

Name:AbdelRahman Moustafa Mohamed Abdallah

Group name: AWS Cloud Specialist (ALX1_SWD8_M1e)

Student ID: 1110242719

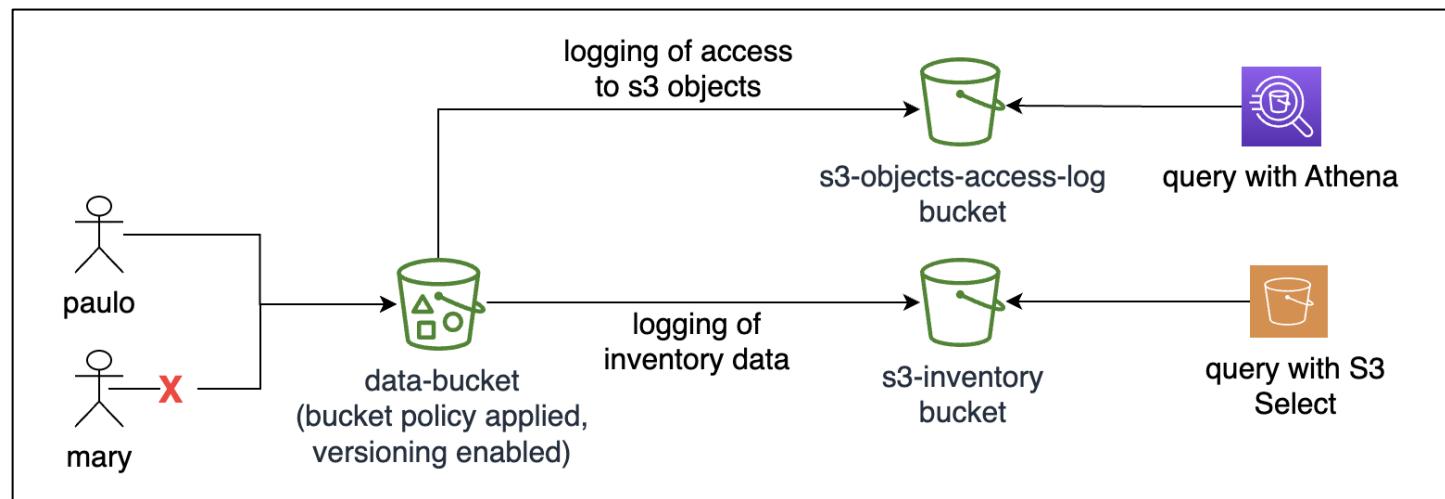
AWS Academy Cloud Security Foundations
Securing and Monitoring Resources with AWS

Supervised 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

The screenshot shows the AWS S3 console with the following details:

- Buckets:** The user is in the 'Buckets' section, viewing the details for the bucket **data-bucket-0153b53120bc83bce**.
- Objects:** The bucket contains 5 objects:
 - aws-academy-graduate-aws-academy-cloud-web-applicat.png**: Type png, Last modified September 28, 2024, 14:42:21 (UTC+03:00), Size 64.8 KB, Storage class Standard.
 - customer-data.csv**: Type csv, Last modified September 30, 2024, 16:07:04 (UTC+03:00), Size 346.0 B, Storage class Standard.
 - customers.csv**: Type csv, Last modified September 27, 2024, 18:11:56 (UTC+03:00), Size 357.0 B, Storage class Standard.
 - loan-data.csv**: Type csv, Last modified September 30, 2024, 15:17:06 (UTC+03:00), Size 184.0 B, Storage class Standard.
 - myfile.txt**: Type txt, Last modified September 27, 2024, 00:50:05 (UTC+03:00), Size 11.0 B, Storage class Standard.
- Actions:** Buttons for Copy S3 URI, Copy URL, Download, Open, Delete, Actions, Create folder, and Upload.

The screenshot shows the AWS S3 Bucket Policy configuration page for the bucket **data-bucket-0153b53120bc83bce**.

Bucket ARN: `arn:aws:s3:::data-bucket-0153b53120bc83bce`

Policy:

```
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     "Action": "s3:*",
13     "Resource": [
14         "arn:aws:s3:::data-bucket-0153b53120bc83bce",
15         "arn:aws:s3:::data-bucket-0153b53120bc83bce/*"
16     ]
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 }
```

Policy examples: [Policy examples](#)

Policy generator: [Policy generator](#)

Right-hand sidebar:

- Edit statement** and **Remove** buttons.
- Add actions** button.
- Choose a service** dropdown with **Filter services** input field.
- Included** section: **S3**.
- Available** section: **AMP**, **API Gateway**, **API Gateway V2**, **ASC**, **Access Analyzer**, **Account**.
- Add a resource** button.

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 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: s3://s3-inventory-0153b53120bc83bce	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: s3://s3-inventory-0153b53120bc83bce	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 rows, which represent two different versions of the 'customers.csv' file. The first row is the original file, while the second and third rows show its subsequent versions.

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 completed query with the following SQL:

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

- Query 2:** A completed query with the following SQL:

```
1 SELECT * FROM "default"."cloudtrail_logs_0153b53"
2 WHERE S3ObjectKey = '120bc83bce';
```

- Query 3:** The currently selected query, which is still running.

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_0153b53'. The 'Views' section is empty. The bottom of the screen shows the results of the completed queries, including a table with columns: #, requester, operation, key, and httpstatus. The results show 17 rows of log entries.

This screenshot shows the results of the completed query from the previous interface. The results are displayed in a table format:

#	requester	operation	key	httpstatus
1	arn:aws:iam::654812467323:user/paulo	REST.PUT.OBJECT	aws-academy-graduate-aws-academy-cloud-web-applicat.png	200
2	arn:aws:iam::654812467323:user/mary	REST.GET.BUCKET	-	403
3	arn:aws:iam::654812467323:user/mary	REST.GET.VERSIONING	-	403
4	arn:aws:iam::654812467323:user/mary	REST.GET.BUCKET	-	403
5	arn:aws:iam::654812467323:user/paulo	REST.GET.BUCKET	-	200
6	arn:aws:iam::654812467323:user/mary	REST.GET.BUCKET	-	403
7	arn:aws:iam::654812467323:user/paulo	REST.HEAD.BUCKET	-	200
8	arn:aws:iam::654812467323:user/mary	REST.GET.BUCKET	-	403
9	arn:aws:iam::654812467323:user/paulo	REST.GET.VERSIONING	-	200
10	arn:aws:iam::654812467323:user/paulo	REST.GET.OWNERSHIP_CONTROLS	-	200
11	arn:aws:iam::654812467323:user/paulo	REST.GET.VERSIONING	-	200
12	arn:aws:iam::654812467323:user/mary	REST.GET.OWNERSHIP_CONTROLS	-	403
13	arn:aws:iam::654812467323:user/paulo	REST.GET.ENCRYPTION	-	200
14	arn:aws:iam::654812467323:user/paulo	REST.GET.OBJECT_LOCK_CONFIGURATION	-	404
15	arn:aws:iam::654812467323:user/paulo	REST.GET.OWNERSHIP_CONTROLS	-	200
16	arn:aws:iam::654812467323:user/mary	REST.HEAD.BUCKET	-	403

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 addresses: `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`
- Elastic IP addresses: `34.231.120.100 (WebServerEIP) [Public IP]`
- Answer private resource DNS name: -
- Instance type: `t2.micro`
- AWS Compute Optimizer finding: `Opt-in to AWS Compute Optimizer for recommendations.` [Learn more]
- Auto-assigned IP address: -
- VPC ID: `vpc-0a4453958694c371e (LabVPC)`
- Subnet ID: `subnet-0ce346cf0a9d8366f (WebServerSubnet)`
- Auto Scaling Group name: -
- 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 Logs console for a log group named 'LabVPCFlowLogs'. Under the 'Log streams' tab, there is one log stream named 'eni-0d048c3a09c3b731e-all'. The log stream was created 3 days ago and has a size of 138.07 KB. The log group details show it is a 'Standard' log group with an ARN of 'arn:aws:logs:us-east-1:654812467323:log-group:LabVPCFlowLogs:*'. The log group has no metric filters, subscription filters, or contributor insights rules.

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

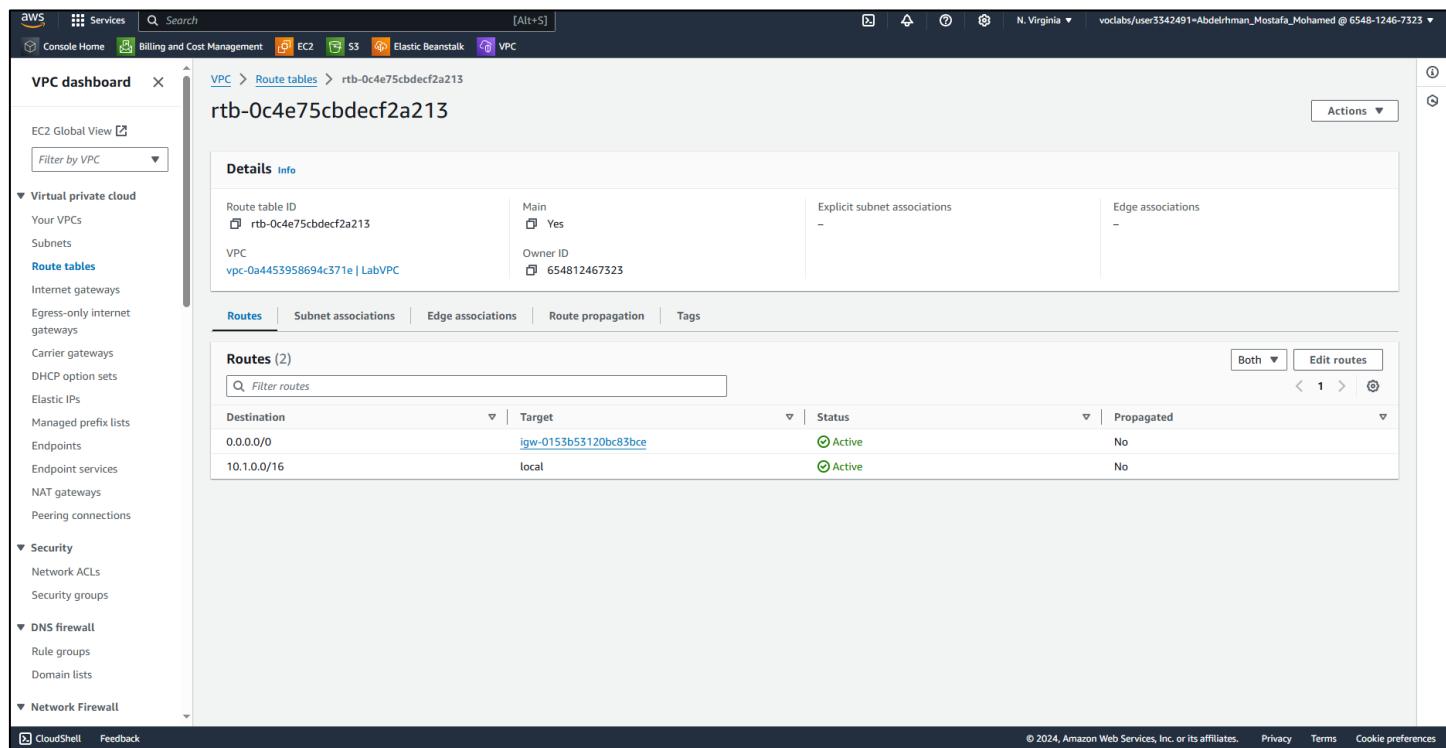
The screenshot shows the AWS CloudWatch Log Groups interface. The left sidebar navigation includes: Services, CloudWatch (selected), Billing and Cost Management, EC2, S3, Elastic Beanstalk, VPC, CloudWatch (selected), Favorites and recent, Dashboards, Alarms, Logs (selected), Log groups (selected), Log 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: -

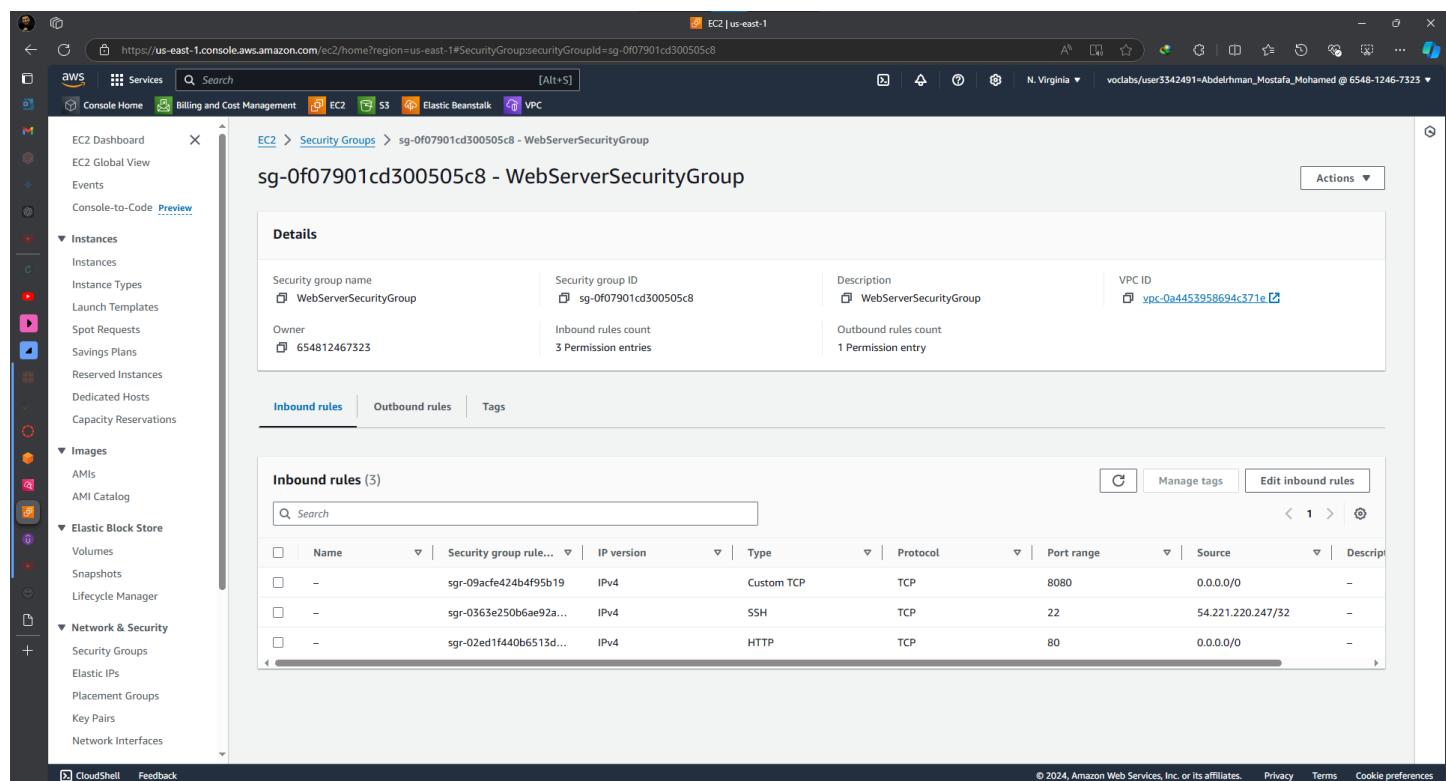
Below the details, the "Log streams" tab is selected, showing one log stream named "eni-0d048c3a09c3b731e-all". The stream's last event time is listed as 2024-10-01 18:50:47 (UTC+03:00). Other tabs include Tags, Anomaly detection, Metric filters, Subscription filters, Contributor Insights, and Data protection.

Task 2.4: Configure route table and security group settings



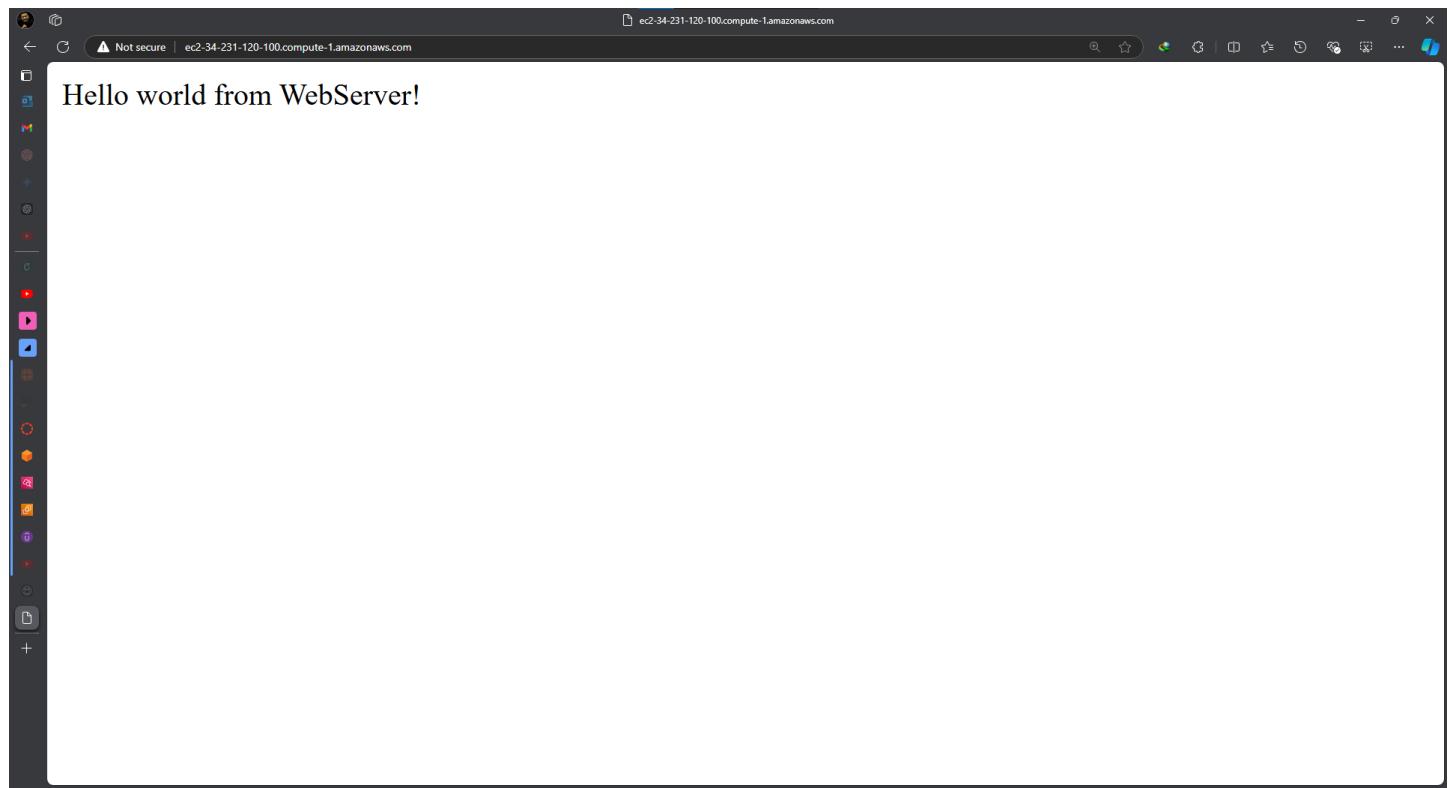
The screenshot shows the AWS VPC dashboard with the route table configuration for 'rtb-0c4e75cbdecf2a213'. The 'Details' tab is selected, showing the route table ID, VPC, and owner information. The 'Routes' tab displays two routes: one to the internet gateway (igw-0153b53120bc83bce) and one to the local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

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0153b53120bc83bce	Active	No
10.1.0.0/16	local	Active	No



The screenshot shows the EC2 Security Groups 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 allowing traffic from specific IP ranges on ports 8080, 22, and 80.

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sgr-09acf424b4f95b19	IPv4	Custom TCP	TCP	8080	0.0.0.0/0	-
-	sgr-0563e250b6ae92a...	IPv4	SSH	TCP	22	54.221.220.247/32	-
-	sgr-02ed1f440b6513d...	IPv4	HTTP	TCP	80	0.0.0.0/0	-



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, associated with subnet-0ce346cf0a9d8366f / WebServerSubnet. The Default setting is Yes, and the VPC ID is vpc-0a4453958694c371e / LabVPC. The Inbound rules section displays three rules:

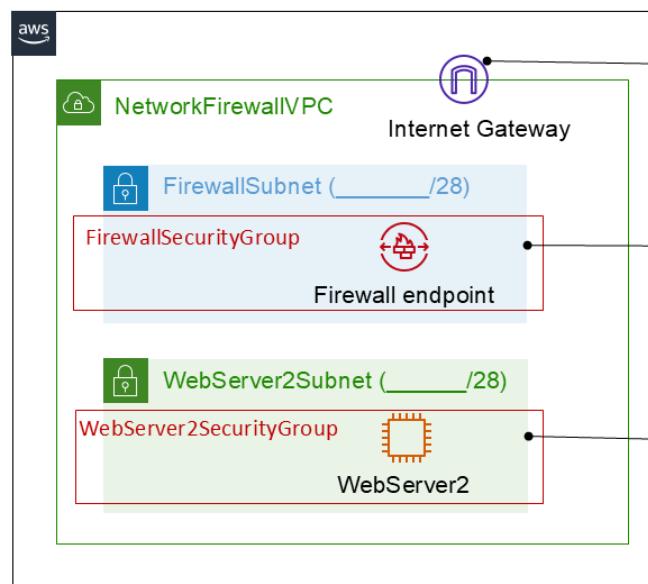
Rule number	Type	Protocol	Port range	Source	Allow/Deny
90	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
100	SSH (22)	TCP (6)	22	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

The screenshot shows a web browser window displaying the content "Hello world from WebServer!". The URL is ec2-34-231-120-100.compute-1.amazonaws.com. The browser status bar indicates "Not secure".

Task 2.6: Review NetworkFirewallVPC and its associated resources

The screenshot shows the AWS VPC Console interface. On the left, there's a navigation sidebar with various VPC-related options like EC2 Global View, Subnets, Route tables, Internet gateways, Carrier gateways, DHCP option sets, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, Peering connections, Security (Network ACLs, Security groups), DNS firewall, Rule groups, Domain lists, and Network Firewall. The main content area is titled "vpc-07a19f79164561498 / NetworkFirewallVPC". It has two tabs: "Details" and "Info". Under "Details", there are sections for VPC ID (vpc-07a19f79164561498), State (Available), DHCP option set (dopt-023796eaa12deae9e), Default VPC (No), Network Address Usage metrics (Disabled), DNS hostnames (Enabled), Main route table (rtb-0fb874aed0360a49a), IPv6 pool (-), Route 53 Resolver DNS Firewall rule groups (-), DNS resolution (Enabled), Main network ACL (acl-07360c4f7d60a4d42), and IPv6 CIDR (Network border group) (-). Below the "Details" tab are tabs for "Resource map", "CIDRs", "Flow logs", "Tags", and "Integrations". The "Resource map" tab is selected, displaying a diagram with four components: "VPC Show details" (Your AWS virtual network, NetworkFirewallVPC), "Subnets (2)" (us-east-1a: FirewallSubnet, WebServer2Subnet), "Route tables (4)" (rtb-0fb874aed0360a49a, WebServer2-Route-Table, IGW-Ingress-Route-Table, Firewall-Route-Table), and "Network connections (1)" (NetworkFirewallIG). At the bottom right of the main window, there are links for "CloudShell", "Feedback", and copyright information: "© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

The screenshot shows a web browser window with the URL "44.208.224.35". The page content is "Hello world from WebServer2!". The browser interface includes a back button, forward button, search bar, and other standard browser controls.



IGW-Ingress-Route-Table	
Destination	Target
10.1.0.0/16	local
10.1.3.0/28	vpce-0ee5aaaf4208bc1d15
Firewall-Route-Table	
Destination	Target
0.0.0.0/0	igw-05afa5bee40c5a0cb
10.1.0.0/16	local
WebServer2-Route-Table	
Destination	Target
0.0.0.0/0	vpce-0ee5aaaf4208bc1d15
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. The left sidebar is expanded to show the Network Firewall section under Security. 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 policy named "FirewallPolicy", and is associated with the VPC "vpc-07a19f79164561498". The "Firewall details" tab is active, showing the VPC association with "vpc-07a19f79164561498" and its subnet "subnet-03a6ae5e7fbfb67bec (IPv4)". The "Firewall endpoints" tab shows one endpoint in the "us-east-1a" availability zone, associated with the same subnet and status as the main firewall.

Availability Zone	Firewall subnet	Endpoint ID	Firewall endpoint status
us-east-1a	subnet-03a6ae5e7fbfb67bec	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 area displays a route table named "rtb-05f531bec6b95b37c / Firewall-Route-Table". The "Details" tab is selected, showing the route table ID, VPC, and subnet associations. The "Routes" tab is active, showing 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 structure are identical to the previous screenshot, but the route table ID is now "rtb-03ef495c1873848db / WebServer2-Route-Table". The "Routes" tab is active, showing 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)

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

Both Edit routes < 1 >

© 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' details. It shows the rule group is Stateful, has a capacity of 100, and is active. There are no rule variables or IP set references defined. The rules section shows five entries:

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

The screenshot shows the AWS Network Firewall Rule Group configuration page for a standard stateful rule group. The left sidebar navigation is identical to the previous screenshot. The main content area displays the 'Stateful standard rule group details'. It shows the rule group is Stateful, has a capacity of 100, and is active. There are no rule variables or IP set references defined. The rules section shows five entries:

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

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. On the left, there's a navigation sidebar with options like 'Customer managed keys' and 'Custom key stores'. The main area displays a 'General configuration' card for a key with ID 99b4b0f1-f94f-49dc-b51b-5ccf5e0c8d1e. The key has an alias 'MyKMSKey', is in an 'Enabled' status, and was created on Sep 30, 2024. It's associated with a single region. Below this, there are tabs for 'Key policy', 'Cryptographic configuration', 'Tags', 'Key rotation', and 'Aliases'. The 'Key policy' tab is selected. Under 'Key policy', there's a section for 'Key administrators' which lists three IAM users: 'voclabs', 'sofia', and 'voclabs'. A 'Switch to policy view' button is also present. At the bottom, there are buttons for 'Add' and 'Remove'.

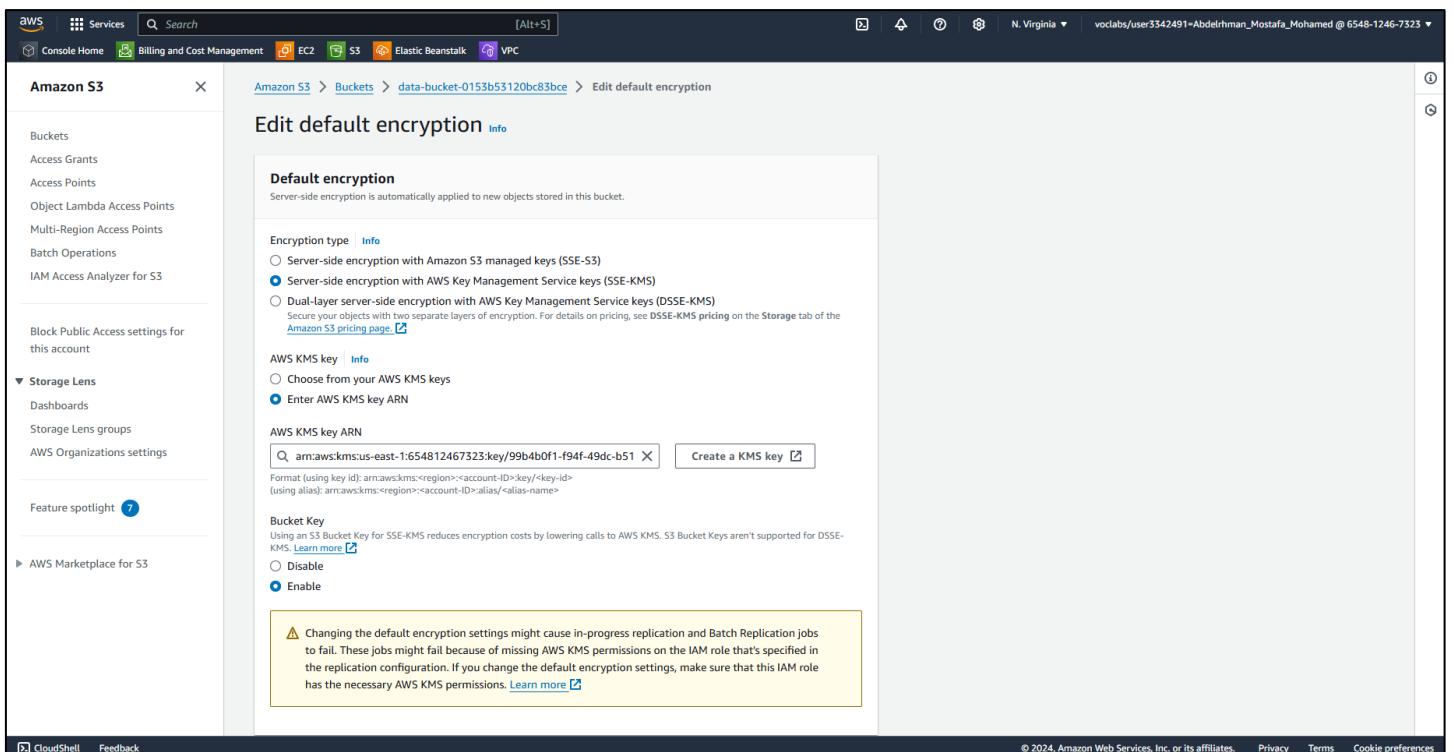
This screenshot shows the same AWS KMS interface, but the 'Key rotation' tab is now selected. The 'Automatic key rotation' section is visible, showing that rotation is enabled with a period of 365 days. The 'On-demand key rotation' section indicates 10 rotations available. A 'Rotate Now' button is present. The 'Key rotation history' section shows 0 entries. The overall layout is identical to the first screenshot, with the 'Key rotation' tab highlighted.

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

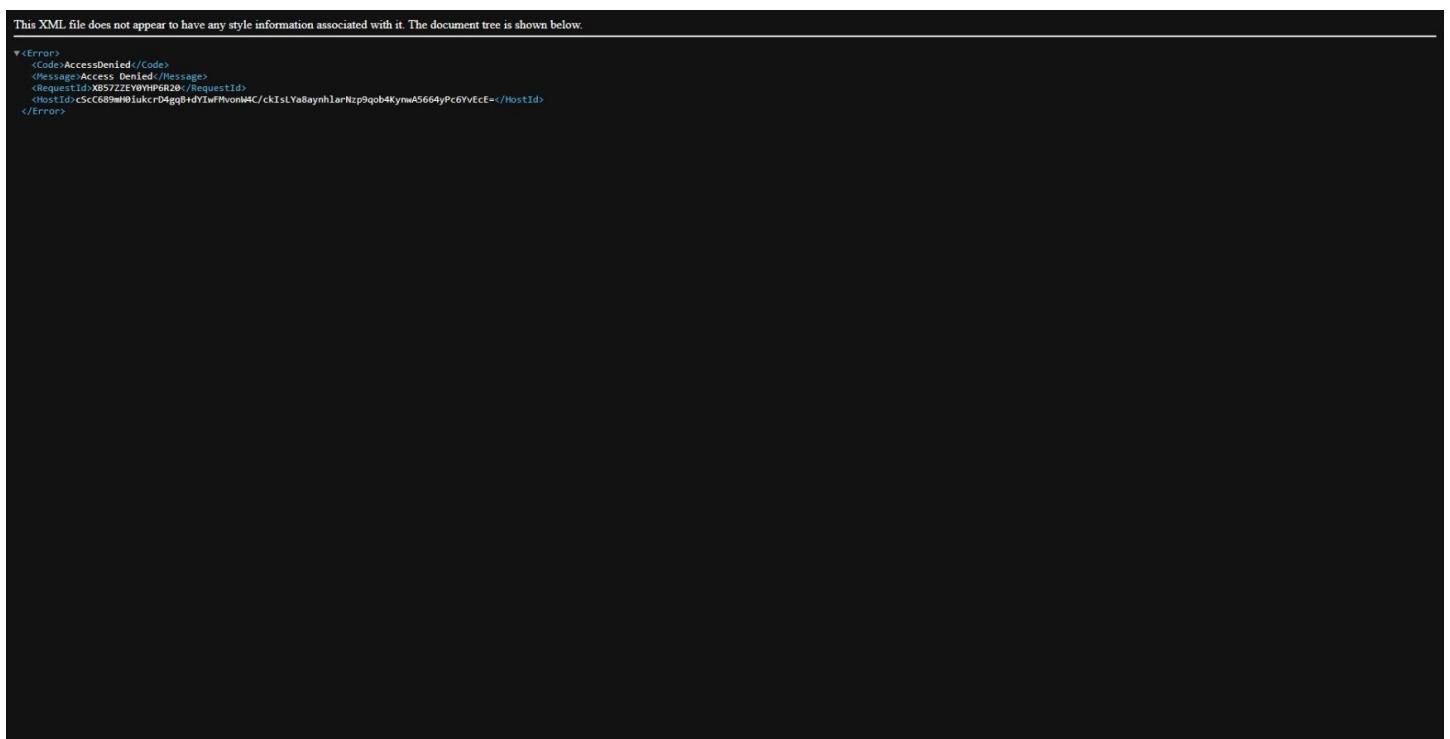


The screenshot shows the AWS IAM Key Policy editor. At the top right are 'Edit' and 'Switch to default view' buttons. The policy document is displayed in a code editor:

```
{  
    "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 'Edit default encryption' page for an Amazon S3 bucket. The left sidebar includes links for Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings, Storage Lens, Dashboards, Storage Lens groups, AWS Organizations settings, Feature spotlight, and AWS Marketplace for S3. The main content area shows the 'Default encryption' section, which is currently set to 'Server-side encryption with AWS Key Management Service keys (SSE-KMS)'. It also shows fields for 'AWS KMS key ARN' (set to 'arn:aws:kms:us-east-1:654812467323:key/99b4b0f1-f94f-49dc-b51') and 'Bucket Key' (set to 'Disable'). A warning message at the bottom states: '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.' The top navigation bar shows the user is in the N. Virginia region.



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>X857ZZEY0H9P6R28</RequestId>  
  <HostId>c5c689ff01a0c04gg0d0Y1wfhnwAC/cKlsLy8aymhlarNzp9qb4KymA5664yPc6YvEcE=</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 section, a table lists the root volume:

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

The 'Encrypted' column for the volume is highlighted with a red box. The 'KMS key ID' column also contains a red box.

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

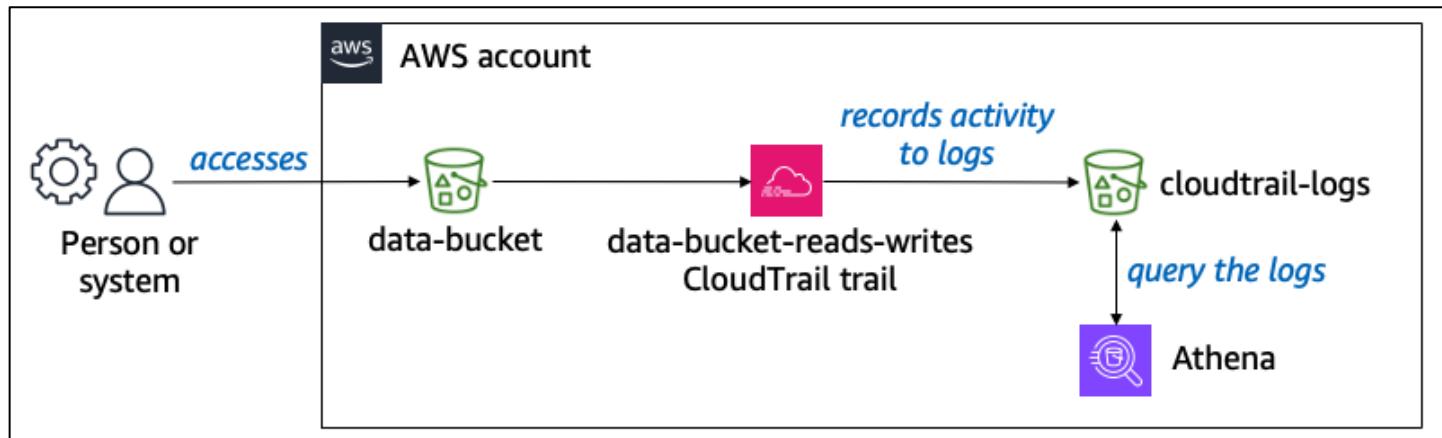
Task 3.6: Use AWS KMS to encrypt a Secrets Manager secret

```
[ec2-user@webserver2 ~]$ aws secretsmanager list-secrets
{
    "SecretList": [
        {
            "ARN": "arn:aws:secretsmanager:us-east-1:654812467323:secret:mysecret",
            "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



Screenshot of the AWS CloudTrail console showing the configuration for the 'data-bucket-reads-writes' trail. The trail is set to log to CloudWatch Logs with the log group 'cloudtrail-logs-0153b53120bc83bce/AWSLogs/654812467323'. It is a multi-region trail and applies to the organization. No SNS notifications are enabled.

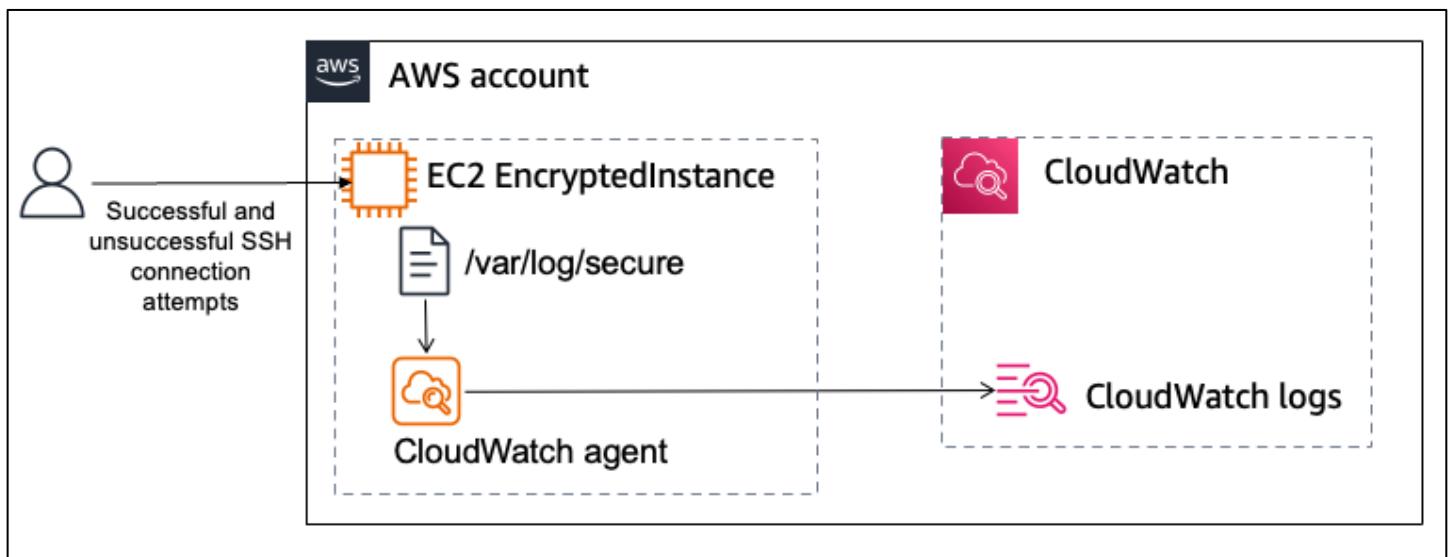
General details
Trail logging: Logging
Trail name: data-bucket-reads-writes
Last log file delivered: October 02, 2024, 00:13:33 (UTC+03:00)
Log file SSE-KMS encryption: Not enabled
SNS notification delivery: Disabled
Apply trail to my organization: Yes

Screenshot of the AWS Athena console showing a query results page. The query retrieves event data from the CloudTrail log group. The results show a single row where an object was put into an S3 bucket.

```
1 | SELECT eventtime, useridentity.principalId, requestParameters, eventName
2 | FROM cloudtrail_logs.cloudtrail_logs_0153b53120bc83bce
3 | WHERE
4 |   eventName IN ('PutObject') AND
5 |   requestParameters LIKE '%customer-data.csv%'
6 | limit 10;
```

#	eventtime	principalId	requestparameters
1	2024-09-30T13:07:03Z	AROAQ5O5KB5Q2WY45ST:user3342491=Abdelrhman_Mostafa_Mohamed	{"X-Amz-Date":"20240930T130702Z","bucketName":"data-bucket-0153b53120bc83bce","keyName":"customer-data.csv"}

Task 4.2: Use CloudWatch Logs to monitor secure logs



Screenshot of the AWS CloudWatch Log Groups interface. The left sidebar shows navigation options like Services, Billing and Cost Management, EC2, S3, Elastic Beanstalk, VPC, CloudWatch, Log groups, Metrics, X-Ray traces, Events, Application Signals, Network monitoring, and Insights. The main area displays the 'EncryptedInstanceSecureLogs' log group details. It includes sections for Log group details (Log class: Info, Standard, ARN: arn:aws:logs:us-east-1:654812467323:log-group:EncryptedInstanceSecureLogs:*, Creation time: 20 hours ago, Retention: 6 months), Metrics filters (1), Subscription filters (0), Contributor Insights rules (-), KMS key ID (-), Anomaly detection (Configure), Data protection (-), and Sensitive data count (-). Below this, the 'Log streams (1)' section shows a single stream named 'EncryptedInstanceSecureLogs-1-0db95d8d3db212bb5' with a last event time of 2024-10-01 22:46:05 (UTC+03:00). Buttons for Actions, View in Logs Insights, Start tailing, and Search log group are at the top right.

Screenshot of the AWS CloudShell terminal window. The terminal shows the command 'sudo service amazon-cloudwatch-agent status' being run on an EC2 instance. The output indicates that the service is active and running. The terminal then displays a long log entry from the Amazon CloudWatch Agent, detailing its configuration and startup process. The log ends with a note about some lines being ellipsized and a prompt for the user to use '-l' to show the full log.

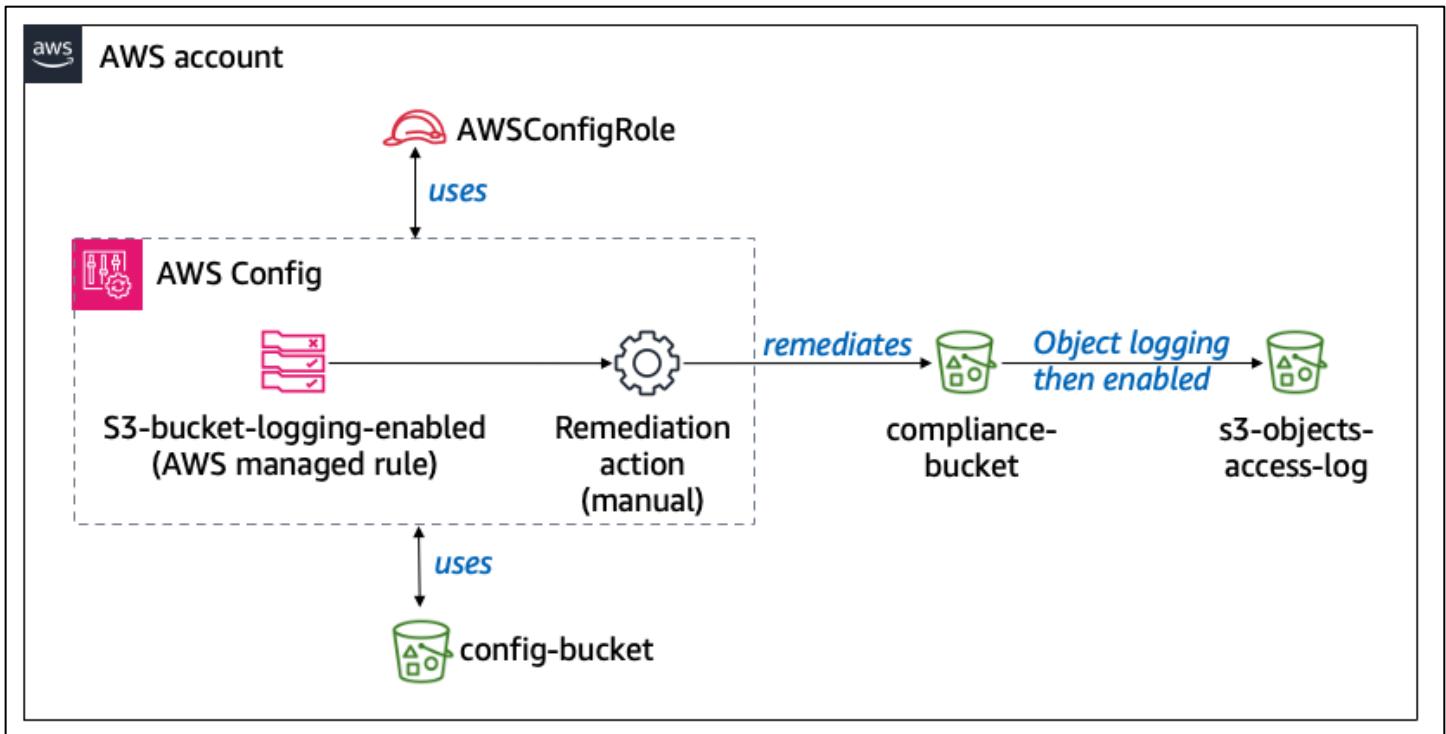
```
aws Services Search [Alt+S]
Console Home Billing and Cost Management EC2 S3 Elastic Beanstalk VPC
[ec2-user@ip-10-1-3-14 ~]$ sudo service amazon-cloudwatch-agent status
Redirecting to /bin/systemctl status amazon-cloudwatch-agent.service
● amazon-cloudwatch-agent.service - Amazon CloudWatch Agent
  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' tab is selected, showing one log stream named 'EncryptedInstanceSecureLogs-1-Odb95d8d3db212bb5' with a last event time of 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 current value is 0. The timeline shows the status from 9/25 to 10/02. 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 a compliance bucket.

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

CloudShell Feedback

[Edit Object Ownership](#)

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.

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-0153b53120bc83bce (Required) Specifies the bucket where you want Amazon S3 to store server access logs. You can have multiple buckets.

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

CloudShell Feedback

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

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

Badge Link

