

# Report 2

## Phase 1: Securing data in Amazon S3

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

The screenshot shows two separate views of the AWS Management Console.

**Top View (AWS Home):** This view shows the main AWS navigation bar and several service links on the left, including Systems Manager, CloudTrail, S3, Secrets Manager, AWS Config, IAM, CloudWatch, Cloud9, and Athena. On the right, there's a sidebar for the current account, organization, service quotas, and billing management. A message at the bottom of the sidebar says "Get started by creating an application." and has a "Create application" button.

**Bottom View (Amazon S3 Buckets):** This view shows the "Amazon S3" service page. It lists "General purpose buckets (9)" under "All AWS Regions". The table includes columns for Name, AWS Region, IAM Access Analyzer, and Creation date. The buckets listed are:

Name	AWS Region	IAM Access Analyzer	Creation date
athena-results-12366556	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	September 26, 2024, 14:40:11 (UTC+03:00)
aws-athena-query-results-332265937753-us-east-1	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	September 30, 2024, 15:47:36 (UTC+03:00)
aws-cloudtrail-logs-332265937753-0f492829	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	September 30, 2024, 15:36:29 (UTC+03:00)
aws-config-085e8dfdad4b1e85f	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	September 26, 2024, 16:53:09 (UTC+03:00)
cloudtrail-logs-085e8dfdad4b1e85f	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	September 26, 2024, 16:53:08 (UTC+03:00)
compliance-bucket-085e8dfdad4b1e85f	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	September 30, 2024, 16:31:33 (UTC+03:00)
data-bucket-085e8dfdad4b1e85f	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	September 26, 2024, 18:05:59 (UTC+03:00)
s3-inventory-085e8dfdad4b1e85f	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	September 26, 2024, 16:53:09 (UTC+03:00)
s3-objects-access-log-085e8dfdad4b1e85f	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	September 26, 2024, 16:53:08 (UTC+03:00)

**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

**Amazon S3 > Buckets > data-bucket-085e8dfdad4b1e85f**

**data-bucket-085e8dfdad4b1e85f** Info

**Objects (4) Info**

Name	Type	Last modified	Size	Storage class
<a href="#">customer-data.csv</a>	csv	September 30, 2024, 15:44:35 (UTC+03:00)	0 B	Standard
<a href="#">customers.csv</a>	csv	September 26, 2024, 21:01:08 (UTC+03:00)	360.0 B	Standard
<a href="#">loan-data.csv</a>	csv	September 30, 2024, 14:17:58 (UTC+03:00)	198.0 B	Standard
<a href="#">myfile.txt</a>	txt	September 26, 2024, 18:10:02 (UTC+03:00)	13.0 B	Standard

**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

**Policy**

```

4 {
5   "Effect": "Allow",
6   "Principal": [
7     "arn:aws:iam::332265937753:user/sofia",
8     "arn:aws:iam::332265937753:role/voclabs",
9     "arn:aws:iam::332265937753:user/paulo"
10    ],
11  },
12  },
13  "Action": "s3:*",
14  "Resource": [
15    "arn:aws:s3:::data-bucket-085e8dfdad4b1e85f",
16    "arn:aws:s3:::data-bucket-085e8dfdad4b1e85f/*"
17  ],
18 },
19 {
20   "Effect": "Deny",
21   "Principal": "*",
22   "Action": "s3:*",
23   "Resource": [
24     "arn:aws:s3:::data-bucket-085e8dfdad4b1e85f",
25     "arn:aws:s3:::data-bucket-085e8dfdad4b1e85f/*"
26   ],
27   "Condition": {
28     "StringNotEquals": {
29       "aws:PrincipalArn": [
30         "arn:aws:iam::332265937753:role/voclabs",
31         "arn:aws:iam::332265937753:user/paulo",
32         "arn:aws:iam::332265937753:root"
33       ]
34     }
35   }
36 }

```

**Edit statement** Remove

**Add actions**

Choose a service

Included S3

Available AMP API Gateway API Gateway V2 ASC Access Analyzer Account

**Add a resource** Add

**Add a condition (optional)** Add

**CloudShell Feedback**

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

The screenshot shows the AWS S3 Properties tab for a bucket named 'data-bucket-085e8dfdad4b1e85f'. The 'Bucket Versioning' section is open, showing that 'Enabled' is selected. There is a note about Multi-factor authentication (MFA) delete, which is currently 'Disabled'. The 'Tags (0)' section is also visible.

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

The screenshot shows the AWS S3 Management tab for the same bucket. The 'Inventory' configuration is displayed. The 'Inventory report source' section shows 'Entire bucket' as the filter. The 'Inventory configuration details' section shows the destination as 's3://s3-inventory-085e8dfdad4b1e85f', format as 'Apache Parquet', and status as 'Enabled'. The 'Last export' date is listed as '2024-10-01'. The 'Inventory report encryption' section indicates server-side encryption protects data at rest.

## Task 1.4: Confirm that versioning works as intended

The screenshot shows the AWS S3 console with the 'Objects (5)' view. 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, Storage Lens, Dashboards, Storage Lens groups, AWS Organizations settings, and Feature spotlight. The main area displays five objects: 'customer-data.csv' (version ID: Wtkp9u5KCz dqzbx.UAwRU\_, type: csv), 'customers.csv' (version ID: hOsAp5ryns. Bo1CVOLLl.0u VZh4d8dmo, type: csv), 'customers.csv' (version ID: 7ExbQ1o.1z BlapytE985h xz.4bk7wmg, type: csv), 'loan-data.csv' (version ID: U2Xt78m3RF V90aATWh2x aorG88ywVA LX, type: csv), and 'myfile.txt' (version ID: null, type: txt). The table includes columns for Name, Type, Version ID, Last modified, Size, and Storage class.

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

The screenshot shows the AWS Athena console. On the left, the 'Database' dropdown is set to 'default'. The 'Tables and views' section lists 'Tables (2)': 'bucket\_logs' and 'cloudtrail\_logs\_aws\_cloudtrail\_logs\_332 265937753\_0f492829'. The 'Views (0)' section is empty. The main area contains a SQL query editor with the following code:

```
5     requestparameters LIKE '%customer-data.csv%'  
6 limit 10;
```

The 'Run again' button is highlighted. Below the editor, the 'Query results' tab is selected, showing a completed query with the following details:

- Time in queue: 78 ms
- Run time: 558 ms
- Data scanned: 16.40 KB

The results table has columns: #, eventtime, principalid, and requestparameters. One row is shown:

#	eventtime	principalid	requestparameters
1	2024-09-30T12:44:34Z	AROAU2XEX3NMSAJZ7DNNW:user3343178=Abdelrahman_Ali_Mohasseb	{"X-Amz-Date":"20240930T124433Z", "X-Amz-SecurityToken": "AQAB..."}

## Cost assessment to secure Amazon S3

Microsoft Excel (Product Activation Failed)

File Home Insert Page Layout Formulas Data Review View

Normal Bad Good Neutral Calculation Check Cell

Clipboard Font Alignment Number Styles Cells Editing

A1 Estimate summary

1 Estimate summary

2 Upfront cc Monthly ci Total 12 m Currency

3 0 0.05 0.6 USD

4 \* Includes upfront cost

5

6

7 Detailed Estimate

8 Group hier Region Description Service Upfront Monthly First 12 m Currency Status Configuration summary

9 My Estima Europe (Ireland) S3 Standard 0 0 0 USD S3 Standard Average Object Size (10 MB), PUT, COPY, POST, LIST requests to S3 Standard (10), GET, SELECT, and all other requests from S3 Standard (10), DT Inbound: Internet (0 GB per month), DT Outbound: Not selected (0 TB per month)

10 My Estima Europe (Ireland) Data Trans 0 0 0 USD

11 My Estima Europe (Ireland) Amazon AI 0 0.05 0.6 USD Total number of queries (100 per month), Amount of data scanned per query (100 MB)

12

13

14

15 Acknowledgement

16 \* 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.

Ready | 100%

The screenshot shows a Microsoft Excel spreadsheet titled "My Estimate1.csv". The spreadsheet contains several sections of data:

- Estimate summary:** Shows an upfront cost of 0, monthly costs of 0.05, and a total monthly cost of 0.6 USD.
- Detailed Estimate:** A table with columns for Group hierarchy, Region, Description, Service, Upfront, Monthly, First 12 m, Currency, Status, and Configuration summary. It includes data for S3 Standard, Data Transfer, and Amazon AI services across different regions.
- Acknowledgement:** A note stating that the AWS Pricing Calculator provides only an estimate and does not include taxes.

## Phase 2: Securing VPCs

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

The screenshot displays two AWS service dashboards side-by-side.

**EC2 Instances Dashboard:** Shows a list of running instances. One instance, "WebServer" (ID: i-014bf9da5402c35f9), is selected. The instance details page is open, showing information such as Public IPv4 address (50.16.105.108), Instance state (Running), and Private IP DNS name (ip-10-1-3-4.ec2.internal).

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
WebServer2	i-0b3f2346dd8fe6f24	Running	t2.micro	2/2 checks pass	View alarms	us-east-1a	ec2-98-
WebServer	i-014bf9da5402c35f9	Running	t2.micro	2/2 checks pass	View alarms	us-east-1a	ec2-50-
EncryptedInst...	i-06b4044c7fc2f05cd	Running	t2.micro	2/2 checks pass	View alarms	us-east-1a	ec2-54-
aws-rlinu9-11	i-07711r734d4rhewpa	Running	t2.micro	2/2 checks pass	View alarms	us-east-1b	ec2-74-

**VPC Dashboard:** Shows the "Your VPCs" section. A VPC named "LabVPC" (ID: vpc-0b40eb17acdd48628) is selected. The "Resource map" tab is active, displaying the network architecture: a single Subnet (WebServerSubnet) in the us-east-1a Availability Zone, which is connected to a single Route Table (rtb-037c11f6e7e3b2a0d) via a line, which in turn connects to a Network interface card (LabVPCIG).

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP
-	vpc-0bcf856b7fa99f266	Available	172.31.0.0/16	-	opt-0
NetworkFirewallVPC	vpc-0c6a06f93ee6aaded3	Available	10.1.0.0/16	-	opt-0
LabVPC	vpc-0b40eb17acdd48628	Available	10.1.0.0/16	-	opt-0

The screenshot shows the AWS IAM console. On the left, the navigation pane is open with the 'Identity and Access Management (IAM)' section selected. Under 'Access management', 'Roles' is also selected. The main content area displays the 'VPCFlowLogsRole' configuration. The 'Summary' tab is active, showing details like creation date (September 26, 2024), last activity (20 minutes ago), ARN (arn:aws:iam::332265937753:role/VPCFlowLogsRole), and maximum session duration (1 hour). Below the summary, the 'Permissions' tab is selected, showing one attached policy: 'VPCFlowLogPolicy'. The policy is a customer inline policy.

## Task 2.2: Create a VPC flow log

The screenshot shows the AWS VPC dashboard. The left sidebar is expanded, showing sections like 'Virtual private cloud' (with 'Your VPCs' selected) and 'Security'. In the main content area, the 'Your VPCs' section lists three VPCs: 'vpc-0bcf856b7fa99f266', 'NetworkFirewallVPC', and 'LabVPC'. The 'LabVPC' row is selected. Below the VPC list, the 'Flow logs' tab is selected in the 'vpc-0b40eb17acdd48628 / LabVPC' section. A single flow log named 'LabVPCFlowLogs' is listed, with its ID 'fl-0cadd7213d610777a' and destination 'cloud-watch-logs'.

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

The screenshot shows the AWS CloudWatch Log streams interface. The left sidebar includes sections for Favorites and recent items, Dashboards, Alarms, Logs (Log groups, Log anomalies, Live Tail, Logs Insights, Contributor Insights), Metrics (All metrics, Explorer, Streams), and X-Ray traces. The main area displays a list of 16 log streams under the heading "Log streams (16)". Each entry includes a checkbox, the log stream name, and the last event time. The log streams listed are:

Log stream	Last event time
/aws/network-firewall/flow/NetworkFirewall_2024-09-30-14	2024-09-30 14:15:45 (UTC)
/aws/network-firewall/flow/NetworkFirewall_2024-09-30-13	2024-09-30 13:59:59 (UTC)
/aws/network-firewall/alert/NetworkFirewall_2024-09-30-13	2024-09-30 13:57:55 (UTC)
/aws/network-firewall/flow/NetworkFirewall_2024-09-30-12	2024-09-30 12:59:58 (UTC)
/aws/network-firewall/alert/NetworkFirewall_2024-09-30-12	2024-09-30 12:56:40 (UTC)
/aws/network-firewall/flow/NetworkFirewall_2024-09-30-11	2024-09-30 11:59:55 (UTC)
/aws/network-firewall/alert/NetworkFirewall_2024-09-30-11	2024-09-30 11:56:01 (UTC)
/aws/network-firewall/flow/NetworkFirewall_2024-09-30-10	2024-09-30 10:59:54 (UTC)
/aws/network-firewall/alert/NetworkFirewall_2024-09-30-10	2024-09-30 10:44:31 (UTC)
/aws/network-firewall/flow/NetworkFirewall_2024-09-28-13	2024-09-28 13:24:06 (UTC)
/aws/network-firewall/alert/NetworkFirewall_2024-09-28-13	2024-09-28 13:09:08 (UTC)
/aws/network-firewall/flow/NetworkFirewall_2024-09-28-12	2024-09-28 12:59:58 (UTC)
log_stream_created_by_aws_to_validate_log_delivery_subscriptions	2024-09-28 12:42:56 (UTC)

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

The screenshot shows the AWS VPC dashboard. The left sidebar includes sections for 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), and Security (Network ACLs). The main area displays the "Details" section for a security group named "WebServerSecurityGroup". The details include:

Security group name	Security group ID	Description	VPC ID
WebServerSecurityGroup	sg-05d65bd4274a6c22	WebServerSecurityGroup	vpc-0b40eb17acdd48628

The "Inbound rules" tab is selected, showing three rules:

Source	Port range	Protocol	Type	IP version
0.0.0.0/0	8080	TCP	Custom TCP	b23bb7dd2...
34.230.189.254/32	22	TCP	SSH	e58975e5c31
0.0.0.0/0	80	TCP	HTTP	:036b42121a

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

The screenshot shows the AWS Management Console interface for Network ACLs. On the left, a navigation pane lists various AWS services like DHCP option sets, Elastic IPs, and Security groups. The main content area displays a table of Network ACLs:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules
-	acl-0e1ac57a7afbaf24	6 Subnets	Yes	vpc-0bcf856b7fa99f266	2 In
-	acl-0559a88c4ea3886d	2 Subnets	Yes	vpc-0c6a06f93ee6aded3 / NetworkFire...	2 In
<b>selected</b>	<b>acl-095f6cb0a270bf143</b>	<b>subnet-008c59f2a3470e2bf / WebServerSubnet</b>	<b>Yes</b>	<b>vpc-0b40eb17acdd48628 / LabVPC</b>	<b>3 In</b>

Below this, a detailed view of the selected Network ACL's inbound rules is shown:

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

## Task 2.6: Review NetworkFirewallVPC and its associated resources

The screenshot shows the AWS Management Console interface for VPCs. The left navigation pane includes endpoints, security, DNS firewall, and network firewall sections. The main content area displays a table of VPCs:

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP
-	vpc-0bcf856b7fa99f266	Available	172.31.0.0/16	-	dopt-0
<b>selected</b>	<b>vpc-0c6a06f93ee6aded3</b>	<b>Available</b>	<b>10.1.0.0/16</b>	-	<b>dopt-0</b>
-	vpc-0b40eb17acdd48628	Available	10.1.0.0/16	-	dopt-0

Below the table, a "Resource map" diagram illustrates the network topology:

- VPC:** NetworkFirewallVPC (Your AWS virtual network)
- Subnets:** us-east-1a
  - FirewallSubnet
  - WebServer2Subnet
- Route tables:** (4)
  - 10.1.3.0/28
  - rtb-0f832c1591c1fa1e3
  - IGW-Ingress-Route-Table
  - WebServer2-Route-Table
- Network connection:** FirewallSubnet is connected to NetworkFirewallVPC.

## Task 2.7: Create a network firewall

The screenshot shows the AWS VPC Network Firewall: Firewalls page. On the left, a navigation pane lists various VPC services like Endpoint services, NAT gateways, Peering connections, Security, DNS firewall, Network Firewall (selected), and Virtual private network (VPN). Under Network Firewall, 'Firewalls' is selected. The main area displays a 'NetworkFirewall' card with the following details:

- Overview:** Firewall status is 'Ready' (green), Associated firewall policy is 'FirewallPolicy', and Associated VPC is 'vpc-0c6a06f93ee6aded3'.
- Firewall details:** Name is 'NetworkFirewall', Description is '-'. There is an 'Edit' button.
- VPC:** Associated VPC is 'vpc-0c6a06f93ee6aded3'. Firewall subnets listed are 'subnet-005bae69b38fe3da0 (IPv4)'.

At the bottom, there are links for CloudShell, Feedback, and the footer includes copyright information and links for Privacy, Terms, and Cookie preferences.

## Task 2.8: Create route tables

The screenshot shows the AWS VPC Route tables page. On the left, a navigation pane lists various VPC services. Under 'Route tables', 'Route tables' is selected. The main area displays a table titled 'Route tables (6) Info' with the following data:

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
-	rtb-0f832c1591c1fa1e3	-	-	Yes	vpc-0c6a06f93ee6adec
IGW-Ingress-Route-Table	rtb-025c3134d88fcc5e2	-	igw-09767d62f314...	No	vpc-0c6a06f93ee6adec
WebServer2-Route-Table	rtb-0e5b12c883d5cab45	subnet-020b2e1f9d3d68...	-	No	vpc-0c6a06f93ee6adec
-	rtb-03cc6b22d015cb30a	-	-	Yes	vpc-0bcf856b7fa99f26

Below the table, a section titled 'Select a route table' is visible. The footer includes copyright information and links for Privacy, Terms, and 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: Favorites and recent, Dashboards, Alarms (0), Logs (Log groups, Log Anomalies, Live Tail, Logs Insights, Contributor Insights), Metrics (All metrics, Explorer, Streams), and X-Ray traces. The main content area displays the 'NetworkFirewallVPCLogs' log group details. The 'Log group details' section shows the following information:

Log class	Info	Stored bytes	KMS key ID
Standard	-	-	-
ARN	Metric filters	Anomaly detection	Configure
arn:aws:logs:us-east-1:332265937753:log-group:NetworkFirewallVPCLogs:*	0	-	-
Creation time	Subscription filters	Data protection	-
3 days ago	0	-	-
Retention	Contributor Insights rules	Sensitive data count	-
6 months	-	-	-

Below this, there are tabs for Log streams, Tags, Anomaly detection, Metric filters, Subscription filters, Contributor Insights, and Data protection. The Log streams tab is selected, showing 'Log streams (0)'. At the bottom, there are buttons for Create log stream, Search all log streams, and filter options.

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

The screenshot shows the AWS Network Firewall Rule Groups interface. The left sidebar navigation includes: 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 (4)' section and a 'Customer managed key' section.

**Rules (4)**

Description	Geo IP	Protocol	Source	Destination	Destination...	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

**Customer managed key**

Key type: AWS owned key

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

## 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, a sidebar navigation includes 'Key Management Service (KMS)', 'Customer managed keys' (which is selected), and 'Custom key stores'. The main content area displays a 'Customer managed keys' page for a specific key. The key ID is 44cc385f-2905-4e7a-8b37-8384201405fd. The 'General configuration' section shows details like Alias (MyKMSKey), Status (Enabled), Creation date (Sep 30, 2024 13:58 GMT+3), ARN (arn:aws:kms:us-east-1:332265937753:key/44cc385f-2905-4e7a-8b37-8384201405fd), and Regionality (Single Region). Below this, tabs for 'Key policy', 'Cryptographic configuration', 'Tags', 'Key rotation' (which is selected), and 'Aliases' are visible. The 'Automatic key rotation' section indicates the key is enabled for rotation every 365 days. The URL in the address bar is https://us-east-1.console.aws.amazon.com/kms/keys/44cc385f-2905-4e7a-8b37-8384201405fd/keyRotation?

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

The screenshot shows the AWS KMS console interface. The sidebar navigation includes 'Key Management Service (KMS)', 'Customer managed keys' (selected), and 'Custom key stores'. The main content area displays a 'Customer managed keys' page for a specific key. The 'Key deletion' section has a checked checkbox for 'Allow key administrators to delete this key'. The 'Key users' section lists two users: 'voclabs' (Role) and 'sofia' (User). A search bar for 'Search Key users' is present. The 'Other AWS accounts' section contains a button to 'Add other AWS accounts'. The URL in the address bar is https://us-east-1.console.aws.amazon.com/kms/keys/44cc385f-2905-4e7a-8b37-8384201405fd/keyPolicy?

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

The screenshot shows the AWS S3 console with the 'Amazon S3' service selected. On the left, the navigation pane includes options 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, Storage Lens, Feature spotlight, and AWS Marketplace for S3.

In the main content area, under 'Default encryption', it is set to 'Server-side encryption with AWS Key Management Service keys (SSE-KMS)'. The 'Encryption key ARN' is listed as `arn:aws:kms:us-east-1:332265937753:key/44cc385f-2905-4e7a-8b37-8384201405fd`. A 'Bucket Key' section indicates that KMS encryption is used to encrypt new objects in the bucket, which reduces costs by lowering calls to AWS KMS. The 'Enabled' status is shown.

At the bottom, there is a section for 'Intelligent-Tiering Archive configurations' with a 'Create configuration' button.

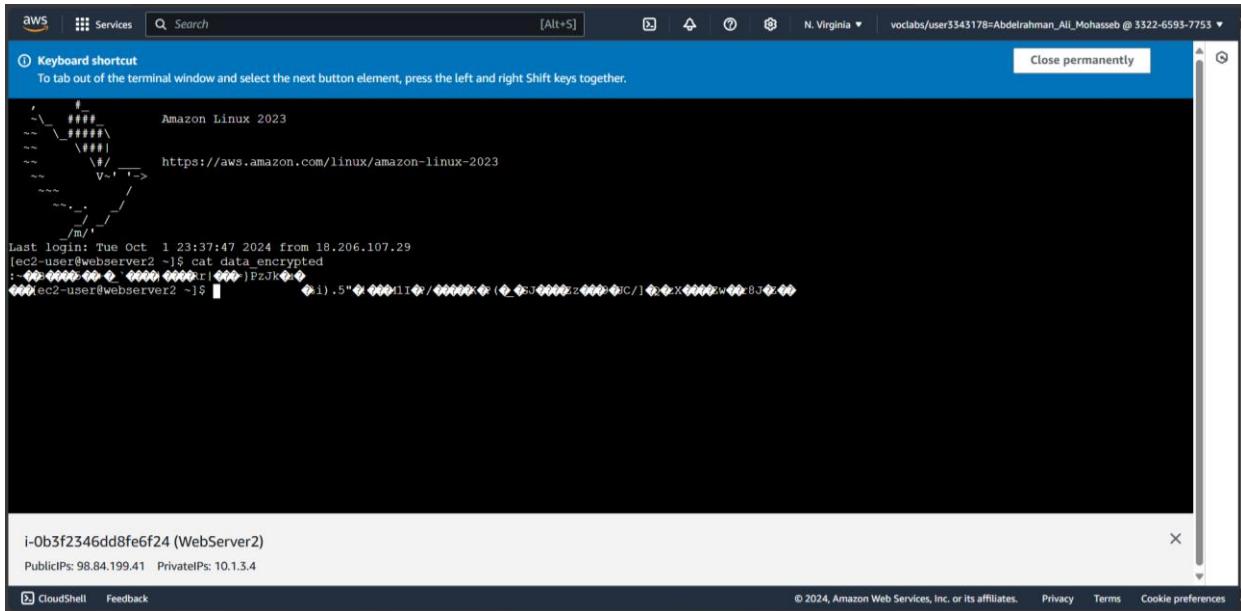
## Task 3.4: Use AWS KMS to encrypt the root volume of an EC2 instance

The screenshot shows the AWS EC2 Instances page. The left sidebar lists various EC2-related services and features. The main table displays four instances, with one instance, 'EncryptedInst...', selected. This instance has an ID of `i-06b4044c7fc2f05cd`.

On the right, the details for the selected instance are shown. Under the 'Storage' tab, it is indicated that the root device is EBS-optimized. The 'Block devices' table shows a single volume attached to the instance:

Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID
<code>vol-0b1cb0ebc78b66113</code>	<code>/dev/xvda</code>	8	Attached	2024/09/30 14:28 GMT+3	Yes	<code>44cc385f-2905-4e7a-8b37-8384201405fd</code>

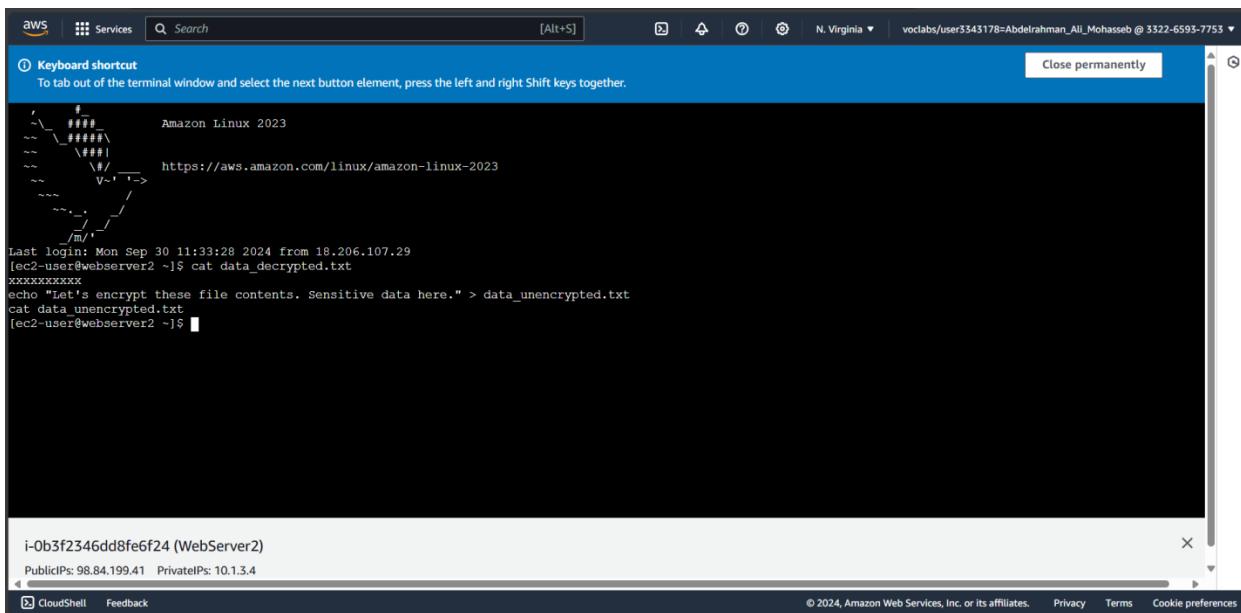
## Task 3.5: Use AWS KMS envelope encryption to encrypt data in place



AWS CloudShell terminal window showing a terminal session on an Amazon Linux 2023 instance. The terminal displays the following command and its output:

```
Last login: Tue Oct  1 23:37:47 2024 from 18.206.107.29
[ec2-user@webserver2 ~]$ cat data_encrypted
-----BEGIN ENCRYPTED DATA-----
```

The terminal window includes a status bar at the bottom with the instance ID (i-0b3f2346dd8fe6f24), Public IP (98.84.199.41), Private IP (10.1.3.4), and the AWS region (N. Virginia).



AWS CloudShell terminal window showing a terminal session on an Amazon Linux 2023 instance. The terminal displays the following command and its output:

```
Last login: Mon Sep 30 11:33:28 2024 from 18.206.107.29
[ec2-user@webserver2 ~]$ cat data_decrypted.txt
xxxxxxxxxx
echo "Let's encrypt these file contents. Sensitive data here." > data_unencrypted.txt
cat data_unencrypted.txt
[ec2-user@webserver2 ~]$
```

The terminal window includes a status bar at the bottom with the instance ID (i-0b3f2346dd8fe6f24), Public IP (98.84.199.41), Private IP (10.1.3.4), and the AWS region (N. Virginia).

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

The screenshot shows a CloudShell terminal window with the following content:

```
aws <command> <subcommand> help
aws: error: the following arguments are required: --secret-id

[ec2-user@webserver2 ~]$ aws secretsmanager list-secrets
{
  "SecretList": [
    {
      "ARN": "arn:aws:secretsmanager:us-east-1:332265937753:secret:mysecret-96b0le",
      "Name": "mysecret",
      "KmsKeyId": "arn:aws:kms:us-east-1:332265937753:key/44cc385f-2905-4e7a-8b37-8384201405fd",
      "LastChangedDate": "2024-09-30T12:02:25.005000+00:00",
      "LastAccessedDate": "2024-09-30T00:00:00+00:00",
      "Tags": [],
      "SecretVersionsToStages": [
        "1dd60e70-9446-44c4-82e3-624e04e5d2a0": [
          "AWS CURRENT"
        ]
      ],
      "CreatedDate": "2024-09-30T12:02:24.935000+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

i-0b3f2346dd8fe6f24 (WebServer2)
PublicIPs: 98.84.199.41 PrivateIPs: 10.1.3.4
```

The screenshot shows a terminal window within the AWS CloudShell interface. The user has run the command `aws secretsmanager get-secret-value`. The output displays the secret's ARN, name, version ID, secret string, and creation date. The terminal also shows the user's AWS session information at the bottom.

```
[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-1:332265937753:secret:mysecret-Q6b0le",
  "Name": "mysecret",
  "VersionId": "1dd60e70-9446-44c4-82e3-624e04e5d2a0",
  "SecretString": "{\"secret\":\"my secret data\"}",
  "VersionStages": [
    {
      "AWSCURRENT"
    }
  ],
  "CreatedDate": "2024-09-30T12:02:25.001000+00:00"
}
[ec2-user@webserver2 ~]$
```

## Cost assessment for using AWS KMS

Microsoft Excel (Product Activation Failed)

File Home Insert Page Layout Formulas Data Review View

Normal Bad Good Neutral Calculation Check Cell

Clipboard Font Alignment Number Styles

AutoSum Fill Clear Sort & Filter Find & Select Cells Editing

My Estimate3.csv

1 Estimate summary

2 Upfront cost: Monthly cost: Total 12 months: Currency

3 0 1.4 16.8 USD

4 \* Includes upfront cost

5

6

7 Detailed Estimate

8 Group hierarchy Region Description Service Upfront Monthly First 12 months Currency Status Configuration summary

9 My Estimate Europe (Ireland) AWS Key 0 1.0006 12.01 USD Number of customer managed Customer Master Keys (CMK) (1), Number of symmetric requests (200)

10 My Estimate Europe (Ireland) AWS Secrets 0 0.4 4.8 USD Number of secrets (1), Average duration of each secret (30 days), Number of API calls (1 per month)

11

12

13

14 Acknowledgement

15 \* 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.

16

17

18

19

20

21

22

23

24

25

26

27

28

Ready | 100% +

Detailed Estimate Data:

Group hierarchy	Region	Description	Service	Upfront	Monthly	First 12 months	Currency	Status	Configuration summary
My Estimate Europe (Ireland)	AWS Key	0	1.0006	12.01	USD	Number of customer managed Customer Master Keys (CMK) (1), Number of symmetric requests (200)			
My Estimate Europe (Ireland)	AWS Secrets	0	0.4	4.8	USD	Number of secrets (1), Average duration of each secret (30 days), Number of API calls (1 per month)			

## Phase 4: Monitoring and logging

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

The screenshot displays two AWS service consoles side-by-side.

**CloudTrail Console (Top):**

- Left sidebar:** Shows navigation links for Dashboard, Event history, Insights, Lake (Dashboard, Query, Event data stores, Integrations), and Trails.
- Right pane:** Shows a trail named "data-bucket-reads-writes".
  - General details:** Trail logging is enabled (Logging checked), Trail log location is "aws-cloudtrail-logs-332265937753-0f492829/AWSLogs/332265937753", Log file validation is Enabled, Last file validation delivered is October 02, 2024, 02:44:08 (UTC+03:00), SNS notification delivery is Disabled, and Last SNS notification is "-".
  - Actions:** Buttons for Delete and Stop logging.

**AWS S3 Console (Bottom):**

- Left sidebar:** Shows Buckets, Storage Lens, and Feature spotlight.
- Right pane:** Shows the contents of the "aws-cloudtrail-logs-332265937753-0f492829" bucket.
  - Objects:** A list of objects with 495 items.
    - Actions:** Buttons for Copy S3 URI, Copy URL, Download, Open, Delete, Actions, Create folder, and Upload.
    - Table:** A detailed table of objects with columns for Name, Type, Last modified, Size, and Storage class.
    - Sample Data:** Two objects are listed:
      - 332265937753\_CloudTrail\_us-east-1\_20240930T1250Z\_c57Bu\_LPInmkwTSRajson.gz (gz type, 753.0 B size, Standard storage)
      - 332265937753\_CloudTrail\_us-east-1\_20240930T1250Z\_h096y\_j9zEftKSAJ.json.gz (gz type, 3.3 KB size, Standard storage)

## 4.2: Use CloudWatch Logs to monitor secure logs

The image displays two screenshots of the AWS CloudWatch Logs interface, illustrating how to monitor secure logs.

**Screenshot 1: Log Group Details**

This screenshot shows the "Log group details" page for the "EncryptedInstanceSecureLogs" group. Key information includes:

- Log class: Info
- Standard: 5.96 KB
- ARN: arn:aws:logs:us-east-1:352265937753:log-group:EncryptedInstanceSecureLogs:\*
- Metric filters: 1
- Anomaly detection: Configure
- Creation time: 1 day ago
- Subscription filters: 0
- Data protection: -
- Retention: 6 months
- Contributor Insights rules: -
- Sensitive data count: -

**Screenshot 2: Log Events**

This screenshot shows the "Log events" page for the same log group. It lists recent log entries:

Timestamp	Message
Sep 30 14:02:50	ip-10-1-3-11 sshd[3230]: Received signal 15; terminating.
Oct 1 22:33:51	ip-10-1-3-11 sshd[3122]: Server listening on 0.0.0.0 port 22.
Oct 1 22:33:51	ip-10-1-3-11 sshd[3122]: Server listening on :: port 22.
Oct 1 23:02:57	ip-10-1-3-11 sshd[3348]: Connection reset by 198.235.24.37 port 59002 [preauth]

The interface includes a search bar, time range controls (Clear, 1m, 30m, 1h, 12h, Custom, UTC timezone), and a display dropdown.

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

The screenshot shows two screenshots of the AWS CloudWatch Metrics Filter and Alarm creation process.

**Screenshot 1: Metric filters (1)**

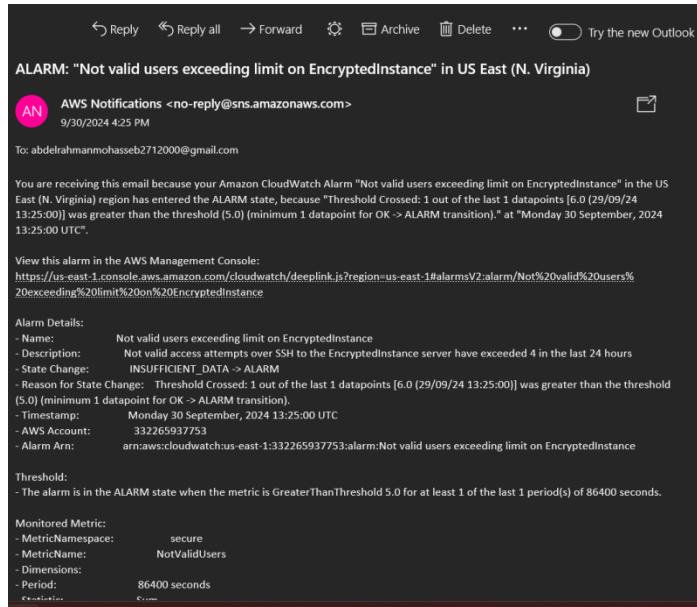
This screenshot shows the CloudWatch Metrics Filter configuration. A single metric filter named "Not valid users" is defined with the following parameters:

- Metric:** secure / NotValidUsers
- Metric value:** 1
- Default value:** 0
- Unit:** Count
- Dimensions:** -
- Alarms:** Not valid users exceeding limit on Encryptedinstance

**Screenshot 2: CloudWatch Alarms (1) - Not valid users exceeding limit on Encryptedinstance**

This screenshot shows the CloudWatch Alarm configuration for the metric filter. The alarm details are as follows:

- Name:** Not valid users exceeding limit on Encryptedinstance
- Type:** Metric alarm
- Description:** Not valid access attempts over SSH to the Encryptedinstance server have exceeded 4 in the last 24 hours
- State:** OK
- Threshold:** NotValidUsers > 5 for 1 datapoints within 1 day
- Statistic:** Sum
- Period:** 1 day
- Actions:** Actions enabled
- ARN:** arn:aws:cloudwatch:us-east-1:32265937753:alarm:Not valid users exceeding limit on Encryptedinstance



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

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: 7d20709efb47be275154c025cd57bd8d672e2601ce0422d744694167a2e29c4b	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account)	-	-

**Note:**  
Public access is blocked because Block Public Access settings are turned on for this bucket.  
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access.

The screenshot shows the AWS Config Rules page. The left sidebar includes links for Dashboard, Conformance packs, Resources, Aggregators (Compliance Dashboard, Conformance packs, Rules), Inventory Dashboard, Resources, Authorizations, Advanced queries (Preview), Settings, and What's new. The main content area is titled "Rules" and contains a table with one row. The table columns are Name, Remediation action, Type, Enabled evaluation mode, and Detective compliance. The single row shows "s3-bucket-logging-enabl..." as the Name, "AWS-ConfigureS3Bucket..." as the Remediation action, "AWS managed" as the Type, "DETECTIVE" as the Enabled evaluation mode, and "8 Noncompliant reso..." as the Detective compliance status.

## Cost assessment for monitoring and logging

The screenshot shows an Excel spreadsheet titled "My Estimate4.csv". The spreadsheet contains several sections of data:

- Estimate summary:**

	Upfront	Monthly	Total	Currency
0	1.71	20.52	USD	

\* Includes upfront cost
- Detailed Estimate:**

Group	Region	Description	Service	Upfront	Monthly	First	12	Currency	Status	Configuration summary
My Estimate Europe	(Ireland)	AWS CloudWatch Metrics		0	1	12	USD			Management events units (millions), Write management trails (1), Read management trails (1), Data events units (millions), S3 trails (1), Lambda trails (1), Infrastructure metrics (1), Number of Metrics (includes detailed and custom metrics) (1), Standard Logs: Data Ingested (0.5 GB), Number of Standard Resolution Alarm Metrics (1)
My Estimate Europe	(Ireland)	Amazon CloudWatch Metrics		0	0.68725	8.25	USD			Number of Metrics (includes detailed and custom metrics) (1), Standard Logs: Data Ingested (0.5 GB), Number of Standard Resolution Alarm Metrics (1)
My Estimate Europe	(Ireland)	AWS Config		0	0.025	0.3	USD			Number of Continuous Configuration items recorded (8), Number of Periodic Configuration items recorded (1), Number of Config rule evaluations (1)
- 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.

Badges and Completion Certificates - Cloud Security Builder

