323:secret:mysecret-ggTta2",
            "Name": "mysecret",
            "KmsKeyId": "arn:aws:kms:us-east-1:654812467323:key/99b4b0f1-f94f-49dc-b51b-5ccf5e0c8d1e",
            "LastChangedDate": "2024-09-30T12:48:58.748000+00:00",
            "Tags": [],
            "SecretVersionsToStages": [
                "fc53aa82-bd3d-4c17-a4f3-41f31bfd37ac": [
                    "AWS CURRENT"
                ]
            ],
            "CreatedDate": "2024-09-30T12:48:58.674000+00:00"
        }
    ]
}
[ec2-user@webserver2 ~]$
```

## Cost assessment for using AWS KMS [CSV file](#)

## Phase 4: Monitoring and logging

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

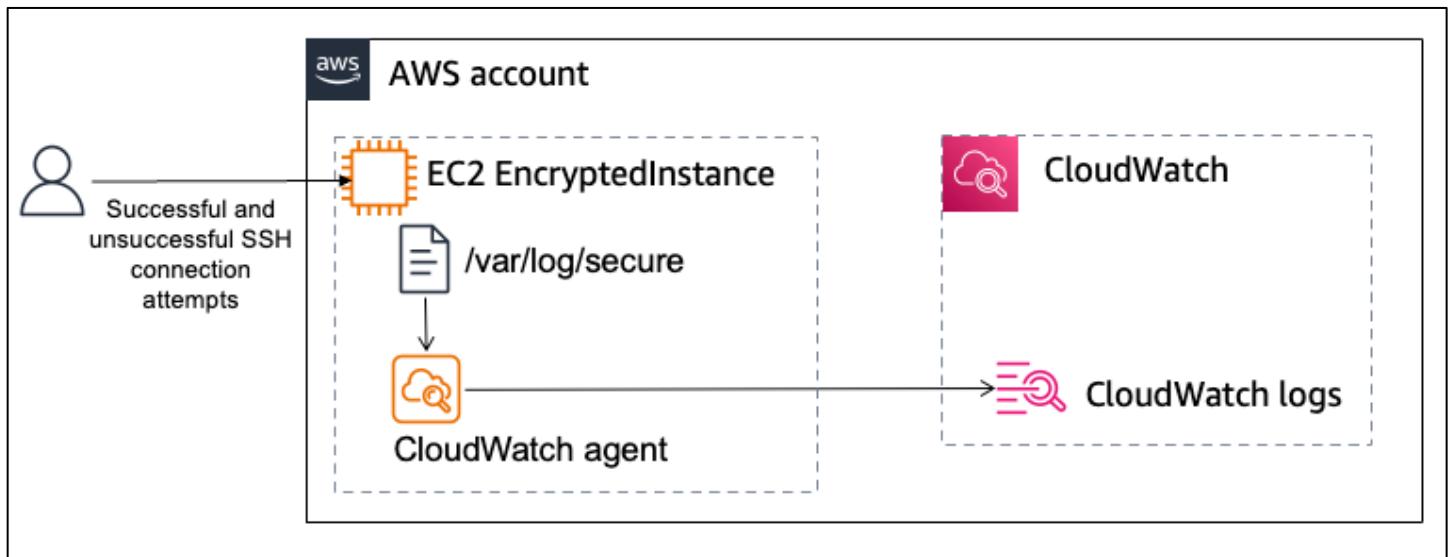


This screenshot shows the AWS CloudTrail console for a specific trail named "data-bucket-reads-writes". The "General details" section displays information such as trail logging status, log location, and validation settings. The "CloudWatch Logs" section indicates no log groups are configured. The "Tags" section shows no tags associated with the trail.

This screenshot shows the AWS Athena console with a query running in the "Editor" tab. The query retrieves event data from the CloudTrail logs bucket. The "Query results" tab displays the results of the query, showing a single row of data.

#	eventtime	principalid	requestparameters
1	2024-09-30T13:07:03Z	AROAQ505KB5Q2WY455T:user3342491=Abdelrhman_Mostafa_Mohamed	{"X-Amz-Date":"20240930T130702Z","bucketName":"data-bucket-0153b53120bc83bce"}

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



This screenshot shows the AWS CloudWatch Log Groups interface. The left sidebar includes sections for Alarms, Logs (with Log groups selected), Metrics, X-Ray traces, Events, Application Signals, Network monitoring, and Insights. The main area displays the "EncryptedInstanceSecureLogs" log group details, including its ARN, creation time (20 hours ago), and retention period (6 months). It also lists stored bytes, metric filters (1), subscription filters (0), and contributor insights rules. Below this, the "Log streams" tab is selected, showing one stream named "EncryptedInstanceSecureLogs-i-0db95d8d3db212bb5" with a last event time of 2024-10-01 22:46:05 UTC+03:00. A search bar and various filter options are visible at the bottom of the log stream list.

This screenshot shows an EC2 terminal session with the command "sudo service amazon-cloudwatch-agent status" run. The output indicates the service is active and running. The terminal then shows a large block of log entries from the CloudWatch Agent. These logs detail the configuration and startup process of the agent, including reading json config files and attempting to detect the region from ec2. Some lines were ellipsized, as indicated by the "Hint: Some lines were ellipsized, use -l to show in full." message at the bottom.

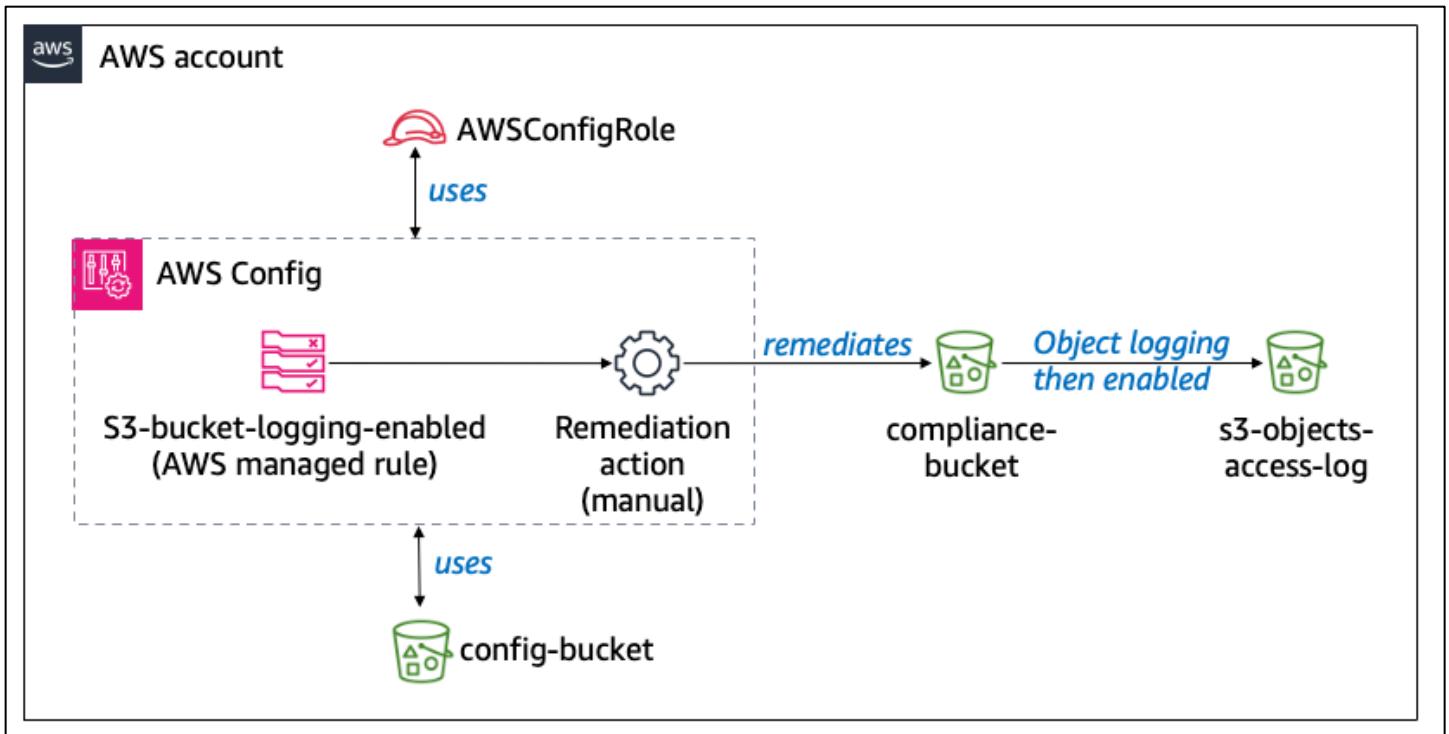
```
aws Services Search [Alt+S]
Console Home Billing and Cost Management EC2 S3 Elastic Beanstalk VPC
[ec2-user@ip-10-1-3-14 ~]$ sudo service amazon-cloudwatch-agent status
Redirecting to /bin/systemctl status amazon-cloudwatch-agent.service
● amazon-cloudwatch-agent.service - Amazon CloudWatch Agent
  Loaded: loaded (/etc/systemd/system/amazon-cloudwatch-agent.service; enabled; vendor preset: disabled)
  Active: active (running) since Tue 2024-10-01 19:45:56 UTC; 1h 45min ago
    Main PID: 2966 (amazon-cloudwat)
   CGroup: /system.slice/amazon-cloudwatch-agent.service
           └─2966 /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml -envconfig /opt/aws/amazon-cloudwatch-agent/e...
Oct 01 19:45:58 ip-10-1-3-14.ec2.internal start-amazon-cloudwatch-agent[2966]: 2024/10/01 19:45:58 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json ...
Oct 01 19:45:58 ip-10-1-3-14.ec2.internal start-amazon-cloudwatch-agent[2966]: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json does not exist or cannot read. Skipping it.
Oct 01 19:45:58 ip-10-1-3-14.ec2.internal start-amazon-cloudwatch-agent[2966]: 2024/10/01 19:45:58 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent/g.json ...
Oct 01 19:45:58 ip-10-1-3-14.ec2.internal start-amazon-cloudwatch-agent[2966]: 2024/10/01 19:45:58 I! Valid Json input schema.
Oct 01 19:45:58 ip-10-1-3-14.ec2.internal start-amazon-cloudwatch-agent[2966]: I! Detecting run_as_user...
Oct 01 19:45:58 ip-10-1-3-14.ec2.internal start-amazon-cloudwatch-agent[2966]: I! Trying to detect region from ec2
Oct 01 19:45:58 ip-10-1-3-14.ec2.internal start-amazon-cloudwatch-agent[2966]: 2024/10/01 19:45:58 D! ec2tagger processor required because append_dimensions is set
Oct 01 19:45:58 ip-10-1-3-14.ec2.internal start-amazon-cloudwatch-agent[2966]: 2024/10/01 19:45:58 Configuration validation first phase succeeded
Oct 01 19:45:58 ip-10-1-3-14.ec2.internal start-amazon-cloudwatch-agent[2966]: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json does not exist or cannot read. Skipping it.
Oct 01 19:45:58 ip-10-1-3-14.ec2.internal start-amazon-cloudwatch-agent[2966]: I! Detecting run_as_user...
Hint: Some lines were ellipsized, use -l to show in full.
[ec2-user@ip-10-1-3-14 ~]$
```

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

The screenshot shows the AWS CloudWatch Log Groups interface. On the left sidebar, under the 'Logs' section, 'Log groups' is selected. In the main content area, the 'EncryptedInstanceSecureLogs' log group is displayed. The 'Log group details' section shows the ARN (arn:aws:logs:us-east-1:654812467323:log-group:EncryptedInstanceSecureLogs:\*) and other metrics like stored bytes, metric filters, and subscription filters. Below this, the 'Log streams' section shows one stream named 'EncryptedInstanceSecureLogs-1-Odb95d8d3db212bb5' with its last event time at 2024-10-01 22:46:05 (UTC+03:00).

The screenshot shows the AWS CloudWatch Alarms interface. Under the 'Alarms' section in the sidebar, 'All alarms' is selected. In the main content area, the 'Not valid users exceeding limit on EncryptedInstance' alarm is displayed. The alarm configuration shows a metric named 'NotValidUsers' with a threshold of 5. The chart shows the count of 'NotValidUsers' over time, starting from 9/25 and ending at 10/02. The status of the alarm is 'OK'. The 'Actions' tab is selected, showing a single notification action: 'When in alarm, send message to topic "Not\_valid\_users\_exceeding\_limit"'.

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



Screenshot of the AWS S3 console showing the details of the **compliance-bucket-0153b53120bc83bce**.

**Buckets:**

- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

**Storage Lens:**

- Dashboards
- Storage Lens groups
- AWS Organizations settings

**Objects (0) Info:**

No objects

You don't have any objects in this bucket.

**Actions:**

- C
- Copy S3 URI
- Copy URL
- Download
- Open
- Delete
- Actions
- Create folder
- Upload

**Filter:** Find objects by prefix

**Columns:** Name, Type, Last modified, Size, Storage class

AWS Services Search [Alt+S]

Console Home Billing and Cost Management EC2 S3 Elastic Beanstalk VPC N. Virginia vocabs/user3342491-Abdelrhman\_Mostafa\_Mohamed @ 6548-1246-7323

### 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 7
- AWS Marketplace for S3

### Edit Object Ownership Info

#### Object Ownership

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.

**ACLs disabled (recommended)**  
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

**ACLs enabled**  
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

**⚠ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.**

**⚠ Enabling ACLs turns off the bucket owner enforced setting for Object Ownership**  
Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.  
 I acknowledge that ACLs will be restored.

**Bucket owner preferred**  
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

**Object writer**  
The object writer remains the object owner.

**ⓘ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)**

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

AWS Services Search [Alt+S]

Console Home Billing and Cost Management EC2 S3 Elastic Beanstalk VPC N. Virginia vocabs/user3342491-Abdelrhman\_Mostafa\_Mohamed @ 6548-1246-7323

### AWS Config

- Dashboard
- Conformance packs
- Rules**
- Resources
- Aggregators**
  - Compliance Dashboard
  - Conformance packs
  - Rules
  - Inventory Dashboard
  - Resources
  - Authorizations
- Advanced queries [Preview](#)
- Settings
- What's new
- Documentation
- Partners
- FAQs
- Pricing

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	bd88d1e494c26f67962fd0ecd7f63194b58faa8f91929325a5fdd0b4379dd1e	(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-0153b53120bc83bce	(Required) Specifies the bucket where you want Amazon S3 to store server access logs. You can ha
TargetObjectKeyPrefix	-	(Optional) Amazon S3 key format for log objects.

#### Resources in scope

ID	Type	Status	Annotation	Compliance
compliance-bucket-0153b53120bc83bce	S3 Bucket	Action executed successfully	-	Compliant
athena-results-25321	S3 Bucket	Action executed successfully	-	Noncompliant
aws-athena-query-results-654812467323-us-east-1	S3 Bucket	-	-	Noncompliant
aws-config-0153b53120bc83bce	S3 Bucket	-	-	Noncompliant
cloudtrail-logs-0153b53120bc83bce	S3 Bucket	-	-	Noncompliant
s3-inventory-0153b53120bc83bce	S3 Bucket	-	-	Noncompliant
s3-objects-access-log-0153b53120bc83bce	S3 Bucket	-	-	Noncompliant

View details Remediate [Edit](#)

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

Cost assessment for monitoring and logging : [CSV File](#)

# Badge Link

