

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 Buckets page. At the top, there's an 'Account snapshot' section with metrics like Total storage (676.0 B), Object count (3), and Average object size (225.3 B). Below this, there are tabs for 'General purpose buckets' and 'Directory buckets'. Under 'General purpose buckets', there are five entries:

Name	AWS Region	IAM Access Analyzer	Creation date
aws-config-014c6d3497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 10:34:16 (UTC-05:00)
cloudtrail-logs-014c6d3497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 10:34:16 (UTC-05:00)
data-bucket-014c6d3497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 19, 2024, 13:53:53 (UTC-05:00)
s3-inventory-014c6d3497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 10:34:16 (UTC-05:00)
s3-objects-access-log-014c6d3497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 10:34:16 (UTC-05:00)

The screenshot shows the AWS S3 Bucket Objects page for the 'data-bucket-014c6d3497022aafe' bucket. It lists one object:

Name	Type	Last modified	Size	Storage class
myfile-014c6d3497022aafe.txt	txt	April 19, 2024, 13:54:26 (UTC-05:00)	11.0 B	Standard

SUCCESSFULLY EDITED BUCKET POLICY

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](#)

```
{ "Version": "2012-10-17", "Id": "Policy1713553409574", "Statement": [ { "Sid": "Stmt1713553378926", "Effect": "Allow", "Principal": "*", "Action": "s3:", "Resource": [ "arn:aws:s3:::data-bucket-014c6d3497022aafe", "arn:aws:s3:::data-bucket-014c6d3497022aafe/*" ] }, {"Condition": { "ArnEquals": { "aws:PrincipalArn": [ "arn:aws:iam:902743396461:user/paulo", "arn:aws:iam:902743396461:user/sofia", "arn:aws:iam:902743396461:role/vocabs" ] } } } ] }
```

Object Ownership [Info](#)

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

Object Ownership [Edit](#)

Bucket owner enforced

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

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

Objects (1) [Info](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Name	Type	Last modified	Size	Storage class
myfile-014c6d3497022aafe.txt	txt	April 19, 2024, 13:54:26 (UTC-05:00)	11.0 B	Standard

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

The screenshot shows the AWS S3 console with the URL us-east-1.console.aws.amazon.com/s3/buckets/aws-config-014c6d3497022aafe?region=us-east-1&bucketType=general&tab=objects. The left sidebar is expanded, showing 'Buckets' and other options like 'Access Grants' and 'Storage Lens'. The main content area shows a single object in the 'Objects' table. A prominent red box highlights an error message: 'Insufficient permissions to list objects. After you or your AWS administrator has updated your permissions to allow the s3>ListBucket action, refresh the page. Learn more about Identity and access management in Amazon S3'.

This screenshot is identical to the one above, showing the AWS S3 console with the same URL and configuration. It displays a single object in the 'Objects' table and features a red box around the 'Insufficient permissions to list objects' error message.

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

Successfully edited Bucket Versioning
To transition, archive, or delete older object versions, configure lifecycle rules for this bucket.

Amazon S3 > Buckets > data-bucket-014c6d3497022aafe

data-bucket-014c6d3497022aafe [Info](#)

Objects **Properties** Permissions Metrics Management Access Points

Bucket overview

AWS Region US East (N. Virginia) us-east-1	Amazon Resource Name (ARN) arn:aws:s3:::data-bucket-014c6d3497022aafe	Creation date April 19, 2024, 13:53:53 (UTC-05:00)
---	--	---

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

Bucket Versioning
Enabled
Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Tags (0) [Edit](#)
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

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

Successfully edited server access logging.

Name	Status	Scope	Days until transition to Archive Access	Days until transition to Deep Archive
No archive configurations No configurations to display.				

Create configuration

Server access logging [Edit](#)
Log requests for access to your bucket. Use CloudWatch to check the health of your server access logging. [Learn more](#)

Server access logging Enabled Destination bucket s3://s3-objects-access-log-014c6d3497022aafe	Log object key format data-bucket[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
--	--

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

Name	Access
No data events No data events to display.	

[Configure in CloudTrail](#)

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

```

{
  "Version": "2012-10-17",
  "Id": "S3-Console-Auto-Gen-Policy-1713552356580",
  "Statement": [
    {
      "Sid": "S3PolicyStmt-DO-NOT-MODIFY-1713552356133",
      "Effect": "Allow",
      "Principal": {
        "Service": "logging.s3.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arnaws:s3:::s3-objects-access-log-014c6d3497022aafe/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "902743596461"
        }
      }
    }
  ]
}

```

Object Ownership [Info](#)

Task 1.3: Implement the S3 Inventory feature on a bucket

Inventory configurations (1) [Info](#)

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

Name	Status	Scope	Destination	Frequency	Last export	Format
Inventory	Enabled	Entire bucket	s3://s3-inventory-014c6...	Daily	-	Apache Parquet

Task 1.4: Confirm that versioning works as intended

A screenshot of the AWS S3 console. The URL is <https://us-east-1.console.aws.amazon.com/s3/buckets/data-bucket-014c6d3497022aafe?region=us-east-1&bucketType=general&tab=objects>. The page shows the 'data-bucket-014c6d3497022aafe' bucket. Under the 'Objects' tab, there are two items: 'customers.csv' (CSV file, 202.0 B, Standard storage class, last modified April 19, 2024, 14:15:43 UTC-05:00) and 'myfile-014c6d3497022aafe.txt' (TXT file, 11.0 B, Standard storage class, last modified April 19, 2024, 13:54:26 UTC-05:00). The interface includes standard AWS navigation and search bars at the top.A screenshot of the AWS S3 console showing the details for the 'customers.csv' object. The URL is <https://us-east-1.console.aws.amazon.com/s3/object/data-bucket-014c6d3497022aafe?region=us-east-1&bucketType=general&prefix=customers.csv&tab=details>. The page displays various settings for the object: Object Lock retention mode is set to 'Disabled'; Default retention period is set to 'None'; Storage class is 'Standard'; Server-side encryption settings show 'Encryption type: SSE-S3'; Additional checksums are off; and Tags are listed as '(0)'. The object has an expiration date of April 19, 2024, 14:15:43 UTC-05:00.

customers.csv - Object in S3

us-east-1.console.aws.amazon.com/s3/object/data-bucket-014c6d3497022aafe?region=us-east-1&bucketType=general&prefix=customers.csv&tab=versions

Incognito (2)

Amazon S3 > Buckets > data-bucket-014c6d3497022aafe > customers.csv

customers.csv Info

Properties | Permissions | **Versions**

Versions (2)

Version ID	Type	Last modified	Size	Storage class
FxSEA4b621kYQtdjTltye45BjQLaWqY (Current version)	csv	April 19, 2024, 14:17:39 (UTC-05:00)	322.0 B	Standard
2Vuk0aPVXibc9KrkRvvNyKaZBn_2HKea	csv	April 19, 2024, 14:15:43 (UTC-05:00)	202.0 B	Standard

customers.csv - Object in S3

us-east-1.console.aws.amazon.com/s3/object/data-bucket-014c6d3497022aafe?region=us-east-1&bucketType=general&prefix=customers.csv&tab=versions

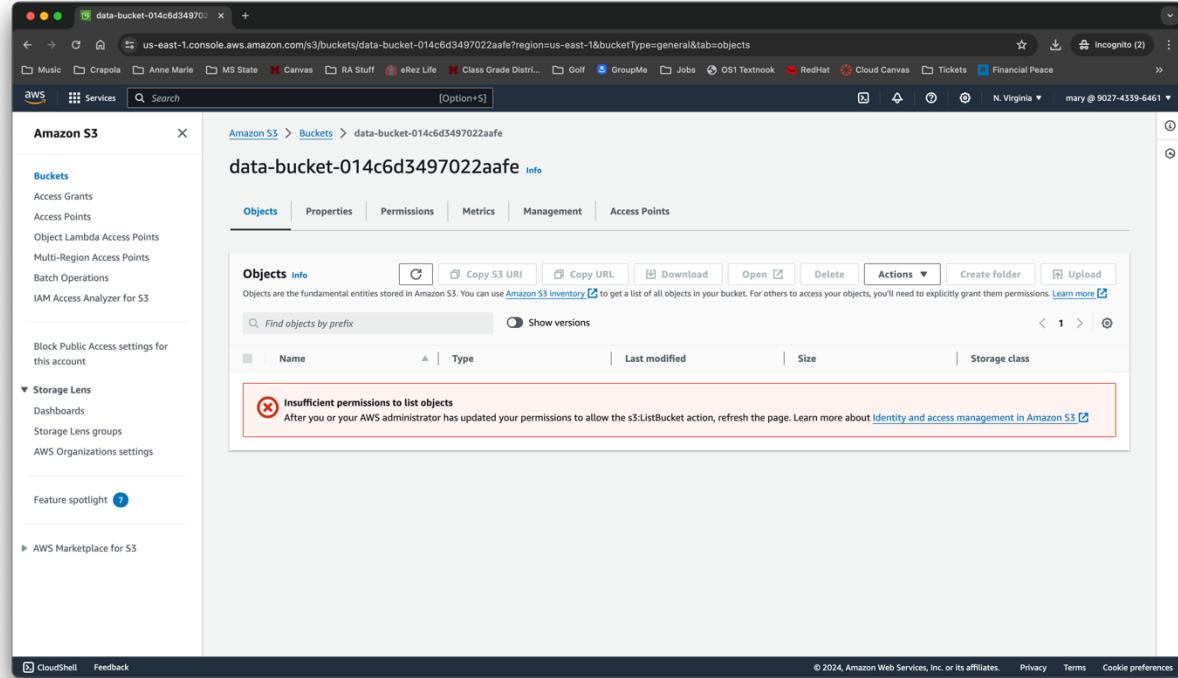
Amazon S3 > Buckets > data-bucket-014c6d3497022aafe > customers.csv

customers.csv Info

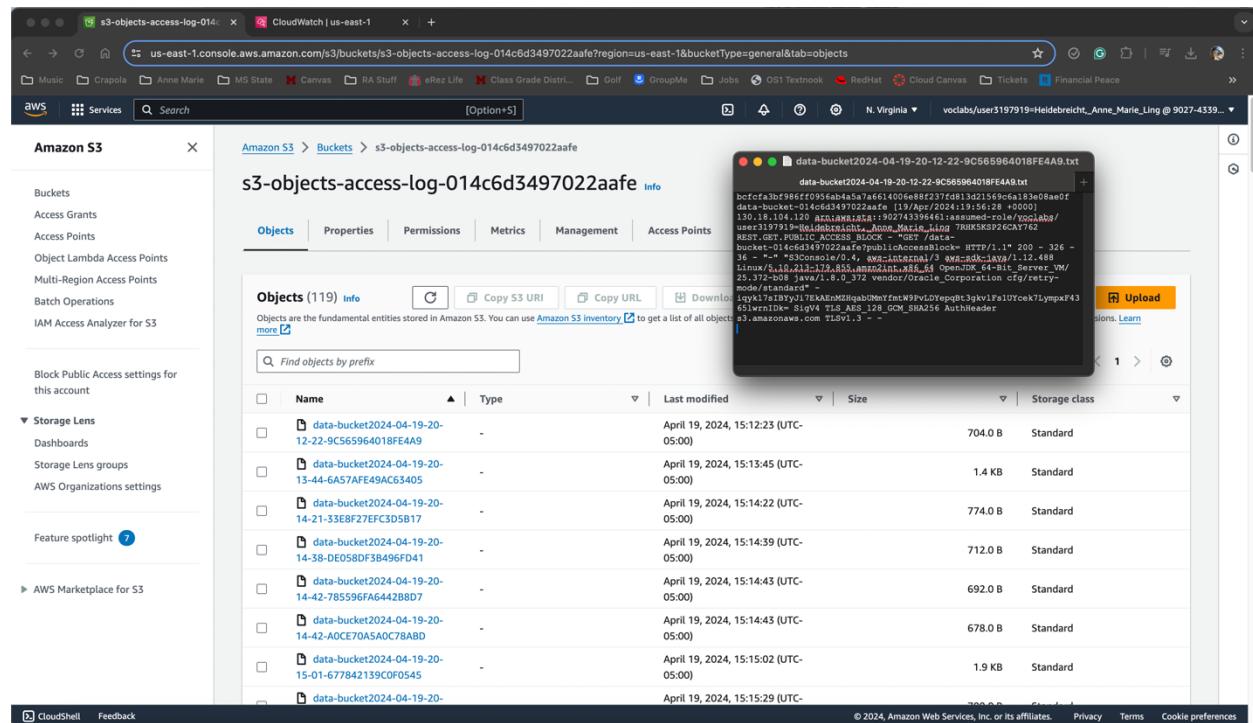
Properties | Permissions

Versions (1/2)

Version ID	Type	Last modified	Size	Storage class
FxSEA4b621kYQtdjTltye45BjQLaWqY (Current version)	csv	April 19, 2024, 14:17:39 (UTC-05:00)	322.0 B	Standard
2Vuk0aPVXibc9KrkRvvNyKaZBn_2HKea	csv	April 19, 2024, 14:15:43 (UTC-05:00)	202.0 B	Standard



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



The screenshot shows the AWS S3 console interface. On the left, the navigation pane includes 'Amazon S3' (selected), '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' (expanded), 'Dashboards', 'Storage Lens groups', 'AWS Organizations settings', 'Feature spotlight' (with a blue notification badge), and 'AWS Marketplace for S3'. The main content area displays an 'Account snapshot' for 'All AWS Regions' last updated on April 18, 2024. It shows 'Total storage' at 676.0 B, 'Object count' at 3, and 'Average object size' at 225.3 B. A note says you can enable advanced metrics in the 'default-account-dashboard' configuration. Below this, there are tabs for 'General purpose buckets' (selected) and 'Directory buckets'. A search bar at the top right allows finding buckets by name. The 'General purpose buckets' section lists six buckets: 'athena-results-20202024', 'aws-config-014c6d5497022aafe', 'cloudtrail-logs-014c6d5497022aafe', 'data-bucket-014c6d5497022aafe', 's3-inventory-014c6d5497022aafe', and 's3-objects-access-log-014c6d5497022aafe'. Each bucket entry includes its name, AWS Region (US East (N. Virginia) us-east-1), IAM Access Analyzer link, and Creation date.

Name	AWS Region	IAM Access Analyzer	Creation date
athena-results-20202024	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 19, 2024, 14:33:49 (UTC-05:00)
aws-config-014c6d5497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 10:34:16 (UTC-05:00)
cloudtrail-logs-014c6d5497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 10:34:16 (UTC-05:00)
data-bucket-014c6d5497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 19, 2024, 13:53:53 (UTC-05:00)
s3-inventory-014c6d5497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 10:34:16 (UTC-05:00)
s3-objects-access-log-014c6d5497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 10:34:16 (UTC-05:00)

The screenshot shows the Amazon Athena Query editor interface. On the left, the navigation pane includes sections for Query editor, Jobs, Administration, and more. The main area displays a SQL query in the Data tab:

```
1 | SELECT * FROM "default"."bucket_logs" limit 10;
```

The results section shows 10 rows of data from the 'bucket_logs' table:

#	bucketowner	bucket_name	requestdatein
1	bfcfa3bf986ff0956ab4a5a7a661400e88f237fd813d21569c5a183e08ae0f	data-bucket-014c6d3497022aafe	19/Apr/2024:1

At the bottom, it indicates a total of 6.89 KB of data scanned.

The screenshot shows the Amazon Athena Query editor interface. The results section displays 6 rows of data from the 'customers' table:

#	requester	operation	key	httpstatus
1	arn:aws:iam::902743396461:user/paulo	REST.HEAD.OBJECT	customers.csv	200
2	arn:aws:iam::902743396461:user/paulo	REST.HEAD.OBJECT	customers.csv	200
3	arn:aws:iam::902743396461:user/paulo	REST.GET.BUCKETVERSIONS	-	200
4	arn:aws:iam::902743396461:user/paulo	REST.GET.BUCKET	-	200
5	arn:aws:iam::902743396461:user/paulo	REST.GET.OWNERSHIP_CONTROLS	-	200

At the bottom, it indicates a total of 126.75 KB of data scanned.

Task 1.6: Review the S3 Inventory report using S3 Select

The screenshot shows the AWS S3 console interface. The left sidebar has sections like Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Storage Lens, AWS Marketplace for S3, and Feature spotlight. The main area shows a bucket structure: Amazon S3 > Buckets > s3-inventory-014c6d3497022aafe > data-bucket-014c6d3497022aafe/ > inventory/ > data/. The 'Objects' tab is selected, showing a table with one item:

Name	Type	Last modified	Size	Storage class
67a628f3-8982-48a0-a2a7-252fbddc5a77.parquet	parquet	April 20, 2024, 05:28:50 (UTC-05:00)	2.7 KB	Standard

The screenshot shows the AWS S3 console interface with the same sidebar as the first screenshot. The main area displays a SQL query window and its results. The query is:

```
SELECT * FROM s3object $ LIMIT 5
```

The results section shows:

Status
Successfully returned 3 records in 651 ms
Bytes returned: 879 B

```
1 {
2   "bucket": "data-bucket-014c6d3497022aafe",
3   "key": "customers.csv",
4   "version_id": "fxSEMb621kYQttdjTitye458JQLoWqY",
5   "is_latest": true,
6   "is_delete_marker": false,
7   "size": 302,
8   "last_modified_date": "2024-04-19T19:17:39.000Z",
9   "is_multipart_uploaded": false,
10  "encryption_status": "SSE-S3",
11  "bucket_key_status": "DISABLED"
12 }
13 {
14   "bucket": "data-bucket-014c6d3497022aafe",
15   "key": "customers.csv",
16   "version_id": "fXuKukdPWXlbc9KrRvNyKaZBn_2hKea",
17   "is_latest": false,
18   "is_delete_marker": false,
19   "size": 202,
20   "last_modified_date": "2024-04-19T19:15:43.000Z",
21   "is_multipart_uploaded": false,
22   "encryption_status": "SSE-S3",
23   "bucket_key_status": "DISABLED"
24 }
25 }
```

```

12 }
13 [
14   {
15     "bucket": "data-bucket-014c6d3497022aafe",
16     "key": "customer.csv",
17     "version_id": "2Vu0k0PVXkb3KrkRvvNyKaZBn_2HKeo",
18     "is_latest": false,
19     "is_delete_marker": false,
20     "size": 182,
21     "last_modified_date": "2024-04-19T19:15:43.000Z",
22     "is_multipart_uploaded": false,
23     "encryption_status": "SSE-S3",
24     "bucket_key_status": "DISABLED"
25   },
26   {
27     "bucket": "data-bucket-014c6d3497022aafe",
28     "key": "customer.txt",
29     "is_latest": true,
30     "is_delete_marker": false,
31     "size": 11,
32     "last_modified_date": "2024-04-19T18:54:26.000Z",
33     "is_multipart_uploaded": false,
34     "encryption_status": "SSE-S3",
35     "bucket_key_status": "DISABLED"
36   }
]

```

Phase 2 – Securing VPCs

Task 2.1: Review LabVPC and its associated resources

Your VPCs (1/3) Info

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table
-	vpc-0b0234ed8aa6f227c	Available	172.31.0.0/16	-	dopt-0ff626a172c07f29e	rtb-0d
NetworkFirewallVPC	vpc-06fb0cd520ceeb5	Available	10.1.0.0/16	-	dopt-0ff626a172c07f29e	rtb-0d
LabVPC	vpc-0f24a5830170545c8	Available	10.1.0.0/16	-	dopt-0ff626a172c07f29e	rtb-03

vpc-0f24a5830170545c8 / LabVPC

Resource map

- VPC Show details**: Your AWS virtual network
- Subnets (1)**: Subnets within this VPC
 - us-east-1a
 - WebServerSubnet
- Route tables (1)**: Route network traffic to resources
 - rtb-03cd698dda2c864af
- Network connections (1)**: Connections to other networks
 - LabVPCIG

Screenshot of the AWS IAM VPC Flow Log Role Permissions page.

Identity and Access Management (IAM)

VPCFlowLogRole | IAM

Last activity: April 16, 2024, 10:33 (UTC-05:00)

Maximum session duration: 1 hour

Permissions

Permissions policies (1) Info

You can attach up to 10 managed policies.

Filter by Type

Policy name: VPCFlowLogPolicy

Type: Customer inline

Attached entities: 0

VPCFlowLogPolicy

```

1: {
2:   "Statement": [
3:     {
4:       "Action": [
5:         "logs:CreateLogGroup",
6:         "logs:CreateLogStream",
7:         "logs:Describe*",
8:         "logs:PutLogEvents"
9:       ],
10:      "Resource": "*",
11:      "Effect": "Allow"
12:    }
13:  ]
14: }

```

Actions

Add permissions

CloudShell Feedback

Screenshot of the AWS EC2 Instances page.

EC2 Dashboard

Instances

Instances

Instances Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity

Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volume

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

IMDSv2

Instances (1/3) Info

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
WebServer	i-026f007f2edf78dbd	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-54-172-231-76.co...	54.172.231.76
WebServer2	i-0710082fb096f8c7e	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-54-81-69-213.com...	54.81.69.213
aws-cloud9-Cl...	i-09cf60e98587056	Running	t2.micro	2/2 checks passed	View alarms	us-east-1c	ec2-44-205-118-188.co...	44.205.118.188

Instance: i-026f007f2edf78dbd (WebServer)

Details

Instance summary

Instance ID	Public IPv4 address	Private IPv4 addresses
i-026f007f2edf78dbd (WebServer)	54.172.231.76 [open address]	10.1.3.4
IPv6 address	Instance state	Public IPv4 DNS
-	Running	ec2-54-172-231-76.compute-1.amazonaws.com [open address]
Hostname type	Private IP DNS name (IPv4 only)	Elastic IP addresses
IP name: ip-10-1-3-4.ec2.internal	ip-10-1-3-4.ec2.internal	54.172.231.76 [WebServerEIP] [Public IP]
Answer private resource DNS name	Instance type	AWS Compute Optimizer finding
-	t2.micro	Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address	VPC ID	Auto Scaling Group name
-	vpc-0f24a5830170545c8 (LabVPC)	-
IAM Role	Subnet ID	
WebServerRole	subnet-059aaada2d4ac9dfc (WebServerSubnet)	

CloudShell Feedback

Instances (1/3) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
WebServer	i-026f007f2edf78dbd	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-54-172-231-76.co...	54.172.231.76...
WebServer2	i-0710082fb96f8c7e	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-54-81-69-213.com...	54.81.69.213
aws-cloud9-Cl...	i-0c9ccf60e98587056	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1c	ec2-44-205-118-188.co...	44.205.118.188

Instance: i-026f007f2edf78dbd (WebServer)

Security details

IAM Role	WebServerRole	Owner ID	902743396461
Security groups	sg-01d1cccd231b9c051 (WebServerSecurityGroup)	Launch time Fri Apr 19 2024 13:43:10 GMT-0500 (Central Daylight Time)	

Inbound rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
-	sgr-027bd894bfec3be16	8080	TCP	0.0.0.0/0	WebServerSecurityGroup	-

Outbound rules

Name	Port range	Protocol	Destination	Description
-	-	-	-	-

Task 2.2: Create a VPC flow log

Your VPCs (1/3) Info

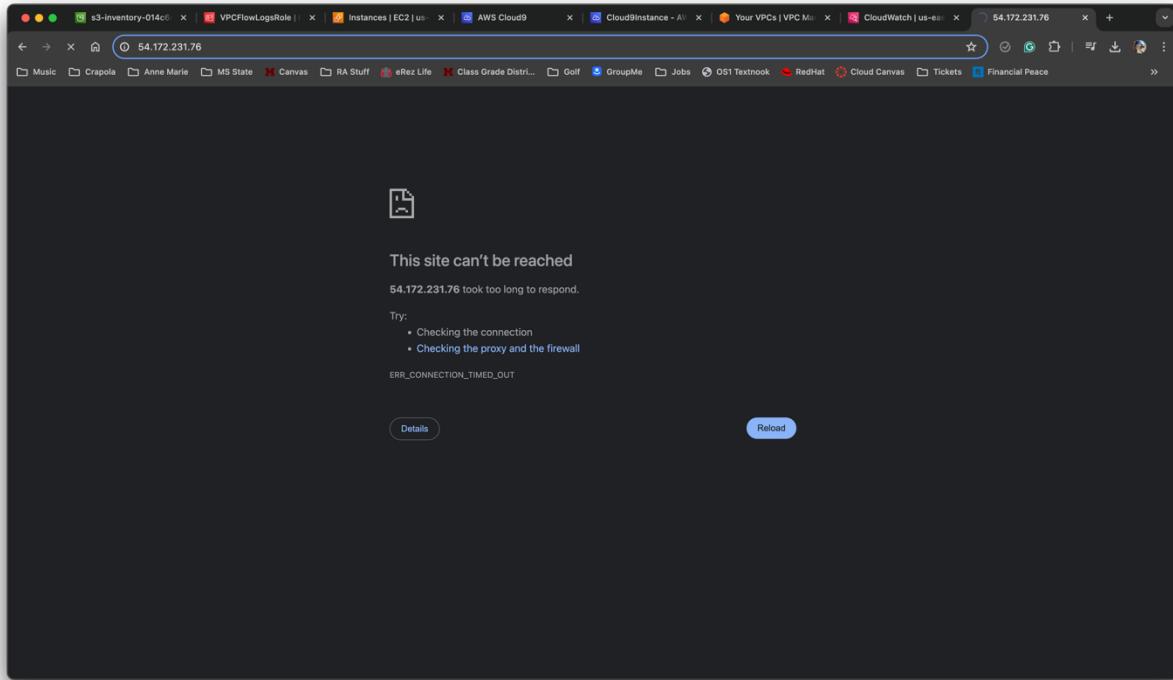
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main r...
-	ypc-0b0234ed8aa6f227c	Available	172.31.0/16	-	dopt-Off626a172c07f29e	rtb-0d...
NetworkFirewallVPC	ypc-06afb0cd520cedbb5	Available	10.1.0/16	-	dopt-Off626a172c07f29e	rtb-0d...
LabVPC	ypc-0f24a5830170545c8	Available	10.1.0/16	-	dopt-Off626a172c07f29e	rtb-03...

vpc-0f24a5830170545c8 / LabVPC

Flow logs (1) Info

Name	Flow log ID	Filter	Destination type	Destination name	IAM role ARN
LabVPCFlowLogs	fl-003aad52a44f45f89	ALL	cloud-watch-logs	LabVPCFlowLogs	arn:aws:iam::9...

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



```
voclabs:~/environment $ nc -vz 54.172.231.76 80
nc: connect to 54.172.231.76 port 80 (tcp) failed: Connection timed out
voclabs:~/environment $ nc -vz 54.172.231.76 22
nc: connect to 54.172.231.76 port 22 (tcp) failed: Connection timed out
voclabs:~/environment $ 
```

A screenshot of the AWS CloudWatch Log Events interface. The left sidebar shows navigation options like CloudWatch, Favorites and recents, Dashboards, Alarms, Logs (selected), Log groups, Log Anomalies, Live Tail, Logs Insights, Metrics, X-Ray traces, Events, Application Signals, Network monitoring, and Insights. The main content area shows a list of log events for the log group "LabVPCFlowLogs" with the log stream "eni-06986621cef57b487-all". The log entries are timestamped and show various network-related messages, such as "REJECT OK" and "REJECT 0K". A filter bar at the top allows searching for specific terms.

The screenshot shows the AWS CloudWatch Log Events interface. The left sidebar is collapsed, showing the CloudWatch navigation bar with 'Log groups' selected. The main content area displays a table of log events under the heading 'Log events'. The table has two columns: 'Timestamp' and 'Message'. The first log entry is:

Timestamp	Message
2024-04-19T16:06:02.000-05:00	Z 982743396461 eni-06986621cef57b487 44.205.118.188 10.1.3.4 52414 80 6 6 360 1713560762 1713560818 REJECT OK

There are four more log entries below it, all with similar timestamps and message patterns.

This screenshot is identical to the one above, but the search bar at the top of the log table contains the IP address '130.18.104.12'. The log table shows the same five log entries as the previous screenshot, but the context indicates a filtered view where only logs matching the IP '130.18.104.12' are displayed.

Task 2.4: Configure the route table and security group settings

The screenshot shows the AWS VPC Route Table Details page for route table ID `rtb-03cd698dda2c864af`. A green banner at the top indicates that routes have been successfully updated. The main table displays two routes:

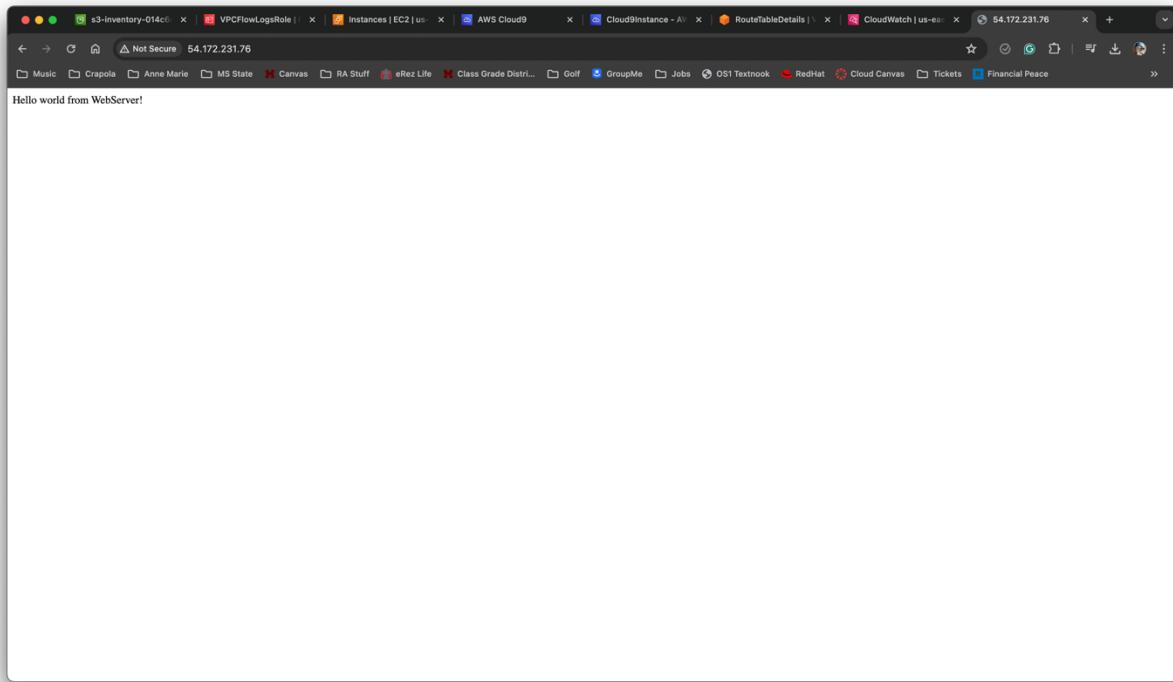
Destination	Target	Status	Propagated
<code>0.0.0.0/0</code>	<code>igw-014c6d3497022aafe</code>	Active	No
<code>10.1.0.16</code>	local	Active	No

```
voclabs:~/environment $ nc -vz 54.172.231.76 80
nc: connect to 54.172.231.76 port 80 (tcp) failed: Connection timed out
```

The screenshot shows the AWS Security Group Inbound Rules page for security group `sg-01d1ccdc231b9c051 - WebServerSecurityGroup`. The table lists three inbound rules:

Security group rule...	IP version	Type	Protocol	Port range	Source	Description
<code>sgr-016516b18f6564c8f</code>	IPv4	HTTP	TCP	<code>80</code>	<code>0.0.0.0/0</code>	HTTP from anywhere
<code>sgr-0bd9461c05f9a6591</code>	IPv4	SSH	TCP	<code>22</code>	<code>18.206.107.24/29</code>	SSH to allow EC2 Insta...
<code>sgr-01ef5321a98ec8a5de</code>	IPv4	SSH	TCP	<code>22</code>	<code>44.205.118.188/32</code>	SSH from Cloud9

```
voclabs:~/environment $ nc -vz 54.172.231.76 22
Connection to 54.172.231.76 22 port [tcp/ssh] succeeded!
```



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

[ec2-user@webserver ~]$ ping -c 3 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (3.162.118.164) 56(84) bytes of data.
64 bytes from server-3-162-118-164.iad61.r.cloudfront.net (3.162.118.164): icmp_seq=1 ttl=249 time=1.37 ms
64 bytes from server-3-162-118-164.iad61.r.cloudfront.net (3.162.118.164): icmp_seq=2 ttl=249 time=1.47 ms
64 bytes from server-3-162-118-164.iad61.r.cloudfront.net (3.162.118.164): icmp_seq=3 ttl=249 time=1.42 ms

--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.365/1.418/1.466/0.041 ms
[ec2-user@webserver ~]$
```

i-026f007f2edf78dbd (WebServer)
PublicIPs: 54.172.231.76 PrivateIPs: 10.1.3.4

Task 2.5: Secure the WebServerSubnet with a network ACL

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

VPC > Network ACLs > acl-091ec911c24e561ef

acl-091ec911c24e561ef

Details Info

Associated with subnet-059aaada2d4ac9dfc / WebServerSubnet Default Yes VPC ID vpc-0f24a5830170545c8 / LabVPC

Owner 902743396461

Inbound rules (2)

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

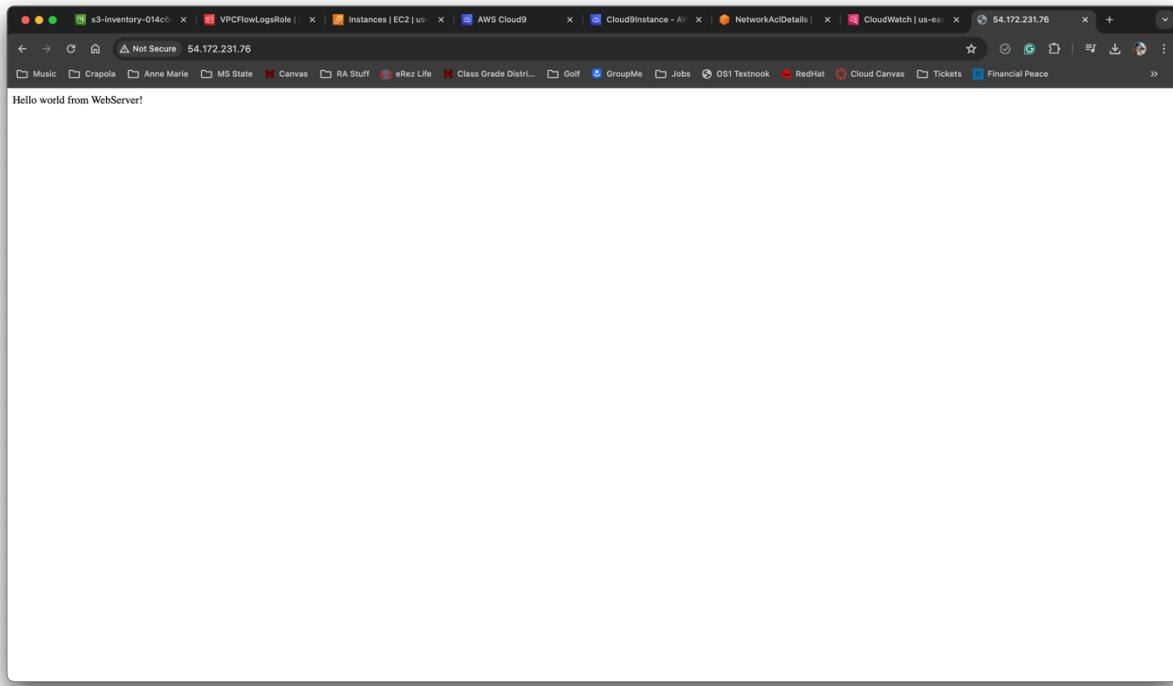
```
voclabs:~/environment $ nc -vz 54.172.231.76 22
nc: connect to 54.172.231.76 port 22 (tcp) failed: Connection timed out
```

This site can't be reached
54.172.231.76 took too long to respond.
Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_TIMED_OUT

```
voclabs:~/environment $ nc -vz 54.172.231.76 22
Connection to 54.172.231.76 22 port [tcp/ssh] succeeded!
```



Task 2.6: Review NetworkFirewallVPC and its associated resources

A screenshot of the AWS VPC console. The left sidebar shows various VPC-related services like VPC dashboard, EC2 Global View, Virtual private cloud, Security, DNS firewall, and CloudShell. The main content area shows a success message: 'You have successfully updated inbound rules for act-091ec911c24e561ef'. Below this, the 'Your VPCs (1/3) Info' table lists three VPCs: NetworkFirewallVPC (selected), LabVPC, and another unnamed VPC. The 'Resource map' section shows the network topology: NetworkFirewallVPC contains Subnets (FirewallSubnet, WebServer2Subnet) which are connected to Route tables (rtb-0d2624910c09aa260) which in turn connect to Network connections (NetworkFirewallIG).

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main r
-	vpc-0b0234ed8aa6f227c	Available	172.31.0.0/16	-	dopt-Off626a172c07f29e	rtb-0d
NetworkFirewallVPC	vpc-06afb0cd520cedbb5	Available	10.1.0.0/16	-	dopt-Off626a172c07f29e	rtb-0d
LabVPC	vpc-0f74a5830170545c8	Available	10.1.0.0/16	-	dopt-Off626a172c07f29e	rtb-03

Screenshot of the AWS VPC Network ACL Details page for Network ACL ID: acl-0297541ca6c015140.

Details

Network ACL ID	acl-0297541ca6c015140	Associated with	2 Subnets
Owner	902743396461	Default	Yes
VPC ID vpc-06afb0cd520cedbb5 / NetworkFirewallVPC			

Inbound rules (2)

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

Screenshot of the AWS EC2 Instances page showing two running instances: WebServer and WebServer2.

Instances (1/3) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv
WebServer	i-026f007f2edf78dbd	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-54-172-231-76.co...	54.172.231.76
WebServer2	i-0710082fb96f8c7e	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-54-81-69-213.com...	54.81.69.213

Instance: i-0710082fb96f8c7e (WebServer2)

Networking

Public IPv4 address	54.81.69.213 [open address]	Private IPv4 addresses	10.1.3.4
Public IPv4 DNS	ec2-54-81-69-213.compute-1.amazonaws.com [open address]	Private IP DNS name (IPv4 only)	ip-10-1-3-4.ec2.internal
Subnet ID	subnet-0633fee724e0b8649 (WebServer2Subnet)	IPV6 addresses	-
Availability zone	us-east-1a	Carrier IP addresses (ephemeral)	-
Use RBN as guest OS hostname	Disabled	Answer RBN DNS hostname IPv4	Disabled

The screenshot shows the AWS EC2 Instances page. The left sidebar includes links for EC2 Dashboard, EC2 Global View, Events, Console-to-Code, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity, Reservations (New), Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Security Groups, Elastic IPs, Placement Groups, CloudShell, and Feedback.

The main content displays the 'Instances (1/3) Info' section. It lists two instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IP
WebServer	i-026f007f2edf78dbd	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-54-172-231-76.co...	54.172.23
WebServer2	i-0710082fb96f8c7e	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-54-81-69-213.com...	54.81.69.

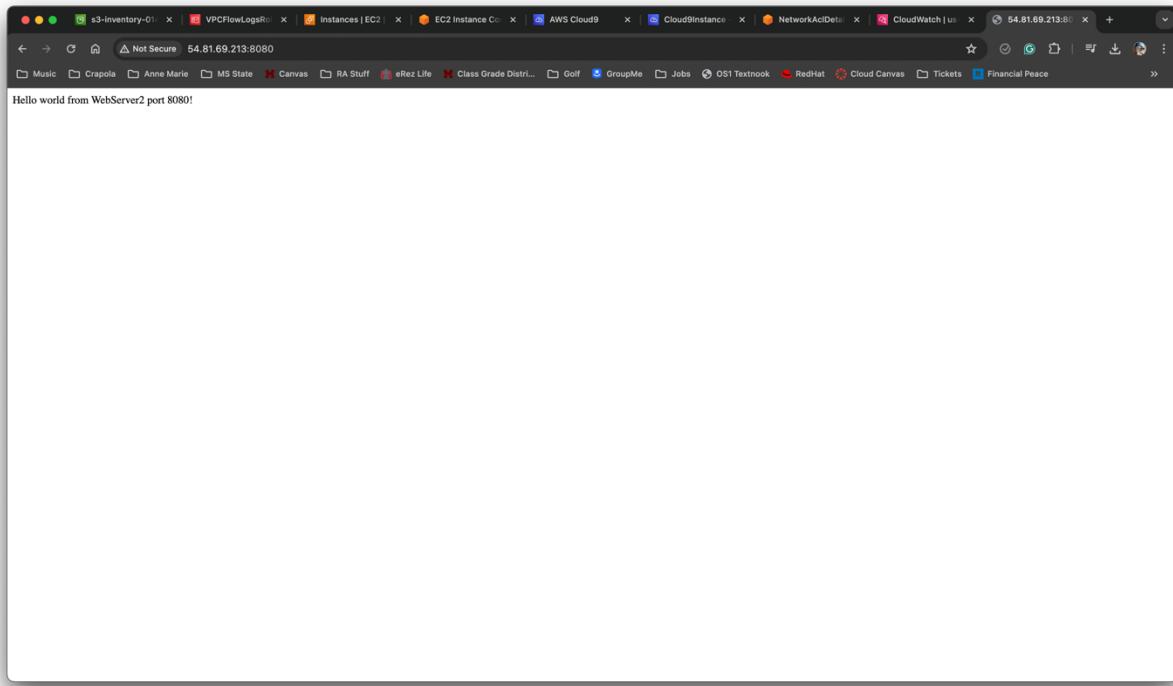
The 'Instance: i-0710082fb96f8c7e (WebServer2)' details page is shown. It includes tabs for Details, Status and alarms (New), Monitoring, Security (selected), Networking, Storage, and Tags. Under Security details, it shows an IAM Role (WebServerRole) and Owner ID (902743396461). Under Inbound rules, it shows three security group rule entries:

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
-	sgr-0fd055fcc7c074a7	8080	TCP	0.0.0.0/0	WebServer2SecurityGroup	-
-	sgr-0aded54143509880f	22	TCP	0.0.0.0/0	WebServer2SecurityGroup	-
-	sgr-0439dbc07ca67fd0	80	TCP	0.0.0.0/0	WebServer2SecurityGroup	-

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

The screenshot shows a web browser window with the URL 54.81.69.213. The page content is "Hello world from WebServer2!". The browser's address bar shows "Not Secure" and the IP address 54.81.69.213. The top navigation bar includes links for Music, Crapola, Anne Marie, MS State, Canvas, RA Stuff, eRez Life, Class Grade Distr..., Golf, GroupMe, Jobs, OS1 Textbook, RedHat, Cloud Canvas, Tickets, Financial Peace, and a feedback link.

```
voclabs:~/environment $ nc -vz 54.81.69.213 22
Connection to 54.81.69.213 22 port [tcp/ssh] succeeded!
```



Task 2.7: Create a network firewall

A screenshot of the AWS VPC Network Firewall interface. The left sidebar shows navigation options like 'VPC dashboard', 'EC2 Global View', and 'Virtual private cloud' (with 'Your VPCs' selected). The main content area is titled 'Firewalls' and shows a table with one entry: 'NetworkFirewall' (Status: Ready, Configuration sync state: In sync). A 'Create firewall' button is visible at the top right of the table.

Task 2.8: Create route tables

Updated routes for rtb-08d73dfea79cbf92d / IGW-Ingress-Route-Table successfully

Details

VPC dashboard EC2 Global View Filter by VPC Select a 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

CloudShell Feedback

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTableDetails:RouteTableId=rtb-08d73dfea79cbf92d

VPC > Route tables > rtb-08d73dfea79cbf92d

rtb-08d73dfea79cbf92d / IGW-Ingress-Route-Table

Actions

Details Info

Route table ID	rtb-08d73dfea79cbf92d	Main	No	Explicit subnet associations	-	Edge associations	-
VPC	vpc-06afb0cd520cedbb5 NetworkFirewallVPC	Owner ID	902743396461				

Routes Subnet associations Edge associations Route propagation Tags

Both Edit routes < 1 > @

Routes (2)

Destination	Target	Status	Propagated
10.1.0.0/16	local	Active	No
10.1.3.0/28	vpc-083ca5ebce8838aca	Active	No

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

You have successfully updated edge associations for rtb-08d73dfea79cbf92d / IGW-Ingress-Route-Table.

VPC > Route tables > rtb-08d73dfea79cbf92d

rtb-08d73dfea79cbf92d / IGW-Ingress-Route-Table

Actions

Details Info

Route table ID	rtb-08d73dfea79cbf92d	Main	No	Explicit subnet associations	-	Edge associations	igw-0e8fe8d007428b875 / NetworkFirewallIG
VPC	vpc-06afb0cd520cedbb5 NetworkFirewallVPC	Owner ID	902743396461				

Routes Subnet associations Edge associations Route propagation Tags

Edit edge associations < 1 > @

Associated internet gateways (1)

ID	State	VPC	Owner
igw-0e8fe8d007428b875 / NetworkFirewallIG	Attached	vpc-06afb0cd520cedbb5	902743396461

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

Updated routes for rtb-0a725f5f4041a5ab8 / Firewall-Route-Table successfully

rtb-0a725f5f4041a5ab8 / Firewall-Route-Table

Details		Info	
Route table ID	rtb-0a725f5f4041a5ab8	Main	No
VPC	vpc-06afb0cd520ceddb5 NetworkFirewallVPC	Owner ID	902743396461
Explicit subnet associations			
Edge associations			

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0e8fe8d007428b875	Active	No
10.1.0.0/16	local	Active	No

You have successfully updated subnet associations for rtb-0a725f5f4041a5ab8 / Firewall-Route-Table.

rtb-0a725f5f4041a5ab8 / Firewall-Route-Table

Details		Info	
Route table ID	rtb-0a725f5f4041a5ab8	Main	No
VPC	vpc-06afb0cd520ceddb5 NetworkFirewallVPC	Owner ID	902743396461
Explicit subnet associations			
Edge associations			

Explicit subnet associations (1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
FirewallSubnet	subnet-0c0b59473bf995a58	10.1.0.0/28	-

Subnets without explicit associations (1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
WebServer2Subnet	subnet-0633fee724e0b8649	10.1.3.0/28	-

Updated routes for rtb-0e64cde4d149d5bbe / WebServer2-Route-Table successfully

Details

VPC > Route tables > rtb-0e64cde4d149d5bbe

rtb-0e64cde4d149d5bbe / WebServer2-Route-Table

Actions

Details Info

Route table ID	rtb-0e64cde4d149d5bbe	Main	No	Explicit subnet associations	Edge associations
VPC	vpc-06afb0cd520cedbb5 NetworkFirewallVPC	Owner ID	902743396461	-	-

Routes Subnet associations Edge associations Route propagation Tags

Both Edit routes

Filter routes

Destination	Target	Status	Propagated
0.0.0.0/0	vpc-083ca5ebce8838aca	Active	No
10.1.0.0/16	local	Active	No

CloudShell Feedback

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

You have successfully updated subnet associations for rtb-0e64cde4d149d5bbe / WebServer2-Route-Table.

VPC > Route tables > rtb-0e64cde4d149d5bbe

rtb-0e64cde4d149d5bbe / WebServer2-Route-Table

Actions

Details Info

Route table ID	rtb-0e64cde4d149d5bbe	Main	No	Explicit subnet associations	Edge associations
VPC	vpc-06afb0cd520cedbb5 NetworkFirewallVPC	Owner ID	902743396461	subnet-0633fee724e0b8649 / WebServer2Subnet	-

Routes Subnet associations Edge associations Route propagation Tags

Edit subnet associations

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
WebServer2Subnet	subnet-0633fee724e0b8649	10.1.0.0/28	-

Explicit subnet associations (1)

Subnets without explicit associations (0)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
-	-	-	-

No subnets without explicit associations

All your subnets are associated with a route table.

CloudShell Feedback

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

The screenshot shows the AWS VPC Route Tables page. On the left, there is a navigation sidebar with various VPC-related options like EC2 Global View, Filter by VPC, Virtual private cloud, Security, DNS firewall, and more. The main content area displays a table titled "Route tables (6) Info" with the following columns: Name, Route table ID, Explicit subnet associa..., Edge associations, Main, and VPC. The table lists six route tables, each associated with a specific VPC and some edge associations.

Name	Route table ID	Explicit subnet associa...	Edge associations	Main	VPC
-	rtb-0d2624910c09aa260	-	-	Yes	vpc-06afb0cd520cedbb5 NetworkFirewallVPC
-	rtb-03cd698ddac864af	-	-	Yes	vpc-0f24a5830170545cb LabVPC
-	rtb-0d95dd14055ee4580b	-	-	Yes	vpc-0b234ed8aa6f227c
IGW-Ingress-Route-Table	rtb-08d73dfa79cbf92d	-	igw-0e8fe8d00742...	No	vpc-06afb0cd520cedbb5 NetworkFirewallVPC
Firewall-Route-Table	rtb-0a725f5f4041a5ab8	subnet-0c0b59473bf995...	-	No	vpc-06afb0cd520cedbb5 NetworkFirewallVPC
WebServer2-Route-Table	rtb-0e64cd4d149d5bbe	subnet-0633fee724e0b8...	-	No	vpc-06afb0cd520cedbb5 NetworkFirewallVPC

Task 2.9: Configure logging for the network firewall

The screenshot shows the AWS CloudWatch Log Groups page. On the left, there is a navigation sidebar with options like Favorites and recents, Alarms, Logs (Log groups, Log Anomalies, Live Tail, Logs Insights), Metrics, X-Ray traces, Events, Application Signals, Network monitoring, and Insights. The main content area displays a table titled "Log groups (4)" with columns: Log group, Log class, Anomaly d..., Data protec..., Sensitive d..., Retention, and Metric filters. The table lists four log groups: Log group, /aws/lambda/c116924a2785851l643652t1-AdjustA..., /aws/lambda/c116924a2785851l643652t1-AdjustB..., LabVPCFlowLogs, and NetworkfirewallVPCLogs. The NetworkfirewallVPCLogs group has a retention period of 6 months.

Log group	Log class	Anomaly d...	Data protec...	Sensitive d...	Retention	Metric filters
Log group	Standard	Configure	-	-	Never expire	-
/aws/lambda/c116924a2785851l643652t1-AdjustA...	Standard	Configure	-	-	Never expire	-
/aws/lambda/c116924a2785851l643652t1-AdjustB...	Standard	Configure	-	-	Never expire	-
LabVPCFlowLogs	Standard	Configure	-	-	Never expire	-
NetworkfirewallVPCLogs	Standard	Configure	-	-	6 months	-

The screenshot shows the AWS VPC Network Firewall configuration page. A success message at the top states "You've successfully updated the firewall NetworkFirewall". The main content area displays the following details:

Resource name	Resource type	Availability Zone	Sync state
FirewallPolicy	Firewall policy	us-east-1a	In sync

Change protections

Delete protection	Enabled	Subnet change protection	Enabled
-------------------	---------	--------------------------	---------

Logging

Log type	Flow, Alert	Alert log destination	CloudWatch log group - NetworkFirewallVPCLogs	Flow log destination	CloudWatch log group - NetworkFirewallVPCLogs
----------	-------------	-----------------------	---	----------------------	---

Customer managed key

Key type	AWS owned key
----------	---------------

Firewall tags (0)

At the bottom, there are links for CloudShell and Feedback, along with standard footer links for 2024, Privacy, Terms, and Cookie preferences.

The screenshot shows a Google Chrome browser window with the address bar set to 54.81.69.213. The main content area displays the classic Google search page with the "Google" logo and a search bar. Below the search bar is a blue circular button with a white plus sign and the text "Add shortcut". In the bottom right corner of the browser window, there is a "Customize Chrome" button.

The screenshot shows the AWS CloudWatch Log Events interface. The left sidebar is collapsed, and the main area displays log events for the path `/aws/network-firewall/flow`. The first event is timestamped `2024-04-19T17:03:55.000-05:00` and contains detailed network traffic information, including source and destination IP addresses, ports, and protocol details. The second event is timestamped `2024-04-19T17:03:55.000-05:00` and also describes a network flow. The interface includes a search bar at the top, various filter and action buttons, and a detailed log view below.

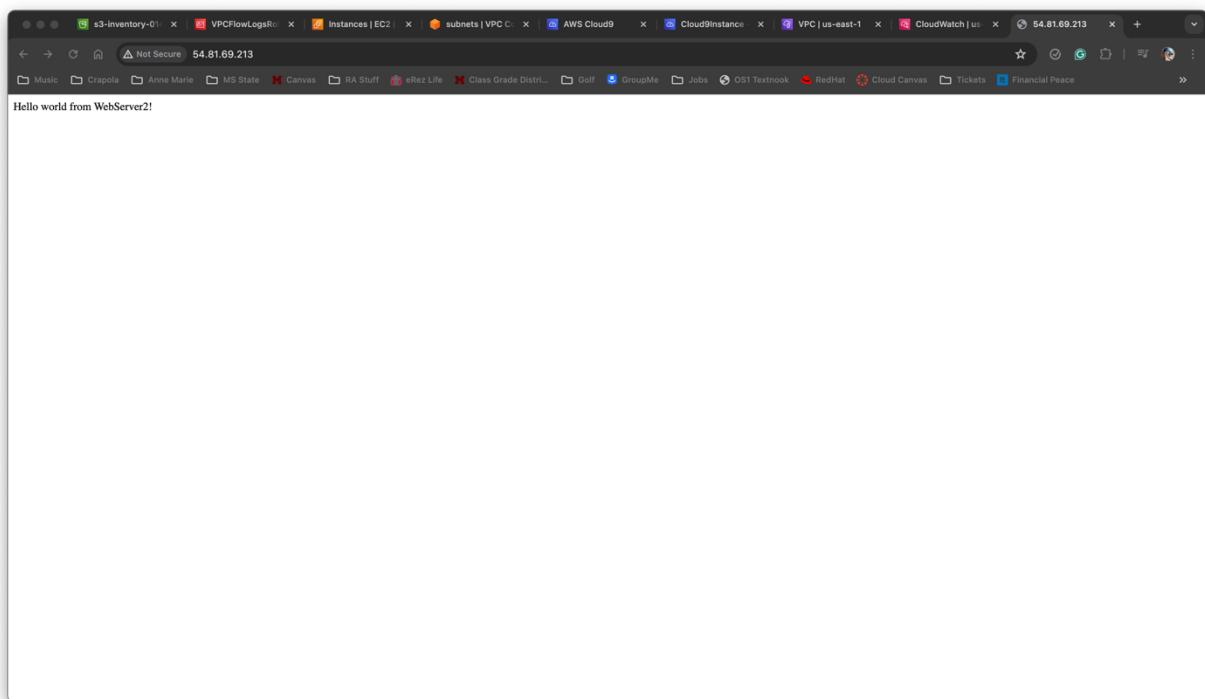
Task 2.10: Configure the firewall policy and test access

The screenshot shows the AWS Network Firewall Create And Add Rule Group wizard. The current step is "Forward". The "Action" section is set to "Pass". The "Rule options - optional" section is collapsed. Below, the "Rules (5)" table lists five rules:

Protocol	Source	Destination	Source port	Destination port	Direction	Action
TCP	ANY	ANY	ANY	8080	Forward	Drop
TCP	ANY	ANY	ANY	80	Forward	Pass
TCP	ANY	ANY	ANY	22	Forward	Pass
TCP	ANY	ANY	ANY	443	Forward	Pass
ICMP	ANY	ANY	ANY	ANY	Forward	Pass

At the bottom, there are "Cancel", "Previous", and "Next" buttons, along with copyright and legal links.

The screenshot shows the AWS Network Firewall VPC Rule Group creation interface. At the top, a success message says "You've successfully created rule group NetworkFirewallVPCRuleGroup". Below this, there's a table header for "Priority" and "Name" with a "Capacity" column. A note below the table says "No stateless rule groups" and "Choose Add rule groups to add stateless rule groups to the policy." Under "Stateful rule evaluation order and default actions", it shows "Rule order" and "Strict order" with "Default actions" set to "Drop established". In the "Stateful rule groups (1)" section, there's a table with columns "Priority", "Name", "Capacity", "Is managed?", and "Run in alert mode?". One entry is listed: "1" for Priority, "NetworkFirewallVPCRuleGroup" for Name, "100" for Capacity, "No" for Is managed?, and "Not available" for Run in alert mode?. Below this, two capacity units sections show "0/10000" and "100/50000". The bottom of the page includes standard AWS footer links.

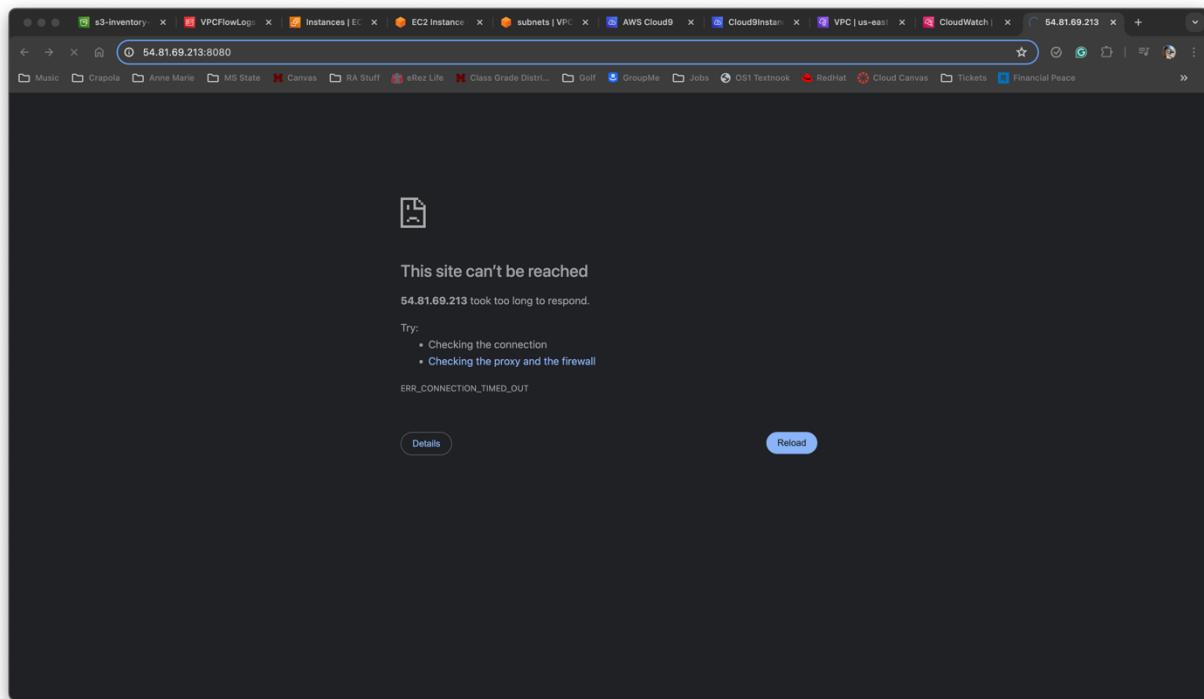


```
voclabs:~/environment $ nc -vz 54.81.69.213 22
Connection to 54.81.69.213 22 port [tcp/ssh] succeeded!
```

```
Last login: Fri Apr 19 21:35:43 2024 from 18.206.107.28
[ec2-user@webserver2 ~]$ ping -c 3 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (3.162.118.164) 56(84) bytes of data.
64 bytes from server-3-162-118-164.iad61.r.cloudfront.net (3.162.118.164): icmp_seq=1 ttl=247 time=3.42 ms
64 bytes from server-3-162-118-164.iad61.r.cloudfront.net (3.162.118.164): icmp_seq=2 ttl=247 time=1.85 ms
64 bytes from server-3-162-118-164.iad61.r.cloudfront.net (3.162.118.164): icmp_seq=3 ttl=247 time=1.95 ms

--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.846/2.403/3.416/0.717 ms
[ec2-user@webserver2 ~]$ sudo netstat -tulpn | grep -i listen
tcp        0      0 0.0.0.0:22          0.0.0.0:*          LISTEN      2291/sshd: /usr/sbi
tcp6       0      0 ::1:80           ::*:*              LISTEN      1954/httpd
tcp6       0      0 ::1:22           ::*:*              LISTEN      2291/sshd: /usr/sbi
[ec2-user@webserver2 ~]$ python3 -m http.server 8080 &
[1] 12146
[ec2-user@webserver2 ~]$ Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...

[ec2-user@webserver2 ~]$ sudo netstat -tulpn | grep -i listen
tcp        0      0 0.0.0.0:8080        0.0.0.0:*          LISTEN      12146/python3
tcp        0      0 0.0.0.0:22          0.0.0.0:*          LISTEN      2291/sshd: /usr/sbi
tcp6       0      0 ::1:80            ::*:*              LISTEN      1954/httpd
tcp6       0      0 ::1:22            ::*:*              LISTEN      2291/sshd: /usr/sbi
[ec2-user@webserver2 ~]$
```



The screenshot shows the AWS CloudWatch Log Groups interface. The left sidebar navigation includes CloudWatch, Favorites and recents, Dashboards, Alarms, Log groups, Metrics, X-Ray traces, Events, Application Signals, Network monitoring, and Insights. Under Log groups, 'Log groups' is expanded, showing Log Anomalies, Live Tail, and Logs Insights. The main content area displays log entries for 'NetworkFirewall'. One entry is expanded to show detailed fields such as 'firewall_name', 'availability_zone', 'event_timestamp', and various network parameters like 'src_ip', 'dst_ip', 'proto', and 'tcp_flags'. Other log entries are visible below it.

Phase 3 – Securing AWS resources

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

The screenshot shows the AWS KMS Customer managed keys interface. The left sidebar navigation includes Key Management Service (KMS), AWS managed keys, Customer managed keys, and Custom key stores (AWS CloudHSM key stores, External key stores). The main content area displays a success message: "Your AWS KMS key was created with alias MyKMSKey and key ID 31c3f5c3-cb39-4b26-89dd-ea1f6de9286a." Below this, a table lists the "Customer managed keys (1)". The table has columns for Aliases, Key ID, Status, Key type, Key spec, and Key usage. It shows one entry: "MyKMSKey" with Key ID "31c3f5c3-cb39-4b26-89dd-ea1f6de9286a", Status "Enabled", Key type "Symmetric", Key spec "SYMMETRIC_DEFAULT", and Key usage "Encrypt and decrypt".

The screenshot shows the AWS KMS console with a success message: "Successfully enabled automatic key rotation". The key details are as follows:

- Alias:** MyKMSKey
- Status:** Enabled
- ARN:** arn:aws:kms:us-east-1:902743396461:key/31c3f5c3-cb39-4b26-89dd-ea1f6de9286a
- Description:** -
- Creation date:** Apr 19, 2024 17:28 CDT
- Regionality:** Single Region

The "Key rotation" tab is selected, showing the following configuration:

- Status:** Enabled
- Rotation period:** 365 days
- Date of last automatic rotation:** -
- Next rotation date:** Apr 19, 2025

The "On-demand key rotation" section indicates 0 remaining rotations.

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

The screenshot shows the AWS KMS console with the key policy for 'MyKMSKey'. The policy document is as follows:

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "AWS",
            "Action": "kms:Decrypt",
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": "arn:aws:iam::902743396461:user/sofia",
            "Action": "kms:Decrypt",
            "Resource": "arn:aws:kms:us-east-1:902743396461:key/31c3f5c3-cb39-4b26-89dd-ea1f6de9286a"
        }
    ]
}

```

Type: Customer managed
Creation time: April 16, 2024, 10:33 (UTC-05:00)
Edited time: April 16, 2024, 10:33 (UTC-05:00)
ARN: arn:aws:iam::902743396461:policy/PolicyForFinancialAdvisors

Permissions defined in this policy

```

3-    "Statement": [
4-        {
5-            "Action": [
6-                "s3:GetAccountPublicAccessBlock",
7-                "s3:GetBucketAcl",
8-                "s3:GetBucketPolicyStatus",
9-                "s3:GetBucketPublicAccessBlock",
10-               "s3:GetObject",
11-               "s3:ListAccessPoints",
12-               "s3>ListAllMyBuckets",
13-               "s3>ListBucket",
14-               "s3:PutObject"
15-            ],
16-            "Resource": "*",
17-            "Effect": "Allow"
18-        },
19-        {
20-            "Action": [
21-                "kms:Encrypt",
22-                "kms:Decrypt"
23-            ]
24-        }
25-    ]
  
```

Copy | Edit | Summary | **JSON**

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

MFA Delete: Disabled

Tags (0)
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

Key	Value
No tags associated with this resource.	

Default encryption

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

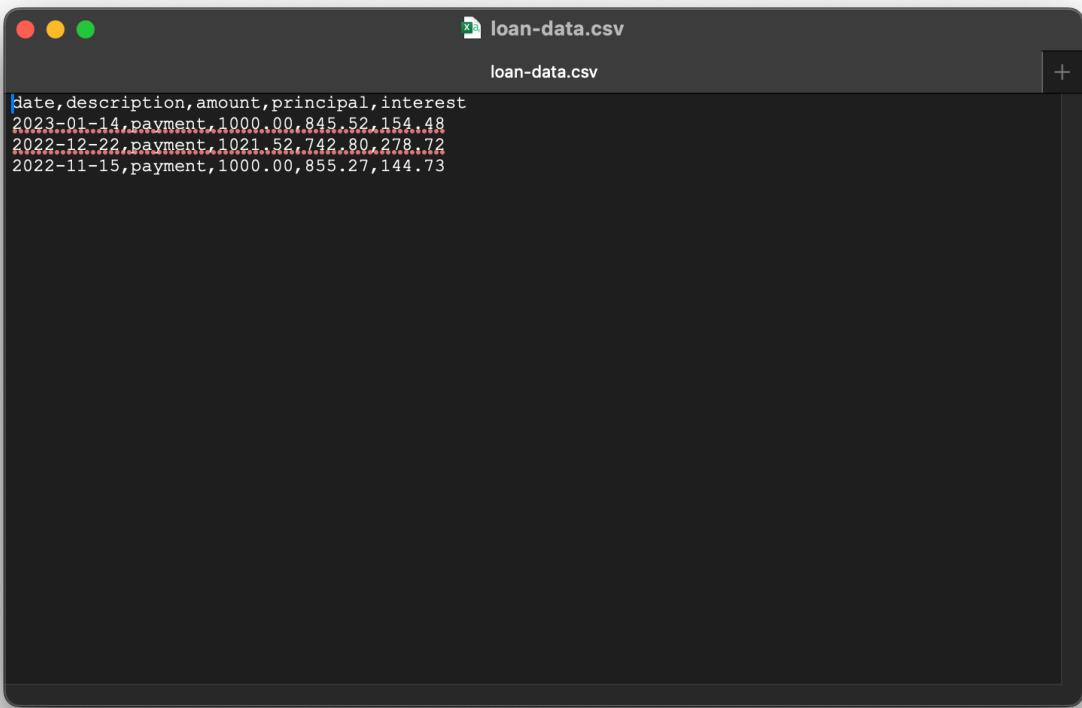
Encryption type: [Info](#)
Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Encryption key ARN: [arn:aws:kms:us-east-1:902743396461:key/31c3f5c3-cb39-4b26-89dd-ea1f6de9286a](#)

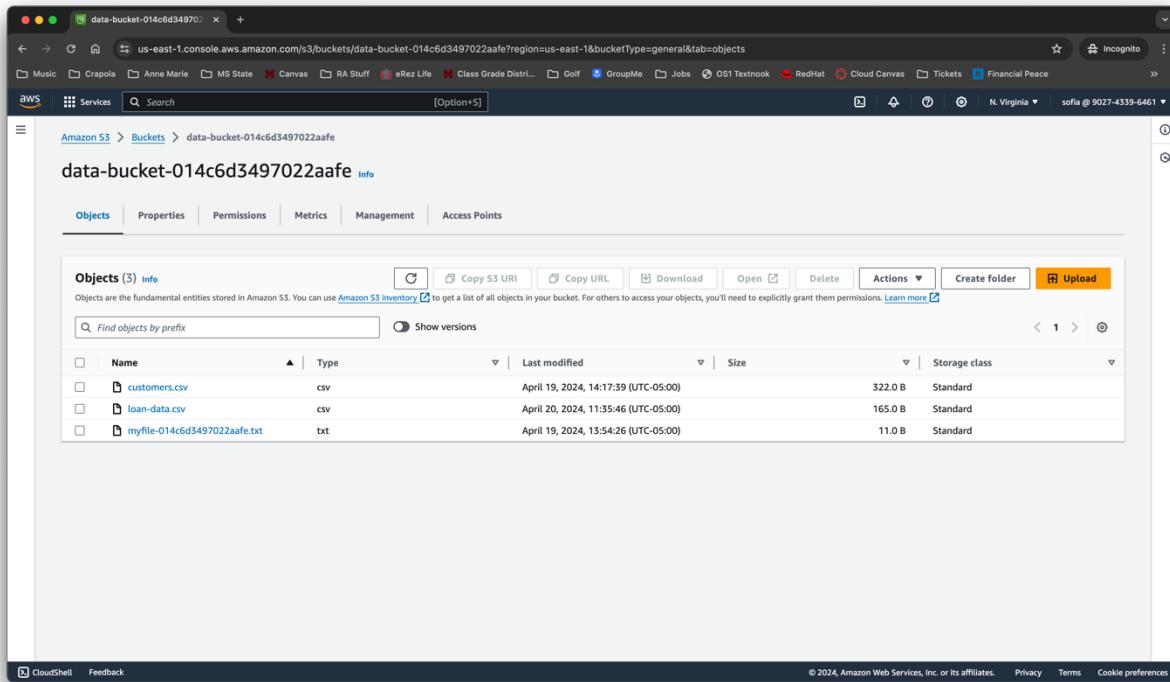
Bucket Key: Enabled

Intelligent-Tiering Archive configurations (0)

Enable objects stored in the Intelligent-Tiering storage class to tier-down to the Archive Access tier or the Deep Archive Access tier which are optimized for objects that will be rarely accessed for long periods of time. [Learn more](#)



```
loan-data.csv
loan-data.csv
date,description,amount,principal,interest
2023-01-14,payment,1000.00,845.52,154.48
2022-12-22,payment,1021.52,742.80,278.72
2022-11-15,payment,1000.00,855.27,144.73
```



Amazon S3 > Buckets > data-bucket-014c6d3497022aafe

data-bucket-014c6d3497022aafe [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Objects (3) [Info](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	customers.csv	csv	April 19, 2024, 14:17:39 (UTC-05:00)	322.0 B	Standard
<input type="checkbox"/>	loan-data.csv	csv	April 20, 2024, 11:35:46 (UTC-05:00)	165.0 B	Standard
<input type="checkbox"/>	myfile-014c6d3497022aafe.txt	txt	April 19, 2024, 13:54:26 (UTC-05:00)	11.0 B	Standard

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

The screenshot shows the AWS S3 console with the object 'loan-data.csv' selected. The page displays various configuration options:

- Default retention period:** Objects will be prevented from being overwritten or deleted for the duration of the retention period.
- Storage class:** Standard
- Server-side encryption settings:** Info
Encryption type: Info
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Encryption key ARN: arn:aws:kms:us-east-1:902743396461:key/31c3f5c3-cb39-4b26-89dd-ea1f6de9286a
Bucket Key: When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS.
Enabled
- Additional checksums:** Checksum functions are used for additional data integrity verification of new objects.

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

The screenshot shows the AWS S3 console with the object 'loan-data.csv' selected. The page displays detailed properties:

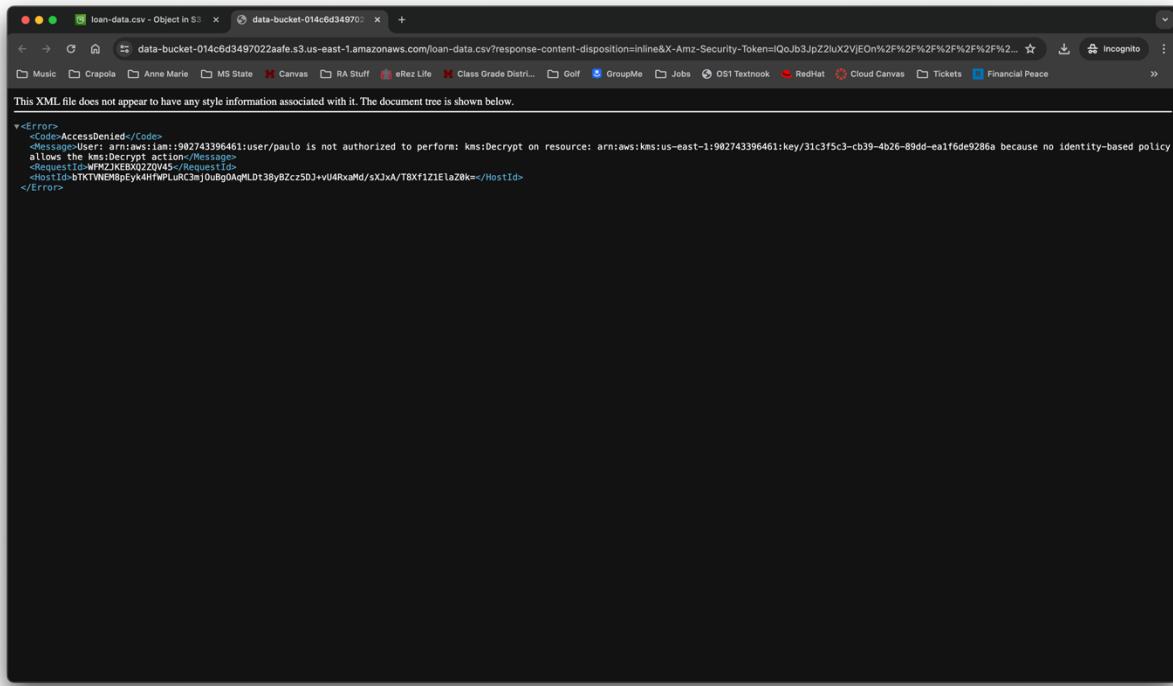
Properties	Value
Owner	awslabsc0w4680897t1666624755
AWS Region	US East (N. Virginia) us-east-1
Last modified	April 20, 2024, 11:35:46 (UTC-05:00)
Size	165.0 B
Type	CSV
Key	loan-data.csv

On the right side, there is a tooltip for the 'Download' icon:

Anyone using this device can see downloaded files

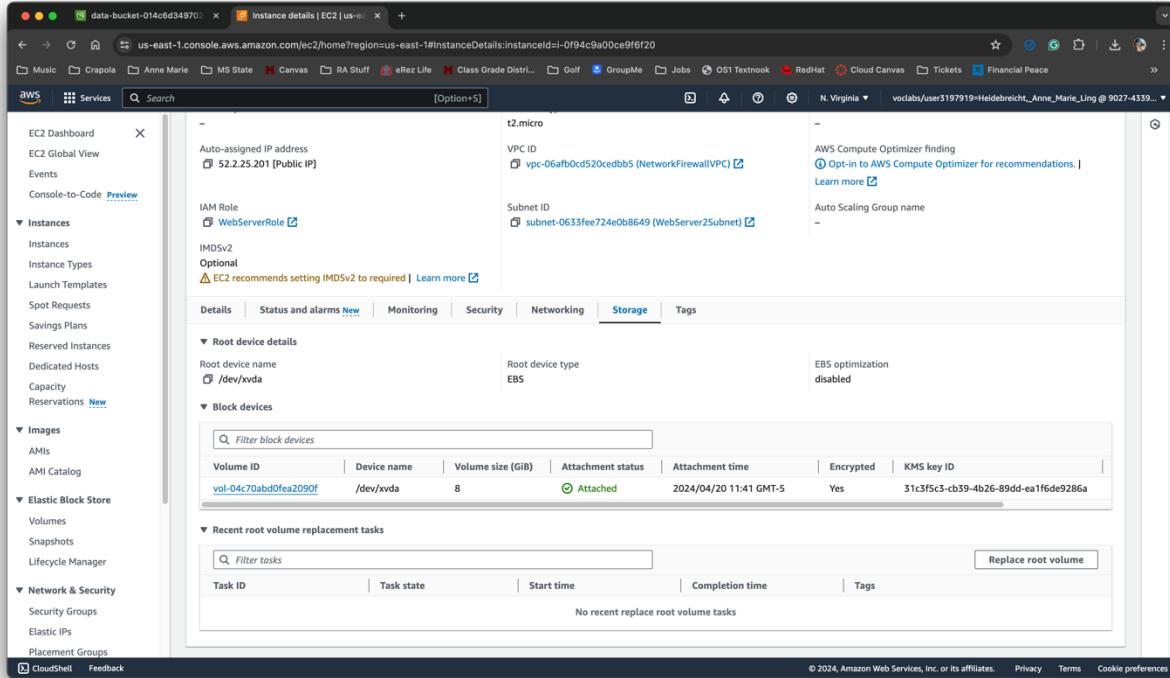
loan-data (1).csv
165 B - Done
67a628f3-8982-48a0-82a7-232f8dde5a77.parquet
2,751 B - 6 minutes ago

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



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

A screenshot of the AWS EC2 Instances page. The left sidebar shows navigation options like EC2 Dashboard, Events, and Instances. The main table lists four instances: 'EncryptedInst...', 'WebServer', 'WebServer2', and 'aws-rln1q-rl'. All instances are running and have t2.micro instance types. The table includes columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, and Public IP. A modal window titled 'Select an instance' is open at the bottom, listing the same four instances.



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

```
[ec2-user@webserver2 ~]$ result=$(aws kms generate-data-key --key-id alias/MyKMSKey --key-spec AES_256)
echo $result | python3 -m json.tool
{
    "CiphertextBlob": "AQIDAQBgaaQgIwTWhbxFalwEK3bxkmxkpolnTAZ5WsqXOCMkIlhgGJbrXFZFI3xnZgHs0YR9uFoAAAfjb8BqkgkhkG9w0BbwagbzTAgEAMGgGCSqGSib3DQEhATAeBglghkgBZQMEAS4wEQQMsfsNzIEPz3XpwHAcgBQgD/dkaL8QV1OPqAmmAUU7QUP/19m8qPMLN1XpVcUhliJdgRtDqFqszs2Sw/YRjxv+Olsg==",
    "Plaintext": "tQdzo2nPFRAwQoJaYmrkSrt14FGcxbpkxyvQ4=",
    "KeyId": "arn:aws:kms:us-east-1:90274396461:key/31c5fc5c3-cb39-4b26-89d-dae1fd9e286a"
}
```

```
[ec2-user@webserver2 ~]$ dk cipher $result | jq '.CiphertextBlob' | cut -d "" -f2)
[ec2-user@webserver2 ~]$ echo $dk_cipher
NOIDAQgATuoTtMbvFclv:iEKJhmrkmpoleTAZ5WqYOCMhIXlngQJbrXZFt3xn2gHs0XR9uFoAAAAAfjB8BgkqhkiG9w0BBwagbzBtAgEAMGgGC5qGSIB3DQEHAeBglghkgBZQHESAS4wEQQMfsNzIEPz3XpwHACHAgEQgDs/dkUa9Aq2VYQIP7xnn
NEUUVQUF/19m8411PN1XGmvCvsuhhiLjdqJ0BoTQBgfszw25w/YrJxv+o1g+-
[ec2-user@webserver2 ~]$ echo $dk_cipher | base64 --decode > data_key_ciphertext
[ec2-user@webserver2 ~]$ echo $dk_cipher | base64 --decode > data_key_ciphertext
[ec2-user@webserver2 ~]$ cat data_key_ciphertext
0o0mhbp One.00000001000000000000-0
    *#*#
    -6x8c6cp10;?vB#
[ec2-user@webserver2 ~]$ aws kms decrypt --ciphertext-blob fileb://./data_key_ciphertext --query Plaintext --output text
[ec2-user@webserver2 ~]$ aws kms decrypt --ciphertext-blob fileb://./data_key_ciphertext --query Plaintext --output text | base64 --decode > data_key_plaintext_encrypted
[ec2-user@webserver2 ~]$ 
[ec2-user@webserver2 ~]$ openssl enc -aes-256-cbc -salt -pbkdf2 -in data_unencrypted.txt -out data_encrypted -pass file:/data_key_plaintext_encrypted
[ec2-user@webserver2 ~]$ cat data_encrypted
Salted__0C0000_P0u0007u0060000000000_0(206000+00_e
    *#*#
    wEDa00000000[ec2-user@webserver2 ~]$ rm data_unencrypted.txt
[ec2-user@webserver2 ~]$ 
[ec2-user@webserver2 ~]$ openssl enc -d -aes-256-cbc -pbkdf2 -in data_encrypted -out data_decrypted.txt -pass file:/data_key_plaintext_encrypted
[ec2-user@webserver2 ~]$ cat data_decrypted.txt
Let's encrypt these file contents. Sensitive data here.
[ec2-user@webserver2 ~]$ 
```

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

The screenshot shows the AWS Secrets Manager console in a web browser. The URL is <https://us-east-1.console.aws.amazon.com/secretsmanager/listsecrets?region=us-east-1>. A green success message at the top states: "You successfully stored the secret mysecret. To show it in the list, choose Refresh. Use the sample code to update your applications to retrieve this secret." Below this, there is a table titled "Secrets" with one row. The row contains the secret name "mysecret", a blank description field, and the last retrieval time "Last retrieved (UTC)". At the bottom right of the table, there is a button labeled "Store a new secret". The browser interface includes standard navigation buttons like back, forward, and search, along with AWS-specific features like CloudShell and Feedback.

Secret name	Description	Last retrieved (UTC)
mysecret		

```

A newer release of "Amazon Linux" is available.
Version 2023.4.20240416:
Run "/usr/bin/dnf check-release-update" for full release and version update info
'-----'
  Amazon Linux 2023
'-----'
  https://aws.amazon.com/linux/amazon-linux-2023

Last login: Sat Apr 20 16:51:56 2024 from 18.206.107.29
[ec2-user@webserver2 ~]$ result=$(aws secretsmanager list-secrets)
[ec2-user@webserver2 ~]$ echo $result
{
  "SecretList": [
    {
      "ARN": "arn:aws:secretsmanager:us-east-1:902743396461:secret:mysecret-hUHBwg",
      "Name": "mysecret",
      "KmsKeyId": "arn:aws:kms:us-east-1:902743396461:key/3lc3f5c3-cb39-4b26-89dd-e1ffde9286a",
      "LastChangedDate": "2024-04-20T16:59:01.090000+00:00",
      "Tags": [],
      "SecretVersionsToStages": [
        {
          "VersionId": "28bd5878-d033-4d76-83d1-69bda00le43b",
          "SecretString": "my secret data",
          "VersionStage": "AWSCURRENT",
          "CreatedDate": "2024-04-20T16:59:01.090000+00:00"
        }
      ]
    }
  ]
}
[ec2-user@webserver2 ~]$ echo $key_arn
arn:aws:secretsmanager:us-east-1:902743396461:secret:mysecret-hUHBwg
[ec2-user@webserver2 ~]$ aws secretsmanager get-secret-value --secret-id $key_arn
{
  "ARN": "arn:aws:secretsmanager:us-east-1:902743396461:secret:mysecret-hUHBwg",
  "Name": "mysecret",
  "VersionId": "28bd5878-d033-4d76-83d1-69bda00le43b",
  "SecretString": "my secret data",
  "VersionStage": "AWSCURRENT",
  "CreatedDate": "2024-04-20T16:59:01.090000+00:00"
}
[ec2-user@webserver2 ~]$ 

```

i-0710082fb96f8c7e (WebServer2)

PublicIPs: 54.81.69.213 PrivateIPs: 10.1.3.4

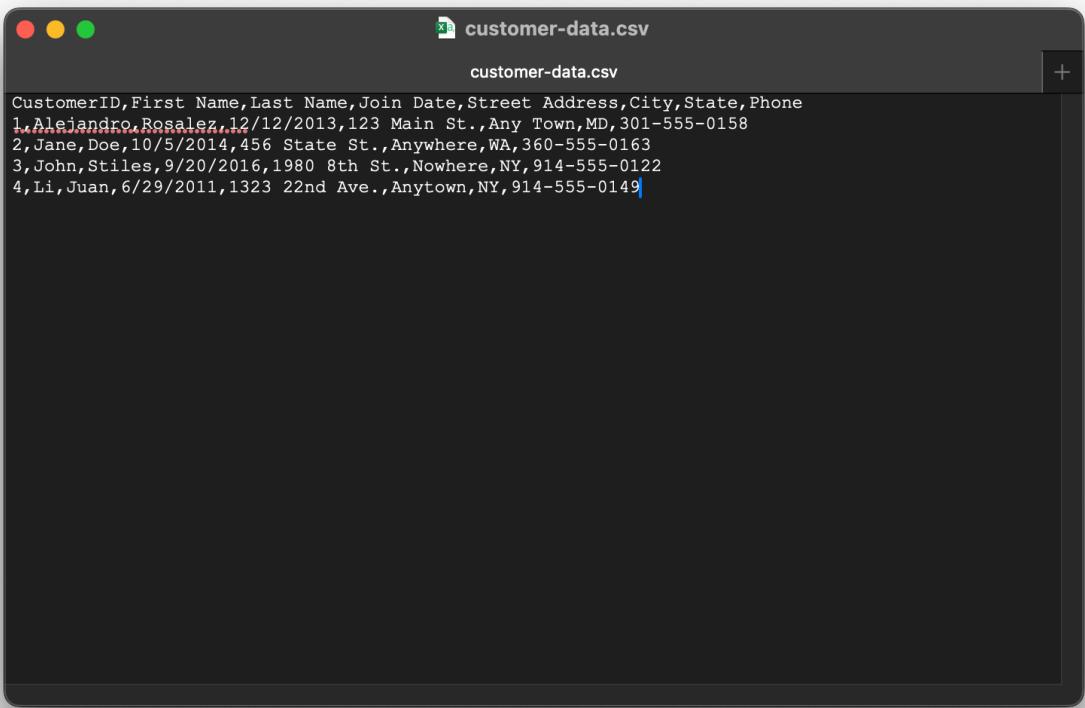
Phase 4 – Monitoring and logging

Task 4.1: Use CloudTrail to record Amazon S3 API calls

CloudTrail > Trails

Trails

Name	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
data-bucket-reads-writes	US East (N. Virginia)	Yes	Disabled	No	cloudtrail-logs-014c6d5497022aafe	-	-	Logging



The screenshot shows the AWS S3 console listing objects in the bucket "data-bucket-014c6d3497022aafe".

Name	Type	Last modified	Size	Storage class
customer-data.csv	csv	April 20, 2024, 12:04:38 (UTC-05:00)	322.0 B	Standard
customers.csv	csv	April 19, 2024, 14:17:39 (UTC-05:00)	322.0 B	Standard
loan-data.csv	csv	April 20, 2024, 11:35:46 (UTC-05:00)	165.0 B	Standard
myfile-014c6d3497022aafe.txt	txt	April 19, 2024, 13:54:26 (UTC-05:00)	11.0 B	Standard

Screenshot of the AWS CloudTrail Event history page. A green banner at the top indicates "Successfully created Athena table: cloudtrail_logs_cloudtrail_logs_014c6d3497022aafe". The main table shows 50+ events from April 20, 2024, including actions like UpdateInstanceInfor..., StartLogging, PutEventSelectors, PutBucketPolicy, CreateTrail, CreateLogStream, UpdateInstanceInfor..., UpdateInstanceInfor..., and SendSSHPublicKey.

Event name	Event time	User name	Event source	Resource type	Resource name
UpdateInstanceInfor...	April 20, 2024, 12:02:56 (UTC-0...)	i-0f94c9a00ce9f6f20	ssm.amazonaws.com	AWS::CloudTrail::Trail	arn:aws:cloudtrail:us-east-1:90274339...
StartLogging	April 20, 2024, 12:02:55 (UTC-0...)	user3197919=Heidebreicht_Anne_Marie_Ling	cloudtrail.amazonaws.c...	AWS::CloudTrail::Trail	arn:aws:cloudtrail:us-east-1:90274339...
PutEventSelectors	April 20, 2024, 12:02:55 (UTC-0...)	user3197919=Heidebreicht_Anne_Marie_Ling	cloudtrail.amazonaws.c...	AWS::CloudTrail::Trail	arn:aws:cloudtrail:us-east-1:90274339...
PutBucketPolicy	April 20, 2024, 12:02:54 (UTC-0...)	user3197919=Heidebreicht_Anne_Marie_Ling	s3.amazonaws.com	AWS::S3::Bucket	cloudtrail-logs-014c6d3497022aafe
CreateTrail	April 20, 2024, 12:02:54 (UTC-0...)	user3197919=Heidebreicht_Anne_Marie_Ling	cloudtrail.amazonaws.c...	AWS::CloudTrail::Trail	arn:aws:cloudtrail:us-east-1:90274339...
CreateLogStream	April 20, 2024, 12:01:59 (UTC-0...)	-	logs.amazonaws.com	-	-
UpdateInstanceInfor...	April 20, 2024, 11:59:48 (UTC-0...)	i-0710082fb96f8...	ssm.amazonaws.com	-	-
UpdateInstanceInfor...	April 20, 2024, 11:59:43 (UTC-0...)	i-0710082fb96f8...	ssm.amazonaws.com	-	-
SendSSHPublicKey	April 20, 2024, 11:59:40 (UTC-0...)	user3197919=Heidebreicht_Anne_Marie_Ling	ec2-instance-connect.amazonaws.co...	AWS::EC2::Instance	i-0710082fb96f8c7e

Screenshot of the AWS Athena Query editor. A query has been run against the "cloudtrail_logs_cloudtrail_logs_014c6d3497022aafe" table. The results show 10 completed rows of event log data.

#	eventversion	useridentity
1	1.09	{type=AssumedRole, principalId=AROASEL5TCBWSUJ3256TC7:user3197919=Heidebreicht_Anne_Marie_Ling, arn=arn:aws:sts::902743396461;assumed-rol...
2	1.08	{type=AWSAccount, principalId=AIDARDSCSRHTNDJVX7J, arn=null, accountId=076376020047, invokedBy=null, accessKeyId=null, username=null, sessio...
3	1.08	{type=AssumedRole, principalId=AROASEL5TCBWSUJ3256TC7:user3197919=Heidebreicht_Anne_Marie_Ling, arn=arn:aws:sts::902743396461;assumed-role/vacareum/resource, accountId=902...
4	1.09	{type=AWSService, principalId=null, arn=null, accountId=null, invokedBy=cloudtrail.amazonaws.com, accessKeyId=null, username=null, sessionContext=null}
5	1.08	{type=AssumedRole, principalId=AROASEL5TCBWSUJ3256TC7:user3197919=Heidebreicht_Anne_Marie_Ling, arn=arn:aws:sts::902743396461;assumed-rol...
6	1.08	{type=AWSService, principalId=null, arn=null, accountId=null, invokedBy=ec2.amazonaws.com, accessKeyId=null, username=null, sessionContext=null}
7	1.09	{type=AssumedRole, principalId=AROASEL5TCBWSUJ3256TC7:user3197919=Heidebreicht_Anne_Marie_Ling, arn=arn:aws:sts::902743396461;assumed-rol...
8	1.09	{type=AssumedRole, principalId=AROASEL5TCBWSUJ3256TC7:user3197919=Heidebreicht_Anne_Marie_Ling, arn=arn:aws:sts::902743396461;assumed-rol...
9	1.09	{type=AssumedRole, principalId=AROASEL5TCBWSUJ3256TC7:user3197919=Heidebreicht_Anne_Marie_Ling, arn=arn:aws:sts::902743396461;assumed-rol...
10	1.08	{type=AssumedRole, principalId=AROASEL5TCBWRK26BYGNJ-0710082fb96f8c7e, arn=arn:aws:sts::902743396461;assumed-role/WebServerRole/i-07...

The screenshot shows the AWS Athena Query Editor interface. The query window contains the following SQL code:

```

1 SELECT eventtime, useridentity.principalid, requestparameters, eventname
2 FROM cloudtrail_logs.cloudtrail_logs_014c6d3497022aafe
3 WHERE
4   eventname in ('PutObject') AND
5   requestparameters LIKE '%customer-data.csv%'
6 limit 10;

```

The results section shows one row of data:

#	eventtime	principalid	requestparameters
1	2024-04-20T17:04:37Z	AROASEL5TCBWSU32S6TC7:user3197919=Heidebrecht_Anne_Marie_Ling	{"X-Amz-Date":"20240420T170435Z","bucketName":"data-bucket"}

The screenshot shows the AWS Athena Query Editor interface. The query window contains the following SQL code:

```

1 SELECT eventtime, useridentity.principalid, requestparameters, eventname, sourceipaddress, useragent
2 FROM cloudtrail_logs.cloudtrail_logs_014c6d3497022aafe
3 WHERE
4   eventname in ('GetObject') AND
5   requestparameters LIKE '%customer-data.csv%'
6 limit 10;

```

The results section shows one row of data:

#	eventtime	principalid	requestparameters
1	2024-04-20T17:05:01Z	AROASEL5TCBWSU32S6TC7:user3197919=Heidebrecht_Anne_Marie_Ling	{"X-Amz-Date":"20240420T170501Z","bucketName":"data-bucket"}

Task 4.2: Use CloudWatch Logs to monitor secure logs

The screenshot shows the AWS CloudWatch Log Groups interface. On the left, there's a sidebar with various navigation options like Dashboards, Alarms, Logs, Metrics, X-Ray traces, Events, Application Signals, Network monitoring, and Insights. The main area is titled "Log groups (5)" and displays a table of log groups. The columns include Log group, Log class, Anomaly d..., Data protec..., Sensitive d..., Retention, and Metric filters. The log groups listed are:

Log group	Log class	Anomaly d...	Data protec...	Sensitive d...	Retention	Metric filters
/aws/lambda/c116924a27858516436522t1-AdjustA...	Standard	Configure	-	-	Never expire	-
/aws/lambda/c116924a27858516436522t1-AdjustB...	Standard	Configure	-	-	Never expire	-
LabVPCFlowLogs	Standard	Configure	-	-	Never expire	-
NetworkfirewallVPCLogs	Standard	Configure	-	-	6 months	-
EncryptedInstanceSecureLogs	Standard	Configure	-	-	Never expire	-

The screenshot shows an EC2 Instance Connect terminal session. The user is installing the Amazon CloudWatch agent on an Amazon Linux 2023 instance. The terminal output is as follows:

```
--- / 
Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/
[ec2-user@ip-10-1-3-9 ~]$ sudo yum install -y amazon-cloudwatch-agent
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
Resolving Dependencies
--> Running transaction check
--> Package amazon-cloudwatch-agent.x86_64 0:1.300033.0-1.amzn2 will be installed
--> Finished Dependency Resolution
Dependencies Resolved

=====
Package           Arch      Version          Repository      Size
=====
Installing:
amazon-cloudwatch-agent x86_64   1.300033.0-1.amzn2 amzn2-core       95 M
Transaction Summary
=====
Install 1 Package

Total download size: 95 M
Installed size: 360 M
Downloading packages:
amazon-cloudwatch-agent-1.300033.0-1.amzn2.x86_64.rpm
Running transaction check
Running transaction test
Running transaction test succeeded
Running transaction
create group cwagent, result: 0
create user cwagent, result: 0
  Installing : amazon-cloudwatch-agent-1.300033.0-1.amzn2.x86_64
  Verifying  : amazon-cloudwatch-agent-1.300033.0-1.amzn2.x86_64
Installed:
amazon-cloudwatch-agent.x86_64 0:1.300033.0-1.amzn2
Complete!
[ec2-user@ip-10-1-3-9 ~]$
```

```
customer-data.csv - Ob... Instances | EC2 | us-east-1 EC2 Instance Connect | u... CloudWatch | us-east-1 Event history | CloudTrail | Query editor | Athena | Secrets | Secrets Manager + https://us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=us-east-1&connType=standard&instanceId=0f94c9a00cef620&osUser=ec2-user&sshPort=22# Services Search [Option+S] N. Virginia v vclabs/user3197919+Heidebrecht,_Anne_Marie_Ling@9027-4339... 24 epel available [ =7.11 *stable ] 25 testing available [ =1.0 *stable ] 26 ecs available [ *stable ] 27 correto8 available \ [ =1.8.0.192 =1.8.0.202 =1.8.0.212 =1.8.0.222 =1.8.0.232 =1.8.0.242 *stable ] 32 lustre2.10 available \ [ =2.10.5 =2.10.8 *stable ] 33 tjava-openjdk11 available [ =11 *stable ] 34 lynx available [ *stable ] 36 pcre available [ =8.42 *stable ] 37 mono available [ =5.x *stable ] 38 nginx1 available [ *stable ] 40 mock available [ *stable ] 43 livepatch available [ *stable ] 44 tpython3.8 available [ *stable ] 45 haproxy2 available [ *stable ] 46 collected=latest enabled [ *stable ] 47 aws-nitro-enclaves-cli available [ *stable ] 48 libcurl available [ *stable ] 49 kernel-5.4 available [ *stable ] 50 nginx-1g available [ *stable ] 52 tomcat9 available [ *stable ] 53 unbound1.13 available [ *stable ] 54 mariadb10.5 available [ *stable ] 55 kernel-5.10=latest enabled [ *stable ] 56 redis6 available [ *stable ] 58 tpostgresql12 available [ *stable ] 59 tpostgresql13 available [ *stable ] 60 mock2 available [ *stable ] 61 dnsmasq2.85 available [ *stable ] 62 kernel-5.15 available [ *stable ] 63 tpostgresql14 available [ *stable ] 64 firefox available [ *stable ] 65 lustre available [ *stable ] 66 tphp8.1 available [ *stable ] 67 awscil1 available [ *stable ] 68 tphp8.2 available [ *stable ] 69 dnsmasq available [ *stable ] 70 unbound1.17 available [ *stable ] _ collected=python3 available [ *stable ] ! Note on end-of-support. Use 'info' subcommand. [ec2-user@ip-10-1-3-9 ~]$
```

```
[ec2-user@ip-10-1-3-9 ~]$ sudo wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-200-ACCAPI-91948/capstone-6-security/a3/config.json -P /opt/aws/amazon-cloudwatch-agent/bin/
--2024-04-20 17:30:22-- https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-200-ACCAPI-91948/capstone-6-security/a3/config.json
Resolving aws-tc-largeobjects.s3.us-west-2.amazonaws.com (aws-tc-largeobjects.s3.us-west-2.amazonaws.com)... 3.5.86.38, 3.5.86.128, 3.5.87.208, ...
Connecting to aws-tc-largeobjects.s3.us-west-2.amazonaws.com (aws-tc-largeobjects.s3.us-west-2.amazonaws.com)|3.5.86.38|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2278 (2.2K) [application/json]
Saving to: '/opt/aws/amazon-cloudwatch-agent/bin/config.json'

100%[=====] 2,278 --.-K/s in 0s

2024-04-20 17:30:22 (87.2 MB/s) - '/opt/aws/amazon-cloudwatch-agent/bin/config.json' saved [2278/2278]

[ec2-user@ip-10-1-3-9 ~]$ sudo cat /opt/aws/amazon-cloudwatch-agent/bin/config.json
{
    "agent": {
        "metrics_collection_interval": 60,
        "run_as_user": "root"
    },
    "logs": {
        "logs_collected": {
            "files": {
                "collect_list": [
                    {
                        "file_path": "/var/log/secure",
                        "log_group_name": "EncryptedInstanceSecureLogs",
                        "log_stream_name": "EncryptedInstanceSecureLogs-(instance_id)",
                        "retention_in_days": 180
                    }
                ]
            }
        }
    },
    "metrics": {
        "aggregation_dimensions": [
            {
                "InstanceId"
            }
        ],
        "append_dimensions": {
            "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
            "ImageId": "${aws:ImageId}",
            "InstanceId": "${aws:instanceId}"
        }
    }
}
```

```
[ec2-user@ip-10-1-3-9 ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json
***** processing amazon-cloudwatch-agent *****
I! Trying to detect region from ec2 D! [EC2] Found active network interface I! imds retry client will retry 1 timesSuccessfully fetched the config and saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp
Start configuration validation...
2024/04/20 17:31:59 Reading json config file path /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp ...
2024/04/20 17:31:59 D! ec2tagger processor required because append_dimensions is set
2024/04/20 17:31:59 D! pipeline hostDeltaMetrics has no receivers
2024/04/20 17:31:59 Configuration validation first phase succeeded
I! Detecting run as user...
I! Trying to detect region from ec2
D! [EC2] Found active network interface
I! Detected region us-east-1
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -schematest -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml
Configuration validation second phase succeeded
Configuration validation succeeded
amazon-cloudwatch-agent has already been stopped
Created symlink from /etc/systemd/system/multi-user.target.wants/amazon-cloudwatch-agent.service to /etc/systemd/system/amazon-cloudwatch-agent.service.
[ec2-user@ip-10-1-3-9 ~]$ sudo service amazon-cloudwatch-agent status
Red Hat System 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 Sat 2024-04-20 17:32:01 UTC; 9s ago
       Main PID: 385 (amazon-cloudwatch)
      CGroup: /system.slice/amazon-cloudwatch-agent.service
           └─ 385 /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml -envconfig /opt/aws/amazon-clo...
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json does not exist or cannot read. ...ping it.
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: 2024/04/20 17:32:02 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cl...json ...
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: 2024/04/20 17:32:02 I! Valid Json input schema.
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: I! Detecting run as user...
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: I! Trying to detect region from ec2
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: D! [EC2] Found active network interface I! imds retry client will retry 1 timesSuccessfully fetched the config and saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: 2024/04/20 17:32:02 D! ec2tagger processor required because append_dimensions is set
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: 2024/04/20 17:32:02 D! pipeline hostDeltaMetrics has no receivers
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: 2024/04/20 17:32:02 Configuration validation first phase succeeded
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json does not exist or cannot read. ...ping it.
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: I! Detecting run as user...
Hint: Some lines were ellipsized, use -l to show in full.
[ec2-user@ip-10-1-3-9 ~]$
```

```

2024/04/20 17:32:02 II Detected runAsUser: root
2024-04-20T17:32:02Z II Changing ownership of [/opt/aws/amazon-cloudwatch-agent/logs /opt/aws/amazon-cloudwatch-agent/etc /opt/aws/amazon-cloudwatch-agent/var] to 0:0
2024-04-20T17:32:03Z II Starting AmazonCloudWatchAgent CNAgent/1.300033.0 (go1.20.12; linux; amd64) with log file /opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log with log target lumberjack
2024-04-20T17:32:03Z II AWS SDK log level not set
2024-04-20T17:32:03Z II creating new log agent
2024-04-20T17:32:03Z II [logagent] starting
2024-04-20T17:32:03Z II [logagent] found plugin cloudwatchlogs is a log backend
2024-04-20T17:32:03Z II [logagent] found plugin logfile is a log collection
2024-04-20T17:32:03Z II [logagent] start log plugin file paths [/var/log/secure]
2024-04-20T17:32:03Z II [inputs/file] turned on log plugin
2024-04-20T17:32:03Z II {"caller": "service@v89.89.0/service.telemetry.go:77", "msg": "Skipping telemetry setup.", "address": "", "level": "None"}
2024-04-20T17:32:03Z II {"caller": "service@v89.89.0/service.videosvc.go:13", "msg": "Starting CWAhome Version: \"1.300033.0\" NumCPU:1"}, "version": "1.300033.0", "numcpu": 1}
2024-04-20T17:32:03Z II {"caller": "extensions/extensions.go:14", "msg": "Starting extensions..."}
2024-04-20T17:32:03Z II {"caller": "extensions/extensions.go:37", "msg": "Extension is starting...,"}, "kind": "extension", "name": "agenthealth/metrics"}
2024-04-20T17:32:03Z II {"caller": "extensions/extensions.go:45", "msg": "Extension started."}, "kind": "extension", "name": "agenthealth/metrics"}
2024-04-20T17:32:03Z II [cloudwatch] get unique roll up list [{InstanceId}]
2024-04-20T17:32:03Z II {"caller": "ec2tagger/ec2tagger.go:435", "msg": "ec2tagger: Check EC2 Metadata.", "kind": "processor", "name": "ec2tagger", "pipeline": "metrics/host"}
2024-04-20T17:32:03Z II [cloudwatch] publish with ForceFlushInterval: lm0s, Publish Jitter: 1.398532963s
2024-04-20T17:32:03Z II {"caller": "ec2tagger/ec2tagger.go:134", "msg": "ec2tagger: EC2 tagger has started initialization."}, "kind": "processor", "name": "ec2tagger", "pipeline": "metrics/host"}
2024-04-20T17:32:03Z II [inputs/socket_listener] Listening on udp://127.0.0.1:25826
2024-04-20T17:32:03Z II [inputs.socket_listener] Listening on: [:18125]
2024-04-20T17:32:03Z II [statd_listener] Listening on: [:18125]
2024-04-20T17:32:03Z II {"caller": "service@v89.89.0/service.go:169", "msg": "Everything is ready. Begin running and processing data."}
2024-04-20T17:32:03Z II {"caller": "ec2tagger/ec2tagger.go:500", "msg": "ec2tagger: Initial retrieval of tags succeeded."}, "kind": "processor", "name": "ec2tagger", "pipeline": "metrics/host"}
2024-04-20T17:32:03Z II {"caller": "ec2tagger/ec2tagger.go:411", "msg": "ec2tagger: EC2 tagger has started, finished initial retrieval of tags and Volumes."}, "kind": "processor", "name": "ec2tagger", "pipeline": "metrics/host"}
2024-04-20T17:32:04Z II First time setting retention for log group EncryptedInstanceSecureLogs, update map to avoid setting twice
2024-04-20T17:32:04Z II [logagent] Configured middleware on AWS client
2024-04-20T17:32:04Z II [logagent] piping log from EncryptedInstanceSecureLogs/EncryptedInstanceSecureLogs-1-0f94c9a00ce9f6f20(/var/log/secure) to cloudwatchlogs with retention 180
2024-04-20T17:32:09Z W! [outputs.cloudwatchlogs] Retried 0 time, going to sleep 132.848538ms before retrying.
[ec2-user@ip-10-1-3-9 ~]$ sudo tail -f /var/log/secure
Apr 20 17:32:10 ip-10-1-3-9 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Apr 20 17:32:10 ip-10-1-3-9 sudo: pam_unix(sudo:session): session closed for user root
Apr 20 17:32:44 ip-10-1-3-9 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/cat#040/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
Apr 20 17:32:44 ip-10-1-3-9 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Apr 20 17:32:44 ip-10-1-3-9 sudo: pam_unix(sudo:session): session closed for user root
Apr 20 17:33:30 ip-10-1-3-9 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/cat#040/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
Apr 20 17:33:30 ip-10-1-3-9 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Apr 20 17:33:30 ip-10-1-3-9 sudo: pam_unix(sudo:session): session closed for user root
Apr 20 17:34:02 ip-10-1-3-9 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/tail#040-f#040/var/log/secure
Apr 20 17:34:02 ip-10-1-3-9 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)

```

```

2024-04-20T17:32:03Z II {"caller": "ec2tagger/ec2tagger.go:500", "msg": "ec2tagger: EC2 tagger has started, finished initial retrieval of tags and Volumes."}, "kind": "processor", "name": "ec2tagger", "pipeline": "metrics/host"}
2024-04-20T17:32:03Z II {"caller": "ec2tagger/ec2tagger.go:411", "msg": "ec2tagger: EC2 tagger has started, finished initial retrieval of tags and Volumes."}, "kind": "processor", "name": "ec2tagger", "pipeline": "metrics/host"}
2024-04-20T17:32:04Z II First time setting retention for log group EncryptedInstanceSecureLogs, update map to avoid setting twice
2024-04-20T17:32:04Z II [logagent] Configured middleware on AWS client
2024-04-20T17:32:04Z II [logagent] piping log from EncryptedInstanceSecureLogs/EncryptedInstanceSecureLogs-1-0f94c9a00ce9f6f20(/var/log/secure) to cloudwatchlogs with retention 180
2024-04-20T17:32:09Z W! [outputs.cloudwatchlogs] Retried 0 time, going to sleep 132.848538ms before retrying.
[ec2-user@ip-10-1-3-9 ~]$ sudo tail -f /var/log/secure
Apr 20 17:32:10 ip-10-1-3-9 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Apr 20 17:32:10 ip-10-1-3-9 sudo: pam_unix(sudo:session): session closed for user root
Apr 20 17:32:44 ip-10-1-3-9 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/cat#040/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
Apr 20 17:32:44 ip-10-1-3-9 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Apr 20 17:32:44 ip-10-1-3-9 sudo: pam_unix(sudo:session): session closed for user root
Apr 20 17:33:30 ip-10-1-3-9 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/cat#040/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
Apr 20 17:33:30 ip-10-1-3-9 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Apr 20 17:33:30 ip-10-1-3-9 sudo: pam_unix(sudo:session): session closed for user root
Apr 20 17:34:02 ip-10-1-3-9 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/tail#040-f#040/var/log/secure
Apr 20 17:34:02 ip-10-1-3-9 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)

```

```
[ec2-user@ip-10-1-3-9 ~]$ exit
logout
Connection to 52.2.25.201 closed.
voclabs:~/environment $ ssh -i labsuser.pem ubuntu@52.2.25.201
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $
```

Apr 20 17:37:17 ip-10-1-3-9 sshd[474]: Accepted publickey for ec2-user from 44.205.118.188 port 50818 ssh2: RSA SHA256:MI86A6eVKb3jUSusU890e0...

Apr 20 17:37:17 ip-10-1-3-9 sshd[474]: Accepted publickey for ec2-user from 44.205.118.188 port 50818 ssh2: RSA SHA256:MI86A6eVKb3jUSusU890e0...

Apr 20 17:37:17 ip-10-1-3-9 sshd[474]: pam_unix(sshd:session): session opened for user ec2-user by (uid=0)

Apr 20 17:37:48 ip-10-1-3-9 sshd[665]: Received disconnect from 44.205.118.188 port 50818:11: disconnected by user

Apr 20 17:37:48 ip-10-1-3-9 sshd[665]: Disconnected from 44.205.118.188 port 50818

Apr 20 17:37:48 ip-10-1-3-9 sshd[474]: pam_unix(sshd:session): session closed for user ec2-user

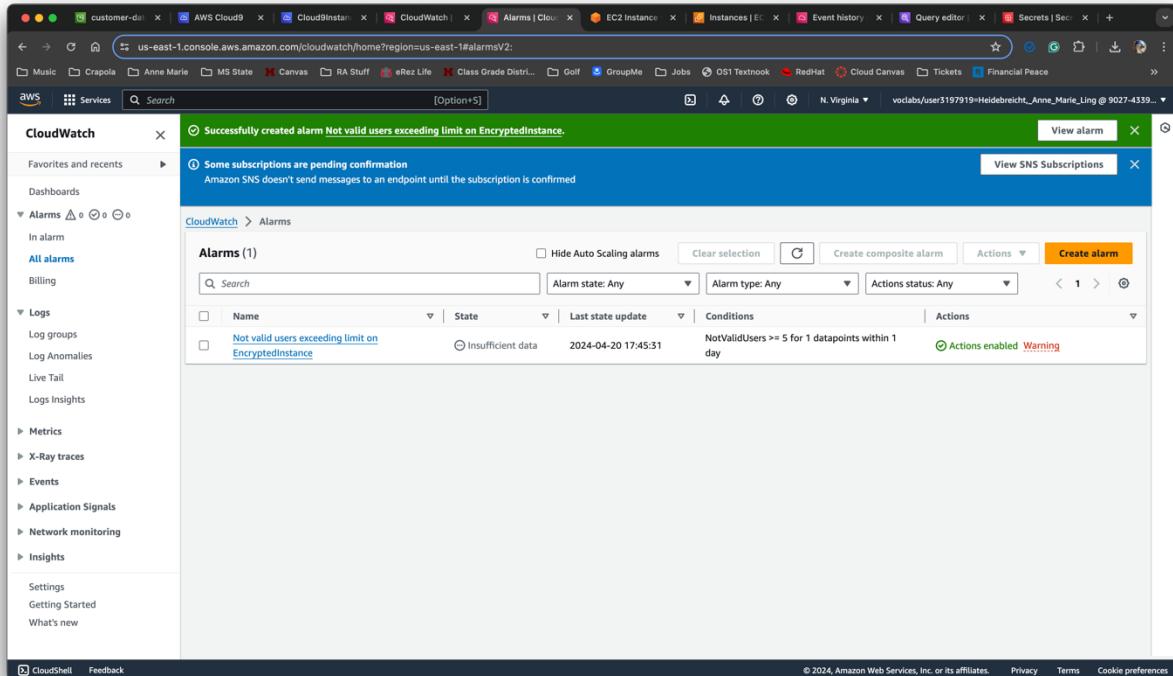
Apr 20 17:38:12 ip-10-1-3-9 sshd[691]: Invalid user ubuntu from 44.205.118.188 port 46930

Apr 20 17:38:12 ip-10-1-3-9 sshd[691]: Invalid user ubuntu from 44.205.118.188 port 46930

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

The screenshot shows the AWS CloudWatch Metrics Filter configuration page. The left sidebar has 'Logs' selected under 'Log groups'. The main area shows a single metric filter named 'Not valid users' with the following details:

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



```
voclabs:~/environment $ ssh -i labsuser.pem chroot@52.2.25.201
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh -i labsuser.pem random@52.2.25.201
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh -i labsuser.pem random3@52.2.25.201
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh -i labsuser.pem random2@52.2.25.201
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh -i labsuser.pem random5@52.2.25.201
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ 
```

The screenshot shows the AWS CloudWatch Log events interface. The left sidebar is collapsed, and the main area displays a list of log entries under the heading "Log events". A search bar at the top allows filtering by "Invalid user". The log entries are timestamped and show messages related to SSHD activity from various IP addresses and ports.

Timestamp	Message
2024-04-20T12:38:13.056-05:00	Apr 20 17:38:12 ip-10-1-3-9 sshd[691]: Invalid user ubuntu from 44.205.118.188 port 46930
2024-04-20T12:59:42 ip-10-1-3-9 sshd[792]:	Invalid user chroot from 44.205.118.188 port 58106
2024-04-20T12:59:50.264-05:00	Apr 20 17:59:50 ip-10-1-3-9 sshd[794]: Invalid user random from 44.205.118.188 port 38584
2024-04-20T12:59:56.781-05:00	Apr 20 17:59:56 ip-10-1-3-9 sshd[796]: Invalid user random3 from 44.205.118.188 port 58418
2024-04-20T13:00:00.791-05:00	Apr 20 18:00:00 ip-10-1-3-9 sshd[798]: Invalid user random2 from 44.205.118.188 port 58422
2024-04-20T13:00:17.587-05:00	Apr 20 18:00:17 ip-10-1-3-9 sshd[806]: Invalid user random5 from 44.205.118.188 port 59290

The screenshot shows the AWS CloudWatch Alarms interface. The left sidebar is collapsed, and the main area displays a table of alarms under the heading "Alarms (1)". One alarm is listed: "Not valid users exceeding limit on EncryptedInstance", which is currently in an "In alarm" state. The condition for this alarm is "NotValidUsers >= 5 for 1 datapoints within 1 day".

Name	State	Last state update	Conditions	Actions
Not valid users exceeding limit on EncryptedInstance	In alarm	2024-04-20 18:01:44	NotValidUsers >= 5 for 1 datapoints within 1 day	Actions enabled

ALARM: "Not valid users exceeding limit on EncryptedInstance" in US East (N. Virginia)

 AWS Notifications <no-reply@sns.amazonaws.com> Today at 1:01PM

To:  Heidebrecht, Anne Marie

You are receiving this email because your Amazon CloudWatch Alarm "Not valid users exceeding limit on EncryptedInstance" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [5.0 (19/04/24 18:01:00)] was greater than or equal to the threshold (5.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Saturday 20 April, 2024 18:01:44 UTC".

View this alarm in the AWS Management Console:
https://secure-web.cisco.com/1fjBq6OBHXDlybhLWhmnQ3IpFLtMjVbEUCBuS2-HOMUUbWcZz6_MlsmtZ1f0gOGgBBy2EcCbb9WjpYM8MGwVP1HFUsDmij9Nb1dNwsLS7KeOYRpWdVnoc1wAjpMm5HxKp8p-1NPV0NRD5FYDd-70G5sZ4QstMkr-NBMf6nonLO-2j2l3B4qfABX0kFmTKeJYAkUecKgbZC9NZB-Q9VuKtm19rtE5IDdz8dtWzSqGz1QhRDqge_5Lv_bVmA5vu7ZY2-BtQaqe-ZTYlDo7AOHxm9Z-i6LqG9/jrKY8nbmTx5UXiYkNgru28/https%3A%2F%2Fus-east-1.console.aws.amazon.com%2Fcloudwatch%2Fdeplink.js%3Fregion%3Dus-east-1%23alarmsV2%3Aalarm%2FNot%2520valid%2520users%2520exceeding%2520limit%2520on%2520EncryptedInstance

Alarm Details:

- Name: Not valid users exceeding limit on EncryptedInstance
- Description: Not valid access attempts over SSH to the EncryptedInstance server have exceeded 4 in the last 24 hours.
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [5.0 (19/04/24 18:01:00)] was greater than or equal to the threshold (5.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Saturday 20 April, 2024 18:01:44 UTC
- AWS Account: 902743396461
- Alarm Arn: arn:aws:cloudwatch:us-east-1:902743396461:alarm:Not valid users exceeding limit on EncryptedInstance

Threshold:

- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 5.0 for at least 1 of the last 1 period(s) of 86400 seconds.

Monitored Metric:

- MetricNamespace: secure
- MetricName: NotValidUsers
- Dimensions:
- Period: 86400 seconds
- Statistic: Sum
- Unit: not specified
- TreatMissingData: missing

State Change Actions:

- OK:
- ALARM: [arn:aws:sns:us-east-1:902743396461:Not_valid_users_exceeding_limit]
- INSUFFICIENT_DATA:

--

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://secure-web.cisco.com/1jK2YHlsOWPZU053lVXLUNRdG6GOEPqxFORQoLezJIBcV3sCpu8gx4UOCRirBUxTIPtXRaKRaugVSIQq-I1I/HVinvVi1v_ZaT39ohO7w5hdVQ7zAvutRW/cn7W/VfeIm7SC51MhM_RmHPU176dwYYVY7AM/C1KinAheueRhAG9QduuYRVITH-IMIIloY1vSCTA1kIvAWVVWfEKeHSn_IRe5nPdHhKklJRAgS2

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

The screenshot shows the AWS IAM console with the URL <https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/details/AWSConfigRole?section=permissions>. The left sidebar is collapsed, showing the main navigation menu. The main content area displays the 'AWSConfigRole' details page under the 'AWSConfigRole' role. The 'Permissions' tab is selected, showing two attached policies: 'AWS_ConfigRole' (AWS managed) and 'S3Full' (Customer inline). The ARN of the role is listed as `arn:aws:iam::902743396461:role/AWSConfigRole`.

The screenshot shows the AWS IAM console with the URL <https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/details/SSMAutomationRole?section=permissions>. The left sidebar is collapsed. The main content area displays the 'SSMAutomationRole' details page under the 'SSMAutomationRole' role. The 'Permissions' tab is selected, showing two attached policies: 'AmazonS3FullAccess' (AWS managed) and 'AmazonSSMAutomationRole' (AWS managed). The ARN of the role is listed as `arn:aws:iam::902743396461:role/SSMAutomationRole`.

The screenshot shows the AWS S3 Buckets page. At the top, there's an "Account snapshot" section with metrics like Total storage (676.0 B), Object count (3), and Average object size (225.3 B). Below this, there are tabs for "General purpose buckets" and "Directory buckets". The "General purpose buckets" tab is selected, showing a list of buckets with columns for Name, AWS Region, IAM Access Analyzer, and Creation date. The list includes:

Name	AWS Region	IAM Access Analyzer	Creation date
athena-results-20202024	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 19, 2024, 14:33:49 (UTC-05:00)
aws-config-014c6d3497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 10:34:16 (UTC-05:00)
cloudtrail-logs-014c6d3497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 10:34:16 (UTC-05:00)
data-bucket-014c6d3497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 19, 2024, 13:53:53 (UTC-05:00)
s3-inventory-014c6d3497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 10:34:16 (UTC-05:00)
s3-objects-access-log-014c6d3497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 10:34:16 (UTC-05:00)

The screenshot shows the AWS S3 Buckets page after a new bucket has been created. A green banner at the top says "Successfully created bucket 'compliance-bucket-014c6d3497022aafe'". Below this, the "Account snapshot" section and the "General purpose buckets" list are visible. The newly created bucket is listed in the table:

Name	AWS Region	IAM Access Analyzer	Creation date
athena-results-20202024	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 19, 2024, 14:33:49 (UTC-05:00)
aws-athena-query-results-902743396461-us-east-1	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 20, 2024, 12:05:46 (UTC-05:00)
aws-config-014c6d3497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 10:34:16 (UTC-05:00)
cloudtrail-logs-014c6d3497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 10:34:16 (UTC-05:00)
compliance-bucket-014c6d3497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 20, 2024, 13:07:41 (UTC-05:00)
data-bucket-014c6d3497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 19, 2024, 13:53:53 (UTC-05:00)
s3-inventory-014c6d3497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 10:34:16 (UTC-05:00)
s3-objects-access-log-014c6d3497022aafe	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 10:34:16 (UTC-05:00)

Screenshot of the AWS S3 console showing the "Edit Object Ownership" page for a specific bucket object.

The "Object Ownership" section is displayed, with the "ACLs enabled" option selected. A note states: "Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs." A warning message below says: "⚠️ 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."

The "Object Ownership preferred" section shows two options:

- 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.

A note in this section states: " ⓘ 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](#)"

At the bottom are "Cancel" and "Save changes" buttons.

Screenshot of the AWS Config console showing the "Dashboard" page.

The left sidebar includes links for Conformance packs, Rules, Resources, Aggregators, Compliance Dashboard, Conformance packs, Rules, Inventory Dashboard, Resources, Authorizations, Advanced queries, Settings, What's new, Documentation, Partners, FAQs, and Pricing.

The main dashboard displays several metrics and status indicators:

- Conformance Packs by Compliance Score:** Shows "No conformance packs deployed. Try deploying a new conformance pack." Learn more.
- Compliance status:** Shows 0 Noncompliant rule(s) and 0 Compliant resource(s).
- Noncompliant rules by noncompliant resource count:** Shows "No noncompliant rules." View all noncompliant rules.
- AWS Config usage metrics:** Shows Configuration Items Recorded and Configuration Recorder Insufficient Per... metrics over time (3h, 1d, 1w, 1d, UTC timezone).
- AWS Config success metrics:** Shows AWS Config success metrics over time (3h, 1d, 1w, 1d, UTC timezone).

At the bottom are "CloudShell" and "Feedback" buttons.

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

AWS Config

Rules

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the compliance results.

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

CloudShell Feedback

Noncompliant

S3 Bucket

No archive configurations
No configurations to display.
Create configuration

Server access logging
Log requests for access to your bucket. Use CloudWatch to check the health of your server access logging. [Learn more](#)
Edit

Server access logging
Disabled

AWS CloudTrail data events (1) [Info](#)
Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. [Learn more](#)
Access
Name: data-bucket-reads-writes
Read, Write

Event notifications
Send a notification when specific events occur in your bucket. [Learn more](#)
Edit Delete Create event notification
Name Event types Filters Destination type Destination
No event notifications
Choose Create event notification to be notified when a specific event occurs.
Create event notification

CloudShell Feedback

The screenshot shows the AWS Config console with a rule named "S3-bucket-logging-enabled". The rule configuration includes:

- Key**: targetBucket, Type: String, Value: -, Description: Target S3 bucket for storing server access logs.
- Key**: targetPrefix, Type: String, Value: -, Description: Prefix of the S3 bucket for storing server access logs.
- Remediation action**: AWS-ConfigureS3BucketLogging, Description: Enables Logging on S3 Bucket.
- Parameters** (Listed below):

Key	Value	Description
AutomationAssumeRole	arn:aws:iam::902743396461:role/SSMAutomationRole	(Optional) The ARN of the role that allows Automation to perform the actions on your behalf.
TargetPrefix	-	(Optional) Specifies a prefix for the keys under which the log files will be stored.
GranteeEmailAddress	-	(Optional) Email address of the grantee.
GranteeType	CanonicalUser	(Optional) Type of grantee.
BucketName	RESOURCE_ID	(Required) The name of the Amazon S3 Bucket for which you want to configure logging.
GranteelId	bfcfa3bf986ff0956ab4a5a7a6614006e88f237fd813d21569c6a185e08ae0f	(Optional) The canonical user ID of the grantee.
GranteeUri	-	(Optional) URI of the grantee group.
GrantedPermission	FULL_CONTROL	(Optional) Logging permissions assigned to the Grantee for the bucket.
TargetBucket	s3-objects-access-log-014c6d3497022aafe	(Required) Specifies the bucket where you want Amazon S3 to store server access logs. You

The screenshot shows the AWS S3 Bucket properties for "compliance-bucket-014c6d3497022aafe". The properties include:

- Buckets**: No archive configurations. No configurations to display. Create configuration.
- Server access logging**: Enabled, Destination bucket: s3://s3-objects-access-log-014c6d3497022aafe, Log object key format: /[YYYY]-[MM]-[DD]-[hh]-[ss]-[UniqueString].
- AWS CloudTrail data events (1)**: Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. Configure in CloudTrail.
- Name**: data-bucket-reads-writes, Access: Read, Write.
- Event notifications**: Send a notification when specific events occur in your bucket. Create event notification.

Reflection

This project was very difficult and time-consuming. However, I did get some hands-on experience with AWS Security tools. It helped me learn about what the different tools did and

how they worked with other tools to create a secure application. Without the guided exercise, this project would have taken me two to three times longer to complete. I wish that we had an entire semester to complete a project like this or Project 1: Web Application Builder. Both of them were complicated and time-consuming. I think assigning one project at the beginning of the semester and having it due around midterms and then assigning the next project until the last day of finals would be a good way to divide the work so it's not so overwhelming. The project definitely was interesting, and under less stressful circumstances, I feel like I would have learned a lot more about AWS Cloud Computing.