

AWS-Cloud-Security-Project

In this project, I worked as a cloud security specialist at a Financial bank.

The company has locations throughout the country. The company provides checking and savings accounts, credit cards, loans, and investment products. All products require the use of personally identifiable information (PII), such as account numbers, contact information, and personal IDs. Your manager, the Director of IT, has tasked you to ensure the security of the company's resources in the AWS Cloud.

Key areas of the AWS infrastructure that need to be secured include S3 buckets, the network that hosts web servers, and keys that are used to encrypt data. Your manager also wants you to monitor and analyze access to these resources so that the bank can improve its security posture as changes and potential security incidents occur.

Your task within this project is to secure these AWS resources based on AWS best practices that are associated with the AWS Well-Architected Framework, the principle of least privilege, and internal company IT standards.

Throughout the project, you will test access to resources as two test users, Paulo and Mary, who are members of the Account Manager Group. In some cases, Paulo has more privileged access than Mary, to certain resources stored in the AWS account. You will compare his access to Mary's access. By comparing their access, you will be able to verify if specific resources have been secured by using mechanisms beyond AWS Identity and Access Management (IAM) policies.

In the AWS KMS phase of the project, you will use a test user named Sofia, who is a member of the Financial Advisor Group.

Solution requirements

This project is split into different phases, and each phase is designed to address one or more solution requirements. The solution must meet the following requirements:

- R1 - Design (phase 2)
- R2 - Optimize cost (phase 2)
- R3 - Restrict access (phases 1, 2, and 3)
- R4 - Enforce compliance (phases 3 and 4)
- R5 - Encrypt data (phase 3)

AWS-Cloud-Security-Project

- R6 - Withstand penetration testing (phase 2)
- R7 - Monitor and log user activity (phases 1 and 4)

R8 - Generate alert and change management notifications (phase 4) In this project, you work as a cloud security specialist at AnyCompany Financial bank.

The company has locations throughout the country. The company provides checking and savings accounts, credit cards, loans, and investment products. All products require the use of personally identifiable information (PII), such as account numbers, contact information, and personal IDs. Your manager, the Director of IT, has tasked you to ensure the security of the company's resources in the AWS Cloud.

Key areas of the AWS infrastructure that need to be secured include S3 buckets, the network that hosts web servers, and keys that are used to encrypt data. Your manager also wants you to monitor and analyze access to these resources so that the bank can improve its security posture as changes and potential security incidents occur.

Your task within this project is to secure these AWS resources based on AWS best practices that are associated with the AWS Well-Architected Framework, the principle of least privilege, and internal company IT standards.

Throughout the project, you will test access to resources as two test users, Paulo and Mary, who are members of the Account Manager Group. In some cases, Paulo has more privileged access than Mary, to certain resources stored in the AWS account. You will compare his access to Mary's access. By comparing their access, you will be able to verify if specific resources have been secured by using mechanisms beyond AWS Identity and Access Management (IAM) policies.

In the AWS KMS phase of the project, you will use a test user named Sofia, who is a member of the Financial Advisor Group.

Solution requirements

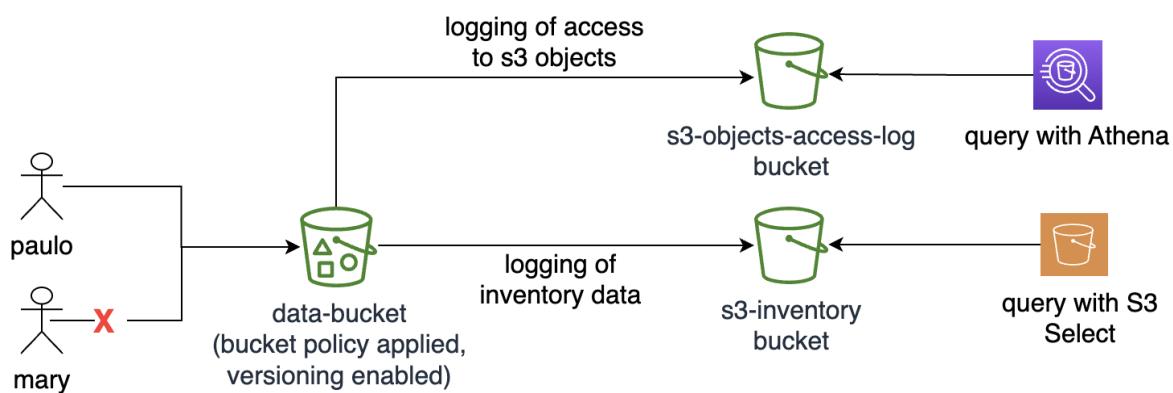
This project is split into different phases, and each phase is designed to address one or more solution requirements. The solution must meet the following requirements:

- R1 - Design (phase 2)
- R2 - Optimize cost (phase 2)
- R3 - Restrict access (phases 1, 2, and 3)

AWS-Cloud-Security-Project

- R4 - Enforce compliance (phases 3 and 4)
- R5 - Encrypt data (phase 3)
- R6 - Withstand penetration testing (phase 2)
- R7 - Monitor and log user activity (phases 1 and 4)
- R8 - Generate alert and change management notifications (phase 4)

Cloud Security Builder: Securing and Monitoring Resources with AWS



Phase 1: Securing data in Amazon S3

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

AWS-Cloud-Security-Project

The screenshot shows the AWS S3 console interface. The left sidebar includes sections for General purpose buckets, Directory buckets, Table buckets (New), Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. A note about Block Public Access settings for this account is also present. The main content area displays an Account snapshot (updated every 24 hours) and a General purpose buckets list. The list shows two buckets: 'aws-config-05c2dbc75fe1d7e55' and 'cloudtrail-logs-'. Both buckets are in the US East (N. Virginia) region (us-east-1). The 'aws-config-' bucket was created on December 9, 2024, at 16:33:32 (UTC-05:00), and its IAM Access Analyzer status is 'View analyzer for us-east-1'. The 'cloudtrail-logs-' bucket was created on December 9, 2024. The list includes columns for Name, AWS Region, IAM Access Analyzer, and Creation date. Action buttons for Copy ARN, Empty, Delete, and Create bucket are available for each row. A search bar at the top of the list allows finding buckets by name. The bottom of the page features a navigation bar with CloudShell, Feedback, and various icons, along with copyright information and a footer with language and date/time settings.

Name	AWS Region	IAM Access Analyzer	Creation date
aws-config-05c2dbc75fe1d7e55	US East (N. Virginia) us-east-1	View analyzer for us-east-1	December 9, 2024, 16:33:32 (UTC-05:00)
cloudtrail-logs-	US East (N. Virginia) us-east-1		December 9, 2024,

AWS-Cloud-Security-Project

The screenshot shows the AWS S3 'Create bucket' wizard. In the 'Advanced settings' section, the 'Bucket Key' option is selected. A note states: 'Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS.' Below this, there are 'Disable' and 'Enable' buttons, with 'Enable' checked. A note below says: 'After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.' At the bottom right is a 'Create bucket' button.

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

Enable

Advanced settings

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Create bucket

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

Amazon S3 > Buckets > data-bucket-05c2dbc75fe1d7e55 > Upload

Files and folders (1 total, 13.0 B)

Name	Type	Size
myfile.txt	text/plain	13.0 B

All files and folders in this table will be uploaded.

Destination [Info](#)

Destination [s3://data-bucket-05c2dbc75fe1d7e55](#)

Destination details
Bucket settings that impact new objects stored in the specified destination.

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

1°C Cloudy

AWS-Cloud-Security-Project

The screenshots show the AWS S3 Bucket Policy editor interface across three different sessions. In each session, the user is editing a bucket policy for the bucket 'data-bucket-05c2dbc75fe1d7e55'. The policy grants access to specific AWS accounts (voclabs, paulo, sofia) and denies access to others.

```
Version: 2012-10-17
Statement: [
    {
        "Effect": "Allow",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": [
            "arn:aws:s3:::data-bucket-05c2dbc75fe1d7e55",
            "arn:aws:s3:::data-bucket-05c2dbc75fe1d7e55/*"
        ],
        "Condition": {
            "StringEquals": {
                "aws:PrincipalArn": [
                    "arn:aws:iam::902625889566:role/voclabs",
                    "arn:aws:iam::902625889566:user/paulo",
                    "arn:aws:iam::902625889566:user/sofia"
                ]
            }
        }
    },
    {
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:GetBucketLocation",
        "Resource": [
            "arn:aws:s3:::data-bucket-05c2dbc75fe1d7e55",
            "arn:aws:s3:::data-bucket-05c2dbc75fe1d7e55/*"
        ],
        "Condition": {
            "StringEquals": {
                "aws:PrincipalArn": [
                    "arn:aws:iam::902625889566:role/voclabs",
                    "arn:aws:iam::902625889566:user/paulo"
                ]
            }
        }
    }
]
```

AWS-Cloud-Security-Project

The screenshot shows the AWS CloudWatch Metrics Insights search interface. At the top, there's a search bar with the placeholder "Search" and a "Reset to default layout" button. Below the search bar, there are two tabs: "Metrics" (selected) and "Logs". The main area displays a table of search results with columns for "Time", "Metric Name", "Dimensions", and "Value". One row in the table is highlighted in yellow. At the bottom of the table, there are buttons for "Next" and "Previous".

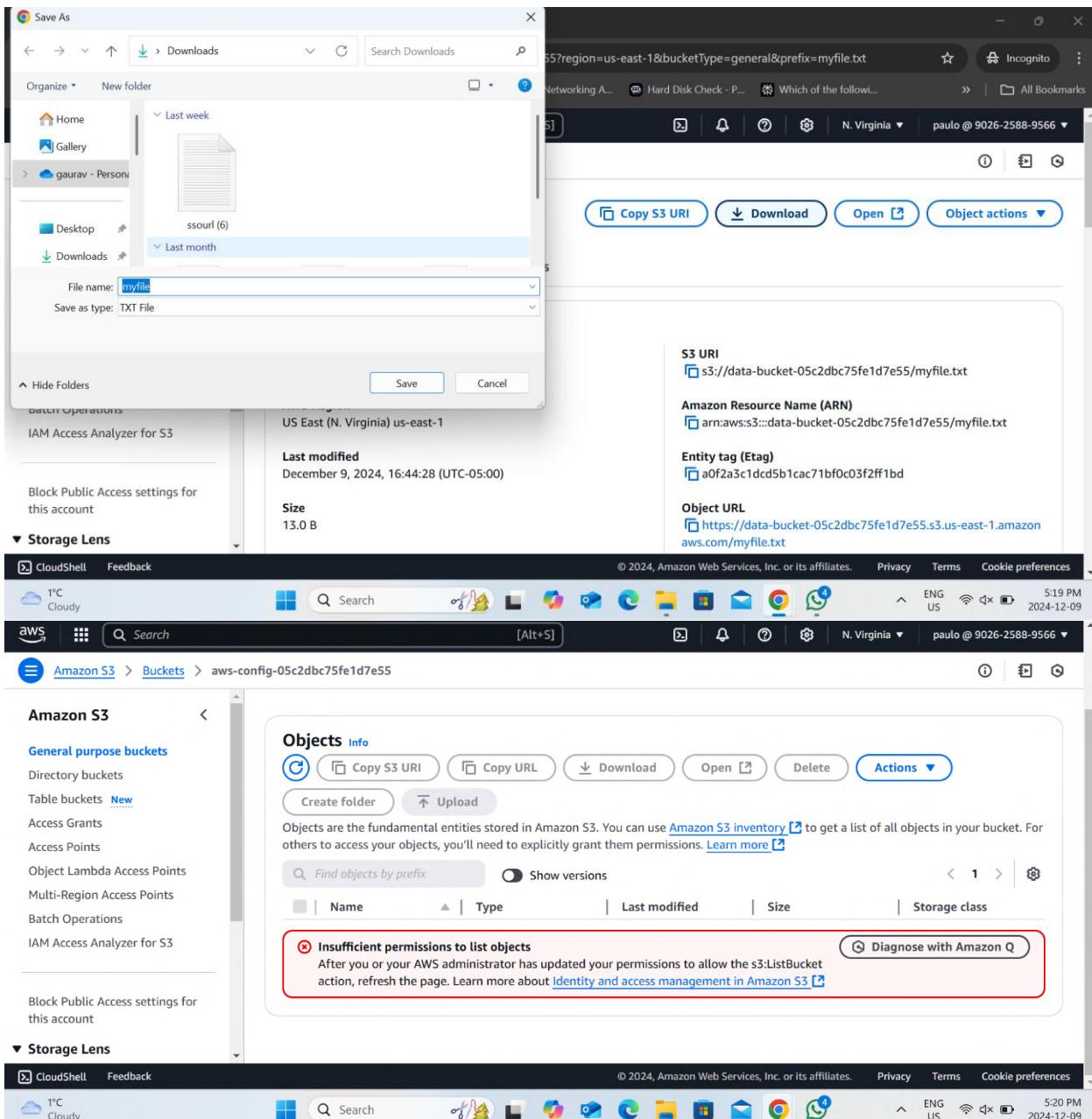
Metrics

Time	Metric Name	Dimensions	Value
2024-12-09T12:00:00Z - 2024-12-09T12:05:00Z	CloudWatch Metrics Insights	CloudWatch Metrics Insights	1

Logs

Time	Log Stream	Message
2024-12-09T12:00:00Z - 2024-12-09T12:05:00Z	CloudWatch Metrics Insights	CloudWatch Metrics Insights

AWS-Cloud-Security-Project



AWS-Cloud-Security-Project

AWS-Cloud-Security-Project

The screenshot shows the AWS S3 console interface. It displays two buckets: `s3-objects-access-log-05c2dbc75fe1d7e55` and `cloudtrail-logs-05c2dbc75fe1d7e55`. Both buckets are listed under the `General purpose buckets` section. On the left sidebar, there is a `Storage Lens` section. The main content area shows the `Objects` tab for each bucket. A red box highlights the error message: `Insufficient permissions to list objects`. Below the message, it says: `After you or your AWS administrator has updated your permissions to allow the s3>ListBucket action.` The browser status bar at the bottom indicates the date and time as 2024-12-09 5:22 PM.

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

AWS-Cloud-Security-Project

The screenshot shows the AWS S3 console interface. On the left, a sidebar lists various S3 features: General purpose buckets, Directory buckets, Table buckets (with a 'New' button), Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, and Block Public Access settings for this account. Below this is a section for Storage Lens.

The main content area displays a table titled "General purpose buckets (5)". The table has columns for Name, AWS Region, IAM Access Analyzer, and Creation date. The buckets listed are:

Name	AWS Region	IAM Access Analyzer	Creation date
cloudtrail-logs-05c2dbc75fe1d7e55	US East (N. Virginia) us-east-1	View analyzer for us-east-1	December 9, 2024, 16:33:32 (UTC-05:00)
data-bucket-05c2dbc75fe1d7e55	US East (N. Virginia) us-east-1	View analyzer for us-east-1	December 9, 2024, 16:41:58 (UTC-05:00)
s3-inventory-05c2dbc75fe1d7e55	US East (N. Virginia) us-east-1	View analyzer for us-east-1	December 9, 2024, 16:33:32 (UTC-05:00)
s3-objects-access-log-05c2dbc75fe1d7e55	US East (N. Virginia) us-east-1	View analyzer for us-east-1	December 9, 2024, 16:33:32 (UTC-05:00)

Below the table, there is a "Bucket Versioning" section. It states: "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." It includes a link to "Learn more". The current setting is "Disabled".

There is also a "Multi-factor authentication (MFA) delete" section, which requires MFA delete settings for changing Bucket Versioning settings and permanently deleting object versions. The current setting is "Disabled".

The "Tags (0)" section allows users to track storage costs and organize buckets, with a "Learn more" link. It currently has 0 tags.

AWS-Cloud-Security-Project

The image displays three screenshots of the AWS S3 console, illustrating the configuration of Bucket Versioning and Server Access Logging.

Screenshot 1: Edit Bucket Versioning

This screenshot shows the "Bucket Versioning" configuration page for the bucket "data-bucket-05c2dbc75fe1d7e55". The "Enable" option is selected, and a note states: "After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects."

Screenshot 2: Edit server access logging

This screenshot shows the "Edit server access logging" configuration page. The "Destination Region" is set to "US East (N. Virginia) us-east-1". The "Destination bucket name" is "s3-objects-access-log-05c2dbc75fe1d7e55". The "Destination prefix" is "data-bucket". The "Log object key format" is set to "[DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]". An example log key is shown as "data-bucket2024-07-10-12-56-[UniqueString]".

AWS-Cloud-Security-Project

The screenshot shows the AWS S3 Permissions overview page for the bucket `s3-objects-access-log-05c2dbc75fe1d7e55`. The **Permissions** tab is selected. On the left sidebar, under **General purpose buckets**, the **Block Public Access** section is expanded, showing that "Block all public access" is set to **On**. A large callout box highlights this setting.

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

On

[Edit](#)

Individual Block Public Access settings for this bucket

Policy

```
1▼ {
2  "Version": "2012-10-17",
3  "Statement": [
4    {
5      "Effect": "Allow",
6      "Principal": "*",
7      "Action": "s3:PutObject",
8      "Resource": "arn:aws:s3:::s3-objects-access-log/data-bucket/*",
9      "Condition": {
10        "StringEquals": {
11          "aws:UserAgent": "aws-internal"
12        }
13      }
14    }
15  ]
16}
17|
```

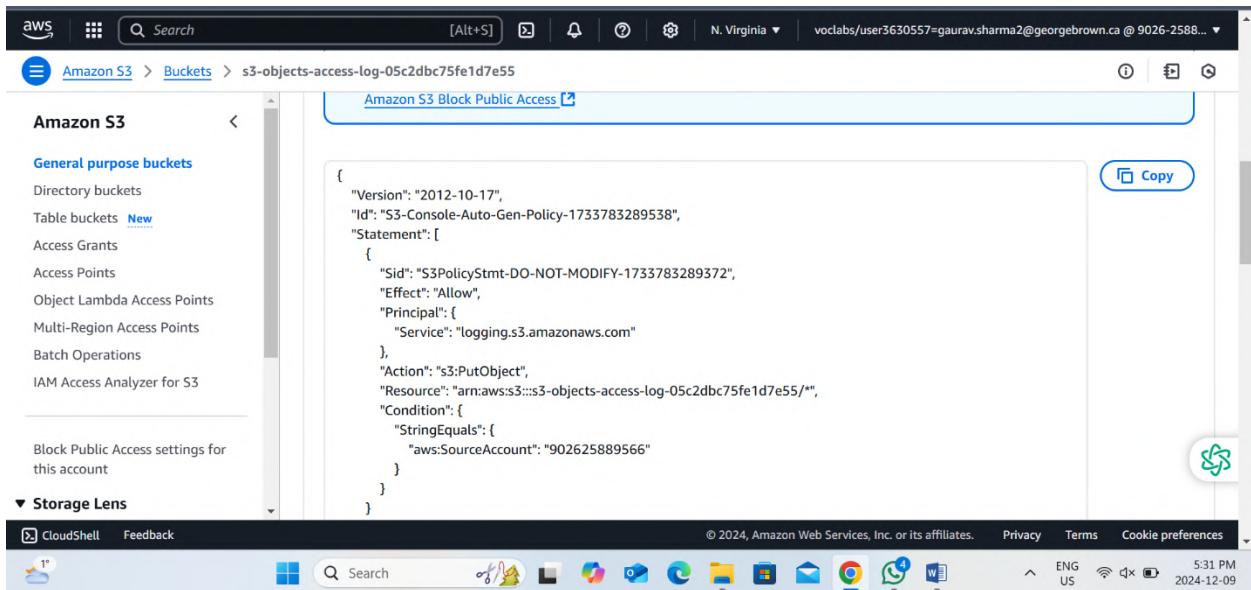
Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

[+ Add new statement](#)

AWS-Cloud-Security-Project



The screenshot shows the AWS S3 console with the path `Buckets > s3-objects-access-log-05c2dbc75fe1d7e55`. The main content area displays the `Amazon S3 Block Public Access` configuration. On the left, there's a sidebar with options like `General purpose buckets`, `Storage Lens`, and `CloudShell`. The central panel contains a JSON policy document:

```
{  
    "Version": "2012-10-17",  
    "Id": "S3-Console-Auto-Gen-Policy-1733783289538",  
    "Statement": [  
        {  
            "Sid": "S3PolicyStmt-DO-NOT-MODIFY-1733783289372",  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "logging.s3.amazonaws.com"  
            },  
            "Action": "s3:PutObject",  
            "Resource": "arn:aws:s3:::s3-objects-access-log-05c2dbc75fe1d7e55/*",  
            "Condition": {  
                "StringEquals": {  
                    "aws:SourceAccount": "902625889566"  
                }  
            }  
        }  
    ]  
}
```

At the bottom right of the JSON pane, there is a `Copy` button and a green circular icon with a white question mark. The status bar at the bottom of the browser window shows the date and time as `2024-12-09 5:31 PM`.

Task 1.3: Implement the S3 Inventory feature on a bucket

AWS-Cloud-Security-Project

The screenshot shows the AWS S3 'Create bucket' wizard with three visible steps:

- General configuration**:
 - AWS Region**: US East (N. Virginia) us-east-1
 - Bucket type**: General purpose (selected) vs Directory
 - Bucket name**: athena-results-12345
 - Copy settings from existing bucket - optional**: Only the bucket settings in the following configuration are copied. A 'Choose bucket' button is available.
- Object Ownership**:
 - Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

AWS-Cloud-Security-Project

The screenshot shows the AWS Athena Query Editor interface. At the top, there are several informational messages: one about setting up a query result location in Amazon S3, and another about typeahead code suggestions for SQL query development. Below these, the Data source is set to 'AwsDataCatalog' and the Database dropdown is set to 'Choose a database'. A 'Tables and views' section is visible. In the center, a modal window titled 'Choose S3 data set' is open, listing S3 buckets. The 'Bucket (1/6)' section shows a single entry: 'athena-results-752895', which is selected (indicated by a blue border). Other buckets listed are 'aws-config-05c2dbc75fe1d7e55', 'cloudtrail-logs-05c2dbc75fe1d7e55', 'data-bucket-05c2dbc75fe1d7e55', 's3-inventory-05c2dbc75fe1d7e55', and 's3-objects-access-log-05c2dbc75fe1d7e55'. The modal has 'Cancel' and 'Choose' buttons at the bottom right.

Task 1.4: Confirm that versioning works as intended

AWS-Cloud-Security-Project

The screenshots illustrate the process of creating an external table in Amazon Athena and executing a query against it.

Screenshot 1: Query Editor - Data Source Selection

The Data source is set to "AwsDataCatalog". The Database dropdown shows "Choose a database". The Tables and views section lists "Tables (0)" and "Views (0)".

Query 1:

```
1+ CREATE EXTERNAL TABLE `default.bucket_logs`(`bucketowner` STRING,`bucket_name` STRING,`requestdatetime` STRING,`remoteip` STRING,`requester` STRING,`requestid` STRING,`operation` STRING,`key` STRING,`request_uri` STRING,`httpstatus` STRING,`errorcode` STRING,`bytessent` BIGINT,`objectsize` BIGINT,`totaltime` STRING,
```

Screenshot 2: Query Editor - Table Creation

The Data source is set to "AwsDataCatalog". The Database dropdown shows "Choose a database". The Tables and views section lists "Tables (1)" containing "bucket_logs" and "Views (0)".

Query 2:

```
1+ CREATE EXTERNAL TABLE `default.bucket_logs`(`bucketowner` STRING,`bucket_name` STRING,`requestdatetime` STRING,`remoteip` STRING,`requester` STRING,`requestid` STRING,`operation` STRING,`key` STRING,`request_uri` STRING,`httpstatus` STRING,`errorcode` STRING,`bytessent` BIGINT,`objectsize` BIGINT,`totaltime` STRING,
```

Screenshot 3: Query Editor - Query Execution

The Data source is set to "AwsDataCatalog". The Database dropdown shows "Choose a database". The Tables and views section lists "Tables (1)" containing "bucket_logs" and "Views (0)".

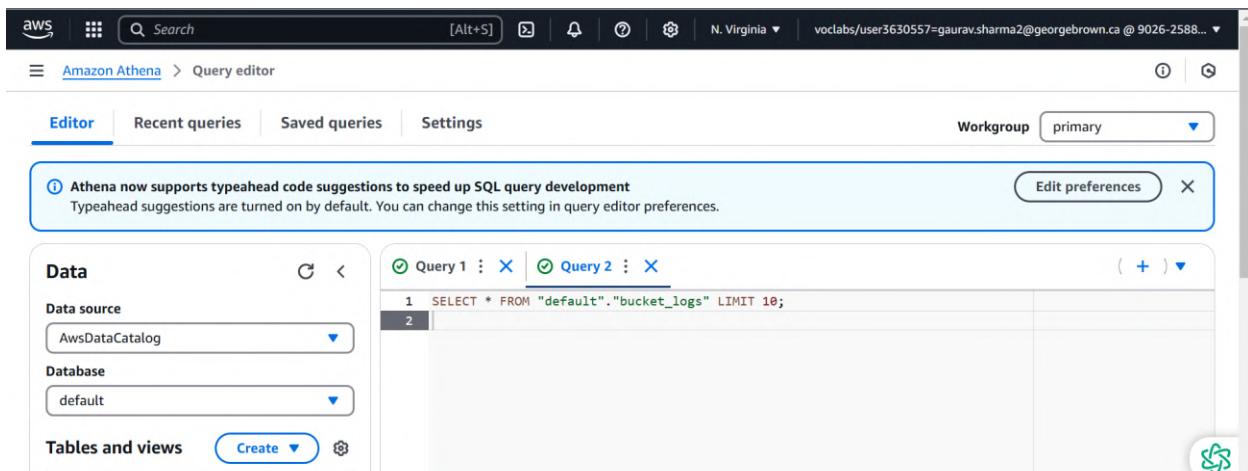
Query 3:

```
1+ SELECT * FROM `default.bucket_logs`
```

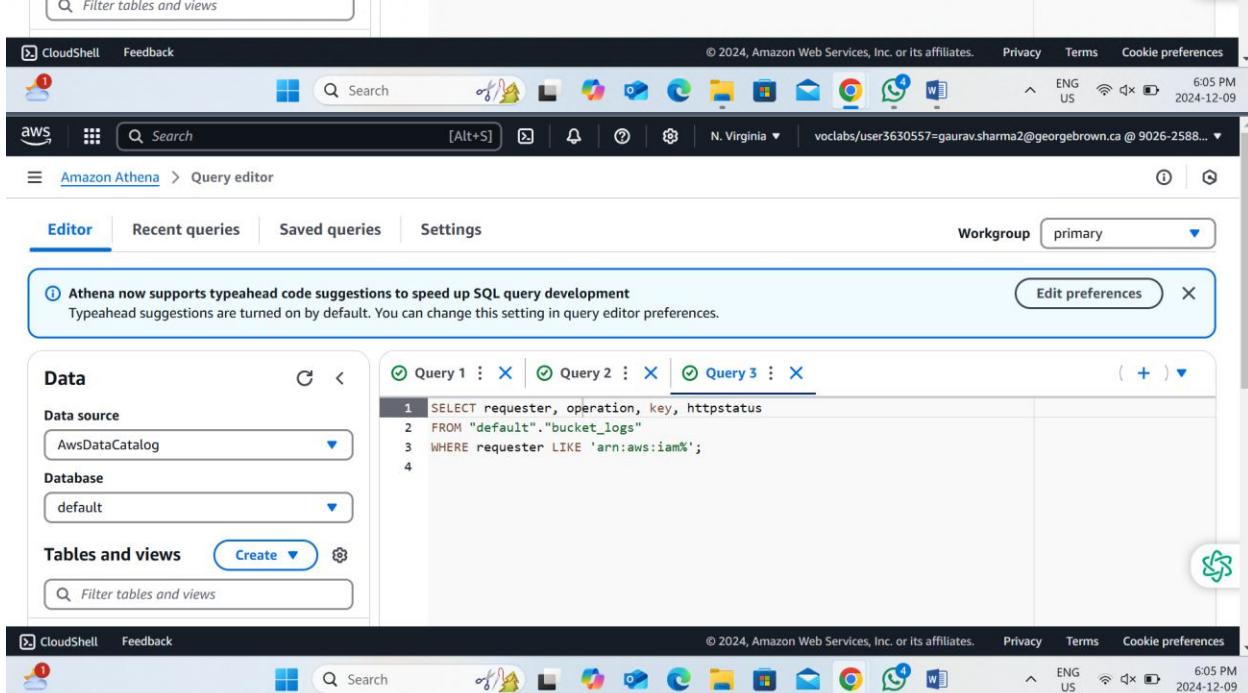
Query Results:

Completed
Time in queue: 85 ms Run time: 340 ms Data scanned: -
Query successful.

AWS-Cloud-Security-Project



```
1 SELECT * FROM "default"."bucket_logs" LIMIT 10;
```

```
1 SELECT requester, operation, key, httpstatus
2 FROM "default"."bucket_logs"
3 WHERE requester LIKE 'arn:aws:iam%';
4
```

AWS-Cloud-Security-Project

The screenshot shows the 'Storage pricing' section of the AWS S3 Pricing page. It discusses various storage classes and their costs, mentioning S3 Intelligent-Tiering and its minimum eligible object size of 128 KB. A live chat bubble is visible in the top right corner.

The screenshot shows the 'Pricing examples' section of the AWS Athena Pricing page. It includes examples for SQL queries and additional costs. A live chat bubble is visible in the top right corner.

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

The screenshot shows the 'Object overview' page for an S3 object named 'data-bucket2024-12-09-23-15-16-403C880F015D8343'. It displays the S3 URI, Amazon Resource Name (ARN), and Entity tag (Etag) for the object.

AWS-Cloud-Security-Project

The screenshot shows the AWS S3 'Create bucket' wizard with three visible steps:

- General configuration**:
 - AWS Region**: US East (N. Virginia) us-east-1
 - Bucket type**: General purpose (selected) vs Directory
 - Bucket name**: athena-results-12345
 - Copy settings from existing bucket - optional**: Only the bucket settings in the following configuration are copied. A 'Choose bucket' button is available.
- Object Ownership**:
 - Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

AWS-Cloud-Security-Project

The screenshot shows the AWS Athena Query Editor interface. At the top, there are several informational messages: one about setting up a query result location in Amazon S3, and another about typeahead code suggestions for speeding up SQL query development. The main area is titled "Query 1" and contains a single row labeled "1". On the left, there's a sidebar for "Data" with sections for "Data source" (set to "AwsDataCatalog") and "Database" (with a dropdown menu). Below that is a "Tables and views" section with a "Create" button. A modal window titled "Choose S3 data set" is open in the foreground, listing S3 buckets. The bucket "athena-results-752895" is selected, indicated by a blue border around its row. Other buckets listed are "aws-config-05c2dbc75fe1d7e55", "cloudtrail-logs-05c2dbc75fe1d7e55", "data-bucket-05c2dbc75fe1d7e55", "s3-inventory-05c2dbc75fe1d7e55", and "s3-objects-access-log-05c2dbc75fe1d7e55". At the bottom of the modal are "Cancel" and "Choose" buttons.

AWS-Cloud-Security-Project

The screenshots illustrate the process of creating an external table in Amazon Athena and executing a query against it.

Screenshot 1: Query Editor - Data Source Selection

The left sidebar shows the "Data" section with "Data source" set to "AwsDataCatalog" and "Database" set to "Choose a database". The "Tables and views" section shows 0 tables and 0 views. The main area displays the SQL code for creating an external table:

```
1 CREATE EXTERNAL TABLE `default.bucket_logs`(`bucketowner` STRING,`bucket_name` STRING,`requestdatetime` STRING,`remoteip` STRING,`requester` STRING,`requestid` STRING,`operation` STRING,`key` STRING,`request_uri` STRING,`httpstatus` STRING,`errorcode` STRING,`bytessent` BIGINT,`objectsize` BIGINT,`totaltime` STRING)
```

Screenshot 2: Query Editor - Table Creation and Execution

The left sidebar shows the "Tables" section with 1 table named "bucket_logs". The main area shows the completed SQL code and the results of the executed query:

```
34 OUTPUTFORMAT
35 'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
36 LOCATION
37 's3://s3-objects-access-log-05c2dbc75fe1d7e55/'
```

Screenshot 3: Query Editor - Results View

The left sidebar shows the "Tables" section with 1 table named "bucket_logs". The main area shows the results of the query execution:

Completed
Time in queue: 85 ms Run time: 340 ms Data scanned: -
Query successful.

AWS-Cloud-Security-Project

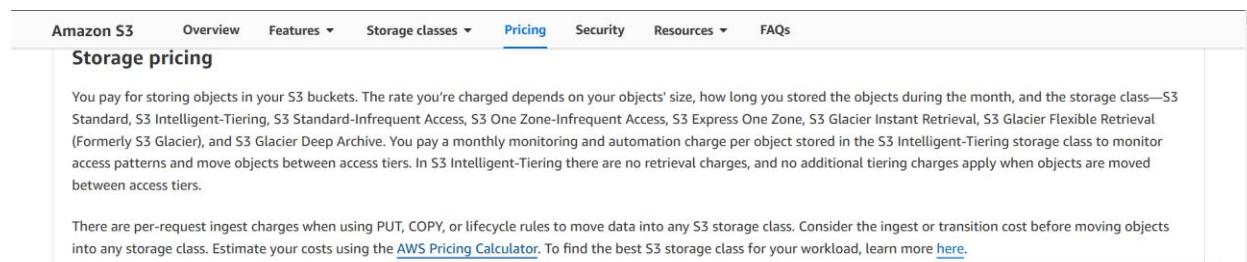
The screenshot shows the Amazon Athena Query Editor interface. At the top, there's a navigation bar with the AWS logo, search bar, and various icons. Below it, the title bar says "Amazon Athena > Query editor". The main menu includes "Editor", "Recent queries", "Saved queries", and "Settings". A "Workgroup" dropdown is set to "primary". A message box at the top left informs users about typeahead code suggestions. The central area has a "Data" sidebar on the left with "Data source" (AwsDataCatalog), "Database" (default), and "Tables and views" sections. Three queries are listed in the main pane:

```
Query 1 : X | Query 2 : X | Query 3 : X
1 SELECT * FROM "default"."bucket_logs" LIMIT 10;
2
3
4
```

```
Query 1 : X | Query 2 : X | Query 3 : X
1 SELECT requester, operation, key, httpstatus
2 FROM "default"."bucket_logs"
3 WHERE requester LIKE 'arn:aws:iam%';
4
```

The bottom of the screen shows a taskbar with icons for CloudShell, Feedback, and several application icons. The status bar indicates the date and time as 2024-12-09 6:05 PM.

AWS-Cloud-Security-Project

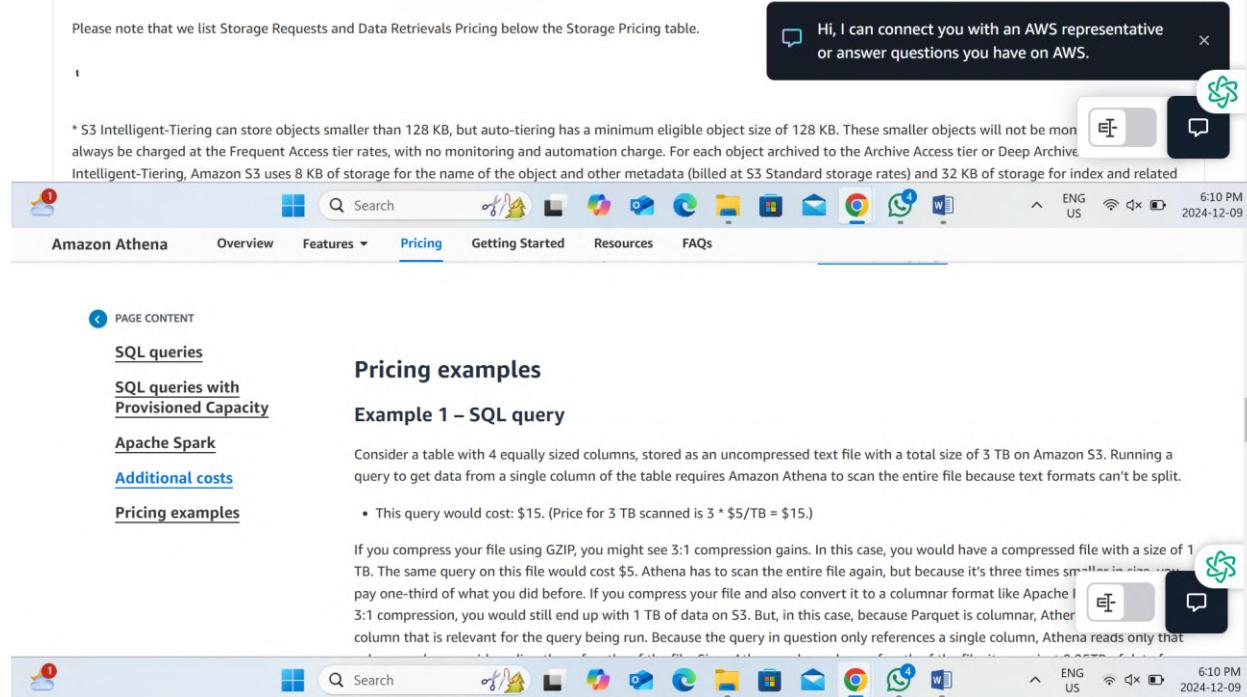


You pay for storing objects in your S3 buckets. The rate you're charged depends on your objects' size, how long you stored the objects during the month, and the storage class—S3 Standard, S3 Intelligent-Tiering, S3 Standard-Infrequent Access, S3 One Zone-Infrequent Access, S3 Express One Zone, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval (Formerly S3 Glacier), and S3 Glacier Deep Archive. You pay a monthly monitoring and automation charge per object stored in the S3 Intelligent-Tiering storage class to monitor access patterns and move objects between access tiers. In S3 Intelligent-Tiering there are no retrieval charges, and no additional tiering charges apply when objects are moved between access tiers.

There are per-request ingest charges when using PUT, COPY, or lifecycle rules to move data into any S3 storage class. Consider the ingest or transition cost before moving objects into any storage class. Estimate your costs using the [AWS Pricing Calculator](#). To find the best S3 storage class for your workload, learn more [here](#).

Please note that we list Storage Requests and Data Retrievals Pricing below the Storage Pricing table.

Hi, I can connect you with an AWS representative or answer questions you have on AWS.



* S3 Intelligent-Tiering can store objects smaller than 128 KB, but auto-tiering has a minimum eligible object size of 128 KB. These smaller objects will not be monitored and will always be charged at the Frequent Access tier rates, with no monitoring and automation charge. For each object archived to the Archive Access tier or Deep Archive tier, Amazon S3 uses 8 KB of storage for the name of the object and other metadata (billed at S3 Standard storage rates) and 32 KB of storage for index and related data.

PAGE CONTENT

- [SQL queries](#)
- [SQL queries with Provisioned Capacity](#)
- [Apache Spark](#)
- [Additional costs](#)
- [Pricing examples](#)

Pricing examples

Example 1 – SQL query

Consider a table with 4 equally sized columns, stored as an uncompressed text file with a total size of 3 TB on Amazon S3. Running a query to get data from a single column of the table requires Amazon Athena to scan the entire file because text formats can't be split.

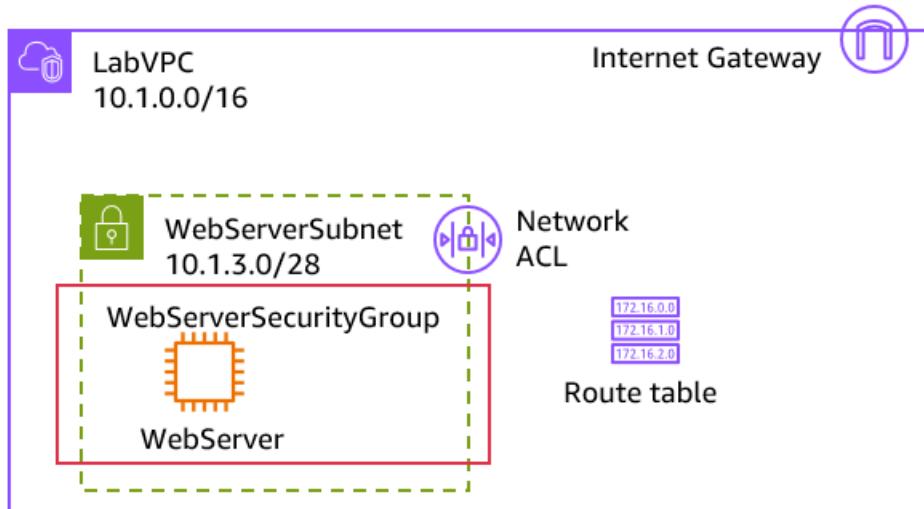
- This query would cost: \$15. (Price for 3 TB scanned is $3 * \$5/\text{TB} = \15 .)

If you compress your file using GZIP, you might see 3:1 compression gains. In this case, you would have a compressed file with a size of 1 TB. The same query on this file would cost \$5. Athena has to scan the entire file again, but because it's three times smaller in size, it only needs to pay one-third of what you did before. If you compress your file and also convert it to a columnar format like Apache Parquet, which uses 3:1 compression, you would still end up with 1 TB of data on S3. But, in this case, because Parquet is columnar, Athena only needs to read the column that is relevant for the query being run. Because the query in question only references a single column, Athena reads only that column.

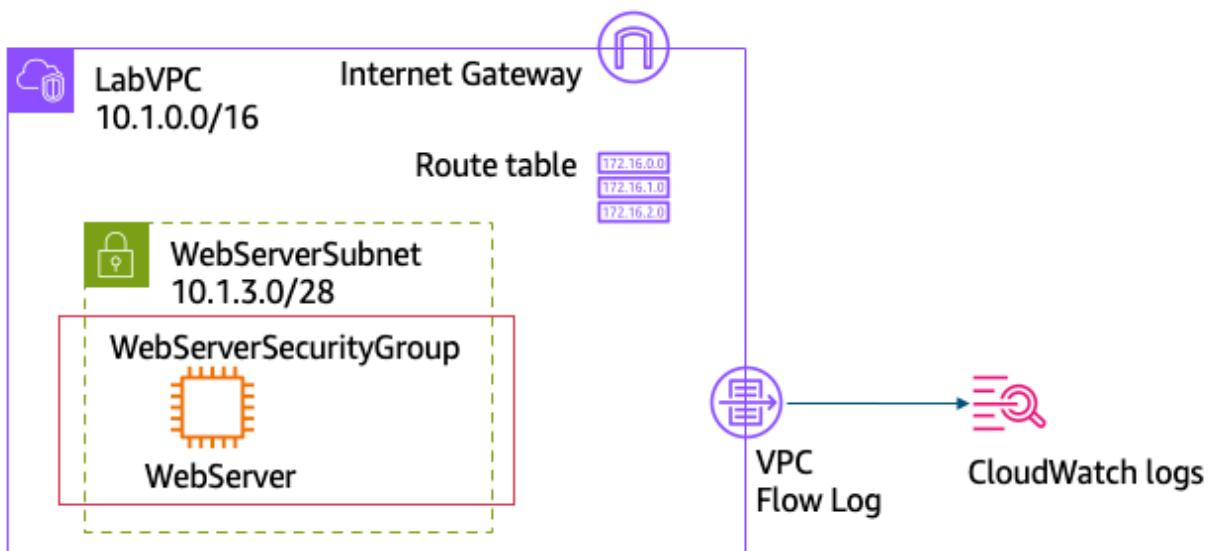
Phase 2: Securing VPCs

AWS-Cloud-Security-Project

Task 2.1: Review LabVPC and its associated resources



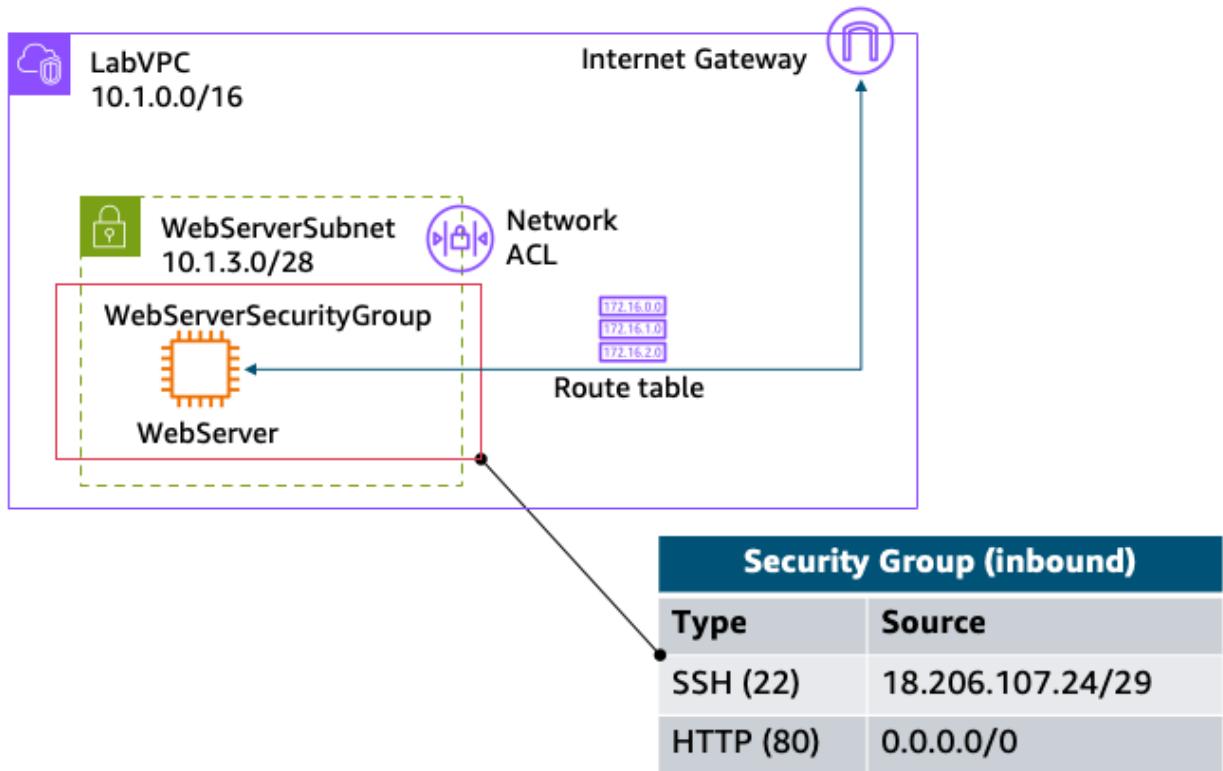
Task 2.2: Create a VPC flow log



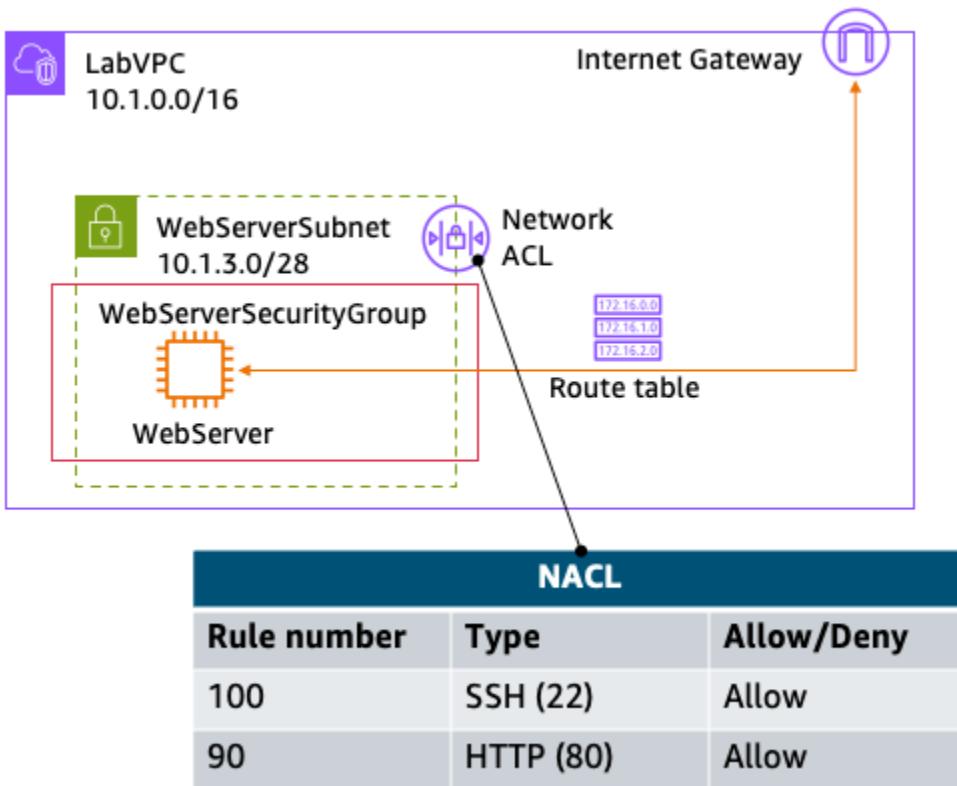
Task 2.3: Access the WebServer instance from the internet and review VPC flow logs in CloudWatch

Task 2.4: Configure route table and security group settings

AWS-Cloud-Security-Project



Task 2.5: Secure the WebServerSubnet with a network ACL



AWS-Cloud-Security-Project

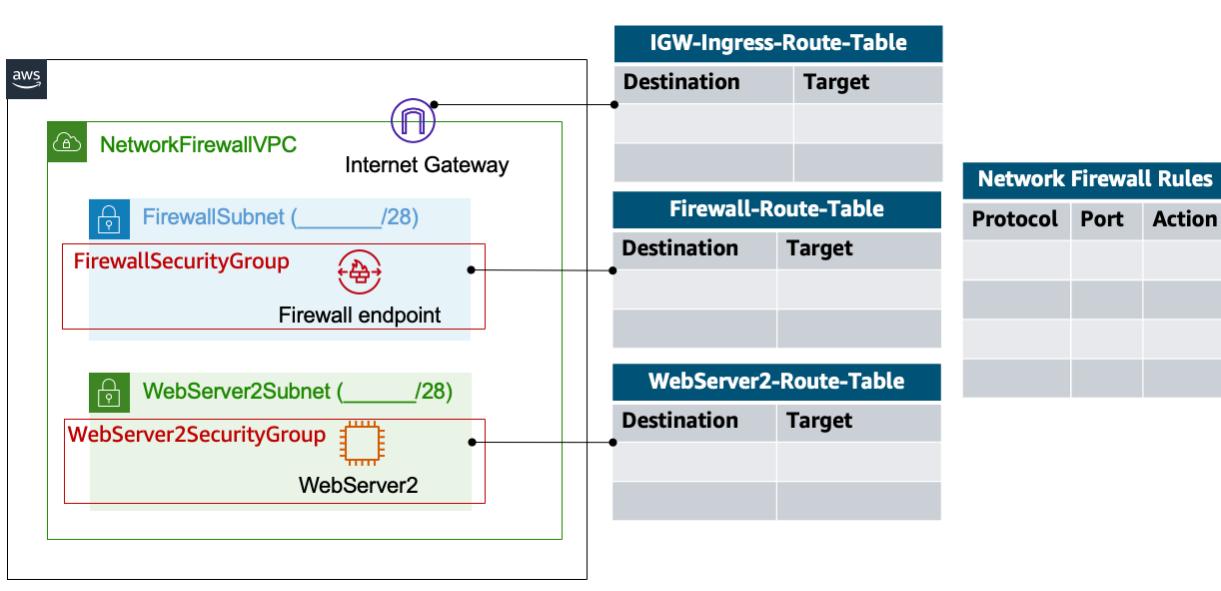
Task 2.6: Review NetworkFirewallVPC and its associated resources

Task 2.7: Create a network firewall

Task 2.8: Create route tables

Task 2.9: Configure logging for the network firewall

Task 2.10: Configure the firewall policy and test access



AWS-Cloud-Security-Project

The screenshot shows the AWS VPC Details page for the VPC `vpc-059424fd9aa796a2c`. The page displays various configuration details:

VPC ID	State	Block Public Access	DNS hostnames
<code>vpc-059424fd9aa796a2c</code>	Available	Off	Enabled
DNS resolution	Tenancy	DHCP option set	Main route table
Enabled	Default	<code>dopt-0ad0897bb7a0084d0</code>	<code>rtb-0519dfa6873cdafec</code>
Main network ACL	Default VPC	IPv4 CIDR	IPv6 pool
<code>acl-072d72f95ff8ddd13</code>	No	<code>10.1.0.0/16</code>	-
IPv6 CIDR (Network border group)	Network Address Usage metrics	Route 53 Resolver DNS Firewall rule groups	Owner ID
-	Disabled	-	<code>902625889566</code>

Below the table, there are tabs for Resource map, CIDRs, Flow logs, Tags, and Integrations.

The screenshot shows the AWS Subnet Details page for the subnet `subnet-0757fe0b1ee40ad48`. The page displays various configuration details:

Subnet ID	Subnet ARN	State	Block Public Access
<code>subnet-0757fe0b1ee40ad48</code>	<code>arn:aws:ec2:us-east-1:902625889566:subnet/subnet-0757fe0b1ee40ad48</code>	Available	Off
IPv4 CIDR	IPv6 CIDR	IPv6 CIDR association ID	-
<code>10.1.3.0/28</code>	-	-	-
Availability Zone	Available IPv4 addresses	Network border group	VPC
<code>us-east-1a</code>	<code>10</code>	<code>us-east-1</code>	<code>vpc-059424fd9aa796a2c LabVPC</code>
Route table	Availability Zone ID	Default subnet	Auto-assign public IPv4 address
<code>rtb-0519dfa6873cdafec</code>	<code>use1-az4</code>	No	Yes
Auto-assign IPv6 address	Network ACL	Customer-owned IPv4 pool	Outpost ID
No	<code>acl-072d72f95ff8ddd13</code>	-	-
Auto-assign customer-owned IPv4 address	Auto-assign customer-owned IPv4 address	IPv6-only	-

Below the table, there are tabs for Resource map, CIDRs, Flow logs, Tags, and Integrations.

AWS-Cloud-Security-Project

Your VPCs (1/1) [Info](#)

VPC ID : vpc-059424fd9aa796a2c [X](#) [Clear filters](#)

Last updated 1 minute ago [Actions](#) [Create VPC](#)

Name	VPC ID	State	Block Public...	IPv4 CIDR
vpc-059424fd9aa796a2c / LabVPC	vpc-059424fd9aa796a2c	Available	Off	10.0.0.0/16

[Details](#) [Resource map](#) [CIDRs](#) [Flow logs](#) [Tags](#) [Integrations](#)

Details

VPC ID	State	Block Public Access	DNS hostnames
vpc-059424fd9aa796a2c	Available	Off	Enabled
DNS resolution	Tenancy	DHCP option set	Main route table
Enabled	Default	dopt-0ad0897bb7a0084d0	rtb-0519dfa6873cdafed
Main network ACL	Default VPC	IPv4 CIDR	IPv6 pool
		10.0.0.0/16	

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 11:04 AM 2024-12-12

VPCFlowLogsRole [Info](#)

Summary

Creation date December 09, 2024, 16:33 (UTC-05:00)

Last activity -

ARN arn:aws:iam::902625889566:role/VPCFlowLogsRole

Maximum session duration 1 hour

[Edit](#) [Delete](#)

Permissions [Trust relationships](#) [Tags \(1\)](#) [Last Accessed](#) [Revoke sessions](#)

Permissions policies (1) [Info](#) [C](#) [Simulate](#) [Remove](#) [Add permissions](#) [Filter by Type](#)

You can attach up to 10 managed policies.

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 11:06 AM 2024-12-12

AWS-Cloud-Security-Project

The screenshot displays two side-by-side AWS EC2 management console pages.

Left Page: Instance summary for i-064b33f20b43b59b5 (WebServer)

- Instance ID:** i-064b33f20b43b59b5
- IPv6 address:** -
- Hostname type:** IP name: ip-10-1-3-4.ec2.internal
- Answer private resource DNS name:** -
- Auto-assigned IP address:** -
- Public IPv4 address:** 52.71.226.27 | open address
- Instance state:** Running
- Private IP DNS name (IPv4 only):** ip-10-1-3-4.ec2.internal
- Instance type:** t2.micro
- VPC ID:** vpc-059424fd9aa796a2c
- Private IPv4 addresses:** 10.1.3.4
- Public IPv4 DNS:** ec2-52-71-226-27.compute-1.amazonaws.com | open address
- Elastic IP addresses:** 52.71.226.27 (WebServerEIP) [Public IP]

Right Page: Security Groups > sg-00928f27d2fac7dd0 - WebServerSecurityGroup

- Security group name:** WebServerSecurityGroup
- Security group ID:** sg-00928f27d2fac7dd0
- Description:** WebServerSecurityGroup
- VPC ID:** vpc-059424fd9aa796a2c
- Owner:** 902625889566
- Inbound rules count:** 1 Permission entry
- Outbound rules count:** 1 Permission entry

Inbound rules (1):

Name	Security group rule ID	IP version	Type	Protocol
-	sgr-0f7ffa891d9689f71	IPv4	Custom TCP	TCP

AWS-Cloud-Security-Project

The image displays three screenshots of the AWS Cloud Services interface, specifically focusing on security groups, subnets, and the VPC dashboard.

Screenshot 1: Security Groups

This screenshot shows the AWS CloudShell interface with the AWS logo and a search bar at the top. The main content area is titled "Security Groups" and shows a single security group named "WebServerSecurityGroup". Key details include:

- Security group ID: sg-00928f27d2fac7dd0
- Description: WebServerSecurityGroup
- VPC ID: vpc-059424fd9aa796a2c
- Owner: 902625889566
- Inbound rules count: 1 Permission entry
- Outbound rules count: 1 Permission entry

The "Outbound rules" tab is selected, displaying one rule:

Name	Security group rule ID	IP version	Type	Protocol
-	sgr-06299fb762cd8d020	IPv4	All traffic	All

Screenshot 2: Subnets

This screenshot shows the AWS CloudShell interface with the AWS logo and a search bar at the top. The main content area is titled "Subnets" and shows a subnet named "subnet-0757fe0b1ee40ad48". Key details include:

Subnet ID	Subnet ARN	State	Block Public Access
subnet-0757fe0b1ee40ad48	arn:aws:ec2:us-east-1:902625889566:subnet/subnet-0757fe0b1ee40ad48	Available	Off
IPv4 CIDR	10.1.3.0/28	IPv6 CIDR	IPv6 CIDR association ID
Availability Zone	us-east-1a	Network border group	VPC
Route table	rtb-0519dfa6873cdafcb	Availability Zone ID	vpc-059424fd9aa796a2c LabVPC
Auto-assign IPv6 address	No	Default subnet	Auto-assign public IPv4 address
		Customer-owned IPv4 pool	Yes
		IPv6-only	Outpost ID

Screenshot 3: VPC dashboard

This screenshot shows the AWS CloudShell interface with the AWS logo and a search bar at the top. The main content area is titled "VPC dashboard" and shows the "Subnets" section. Key details include:

- EC2 Global View
- Virtual private cloud: Your VPCs
- Subnets: subnet-0757fe0b1ee40ad48 / WebServerSubnet
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists

AWS-Cloud-Security-Project

The screenshot shows the AWS VPC dashboard for a VPC named "vpc-059424fd9aa796a2c / LabVPC". The "Details" tab is selected. Key configuration details include:

- VPC ID: `vpc-059424fd9aa796a2c`
- State: Available
- Block Public Access: Off
- DNS resolution: Enabled
- Tenancy: default
- Main network ACL: `acl-072d72f95ff8ddd13`
- Default VPC: No
- IPv4 CIDR: `10.1.0.0/16`
- IPv6 CIDR (Network border group): -
- Network Address Usage metrics: Disabled
- Route 53 Resolver DNS: Firewall rule groups: -
- IPv6 pool: -
- Owner ID: `902625889566`

The "Actions" menu is open, showing options like "Create flow log", "Edit VPC settings", "Edit CIDRs", etc.

Flow logs section (bottom of the screenshot):

Name - optional: LabVPCFlowLogs

Filter: All (radio button selected)

Maximum aggregation interval: 10 minutes (radio button selected)

Destination:

- Send to CloudWatch Logs (radio button selected)
- Send to an Amazon S3 bucket
- Send to Amazon Data Firehose in the same account
- Send to Amazon Data Firehose in a different account

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 11:18 AM 2024-12-12

AWS-Cloud-Security-Project

The screenshot shows two windows side-by-side. The top window is a web browser in Incognito mode, displaying a message about privacy. The bottom window is the AWS Management Console showing details for an EC2 instance.

Incognito Mode Message:

You've gone Incognito

Others who use this device won't see your activity, so you can browse more privately. This won't change how data is collected by websites you visit and the services they use, including Google. Downloads, bookmarks and reading list items will be saved. [Learn more](#)

Chrome won't save:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

Block third-party cookies

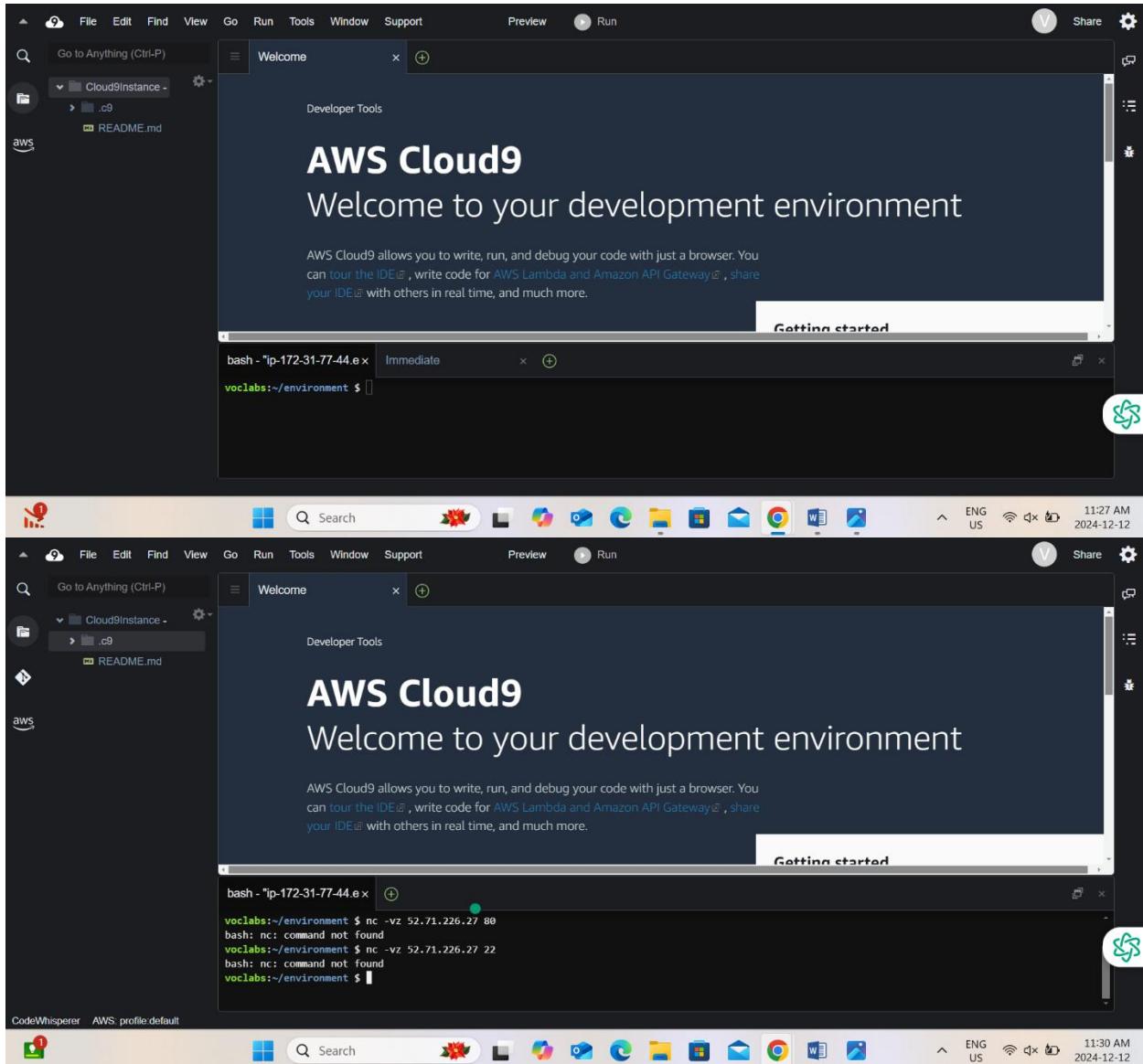
When on, sites can't use cookies that track you across the web. Features on some sites may break.

AWS EC2 Instance Summary:

Instance summary for i-064b33f20b43b59b5 (WebServer)

Attribute	Value
Instance ID	i-064b33f20b43b59b5
IPv6 address	-
Hostname type	IP name: ip-10-1-3-4.ec2.internal
Answer private resource DNS name	-
Public IPv4 address	52.71.226.27
Private IP4 addresses	10.1.3.4
Public IPv4 DNS	ec2-52-71-226-27.compute-1.amazonaws.com
Elastic IP addresses	52.71.226.27 (WebServerEIP) [Public IP]
VPC ID	-

AWS-Cloud-Security-Project



AWS-Cloud-Security-Project

The screenshot shows two side-by-side browser windows for the AWS CloudWatch service.

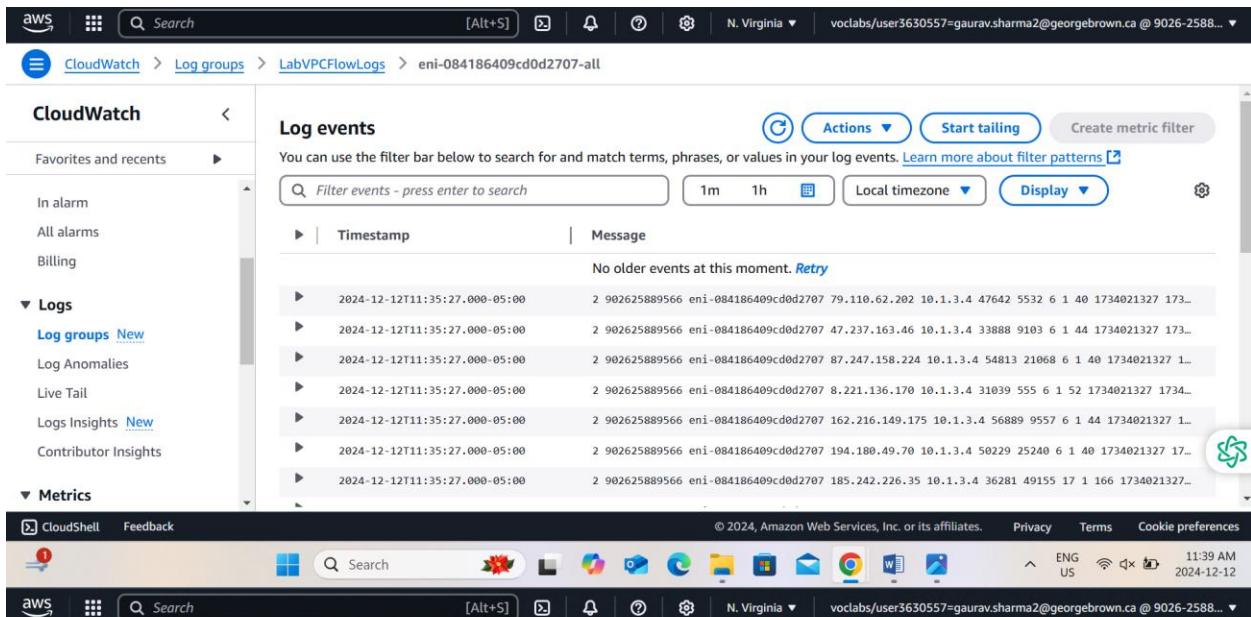
Left Window (Metrics):

- URL: <https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2/log-groups>
- Header: AWS CloudWatch > Dashboards
- Left sidebar: CloudWatch, Favorites and recent, Alarms, Logs (Log groups, Log Anomalies, Live Tail, Logs Insights, Contributor Insights), Metrics.
- Main content: "Custom dashboards" tab selected. Subtitle: "Custom Dashboards (0) Info". Buttons: Share dashboard, Delete, Create dashboard. A message: "No dashboards. You have not created any dashboards." with a "Create dashboard" button.

Right Window (Log groups):

- URL: <https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2/log-groups>
- Header: AWS CloudWatch > Log groups > LabVPCFlowLogs
- Left sidebar: CloudWatch, Favorites and recent, Alarms, Logs (Log groups, Log Anomalies, Live Tail, Logs Insights, Contributor Insights), Metrics.
- Main content: "LabVPCFlowLogs" page. Subtitle: "Log group details".
 - Log class: Standard
 - ARN: arn:aws:logs:us-east-1:902625889566:log-group:LabVPCFlowLogs:*
 - Metric filters: 0
 - Subscription filters: 0
 - Contributor Insights rules: -
 - KMS key ID: -
 - Anomaly detection: Configure
 - Data protection: -
 - Sensitive data count: -
 - Field indexes: Configure
 - Transformer: Configure

AWS-Cloud-Security-Project



CloudWatch > Log groups > LabVPCFlowLogs > eni-084186409cd0d2707-all

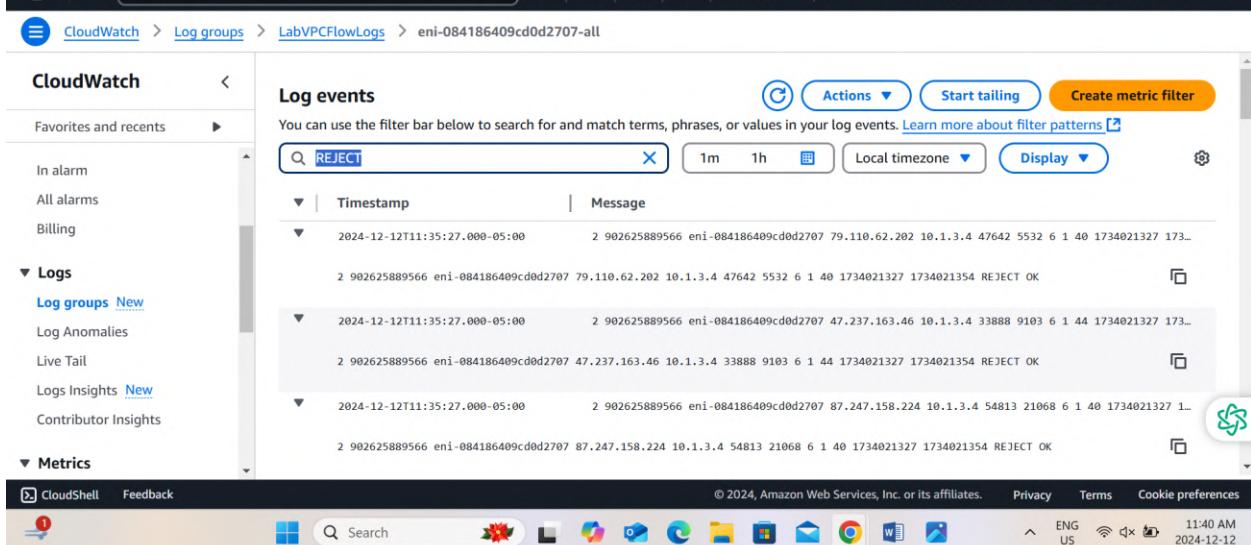
Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Filter events - press enter to search | 1m | 1h | Local timezone | Display | Actions | Start tailing | Create metric filter

Timestamp	Message
2024-12-12T11:35:27.000-05:00	2 902625889566 eni-084186409cd0d2707 79.110.62.202 10.1.3.4 47642 5532 6 1 40 1734021327 173...
2024-12-12T11:35:27.000-05:00	2 902625889566 eni-084186409cd0d2707 47.237.163.46 10.1.3.4 33888 9103 6 1 44 1734021327 173...
2024-12-12T11:35:27.000-05:00	2 902625889566 eni-084186409cd0d2707 87.247.158.224 10.1.3.4 54813 21068 6 1 40 1734021327 1...
2024-12-12T11:35:27.000-05:00	2 902625889566 eni-084186409cd0d2707 8.221.136.170 10.1.3.4 31039 555 6 1 52 1734021327 173...
2024-12-12T11:35:27.000-05:00	2 902625889566 eni-084186409cd0d2707 162.216.149.175 10.1.3.4 56889 9557 6 1 44 1734021327 1...
2024-12-12T11:35:27.000-05:00	2 902625889566 eni-084186409cd0d2707 194.180.49.70 10.1.3.4 50229 25240 6 1 40 1734021327 17...
2024-12-12T11:35:27.000-05:00	2 902625889566 eni-084186409cd0d2707 185.242.226.35 10.1.3.4 36288 49155 17 1 166 1734021327...

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 11:39 AM 2024-12-12



CloudWatch > Log groups > LabVPCFlowLogs > eni-084186409cd0d2707-all

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

REJECT | 1m | 1h | Local timezone | Display | Actions | Start tailing | Create metric filter

Timestamp	Message
2024-12-12T11:35:27.000-05:00	2 902625889566 eni-084186409cd0d2707 79.110.62.202 10.1.3.4 47642 5532 6 1 40 1734021327 173...
2 902625889566 eni-084186409cd0d2707 79.110.62.202 10.1.3.4 47642 5532 6 1 40 1734021327 1734021354 REJECT OK	REJECT
2024-12-12T11:35:27.000-05:00	2 902625889566 eni-084186409cd0d2707 47.237.163.46 10.1.3.4 33888 9103 6 1 44 1734021327 173...
2 902625889566 eni-084186409cd0d2707 47.237.163.46 10.1.3.4 33888 9103 6 1 44 1734021327 1734021354 REJECT OK	REJECT
2024-12-12T11:35:27.000-05:00	2 902625889566 eni-084186409cd0d2707 87.247.158.224 10.1.3.4 54813 21068 6 1 40 1734021327 1...
2 902625889566 eni-084186409cd0d2707 87.247.158.224 10.1.3.4 54813 21068 6 1 40 1734021327 1734021354 REJECT OK	REJECT

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 11:40 AM 2024-12-12

AWS-Cloud-Security-Project

The screenshot shows a terminal window and an AWS VPC dashboard side-by-side.

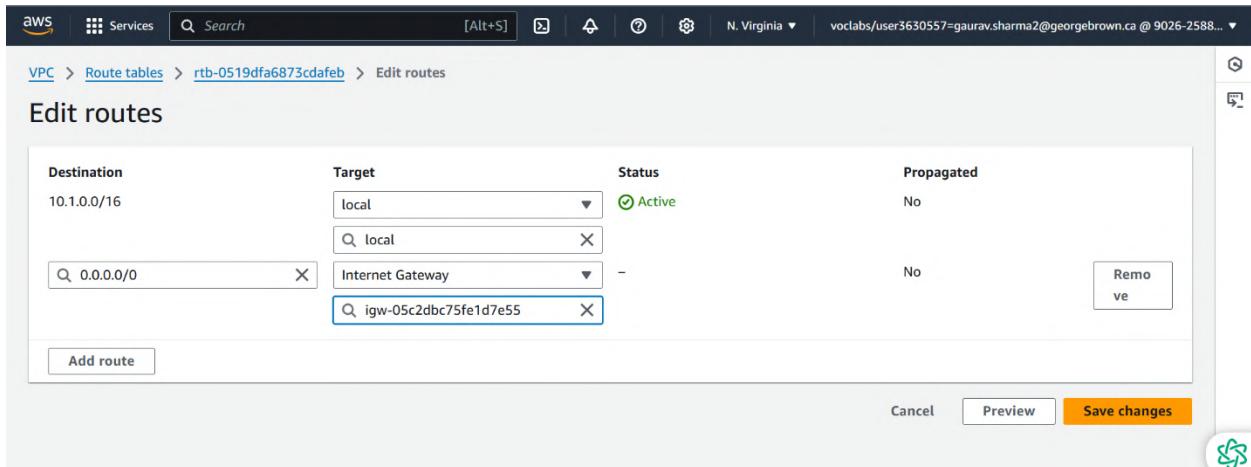
Terminal Window (curl -i 12-31-7-44.ec x):

```
voclabs:~/environment $ nc -vz 52.71.226.27 80
bash: nc: command not found
voclabs:~/environment $ nc -vz 52.71.226.27 22
bash: nc: command not found
voclabs:~/environment $ clear
voclabs:~/environment $ curl http://169.254.169.254/latest/meta-data/public-ipv4
44.213.238.3voclabs:~/environment $
```

VPC Dashboard - subnet-0757fe0b1ee40ad48 / WebServerSubnet:

Details	
Subnet ID	subnet-0757fe0b1ee40ad48
Subnet ARN	arn:aws:ec2:us-east-1:902625889566:subnet/subnet-0757fe0b1ee40ad48
State	Available
IPv6 CIDR	-
Available IPv4 addresses	10
Network border group	us-east-1
IPv6 CIDR association ID	-
Availability Zone	us-east-1a
Availability Zone ID	use1-az4
Default subnet	No
VPC	vpc-059424fd9aa796a2c LabVPC
Route table	rtb-0519dfa6873cdafab
Network ACL	acl-072d72f95ff8ddd13
Customer-owned IPv4 pool	-
Auto-assign IPv6 address	No
Auto-assign customer-owned IPv4 address	-
IPv6-only	-
Auto-assign public IPv4 address	Yes
Outpost ID	-

AWS-Cloud-Security-Project

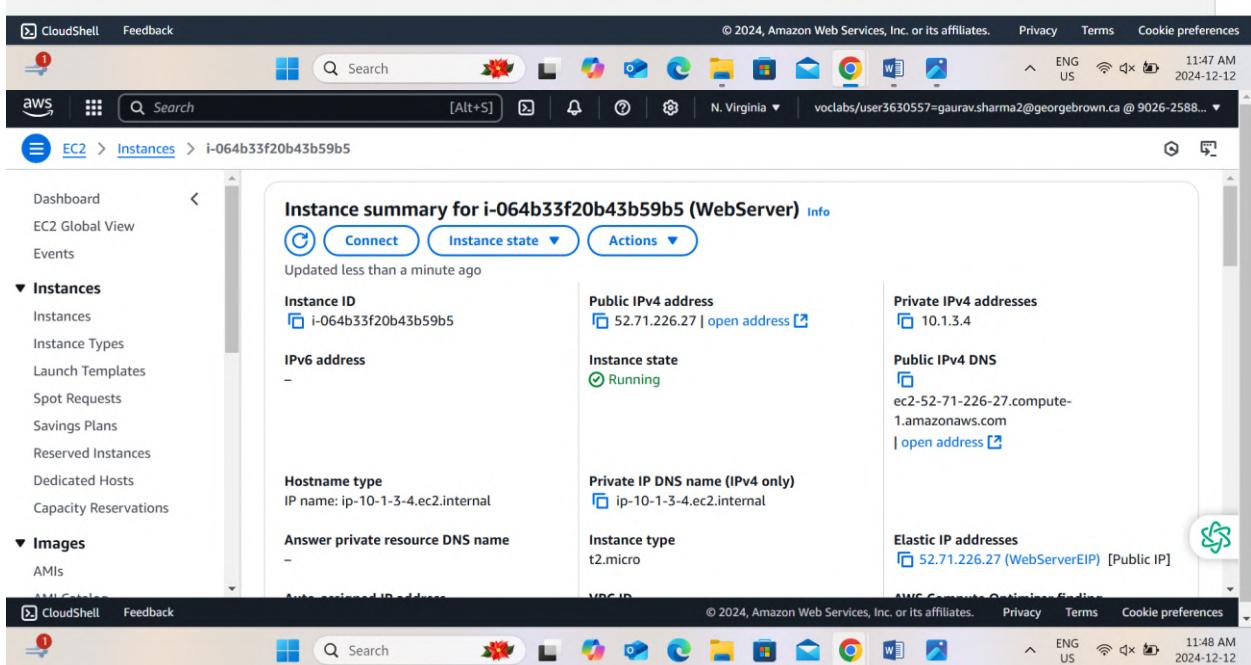


The screenshot shows the 'Edit routes' page for a specific route table. The table has one existing route:

Destination	Target	Status	Propagated
10.1.0.0/16	local	Active	No

Below this, there is a search bar for '0.0.0.0/0' and a dropdown menu showing 'Internet Gateway' and 'igw-05c2dbc75fe1d7e55'. A button labeled 'Add route' is visible.

Buttons at the bottom include 'Cancel', 'Preview', and 'Save changes'.



The screenshot shows the 'Instance summary for i-064b33f20b43b59b5 (WebServer)' page. Key details include:

- Public IPv4 address:** 52.71.226.27 (with a 'Connect' button)
- Private IP4 addresses:** 10.1.3.4
- Public IPv4 DNS:** ec2-52-71-226-27.compute-1.amazonaws.com
- Private IP DNS name (IPv4 only):** ip-10-1-3-4.ec2.internal
- Instance state:** Running
- Instance type:** t2.micro
- Elastic IP addresses:** 52.71.226.27 (WebServerEIP) [Public IP]

The left sidebar shows navigation links for CloudShell, Feedback, Services, Search, and various AWS services like Lambda, S3, and CloudWatch.

AWS-Cloud-Security-Project

The screenshot displays three stacked screenshots of the AWS Cloud Security Project interface.

Top Screenshot: Shows the EC2 instance details for i-064b33f20b43b59b5. The Security tab is selected. Key details include:

- IAM Role:** WebServerRole
- Owner ID:** 902625889566
- Launch time:** Thu Dec 12 2024 11:00:53 GMT-0500 (Eastern Standard Time)
- Security groups:** sg-00928f27d2fac7dd0 (WebServerSecurityGroup)

Middle Screenshot: Shows the Inbound rules for the security group sg-00928f27d2fac7dd0. The table lists two rules:

Name	Protocol	Port range	Source	Description - optional
-	HTTP	TCP 80	A... 0.0.0.0/0	
-	SSH	TCP 22	C... 44.213.238.3/	44.213.238.3/32

Bottom Screenshot: Shows the CloudShell interface with the command history and environment information.

AWS-Cloud-Security-Project

The image consists of three vertically stacked screenshots of a terminal window, likely from a Cloud9 instance or AWS Lambda environment. Each screenshot shows a different step in the deployment process.

Screenshot 1: The terminal shows the download and installation of the jq package. It includes a progress bar for the download of 'jq-1.5-1.amzn2.0.2.x86_64.rpm' (154 kB) and the command to install it.

```
(2/2): jq-1.5-1.amzn2.0.2.x86_64.rpm
Total
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : oniguruma-5.9.6-1.amzn2.0.7.x86_64
  Installing : jq-1.5-1.amzn2.0.2.x86_64
  Verifying : jq-1.5-1.amzn2.0.2.x86_64
  Verifying : oniguruma-5.9.6-1.amzn2.0.7.x86_64

Installed:
  jq.x86_64 0:1.5-1.amzn2.0.2

Dependency Installed:
  oniguruma.x86_64 0:5.9.6-1.amzn2.0.7

Complete!
```

Screenshot 2: The terminal shows the curl command to fetch AWS IP ranges and the jq command to parse the JSON output to filter regions and services.

```
vclabs:~/environment $ curl https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select(.region=="us-east-1") | select(.service=="EC2_INSTANCE_CONNECT") | .ip_prefix'
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload  Upload Total Spent   Left  Speed
100 1738k  100 1738k    0     0  13.6M      0 --:--:-- --:--:-- 13.6M
18.206.107.24/29
vclabs:~/environment $
vclabs:~/environment $
```

Screenshot 3: The terminal shows the sudo yum command to install jq, followed by the same curl and jq command as in Screenshot 2.

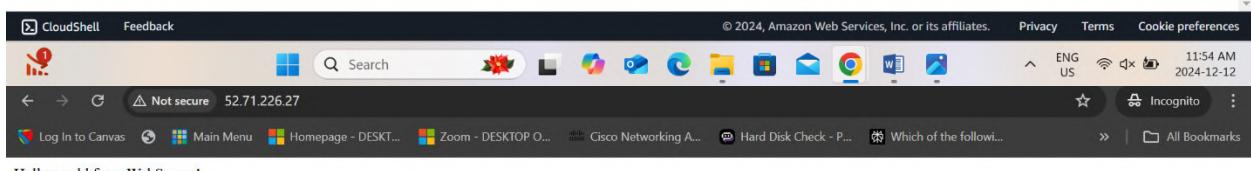
```
vclabs:~/environment $ sudo yum install -y jq
Loaded plugins: extras suggestions, langpacks, priorities, update-motd
237 packages excluded due to repository priority protections
Package jq-1.5-1.amzn2.0.2.x86_64 already installed and latest version
Nothing to do
vclabs:~/environment $ curl https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select(.region=="us-east-1") | select(.service=="EC2_INSTANCE_CONNECT") | .ip_prefix'
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload  Upload Total Spent   Left  Speed
100 1738k  100 1738k    0     0  22.7M      0 --:--:-- --:--:-- 22.9M
18.206.107.24/29
vclabs:~/environment $
vclabs:~/environment $ curl https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select(.region=="us-east-1") | select(.service=="EC2_INSTANCE_CONNECT") | .ip_prefix'
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload  Upload Total Spent   Left  Speed
100 1738k  100 1738k    0     0  25.3M      0 --:--:-- --:--:-- 25.3M
18.206.107.24/29
vclabs:~/environment $
```

AWS-Cloud-Security-Project

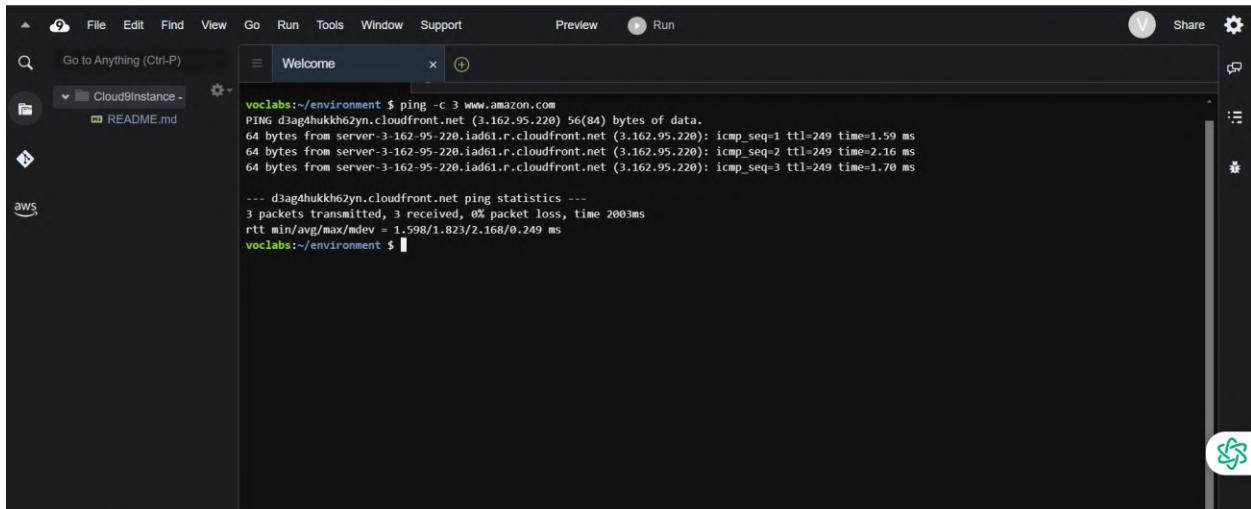
The screenshot shows the AWS CloudShell interface. At the top, there's a navigation bar with the AWS logo, a search bar containing "cloud WAN", and various icons. Below the navigation bar, the URL is "EC2 > Security Groups > sg-00928f27d2fac7dd0 - WebServerSecurityGroup > Edit inbound rules". The main area displays a table of security group rules:

Rule ID	Protocol	Port Range	Action
sgr-00b075fa218904ead	HTTP	80	Allow (0.0.0.0/0)
sgr-0469af9c1a8c528bc	SSH	22	Allow (44.213.238.3/32)
-	SSH	22	Allow (1.206.107.24/29)
-	SSH	22	Allow (18.206.107.24/29)

At the bottom right of the CloudShell window, there are buttons for "Cancel", "Preview changes", "Save rules", and a green checkmark icon.

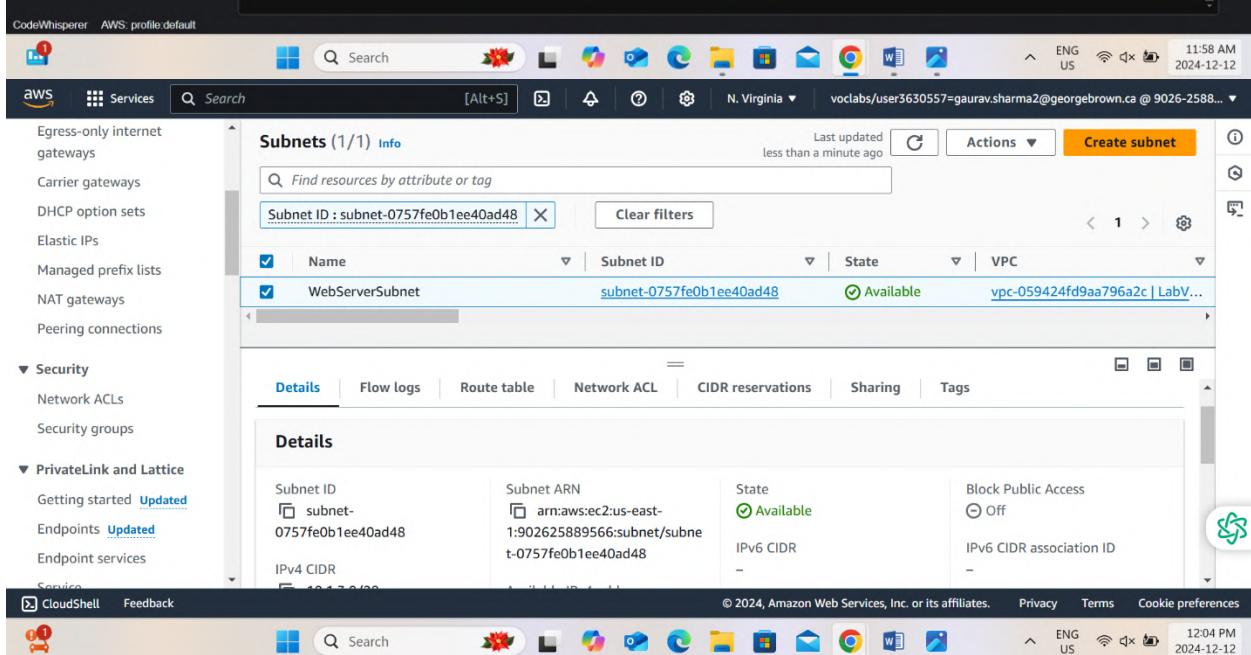


AWS-Cloud-Security-Project



voclabs:~/environment \$ ping -c 3 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (3.162.95.220) 56(84) bytes of data.
64 bytes from server-3-162-95-220.iad61.r.cloudfront.net (3.162.95.220): icmp_seq=1 ttl=249 time=1.59 ms
64 bytes from server-3-162-95-220.iad61.r.cloudfront.net (3.162.95.220): icmp_seq=2 ttl=249 time=2.16 ms
64 bytes from server-3-162-95-220.iad61.r.cloudfront.net (3.162.95.220): icmp_seq=3 ttl=249 time=1.70 ms
--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.598/1.823/2.168/0.249 ms
voclabs:~/environment \$

CodeWhisperer AWS profile.default



Subnets (1/1) Info Last updated less than a minute ago Actions Create subnet

Name	Subnet ID	State	VPC
WebServerSubnet	subnet-0757fe0b1ee40ad48	Available	vpc-059424fd9aa796a2c LabV...

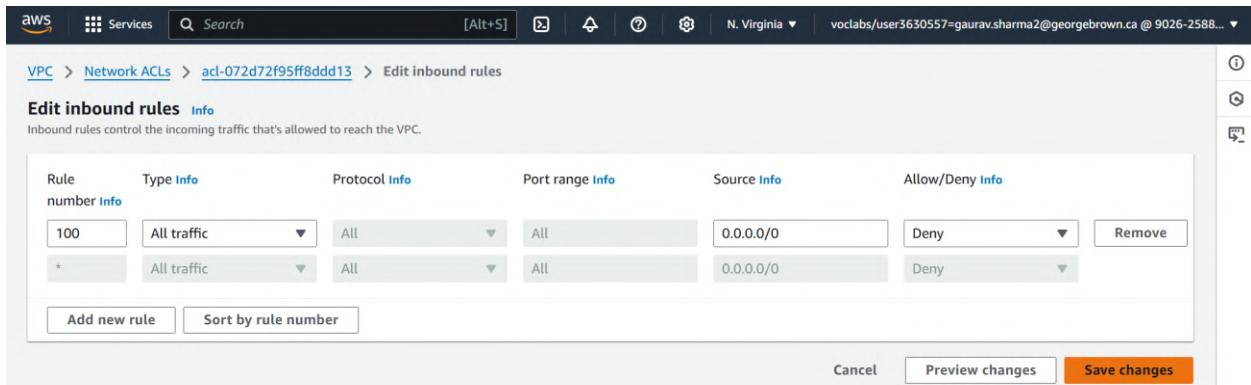
Details Flow logs Route table Network ACL CIDR reservations Sharing Tags

Details

Subnet ID	subnet-0757fe0b1ee40ad48	Subnet ARN	arn:aws:ec2:us-east-1:902625889566:subnet/subnet-0757fe0b1ee40ad48	State	Available	Block Public Access	Off
IPv4 CIDR	10.1.2.0/20			IPv6 CIDR	-	IPv6 CIDR association ID	-

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

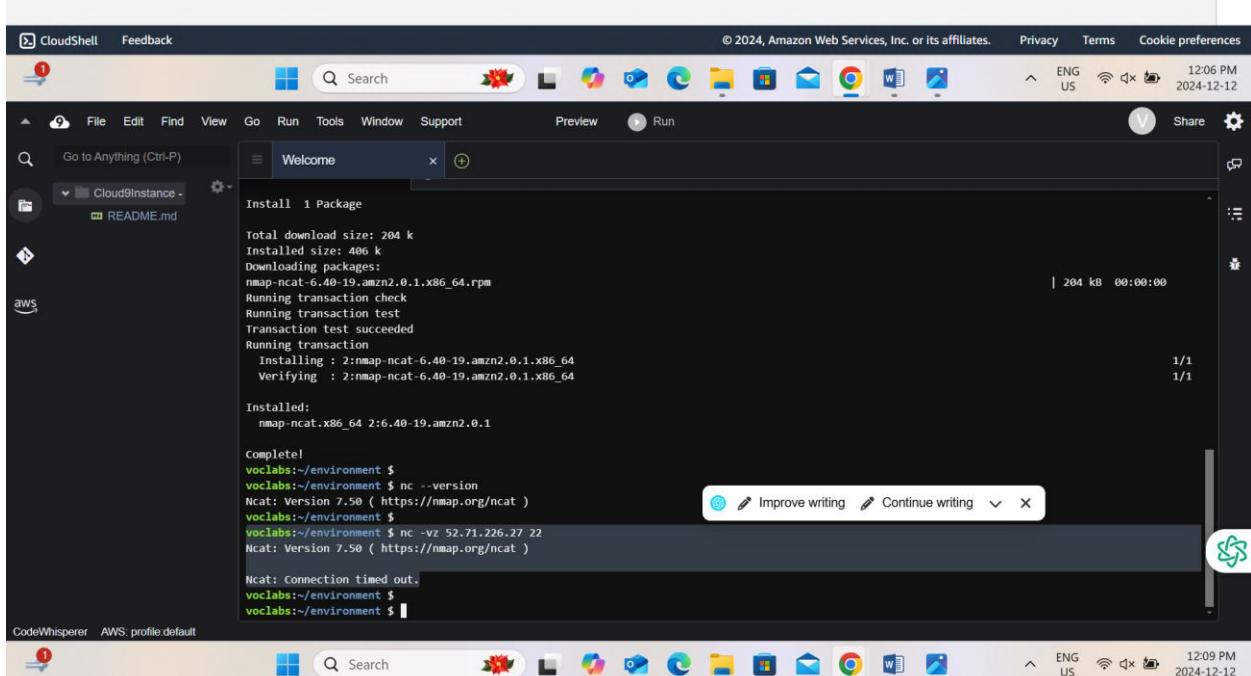
AWS-Cloud-Security-Project



The screenshot shows the AWS VPC Network ACLs configuration page. It displays two inbound rules:

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

Buttons at the bottom include 'Add new rule', 'Sort by rule number', 'Cancel', 'Preview changes', and 'Save changes'.



The screenshot shows the AWS CloudShell terminal window. A package named 'nmap-ncat' is being installed from the Amazon Linux repository. The terminal output shows:

```
Total download size: 264 k
Installed size: 406 k
Downloading packages:
nmap-ncat-6.40-19.amzn2.0.1.x86_64.rpm
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : 2:nmap-ncat-6.40-19.amzn2.0.1.x86_64
  Verifying : 2:nmap-ncat-6.40-19.amzn2.0.1.x86_64
1/1
1/1

Installed:
  nmap-ncat.x86_64 2:6.40-19.amzn2.0.1

Complete!
```

The terminal also shows a few commands being run:

```
voclabs:~/environment $ nc --version
Ncat: Version 7.50 ( https://nmap.org/ncat )
voclabs:~/environment $
voclabs:~/environment $ nc -vz 52.71.226.27 22
Ncat: Version 7.50 ( https://nmap.org/ncat )

Ncat: Connection timed out.
voclabs:~/environment $
voclabs:~/environment $
```

CodeWhisperer and AWS profile default are listed at the bottom of the terminal window.

AWS-Cloud-Security-Project

The screenshot shows the AWS CloudShell interface. At the top, there's a navigation bar with File, Edit, Find, View, Go, Run, Tools, Window, Support, Preview, and Run buttons. Below the navigation bar is a search bar labeled "Go to Anything (Ctrl-P)". A sidebar on the left shows a "Cloud9Instance" folder containing "README.md". The main area is titled "Welcome" and displays terminal output:

```
Downloading packages:
nmap-ncat-6.40-19.amzn2.0.1.x86_64.rpm
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Installing : 2:nmap-ncat-6.40-19.amzn2.0.1.x86_64
1/1
1/1
Installed:
nmap-ncat.x86_64 2:6.40-19.amzn2.0.1

Complete!
vclabs:~/environment $ vclabs:~/environment $ nc --version
Ncat: Version 7.50 ( https://nmap.org/ncat )
vclabs:~/environment $
vclabs:~/environment $ nc -vz 52.71.226.27 22
Ncat: Connected to 52.71.226.27:22.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
vclabs:~/environment $
```

At the bottom of the terminal window, there are buttons for "Improve writing" and "Continue writing". The status bar at the bottom right shows "ENG US" and the date "2024-12-12".

The screenshot shows the "Edit inbound rules" page for a specific Network ACL. The URL is "VPC > Network ACLs > acl-072d72f95ff8ddd13 > Edit inbound rules". The page has a header with "Edit inbound rules" and "Info". Below the header, it says "Inbound rules control the incoming traffic that's allowed to reach the VPC." There is a table with columns: Rule number, Type Info, Protocol Info, Port range Info, Source Info, and Allow/Deny Info.

Rule number	Type Info	Protocol Info	Port range Info	Source Info	Allow/Deny Info
100	SSH (22)	TCP (6)	22	44.213.238.3/32	Allow
90	Custom TCP	TCP (6)	80	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Buttons at the bottom include "Add new rule", "Sort by rule number", "Cancel", "Preview changes", and "Save changes". The status bar at the bottom right shows "ENG US" and the date "2024-12-12".

AWS-Cloud-Security-Project

A screenshot of the AWS Management Console showing the 'Edit inbound rules' page for a Network ACL. The page displays three rules:

Rule number	Type	Protocol	Port range	Source	Action
90	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
100	SSH (22)	TCP (6)	22	44.213.238.3/32	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Buttons at the bottom include 'Add new rule', 'Sort by rule number', 'Cancel', 'Preview changes', and 'Save changes'.

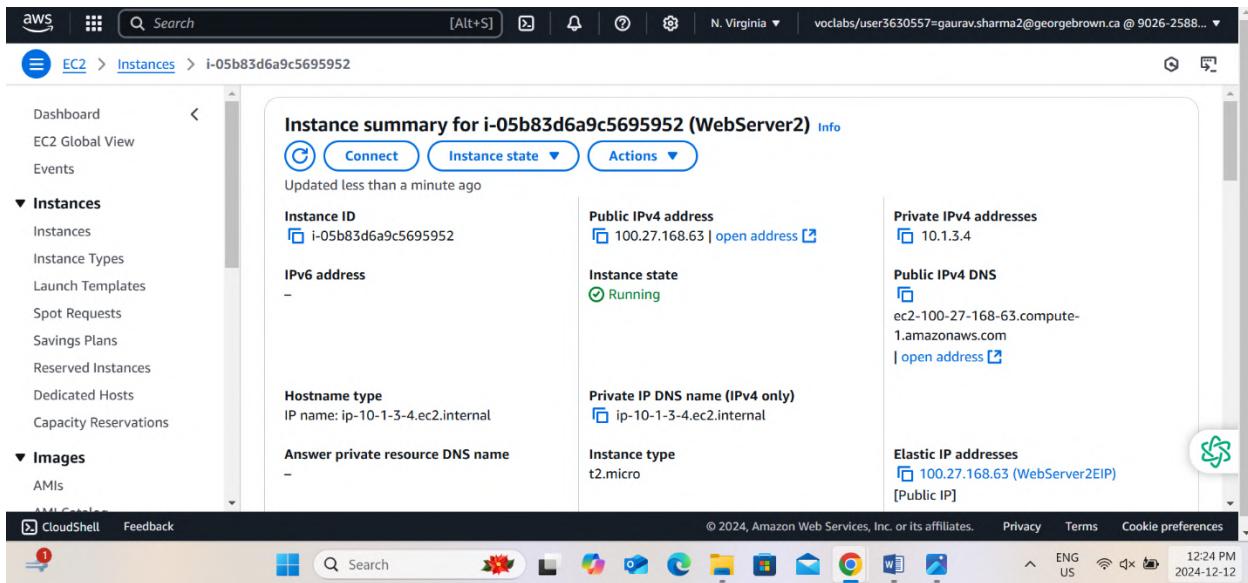
AWS-Cloud-Security-Project

The screenshot shows the AWS CloudShell interface. On the left, a sidebar lists various AWS services: TLS inspection configurations, Network Firewall resource groups, Virtual private network (VPN), Customer gateways, Virtual private gateways, Site-to-Site VPN connections, Client VPN endpoints, and AWS Verified Access. The main area displays a terminal window titled "Welcome" on a "Cloud9Instance" session. The terminal output shows:

```
voclabs:~/environment $ python3 -m http.server 8080 &
[1] 3923
voclabs:~/environment $ Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

The CloudShell interface includes a navigation bar with CloudShell and Feedback buttons, and a status bar at the bottom indicating "CodeWhisperer AWS: profile default". The status bar also shows system information: ENG US, 12:20 PM, 2024-12-12.

AWS-Cloud-Security-Project



Instance summary for i-05b83d6a9c5695952 (WebServer2) [Info](#)

Updated less than a minute ago

Instance ID	Public IPv4 address	Private IPv4 addresses
i-05b83d6a9c5695952	100.27.168.63 open address	10.1.3.4
IPv6 address	Instance state	Public IPv4 DNS
-	Running	ec2-100-27-168-63.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	100.27.168.63 (WebServer2EIP) [Public IP]
Answer private resource DNS name	Instance type	
-	t2.micro	

Hello world from WebServer2!



AWS-Cloud-Security-Project

The screenshot displays two main windows from the AWS CloudShell interface.

Top Window (Terminal):

```
voclabs:~/environment $ python3 -m http.server 8080 &
[1] 3923
voclabs:~/environment $ serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
voclabs:~/environment $ nc -vz 100.27.168.63 22
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 100.27.168.63:22.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
voclabs:~/environment $
```

Bottom Window (AWS Network Firewall):

The AWS Network Firewall interface shows the following details:

- Section:** Security, Identity, and Compliance
- Title:** AWS Network Firewall
- Description:** Managed network firewall service for your Amazon VPC
- Text:** AWS Network Firewall is a stateful, managed network firewall and intrusion prevention/detection service that allows customers to filter traffic at the perimeter of their VPC.
- Buttons:** Start using AWS Network Firewall (with Create firewall button) and Getting started
- Links:** Getting started, What is AWS Network Firewall

AWS-Cloud-Security-Project

The screenshots show the AWS Network Firewall creation process across three steps:

- Step 1: Describe firewall**
 - Firewall details:** Name the firewall "NetworkFirewall".
 - Description - optional:** Enter "Enter firewall description".
- Step 2: Configure VPC and subnets**
 - VPC:** Choose "NetworkFirewallVPC".
 - Firewall subnets:** Set Availability Zone to "us-east-1a", Subnet to "subnet-06949acb...", and IP address type to "IPv4".
- Step 3: Associate firewall policy**
 - No specific configuration shown.

AWS-Cloud-Security-Project

The screenshot shows two separate AWS VPC management interfaces side-by-side.

Top Interface (Network Firewall):

- Header:** AWS Services Search [Alt+S] N. Virginia vclabs/user3630557=gaurav.sharma2@georgebrown.ca @ 9026-2588...
- Left Sidebar:** VPC dashboard, EC2 Global View, Filter by VPC, Virtual private cloud (Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists).
- Middle Content:** NetworkFirewall Overview. Firewall status: Provisioning. Associated firewall policy: Firewallpolicy. Associated VPC: vpc-00d251b85fc2e8405.
- Bottom Navigation:** Firewall details, Firewall policy settings, Monitoring.

Bottom Interface (Route Tables):

- Header:** AWS Services Search [Alt+S] N. Virginia vclabs/user3630557=gaurav.sharma2@georgebrown.ca @ 9026-2588...
- Left Sidebar:** EC2 Global View, Filter by VPC, Virtual private cloud (Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways).
- Middle Content:** Route tables (1/3) Info. A table lists three route tables:

Name	Route table ID	Explicit subnet associations	Edge associations	Main
-	rtb-0b3ea8ad78528c9a1	-	-	Yes
-	rtb-0c52a182d51002eb9	-	-	Yes
<input checked="" type="checkbox"/> -	rtb-0519dfa6873cdafab	-	-	Yes
- Bottom Navigation:** Details, Routes, Subnet associations, Edge associations, Route propagation, Tags.

AWS-Cloud-Security-Project

The screenshot shows the 'Create route table' page in the AWS VPC service. In the 'Route table settings' section, a tag named 'IGW-Ingress-Route-Table' is being added under the 'Name - optional' field. The VPC dropdown is set to 'vpc-00d251b85fc2e8405 (NetworkFirewallVPC)'. Below this, the 'Tags' section is visible, showing a single tag 'IGW-Ingress-Route-Table' assigned to the route table.

The screenshot shows the 'Edit routes' page for the previously created route table. It lists two routes:

Destination	Target	Status	Propagated
10.1.0.0/16	local	Active	No
10.1.3.0/28	Gateway Load Balancer Endpoint	-	No

At the bottom, there are 'Add route', 'Cancel', 'Preview', and 'Save changes' buttons.

The screenshot shows the same 'Edit routes' page after changes have been made. The second route's target has been changed from 'Gateway Load Balancer Endpoint' to 'vpce-00f0fd7fc9ee68ad3'. The 'Save changes' button is highlighted.

AWS-Cloud-Security-Project

The screenshot shows the AWS CloudFormation console with the title "Edit edge associations (1)". It displays basic details for a route table, including its ID (rtb-0519dfa6873cdafab), name (empty), and VPC ID (vpc-059424fd9aa796a2c). A modal window titled "Internet gateway" is open, showing an attached gateway (igw-05c2dbc75fe1d7e55 / LabVPCIG) with a checked "Attached" status. Buttons for "Cancel" and "Save changes" are visible.

Route table basic details

Route table ID rtb-0519dfa6873cdafab	Route table name -	Route table VPC ID vpc-059424fd9aa796a2c
-----------------------------------------	-----------------------	---------------------------------------------

Internet gateway

Gateway ID
[igw-05c2dbc75fe1d7e55 / LabVPCIG](#)

State
 Attached

Owner or ASN (Amazon side)
902625889566

Cancel **Save changes**

The screenshot shows the AWS CloudShell interface with the title "Create route table". It provides instructions for creating a route table, stating that it specifies how packets are forwarded between subnets, the internet, and VPN connections. A "Route table settings" section includes a "Name - optional" field containing "Firewall-Route-Table" and a "VPC" dropdown set to "vpc-00d251b85fc2e8405 (NetworkFirewallVPC)". A "Tags" section explains what tags are and how they can be used to search and filter resources. The CloudShell interface includes standard browser navigation and search bars at the top.

Create route table info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
Firewall-Route-Table

VPC
The VPC to use for this route table.
vpc-00d251b85fc2e8405 (NetworkFirewallVPC)

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

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

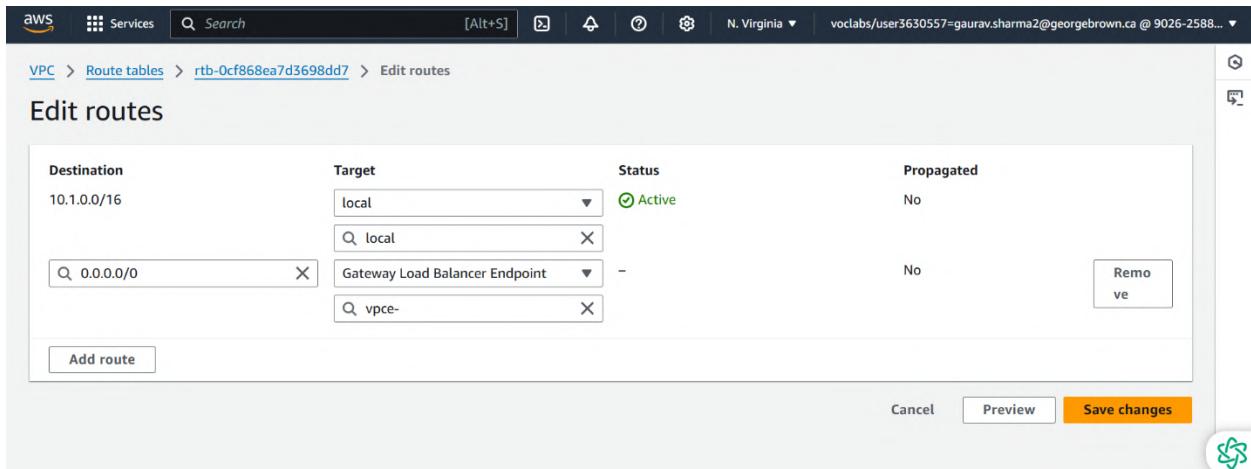
CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS-Cloud-Security-Project

The screenshot shows three sequential steps in the AWS VPC console:

- Edit subnet associations:** A table lists available subnets (WebServer2Subnet and FirewallSubnet) and selected subnets (FirewallSubnet). The selected subnet is highlighted.
- Create route table:** A form for creating a new route table named "WebServer2-Route-Table". It specifies the VPC as "vpc-00d251b85fc2e8405 (NetworkFirewallVPC)".
- Create route table:** A confirmation step where the "Create route table" button is visible.

AWS-Cloud-Security-Project



The screenshot shows the 'Edit routes' page for a specific route table. A route is defined with a destination of 10.1.0.0/16, a target of 'local', and a status of 'Active'. There is also a note indicating 'No propagated routes'. An 'Add route' button is present. Action buttons for 'Cancel', 'Preview', and 'Save changes' are at the bottom.

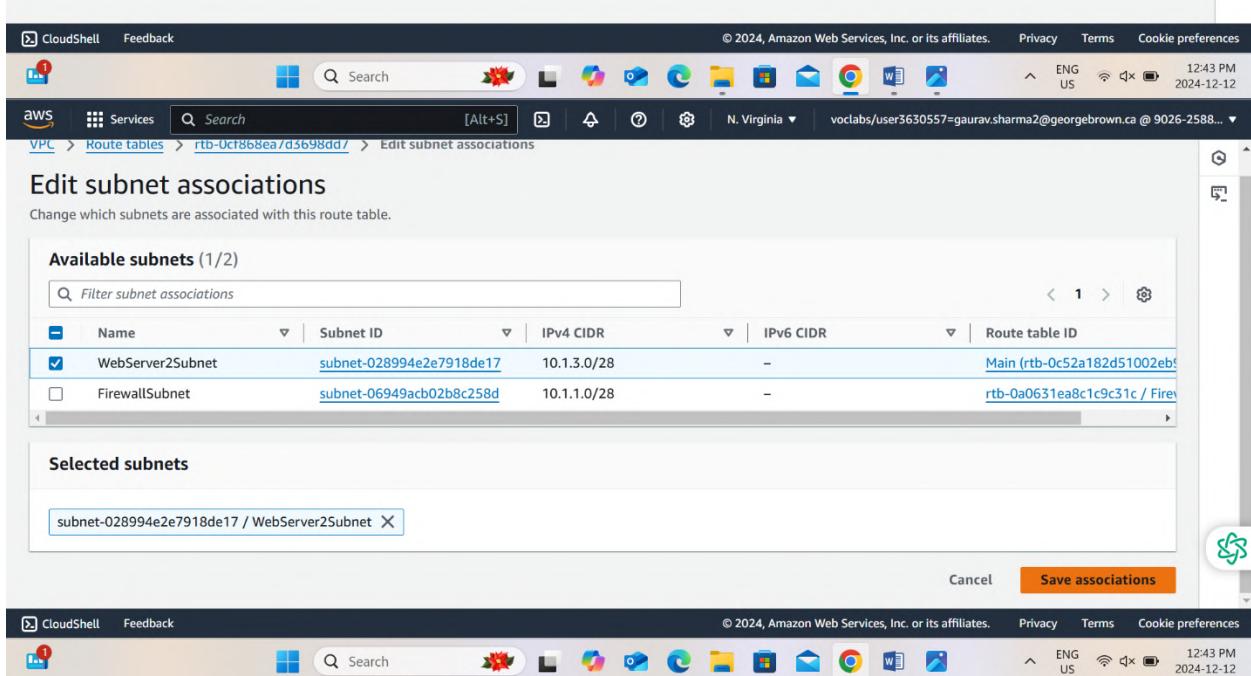
Available subnets (1/2)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/> WebServer2Subnet	subnet-028994e2e7918de17	10.1.3.0/28	-	Main (rtb-0c52a182d51002eb)
<input type="checkbox"/> FirewallSubnet	subnet-06949acb02b8c258d	10.1.1.0/28	-	rtb-0a0631ea8c1c9c31c / Firewall

Selected subnets

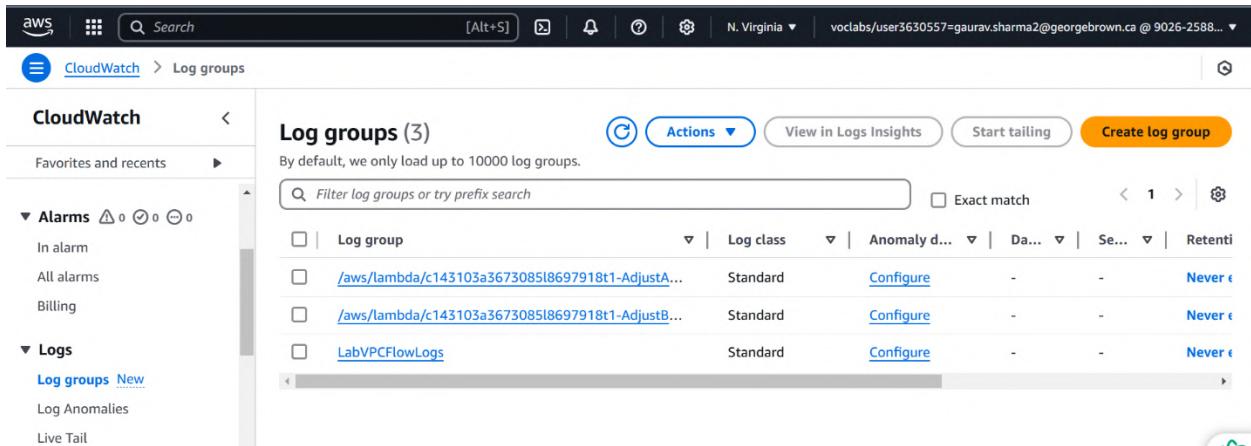
[subnet-028994e2e7918de17 / WebServer2Subnet](#) X

Action buttons: Cancel, Save associations



The screenshot shows the 'Edit subnet associations' page. It lists available subnets and selected subnets. The selected subnet is 'subnet-028994e2e7918de17 / WebServer2Subnet'. Action buttons for 'Cancel' and 'Save associations' are at the bottom.

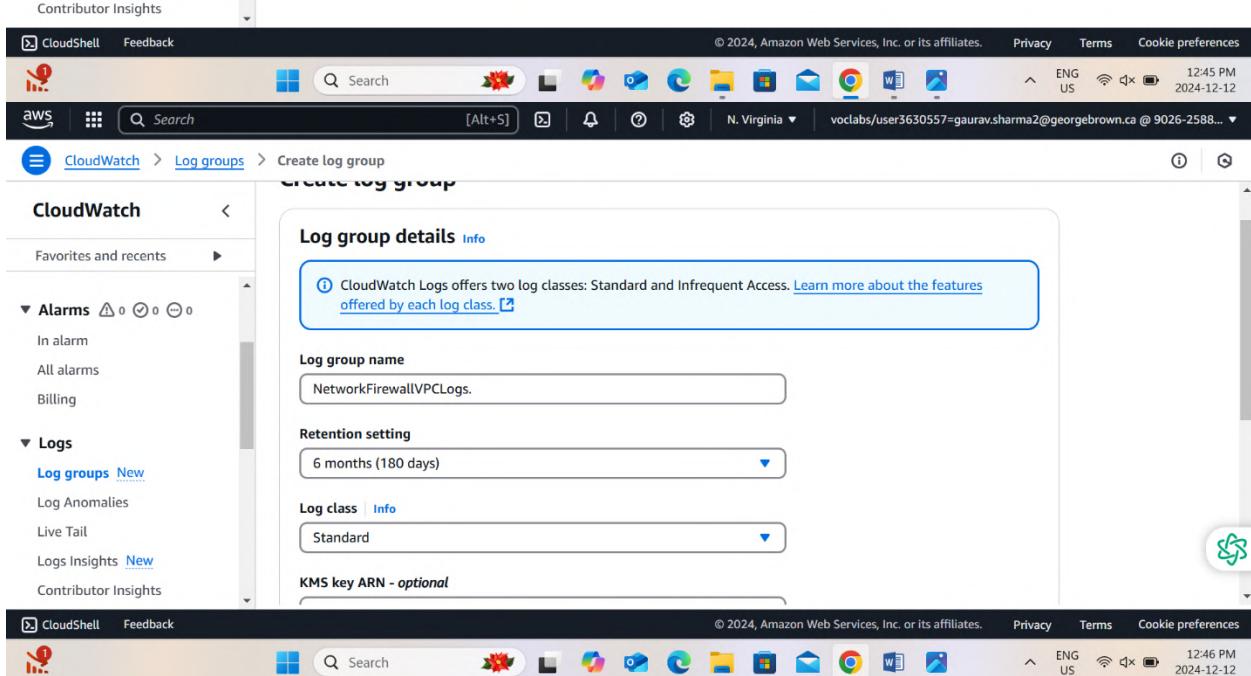
AWS-Cloud-Security-Project



The screenshot shows the AWS CloudWatch Log groups interface. On the left, there's a navigation sidebar with 'CloudWatch' selected. Under 'Logs', 'Log groups' is also selected. The main area displays 'Log groups (3)'. A table lists three log groups:

Log group	Log class	Anomaly d...	Data...	Se...	Retenti...
/aws/lambda/c143103a3673085l8697918t1-AdjustA...	Standard	Configure	-	-	Never
/aws/lambda/c143103a3673085l8697918t1-AdjustB...	Standard	Configure	-	-	Never
LabVPCFlowLogs	Standard	Configure	-	-	Never

On the right, there are buttons for 'Actions', 'View in Logs Insights', 'Start tailing', and 'Create log group'. Below the table is a search bar and some filtering options.



The screenshot shows the 'Create log group' interface. The left sidebar is identical to the previous screen. The main area has a title 'Create log group' and a section titled 'Log group details'. It contains the following fields:

- Log group name:** NetworkFirewallVPCLogs.
- Retention setting:** 6 months (180 days)
- Log class:** Standard
- KMS key ARN - optional:** (empty field)

At the bottom, there are 'Create' and 'Cancel' buttons.

AWS-Cloud-Security-Project

The image displays three vertically stacked screenshots of the AWS Network Firewall configuration interface, showing different sections of the settings.

Screenshot 1: Change protections

Change protections

Delete protection	Subnet change protection
Disabled	Disabled

Logging

Network Firewall generates logs for stateful rule groups. You can configure different destinations for different log types.

Log type	Alert log destination	Flow log destination	TLS log destination
Not configured	Not configured	Not configured	Not configured

Customer managed key

Key type: AWS owned key

Screenshot 2: Log type configuration

Log type

You can choose to emit alert logs, flow logs, or both.

Alert

Flow

TLS

Alert log destination

Log destination

You can send each log type to a S3 bucket, a CloudWatch log group, or a Kinesis Data Firehose delivery stream.

S3

CloudWatch log group

Kinesis data firehose

CloudWatch log group

Send the logs to a CloudWatch log group.

NetworkFirewallVPCLogs. Create log group

Screenshot 3: Alert log destination configuration

Alert log destination

Log destination

You can send each log type to a S3 bucket, a CloudWatch log group, or a Kinesis Data Firehose delivery stream.

S3

CloudWatch log group

Kinesis data firehose

CloudWatch log group

Send the logs to a CloudWatch log group.

NetworkFirewallVPCLogs. Create log group

AWS-Cloud-Security-Project

The screenshot shows the AWS EC2 Instances page. A specific instance, i-05b83d6a9c5695952 (WebServer2), is selected. The instance summary panel displays details like Instance ID (i-05b83d6a9c5695952), Instance state (Running), and Private IP4 address (10.1.3.4). A green callout bubble highlights the Public IPv4 address (100.27.168.63) which has been copied. The browser toolbar at the bottom shows the URL 100.27.168.63.



100.27.168.63 doesn't support a secure connection

You are seeing this warning because this site does not support HTTPS and you are in Incognito mode. [Learn more about this warning](#)

This screenshot shows a browser window with the same warning message: "100.27.168.63 doesn't support a secure connection". It includes the "Continue to site" and "Go back" buttons. The browser toolbar at the top shows the URL 100.27.168.63.

AWS-Cloud-Security-Project

The image displays three screenshots of the AWS CloudWatch Log Events interface, the Network Firewall Overview page, and the Network Firewall Details page.

CloudWatch Log Events (Top Screenshot):

- Left sidebar: CloudWatch, Alarms, Logs (Log groups, New).
- Log group: NetworkFirewallVPCLogs.
- Log events search bar: dest_port: 80.
- Log events table:

Timestamp	Message
2024-12-12T12:48:42.000-05:00	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "17340257..."}
2024-12-12T12:48:48.000-05:00	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "17340257..."}

Network Firewall Overview (Middle Screenshot):

- Left sidebar: Services (configurations, Resource gateways, Target 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 Firewall: Firewalls > NetworkFirewall.
- NetworkFirewall Info:

 - Overview Info:

Firewall status: Ready	Associated firewall policy: Firewallpolicy	Associated VPC: vpc-00d251b85fc2e8405
------------------------	--------------------------------------------	-------------------------------------------------------

 - Firewall details tab selected.
 - Firewall details table:

Name	Description
NetworkFirewall	-

Network Firewall Details (Bottom Screenshot):

- Left sidebar: CloudShell, Feedback.
- NetworkFirewall Info:
- Firewall details tab selected.
- Firewall details table:

Name	Description
NetworkFirewall	-

AWS-Cloud-Security-Project

The screenshots illustrate the process of creating a stateful rule group in the AWS Cloud Firewall service.

Screenshot 1: Stateful Rule Groups Overview

This screenshot shows the "Stateful rule groups (0)" section. It includes a table header for Priority, Name, Capacity, and Is active. A modal window is open, showing the "Actions" dropdown menu with options: "Edit priority", "Create stateful rule group", "Add unmanaged stateful rule groups", "Add managed stateful rule groups", "Disassociate from policy", and "Rule group details".

Screenshot 2: Step 2 - Describe rule group

This screenshot shows the "Step 2 - Describe rule group" page. On the left, a sidebar lists steps: Step 3 (Configure rules), Step 4 - optional (Configure advanced settings), Step 5 - optional (Add tags), and Step 6 (Review and create). The main area is titled "Rule group details". It contains fields for "Name" (NetworkFirewallVPCRuleGroup) and "Description - optional" (Enter rule group description). Below these, there is a "Capacity" field set to 100, with a note: "The capacity must be greater than or equal to 1 and less than 30,000".

Screenshot 3: Step 6 - Review and create

This screenshot shows the "Step 6 - Review and create" page. It displays the summary information entered in the previous step: Name (NetworkFirewallVPCRuleGroup), Description (Enter rule group description), and Capacity (100).

AWS-Cloud-Security-Project

The screenshots show the configuration of a Firewall Rule Set in the AWS CloudFront console.

Screenshot 1: Firewall Rule Configuration

Protocol: TCP

Source: Any

Source port: Any port

Destination: Any

Destination port: Custom (8080)

Screenshot 2: Rules List

Rules (5):

Action	Keyword
Drop	sid:1
Pass	sid:2
Pass	sid:3
Pass	sid:4
Pass	sid:5

Screenshot 3: Firewall Rule Set Summary

Protocol: TCP

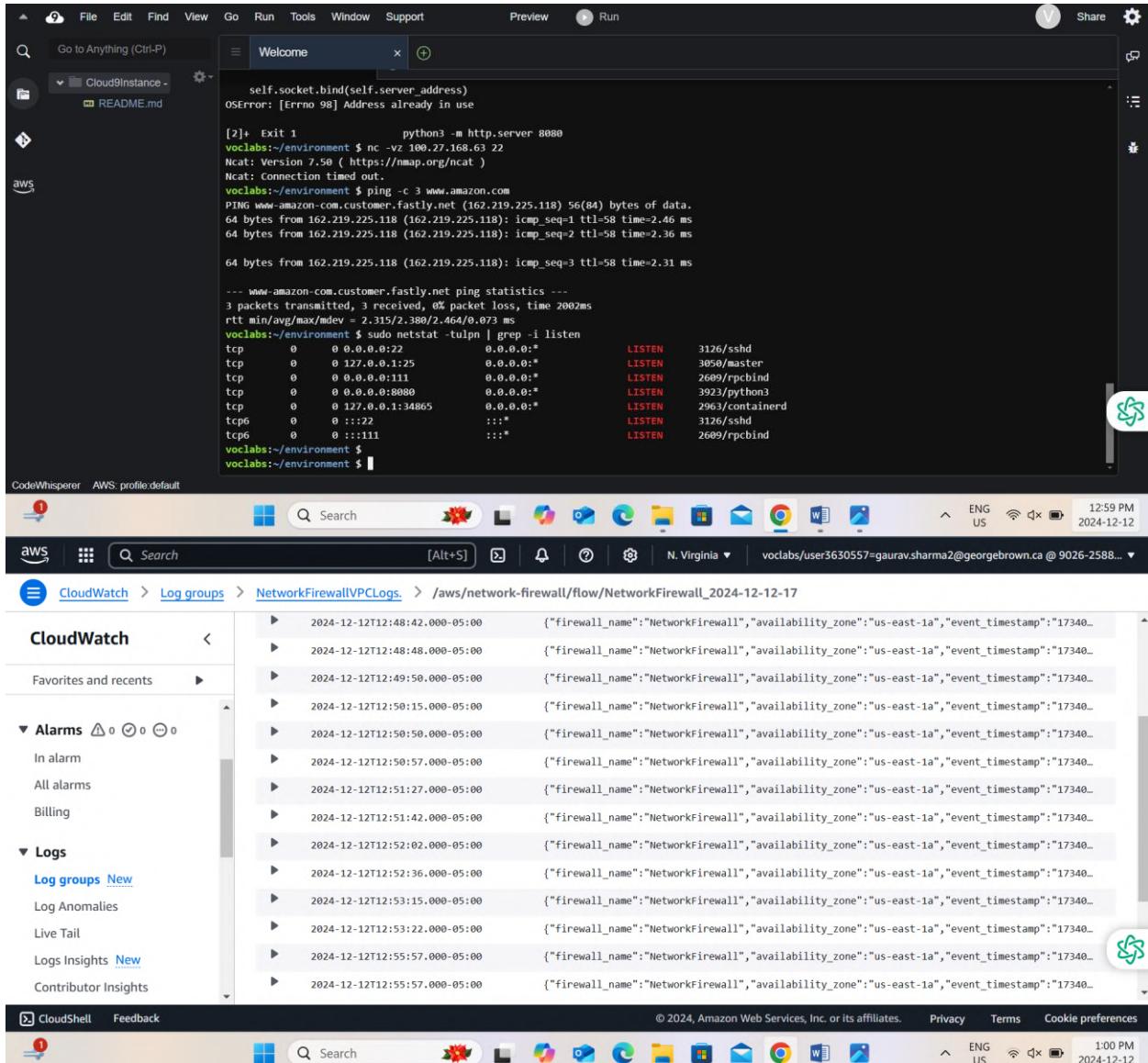
Source: Any

Source port: Any port

Destination: Any

Destination port: Custom (8080)

AWS-Cloud-Security-Project



The screenshot shows a terminal window with a dark theme. The title bar says "Welcome". The terminal content displays several command-line sessions:

```
self.socket.bind(self.server_address)
oserror: [Errno 98] Address already in use

[2]+  Exit 1                  python3 -m http.server 8080
voclabs:~/environment $ nc -vz 100.27.168.63 22
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connection timed out.
voclabs:~/environment $ ping -c 3 www.amazon.com
PING www.amazon.com.customer.fastly.net (162.219.225.118) 56(84) bytes of data.
64 bytes from 162.219.225.118 (162.219.225.118): icmp_seq=1 ttl=58 time=2.46 ms
64 bytes from 162.219.225.118 (162.219.225.118): icmp_seq=2 ttl=58 time=2.36 ms
64 bytes from 162.219.225.118 (162.219.225.118): icmp_seq=3 ttl=58 time=2.31 ms
--- www.amazon.com.customer.fastly.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 2.315/2.380/2.464/0.073 ms
voclabs:~/environment $ sudo netstat -lupn | grep -i listen
tcp        0      0 0.0.0.0:22              0.0.0.0:*          LISTEN      3126/sshd
tcp        0      0 0.0.0.0:125             0.0.0.0:*          LISTEN      3090/master
tcp        0      0 0.0.0.0:111             0.0.0.0:*          LISTEN      2609/rpcbind
tcp        0      0 0.0.0.0:8880            0.0.0.0:*          LISTEN      3923/python3
tcp        0      0 0.0.0.0:134865           0.0.0.0:*          LISTEN      2963/containerd
tcp6       0      0 ::1:22                 ::*               LISTEN      3126/sshd
tcp6       0      0 ::1:111                ::*               LISTEN      2609/rpcbind
voclabs:~/environment $
voclabs:~/environment $
```

Below the terminal, the AWS CloudWatch interface is shown. The left sidebar has sections for CloudWatch, Favorites and recents, Alarms, and Logs. Under Logs, Log groups are listed. The main pane shows log entries for "/aws/network-firewall/flow/NetworkFirewall_2024-12-12-17".

Date	Log Content
2024-12-12T12:48:42.000-05:00	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "17340..."}
2024-12-12T12:48:48.000-05:00	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "17340..."}
2024-12-12T12:49:50.000-05:00	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "17340..."}
2024-12-12T12:50:15.000-05:00	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "17340..."}
2024-12-12T12:50:50.000-05:00	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "17340..."}
2024-12-12T12:50:57.000-05:00	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "17340..."}
2024-12-12T12:51:27.000-05:00	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "17340..."}
2024-12-12T12:51:42.000-05:00	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "17340..."}
2024-12-12T12:52:02.000-05:00	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "17340..."}
2024-12-12T12:52:36.000-05:00	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "17340..."}
2024-12-12T12:53:15.000-05:00	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "17340..."}
2024-12-12T12:53:22.000-05:00	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "17340..."}
2024-12-12T12:55:57.000-05:00	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "17340..."}
2024-12-12T12:55:57.000-05:00	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "17340..."}

Phase 3: Securing AWS resources by using AWS KMS

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

AWS-Cloud-Security-Project

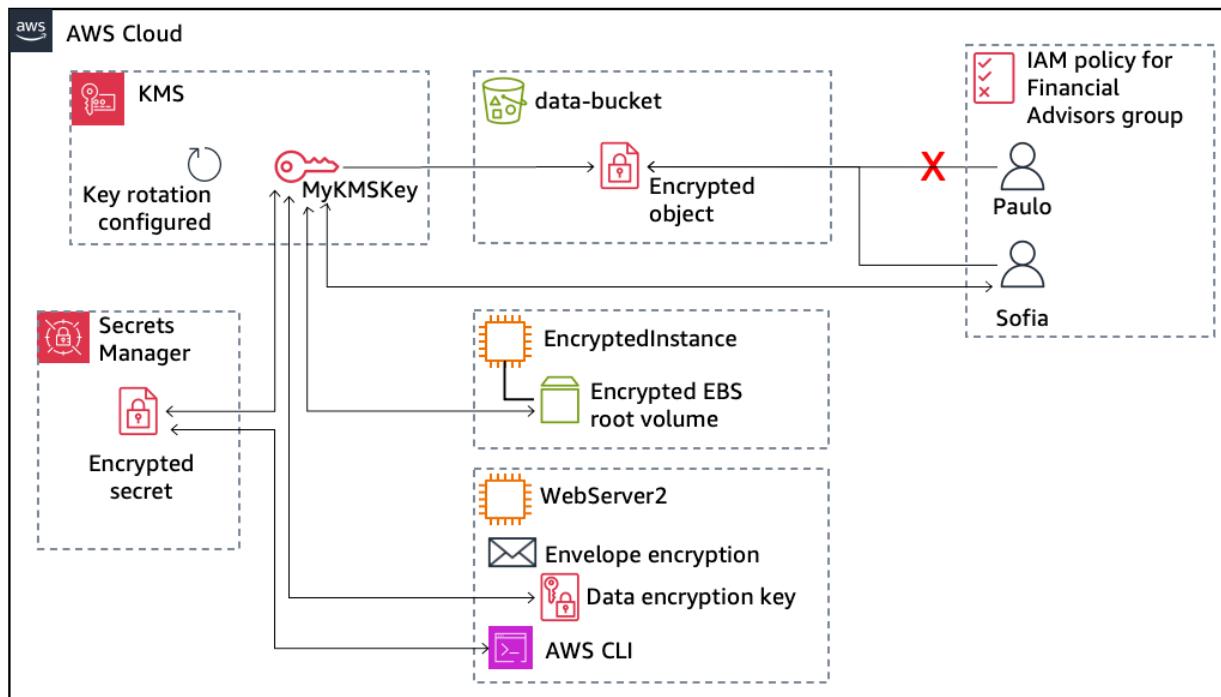
Task 3.2: Update the AWS KMS key policy and analyze an IAM policy

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

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

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

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



AWS-Cloud-Security-Project

The screenshot shows the AWS Key Management Service (KMS) landing page. The top navigation bar includes the AWS logo, search bar, and account information (N. Virginia). The left sidebar has a navigation menu with sections like 'Key Management Service (KMS)', 'AWS managed keys', 'Customer managed keys', and 'Custom key stores' (which is expanded to show 'AWS CloudHSM key stores' and 'External key stores'). The main content area features a dark background with white text. It says 'Security, Identity & Compliance' at the top, followed by 'AWS Key Management Service' in large bold letters, and 'Easily create keys and control encryption across AWS and beyond' in a larger font. Below this is a detailed description of KMS: 'AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and manage keys and control the use of encryption across a wide range of AWS services. KMS is a secure and resilient service that uses FIPS 140-2 validated hardware security modules to isolate and protect your keys.' A call-to-action button labeled 'Create a key' is prominently displayed. The bottom of the page includes standard footer links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences, along with system status icons.

AWS-Cloud-Security-Project

The image consists of three vertically stacked screenshots of the AWS KMS console.

Screenshot 1: Configure key (Step 1)

This screenshot shows the 'Configure key' step of the 'Create key' wizard. On the left, a sidebar lists steps: Step 1 (Configure key, marked with a blue circle), Step 2 (Add labels), Step 3 (Define key administrative permissions), Step 4 (Define key usage permissions), and Step 5 (Review). The main area is titled 'Configure key' and contains two sections: 'Key type' and 'Key usage'. Under 'Key type', 'Symmetric' is selected (marked with a blue circle) and described as 'A single key used for encrypting and decrypting data or generating and verifying HMAC codes'. Under 'Key usage', 'Encrypt and decrypt' is selected (marked with a blue circle) and described as 'Use the key only to encrypt and decrypt data.' A green circular icon with a white question mark is located in the bottom right corner of this section.

Screenshot 2: Customer managed keys (Success)

This screenshot shows the 'Customer managed keys' page after a key has been created. It features a green success message: 'Success Your AWS KMS key was created with alias MyKMSKey and key ID b11c0e6b-3d3e-4ef4-bab5-d9e03663a6b7.' Below this, a table lists the newly created key: **MyKMSKey** (Key ID: b11c0e6b-3d3e-4ef4-bab5-d9e03663a6b7, Status: Enabled, Key type: Symmetric, Key spec: SYMMETRIC_D..., Key usage: Encrypt and de...).

Screenshot 3: Customer managed keys (List View)

This screenshot shows the same 'Customer managed keys' page but with a different view. It displays a table with one row for the key 'MyKMSKey'. The columns are Aliases (empty), Key ID (b11c0e6b-3d3e-4ef4-bab5-d9e03663a6b7), Status (Enabled), Key type (Symmetric), Key spec (SYMMETRIC_D...), and Key usage (Encrypt and de...). The table includes filters for Aliases, Key ID, Status, Key type, Key spec, and Key usage.

AWS-Cloud-Security-Project

The screenshot shows the AWS KMS console interface. A search bar at the top has 'voc' entered. The left sidebar shows 'Customer managed keys' selected under 'Key Management Service (KMS)'. The main area displays two dialog boxes:

Add key administrators

Choose the IAM users and roles who can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this console. [Learn more](#)

Key administrators (1/28)

Name	Path	Type
vocareum	/	Role
vocareum...	/	Role
<input checked="" type="checkbox"/> voclabs	/	Role

Add key users

The following IAM users and roles can use this key to encrypt and decrypt data from within applications and when using AWS services integrated with KMS.

Key users (1/28)

Name	Path	Type
vocareum	/	Role
vocareum...	/	Role
<input checked="" type="checkbox"/> voclabs	/	Role

Both dialog boxes have 'Cancel' and 'Add' buttons at the bottom.

AWS-Cloud-Security-Project

The image displays three screenshots of the AWS Cloud interface:

- Screenshot 1: AWS KMS - Edit automatic key rotation**

This screenshot shows the "Edit automatic key rotation" page for a specific key. It includes a sidebar for "Key Management Service (KMS)" and "Customer managed keys". The main area shows "Automatic key rotation" settings with "Enable" selected, a "Rotation period (in days)" input set to 365, and a note about the range between 90 and 2560 days. Buttons for "Cancel", "Save", and a green "Next Step" icon are at the bottom.
- Screenshot 2: CloudShell - Edit policy**

This screenshot shows the JSON editor for a policy. The policy document includes statements allowing use of the key for specific principals and actions like Encrypt, Decrypt, ReEncrypt, GenerateDataKey, and DescribeKey. A tooltip for "Action" is visible. The JSON code is as follows:

```
37 {  
38     "Sid": "Allow use of the key",  
39     "Effect": "Allow",  
40     "Principal": {  
41         "AWS": [  
42             "arn:aws:iam::902625889566:role/voclabs",  
43             "arn:aws:iam::902625889566:user/sofia"  
44         ]  
45     },  
46     "Action": [  
47         "kms:Encrypt",  
48         "kms:Decrypt",  
49         "kms:ReEncrypt*",  
50         "kms:GenerateDataKey*",  
51         "kms:DescribeKey"  
52     ],  
53     "Resource": "*"  
54 }
```
- Screenshot 3: Amazon S3 - Bucket Objects**

This screenshot shows the "data-bucket-05c2dbc75fe1d7e55" bucket details. The "Objects" tab is selected, showing two objects: "Customer.csv.txt" and "Customer.csv". The table lists the object name, type, last modified date (December 9, 2024, 17:44:23 UTC-05:00), size (328.0 B), and storage class (Standard). Buttons for "Actions" (Copy S3 URI, Copy URL, Download, Open, Delete, Create folder, Upload) and "Metrics" are available.

AWS-Cloud-Security-Project

The screenshot displays three windows from the AWS Cloud Security Project:

- S3 Bucket Encryption Settings:** Shows the "Default encryption" configuration for a bucket named "data-bucket-05c2dbc75fe1d7e55". It specifies "Server-side encryption with AWS Key Management Service keys (SSE-KMS)" as the encryption type. An "AWS KMS key" dropdown shows "arn:aws:kms:us-east-1:902625889566:key/b11c0e6b-3d3...". A "Bucket Key" section indicates "Disable".
- IAM User Sign-In:** A form for logging in with an IAM user. Fields include "Account ID (12 digits) or account alias" (902625889566), "IAM username" (sofia), and "Password" (redacted). Buttons include "Sign in" and "Sign in using root user email".
- re:Invent Advertisement:** Promotes "Aurora DSQ: active-active distributed SQL database with fastest reads and writes". It includes the text "Build always-available apps with Aurora DSQ: active-active distributed SQL database with fastest reads and writes" and a button "In preview today".

AWS-Cloud-Security-Project

The image consists of three vertically stacked screenshots of the AWS S3 console, illustrating the process of uploading files to a bucket.

Screenshot 1: Bucket Overview

This screenshot shows the 'Objects' tab of the S3 bucket 'data-bucket-05c2dbc75fe1d7e55'. It displays one object, 'Customer.csv.txt', which is a text file (txt) from December 9, 2024, at 17:44:23 UTC-05:00, with a size of 328.0 B and a storage class of Standard. The interface includes navigation links like 'Amazon S3', 'General purpose buckets', and 'Storage Lens', along with tabs for 'Objects', 'Metadata - Preview', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. A prominent 'Upload' button is visible.

Screenshot 2: File Upload Step

This screenshot shows the 'Upload' step in the process. A large blue dashed box is centered, prompting the user to 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' Below this, a table lists the file 'loan-data.csv.txt' with its details: Name (loan-data.csv.txt), Type (text/plain), and Size (170.0 B). Buttons for 'Remove', 'Add files', and 'Add folder' are available.

Screenshot 3: Destination Configuration Step

This screenshot shows the 'Destination' configuration step. It lists the destination as 's3://data-bucket-05c2dbc75fe1d7e55'. A section titled 'Destination details' explains that it impacts new objects stored in the specified destination. The interface includes standard AWS navigation and status bars at the top.

AWS-Cloud-Security-Project

The image consists of three vertically stacked screenshots of the AWS S3 console.

Screenshot 1: File Upload Confirmation

A green notification bar at the top left says "Upload succeeded". Below it, a message says "For more information, see the [Files and folders](#) table." The URL <s3://data-bucket-05c2dbc75fe1d7e55> is shown, along with a status summary: "1 file, 170.0 B (100.00%)".

Screenshot 2: Bucket Configuration

The "Configuration" tab is selected. It shows a table of files and folders:

Name	Folder	Type	Size	Status	Error
loan-data.csv.txt	-	text/plain	170.0 B	Succeeded	-

Screenshot 3: Server-Side Encryption Settings

The "Standard" storage class is selected. The "Server-side encryption settings" section includes:

- Encryption type:** Info → Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- Encryption key ARN:** [arn:aws:kms:us-east-1:902625889566:key/b11c0e6b-3d3e-4ef4-bab5-d9e03663a6b7](#)
- Bucket Key:** When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)

The "Additional checksums" section notes that checksum functions are used for additional data integrity verification of new objects. [Learn more](#)

AWS-Cloud-Security-Project

The screenshot shows a web browser window with two main panels. On the left, the AWS IAM user sign-in page is displayed, requiring an Account ID (12 digits) or account alias (902625889566), an IAM username (paulo), and a Password (redacted). A 'Sign in' button is present, along with links for 'Sign in using root user email' and 'Having trouble?'. On the right, a large advertisement for AWS re:Invent 2024 is shown, featuring the text 'AWS Data Depot' and 'A secure, physical location for fast data transfer to AWS'.

The screenshot shows the Amazon S3 console. The left sidebar lists 'General purpose buckets', 'Table buckets (New)', 'Access Grants', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', and 'IAM Access Analyzer for S3'. The main area displays the properties of the file 'loan-data.csv.txt' in the bucket 'data-bucket-05c2dbc75fe1d7e55'. The 'Properties' tab is selected, showing details such as Owner (awslabsc0w6206701t1693431506), AWS Region (US East (N. Virginia) us-east-1), Last modified (December 12, 2024, 16:10:55 (UTC-05:00)), and Size (170.0 B). The 'Info' tab is also visible. To the right, there are buttons for 'Copy S3 URI', 'Download', 'Open', and 'Object actions'. The browser's address bar shows the full URL: 'Amazon S3 > Buckets > data-bucket-05c2dbc75fe1d7e55 > loan-data.csv.txt'.

AWS-Cloud-Security-Project

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

```
<Error>
  <Code>AccessDenied</Code>
  <Message>User: arn:aws:iam::902625889566:user/paulo is not authorized to perform: kms:Decrypt on resource: arn:aws:kms:us-east-1:902625889566:key/b11c0e6b-3d3e-4ef4-bab5-d9e03663a6b7 because no identity-based policy allows the kms:Decrypt action</Message>
  <RequestId>E376VQNEE1RH5XW2</RequestId>
  <HostId>yC10I70bID1zpbX89kH9HzUvtZgNjAbu3gImL7yJIKtE+MFRI55z9MOnUs6IU8NiEZ7yg8fo4YFQ=</HostId>
</Error>
```

The screenshot shows the AWS EC2 'Launch an instance' wizard. The top navigation bar includes the AWS logo, search bar, and user information: voclabs/user363055=gaurav.sharma2@georgebrown.ca @ 9026-2588... The main content area has two tabs: 'Name and tags' and 'Application and OS Images (Amazon Machine Image)'. The 'Name and tags' tab shows a text input field with 'e.g. My Web Server' and a button 'Add additional tags'. The 'Application and OS Images (Amazon Machine Image)' tab shows a search bar with 'Search our full catalog including 1000s of application and OS images'. To the right, the 'Summary' section displays the following configuration:

- Number of instances:** 1
- Software Image (AMI):** Amazon Linux 2023.6.2... [read more](#) ami-0453ec754f44f9a4a
- Virtual server type (instance type):** t2.micro
- Firewall (security group):** New security group

At the bottom right of the summary section are 'Cancel', 'Launch instance' (in orange), and 'Preview code' buttons. The status bar at the bottom indicates: © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 4:14 PM 2024-12-12.

AWS-Cloud-Security-Project

The screenshots show the AWS EC2 Instances page for an encrypted instance (i-092b1bbc86edc4cce). The top screenshot displays the instance summary with details like Public IPv4 address (54.226.106.21), Instance state (Running), and Private IP DNS name (ip-10-1-3-10.ec2.internal). The middle screenshot shows the Storage tab, where the root device (/dev/xvda) is EBS-optimized. A block device table lists a volume (vol-077db1230a2642d54) attached to /dev/xvda with a size of 8 GiB. The bottom screenshot shows the Volume monitoring section, which is currently empty.

Instance summary for i-092b1bbc86edc4cce (EncryptedInstance)

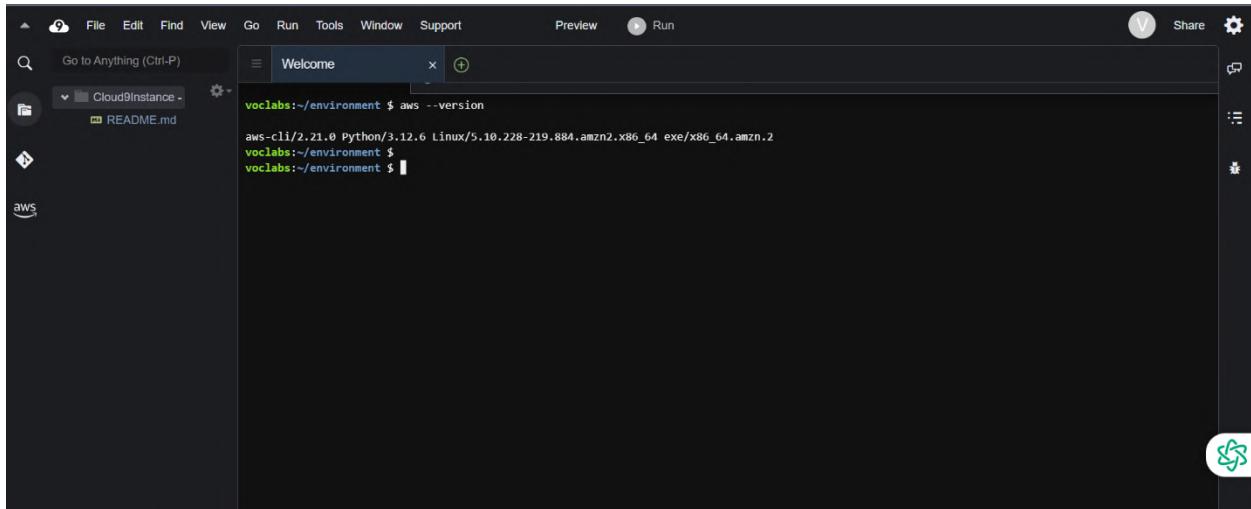
Instance ID	Public IPv4 address	Private IP4 addresses
i-092b1bbc86edc4cce	54.226.106.21 open address	10.1.3.10
IPv6 address	Instance state	Public IPv4 DNS
-	Running	ec2-54-226-106-21.compute-1.amazonaws.com open address
Hostname type	Private IP DNS name (IPv4 only)	Elastic IP addresses
IP name: ip-10-1-3-10.ec2.internal	ip-10-1-3-10.ec2.internal	-
Answer private resource DNS name	Instance type	AWS Compute Optimizer findings
-	t2.micro	-

Storage

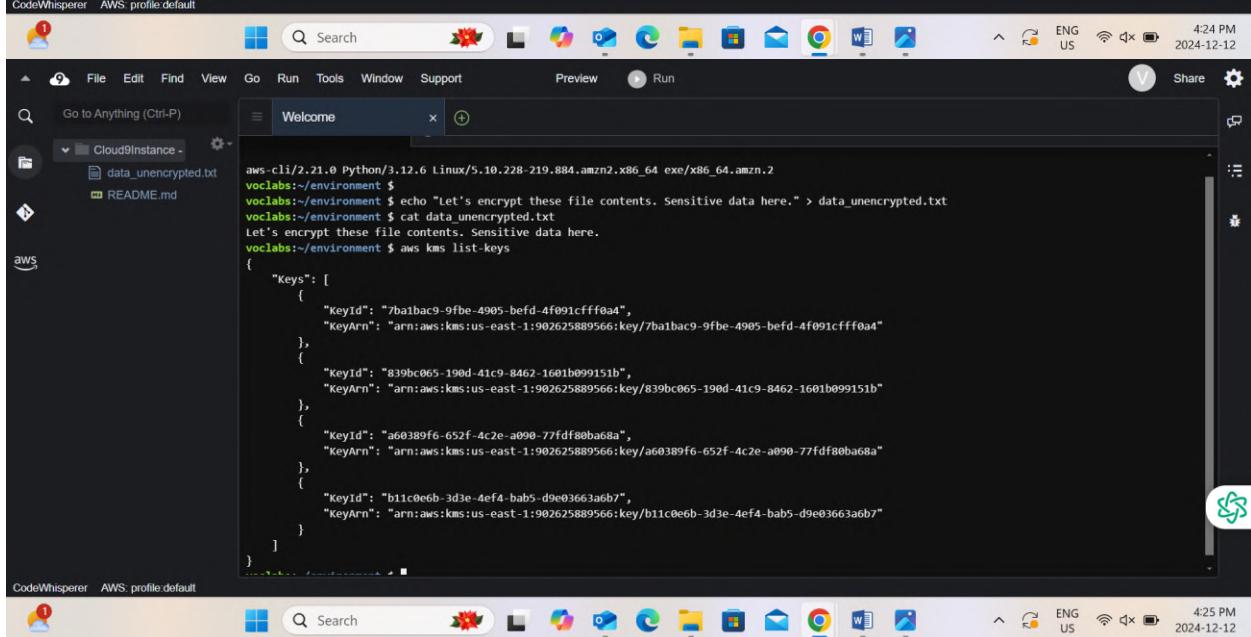
Root device details	Block devices										
Root device name: /dev/xvda, Root device type: EBS, EBS optimization: disabled	<table border="1"><thead><tr><th>Volume ID</th><th>Device name</th><th>Volume size (GiB)</th><th>Attachment status</th><th>Attachment time</th></tr></thead><tbody><tr><td>vol-077db1230a2642d54</td><td>/dev/xvda</td><td>8</td><td>Attached</td><td>2024/12/12 16:21 GMT-5</td></tr></tbody></table>	Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	vol-077db1230a2642d54	/dev/xvda	8	Attached	2024/12/12 16:21 GMT-5
Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time							
vol-077db1230a2642d54	/dev/xvda	8	Attached	2024/12/12 16:21 GMT-5							

Volume monitoring (1)

AWS-Cloud-Security-Project



```
voclabs:~/environment $ aws --version
aws-cli/2.21.0 Python/3.12.6 Linux/5.10.228-219.884.amzn2.x86_64 exe/x86_64.amzn.2
voclabs:~/environment $
voclabs:~/environment $
```



```
aws-cl/2.21.0 Python/3.12.6 Linux/5.10.228-219.884.amzn2.x86_64 exe/x86_64.amzn.2
voclabs:~/environment $
voclabs:~/environment $ echo "Let's encrypt these file contents. Sensitive data here." > data_unencrypted.txt
voclabs:~/environment $ cat data_unencrypted.txt
Let's encrypt these file contents. Sensitive data here.
voclabs:~/environment $ aws kms list-keys
{
  "Keys": [
    {
      "KeyId": "7ba1bac9-9fbe-4905-befd-af091cffff0a4",
      "KeyArn": "arn:aws:kms:us-east-1:902625889566:key/7ba1bac9-9fbe-4905-befd-af091cffff0a4"
    },
    {
      "KeyId": "839bc065-190d-41c9-8462-1601b099151b",
      "KeyArn": "arn:aws:kms:us-east-1:902625889566:key/839bc065-190d-41c9-8462-1601b099151b"
    },
    {
      "KeyId": "a60389f6-652f-4c2e-a090-77fdf80ba68a",
      "KeyArn": "arn:aws:kms:us-east-1:902625889566:key/a60389f6-652f-4c2e-a090-77fdf80ba68a"
    },
    {
      "KeyId": "b11c0e6b-3d3e-4ef4-bab5-d9e03663a6b7",
      "KeyArn": "arn:aws:kms:us-east-1:902625889566:key/b11c0e6b-3d3e-4ef4-bab5-d9e03663a6b7"
    }
  ]
}
```

AWS-Cloud-Security-Project

The screenshot shows three instances of the AWS Cloud9 IDE interface. Each instance has a terminal window open with the following command history:

```
CodeWhisperer AWS: profile.default
File Edit Find View Go Run Tools Window Support Preview Run
Cloud9Instance - Welcome
Go Anything (Ctrl-P) + 
Cloud9Instance - data_key_ciphertext data_unencrypted.txt README.md
aws
voclabs:~/environment $ result=$(aws kms generate-data-key --key-id alias/MyKMSKey --key-spec AES_256)
voclabs:~/environment $ echo $result | python3 -m json.tool
{
    "KeyId": "a60389f6-652f-4c2e-a090-77fdf80ba68a",
    "KeyArn": "arn:aws:kms:us-east-1:902625889566:key/a60389f6-652f-4c2e-a090-77fdf80ba68a"
}
voclabs:~/environment $ dk_cipher=$(echo $result | jq '.CiphertextBlob' | cut -d '"' -f2)
voclabs:~/environment $ echo $dk_cipher | base64 --decode > data_key_ciphertext
voclabs:~/environment $ cat data_key_ciphertext
x:R
000001 `He.0 *H
S/P;vMx(>My]nKz{5LryG>voclabs:~/environment $ aws kms decrypt --ciphertext-blob file:///data_key_ciphertext --query Plaintext --output plaintext_encrypted --decode > data_key
voclabs:~/environment $ openssl enc -aes-256-cbc -salt -pbkdf2 -in data_unencrypted.txt -out data_encrypted -pass file:data_key_plaintext_encrypted
unknown option '-pbkdf2'
options are
-in <file>      input file
-out <file>       output file
-pass <arg>      pass phrase source
-e               encrypt
-d               decrypt
-a/-base64     base64 encode/decode, depending on encryption flag
-k               passphrase is the next argument
-kfile          passphrase is the first line of the file argument
-md              the next argument is the md to use to create a key
                 from a passphrase. See openssl dgst -h for list.
-s               salt in hex is the next argument
-K/-iv          key/iv in hex is the next argument
-[Pp]           print the iv/key (then exit if -P)
-bufsize <n>     buffer size
-nopad          disable standard block padding
```

The terminal window also displays the AWS Cloud9 navigation bar at the top and bottom status bars indicating the date and time.

AWS-Cloud-Security-Project

The screenshot displays three main windows from the AWS CloudShell interface:

- Terminal Window:** Shows a terminal session with the following command and output:

```
voclabs:~/environment $ rm data.unencrypted.txt
voclabs:~/environment $ openssl enc -d -aes-256-cbc -pbkdf2 -in data_encrypted -out data_decrypted.txt -pass file:/data/key_plaintext_encrypted
unknown option '-pbkdf2'
```
- AWS Secrets Manager:** The main page for AWS Secrets Manager. It features a large heading "AWS Secrets Manager" and subtext "Easily rotate, manage, and retrieve secrets throughout their lifecycle". A "Get started" call-to-action button is visible.
- Bottom Navigation Bar:** Includes links for "CloudShell", "Feedback", and the AWS logo, along with standard browser navigation icons and status information (ENG US, 4:28 PM, 2024-12-12).

AWS-Cloud-Security-Project

The image consists of three vertically stacked screenshots of the AWS Secrets Manager web console.

Screenshot 1: Step 4 - Store a new secret

This screenshot shows the final step of creating a new secret. The "Other type of secret" option is selected. A key-value pair "secret" with value "my secret data" is added. An encryption key "MyKMSKey" is chosen.

Screenshot 2: Secrets page after successful storage

This screenshot shows the "Secrets" page after a secret has been successfully stored. A green banner at the top says: "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." It includes "View details" and "See sample code" buttons. A "Store a new secret" button is also present.

Screenshot 3: Secrets page showing no secrets

This screenshot shows the "Secrets" page again, but this time it displays "No secrets". It includes a "Start a new search" input field and a "Store a new secret" button.

AWS-Cloud-Security-Project

```
-seed-ofb
voclabs:~/environment $ aws secretsmanager list-secrets
{
  "SecretList": [
    {
      "ARN": "arn:aws:secretsmanager:us-east-1:902625889566:secret:mysecret-CI3yAF",
      "Name": "mysecret",
      "KmsKeyId": "arn:aws:kms:us-east-1:902625889566:key/b11c0e6b-3d3e-4ef4-bab5-d9e03663a6b7",
      "LastChangedDate": "2024-12-12T21:30:12.589000+00:00",
      "Tags": [],
      "SecretVersionsToStages": {
        "9b62bed4-cfff-4cb3-a162-a2fad9af16d2": [
          "AWSCURRENT"
        ]
      },
      "CreatedDate": "2024-12-12T21:30:12.524000+00:00"
    }
  ]
}
voclabs:~/environment $
voclabs:~/environment $
```

```
-seed-cbc -seed-cfb -seed-ecb
-seed-ofb
voclabs:~/environment $ aws secretsmanager list-secrets
{
  "SecretList": [
    {
      "ARN": "arn:aws:secretsmanager:us-east-1:902625889566:secret:mysecret-CI3yAF",
      "Name": "mysecret",
      "KmsKeyId": "arn:aws:kms:us-east-1:902625889566:key/b11c0e6b-3d3e-4ef4-bab5-d9e03663a6b7",
      "LastChangedDate": "2024-12-12T21:30:12.589000+00:00",
      "Tags": [],
      "SecretVersionsToStages": {
        "9b62bed4-cfff-4cb3-a162-a2fad9af16d2": [
          "AWSCURRENT"
        ]
      },
      "CreatedDate": "2024-12-12T21:30:12.524000+00:00"
    }
  ]
}
voclabs:~/environment $
voclabs:~/environment $ aws secretsmanager get-secret-value --secret-id mysecret

An error occurred (AccessDeniedException) when calling the GetSecretValue operation: User: arn:aws:sts::902625889566:assumed-role/voclabs/user3630557-gaurav.sharma@georgebrown.ca is not authorized to perform: secretsmanager:GetSecretValue on resource: mysecret because no identity-based policy allows the secretsmanager:GetSecretValue action
```

```
CodeWhisperer AWS profile.default
```

Question: In this lab, does your use of AWS KMS result in additional cost in the account? If so, what usage would you be charged for?

Yes, using AWS KMS incurs additional costs in your account.

Charges for AWS KMS Usage:

Key Usage: Each request to AWS KMS to encrypt, decrypt, or generate a data key incurs a cost.

Customer-Managed Keys:

Creation and storage of customer-managed keys are free. However, you pay \$1 per month for each key if it is actively used.

Key Rotation: If enabled, automatic key rotation is included at no additional cost.

AWS-Cloud-Security-Project

Secrets Manager: Storing secrets in Secrets Manager incurs charges starting at \$0.40 per secret per month.

Usage Scenarios Resulting in Costs:

Encrypting and decrypting secrets with AWS KMS.

Retrieving secrets using the Secrets Manager API.

Generating data keys for encryption operations.

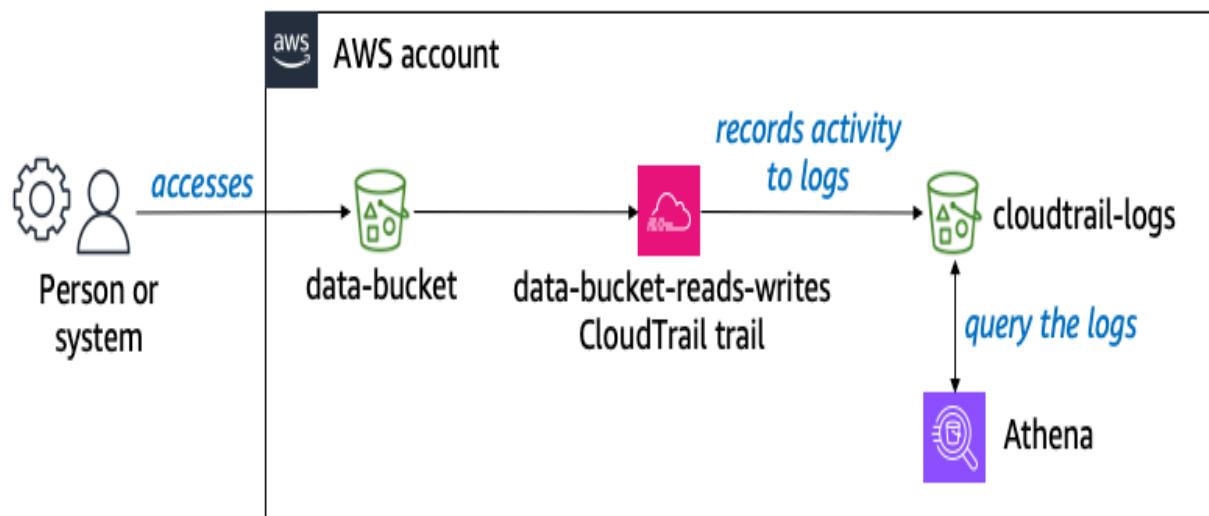
Phase 4: Monitoring and logging

Task 4.1: Use CloudTrail to record Amazon S3 API calls

Task 4.2: Use CloudWatch Logs to monitor secure logs

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

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



AWS-Cloud-Security-Project

The screenshot shows the AWS CloudTrail service page. The main heading is "AWS CloudTrail" with the subtext "Continuously log your AWS account activity". A call-to-action button "Create a trail" is visible. Below this, a section titled "How it works" is shown. A modal dialog box is overlaid on the page, titled "Choose S3 bucket". It lists several S3 buckets:

Name
athena-results-752895
aws-config-05c2dbc75fe1d7e55
cloudtrail-logs-05c2dbc75fe1d7e55
data-bucket-05c2dbc75fe1d7e55
s3-inventory-05c2dbc75fe1d7e55
s3-objects-access-log-05c2dbc75fe1d7e55

The "cloudtrail-logs-05c2dbc75fe1d7e55" bucket is selected. The "Choose" button at the bottom right of the modal is highlighted.

AWS-Cloud-Security-Project

The image consists of three vertically stacked screenshots from the AWS CloudTrail service interface.

Screenshot 1: Step 3 - Review and create

This screenshot shows the final step of creating a CloudTrail trail. The "Trail name" is set to "data-bucket-reads-writes". The "Storage location" section has "Use existing S3 bucket" selected, pointing to an S3 bucket named "cloudtrail-logs-05c2dbc75fe1d7e55". A "Prefix - optional" field contains "prefix".

Screenshot 2: CloudTrail Lake setup!

This screenshot shows the confirmation of trail creation. It displays a green banner stating "Trail successfully created". The "Trails" table lists the newly created trail:

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-05c2dbc75fe1d7e55	-	-	Logging

Screenshot 3: Amazon S3 - Upload

This screenshot shows the "Upload" step in the S3 console. A file named "Customer-data.csv.txt" (Type: text/plain, Size: 328.0 B) is selected for upload to the "data-bucket-05c2dbc75fe1d7e55" bucket.

AWS-Cloud-Security-Project

```
CustomerID,First Name,Last Name,Join Date,Street Address,City,State,Phone
1,Alejandro,Rosalez,12/12/2013,123 Main St.,Any Town,MD,301-555-0158
2,Jane,Doe,10/5/2014,456 State St.,Anywhere,WA,360-555-0163
3,John,Stiles,9/20/2016,1980 8th St.,Nowhere,NY,914-555-0122
4,Li,Juan,6/29/2011,1323 22nd Ave.,Anytown,NY,914-555-0149
```

The screenshot shows the Amazon Athena Query editor interface. On the left, the 'Data' sidebar displays the 'AwsDataCatalog' data source and 'default' database. Under 'Tables and views', there are two tables listed: 'Tables (2)' and 'Views (0)'. The main workspace contains four tabs: 'Query 1' (selected), 'Query 2', 'Query 3', and 'Query 4'. The 'Query 1' tab contains the following SQL code:

```
1 - CREATE EXTERNAL TABLE cloudtrail_logs (
2     eventVersion STRING,
3     userIdentity STRUCT<type: STRING, principalId: STRING>,
4     eventTime STRING,
5     eventName STRING,
6     awsRegion STRING,
7     sourceIPAddress STRING,
8     userAgent STRING,
9     requestParameters STRING,
10    responseElements STRING
11 )
12 LOCATION 's3://cloudtrail-logs/';
```

The status bar at the bottom indicates the query was run at 4:47 PM on 2024-12-12.

AWS-Cloud-Security-Project

The image displays three vertically stacked screenshots of the AWS Athena Query Editor interface. Each screenshot shows a query being run against the 'cloudtrail_logs' table in the 'AwsDataCatalog' database.

Screenshot 1 (Top): The query retrieves 10 rows where the event name is 'PutObject' and the request parameters contain '%customer-data.csv%'. The results are displayed in a table format.

```
1 SELECT eventTime, userIdentity.principalId, requestParameters, eventName
2 FROM "cloudtrail_logs"
3 WHERE
4     eventName = 'PutObject' AND
5     requestParameters LIKE '%customer-data.csv%'
6 LIMIT 10;
7
```

Screenshot 2 (Middle): The query retrieves 10 rows where the event name is 'GetObject' and the request parameters contain '%customer-data.csv%'. The results are displayed in a table format.

```
1 SELECT eventTime, sourceIPAddress, userAgent, requestParameters
2 FROM cloudtrail_logs
3 WHERE
4     eventName = 'GetObject' AND
5     requestParameters LIKE '%customer-data.csv%'
6 LIMIT 10;
7
8
```

Screenshot 3 (Bottom): This screenshot is identical to Screenshot 2, showing the same query and results.

```
1 SELECT eventTime, sourceIPAddress, userAgent, requestParameters
2 FROM cloudtrail_logs
3 WHERE
4     eventName = 'GetObject' AND
5     requestParameters LIKE '%customer-data.csv%'
6 LIMIT 10;
7
8
```

AWS-Cloud-Security-Project

The screenshot shows two views of the AWS CloudWatch Logs interface. The top view displays a list of existing log groups, while the bottom view shows a form for creating a new log group.

Log groups (4)

Log group	Log class	Anomaly detection	Data retention	Retention setting	
/aws/lambda/c143103a3673085l8697918t1-AdjustA...	Standard	Configure	-	-	Never
/aws/lambda/c143103a3673085l8697918t1-AdjustB...	Standard	Configure	-	-	Never
LabVPCFlowLogs	Standard	Configure	-	-	Never
NetworkFirewallVPCLogs	Standard	Configure	-	-	6 months

Create log group

Log group name: EncryptedInstanceSecureLogs

Retention setting: Never expire

Log class: Standard

KMS key ARN - optional: (empty)

Tags

A tag is a label that you assign to an Amazon Web Services resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your Amazon Web Services costs.

AWS-Cloud-Security-Project

The screenshot shows a terminal window titled "Welcome" running on a Cloud9 instance. The user is installing the Amazon CloudWatch Agent via yum. The terminal output includes:

```
voclabs:~/environment $ sudo yum install -y amazon-cloudwatch-agent
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
237 packages excluded due to repository priority protections
Resolving Dependencies
--> Running transaction check
--> Package amazon-cloudwatch-agent.x86_64 0:1.300044.0-1.amzn2 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package           Arch      Version       Repository   Size
=====
Installing:
amazon-cloudwatch-agent    x86_64    1.300044.0-1.amzn2   amzn2-core   135 M

Transaction Summary
=====
Install 1 Package

Total download size: 135 M
Installed size: 445 M
Downloading packages:
amazon-cloudwatch-agent-1.300044.0-1.amzn2.x86_64.rpm | 135 MB  00:00:02
Running transaction check
Running transaction test
```

CodeWhisperer AWS profile.default

The screenshot shows a terminal window titled "Welcome" running on a Cloud9 instance. The user is configuring the CloudWatch Agent by downloading its configuration file from a specific URL and saving it to the agent's bin directory. The terminal output includes:

```
voclabs:~/environment $ sudo wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-200-ACCAP6-91948/capstone-6-security/s3/config.json
-P /opt/aws/amazon-cloudwatch-agent/bin/
--2024-12-12 21:58:50 - https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-200-ACCAP6-91948/capstone-6-security/s3/config.json
Resolving aws-tc-largeobjects.s3.us-west-2.amazonaws.com (aws-tc-largeobjects.s3.us-west-2.amazonaws.com)... 3.5.86.67, 52.92.240.66, 3.5.81.142, ...
Connecting to aws-tc-largeobjects.s3.us-west-2.amazonaws.com (aws-tc-largeobjects.s3.us-west-2.amazonaws.com)|3.5.86.67|: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
2024-12-12 21:58:50 (128 MB/s) - '/opt/aws/amazon-cloudwatch-agent/bin/config.json' saved [2278/2278]

voclabs:~/environment $
```

CodeWhisperer AWS profile.default

AWS-Cloud-Security-Project

The screenshot shows the AWS Cloud9 Instance Connect interface. At the top, there's a search bar with 'Search' and a note: 'Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ec2-user.' A search input field contains 'ec2-user'. Below it, a note says: 'Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.' On the right, there are 'Cancel' and 'Connect' buttons. The main area is a terminal window titled 'Welcome' with the following content:

```
voclabs:~/environment $ 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"
            ]
        ]
    }
}
```

The terminal window has a dark theme. The status bar at the bottom shows 'CodeWhisperer AWS: profile default'.

AWS-Cloud-Security-Project

The image displays three vertically stacked screenshots of a terminal window, likely from a Windows operating system, showing the configuration and operation of the Amazon CloudWatch Agent on an EC2 instance.

Top Screenshot: The terminal shows the configuration of the CloudWatch Agent. It starts with a JSON configuration file:

```
    "metrics_aggregation_interval": 60,
    "metrics_collection_interval": 10,
    "service_address": ":8125"
  }
}

}voclabs:~/environment $ 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 a
nd saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp
Start configuration validation...
2024/12/12 21:59:55 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp ...
2024/12/12 21:59:55 D! Valid Json input schema.
2024/12/12 21:59:55 D! ec2tagger processor required because append_dimensions is set
2024/12/12 21:59:55 Configuration validation first phase succeeded
I! Detecting run as user...
I! Trying to detect region from ec2
D! [EC2] Found active network interface
I! imds retry client will retry 1 times
/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.serv
ice.
voclabs:~/environment $
```

Middle Screenshot: The terminal shows the status of the CloudWatch Agent service:

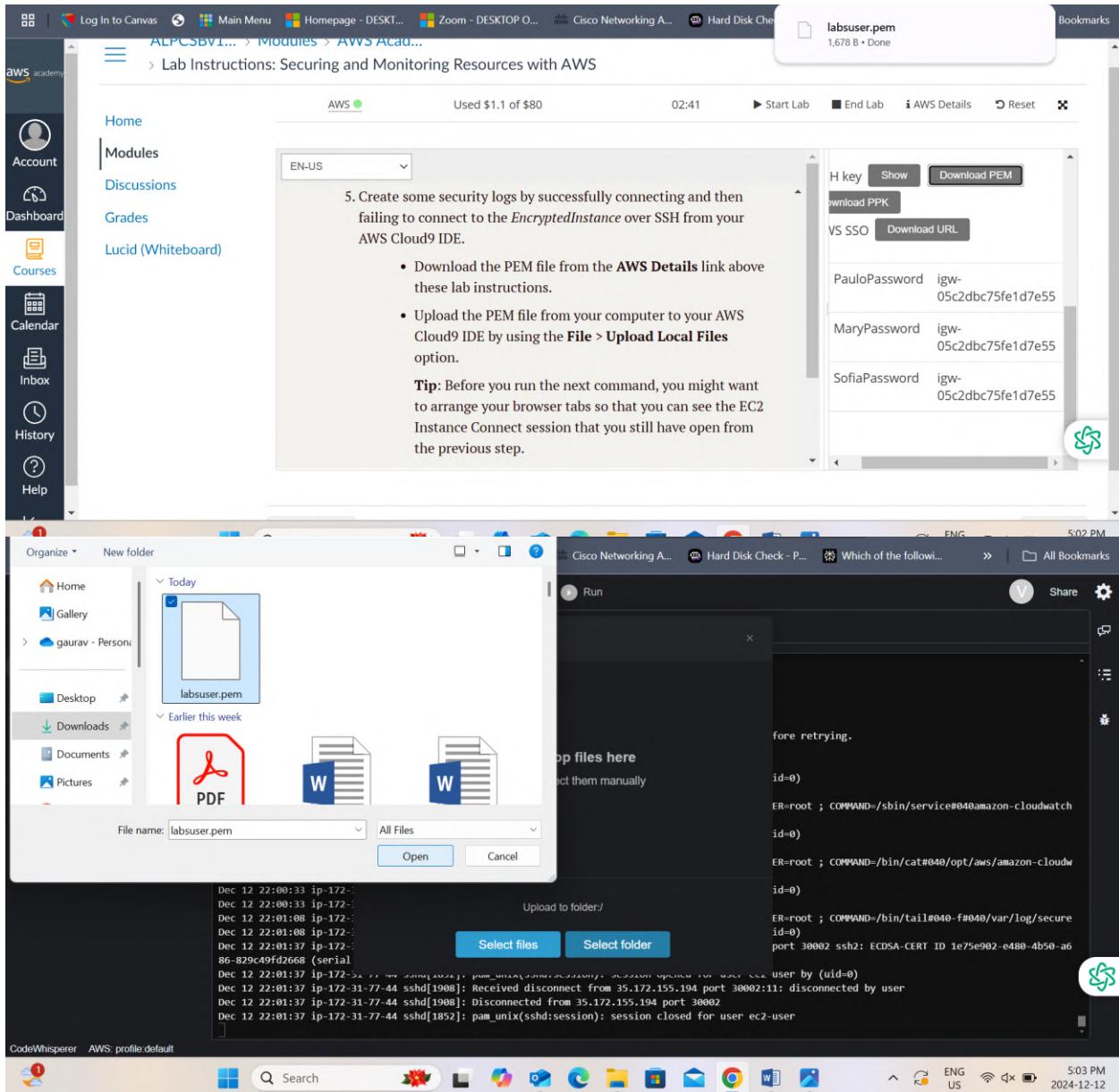
```
Configuration validation succeeded
amazon-cloudwatch-agent has already been stopped
Created symlink from /etc/systemd/system/multi-user.target.wants/amazon-cloudwatch-agent.service to /etc/systemd/system/amazon-cloudwatch-agent.serv
ice.
voclabs:~/environment $ sudo service amazon-cloudwatch-agent status
Redirecting to /bin/systemctl status amazon-cloudwatch-agent.service
● amazon-cloudwatch-agent.service - Amazon CloudWatch Agent
  Loaded: loaded (/etc/systemd/system/amazon-cloudwatch-agent.service; enabled; vendor preset: disabled)
  Active: active (running) since Thu 2024-12-12 21:59:57 UTC; 18s ago
    Main PID: 1119 (amazon-cloudwatch)
      Tasks: 6
     Memory: 116.5M
       CGroup: /system.slice/amazon-cloudwatch-agent.service
           1119 /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-age...
Dec 12 21:59:57 ip-172-31-77-44.ec2.internal start-amazon-cloudwatch-agent[1119]: 2024/12/12 21:59:57 Reading json config file path: /opt/aws... ...
Dec 12 21:59:57 ip-172-31-77-44.ec2.internal start-amazon-cloudwatch-agent[1119]: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agen... it.
Dec 12 21:59:57 ip-172-31-77-44.ec2.internal start-amazon-cloudwatch-agent[1119]: 2024/12/12 21:59:57 Reading json config file path: /opt/aws... ...
Dec 12 21:59:57 ip-172-31-77-44.ec2.internal start-amazon-cloudwatch-agent[1119]: 2024/12/12 21:59:57 D! Valid Json input schema.
Dec 12 21:59:57 ip-172-31-77-44.ec2.internal start-amazon-cloudwatch-agent[1119]: I! Detecting run as user...
Dec 12 21:59:57 ip-172-31-77-44.ec2.internal start-amazon-cloudwatch-agent[1119]: I! Trying to detect region from ec2
Dec 12 21:59:57 ip-172-31-77-44.ec2.internal start-amazon-cloudwatch-agent[1119]: 2024/12/12 21:59:57 D! ec2tagger processor required because... set
Dec 12 21:59:57 ip-172-31-77-44.ec2.internal start-amazon-cloudwatch-agent[1119]: 2024/12/12 21:59:57 Configuration validation first phase succeeded
Dec 12 21:59:57 ip-172-31-77-44.ec2.internal start-amazon-cloudwatch-agent[1119]: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agen... it.
Dec 12 21:59:57 ip-172-31-77-44.ec2.internal start-amazon-cloudwatch-agent[1119]: I! Detecting run as user...
Hint: Some lines were ellipsized, use -l to show in full.
voclabs:~/environment $
```

Bottom Screenshot: The terminal shows log entries from the CloudWatch Agent log file:

```
<head>
<title>404 - Not Found</title>
</head>
<body>
<h1>404 - Not Found</h1>
</body>
</html>

status code: 404, request id:
2024-12-12T22:00:07Z W! [outputs.cloudwatchlogs] Retried 5 time, going to sleep 32.503784182s before retrying.
voclabs:~/environment $
voclabs:~/environment $ sudo tail -f /var/log/secure
Dec 12 21:59:54 ip-172-31-77-44 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Dec 12 21:59:57 ip-172-31-77-44 sudo: pam_unix(sudo:session): session closed for user root
Dec 12 22:00:15 ip-172-31-77-44 sudo: ec2-user : TTY=pts/1 ; PWD=/home/ec2-user/environment ; USER=root ; COMMAND=/sbin/service#040amazon-cloudwatch-agent#040status
Dec 12 22:00:15 ip-172-31-77-44 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Dec 12 22:00:15 ip-172-31-77-44 sudo: pam_unix(sudo:session): session closed for user root
Dec 12 22:00:33 ip-172-31-77-44 sudo: ec2-user : TTY=pts/1 ; PWD=/home/ec2-user/environment ; USER=root ; COMMAND=/bin/cat#040/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
Dec 12 22:00:33 ip-172-31-77-44 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Dec 12 22:00:33 ip-172-31-77-44 sudo: pam_unix(sudo:session): session closed for user root
Dec 12 22:01:08 ip-172-31-77-44 sudo: ec2-user : TTY=pts/1 ; PWD=/home/ec2-user/environment ; USER=root ; COMMAND=/bin/tail#040-f#040/var/log/secure
Dec 12 22:01:08 ip-172-31-77-44 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
```

AWS-Cloud-Security-Project



AWS-Cloud-Security-Project

The screenshots show the AWS CloudWatch Log Groups interface for the log group `EncryptedInstanceSecureLogs`.

Screenshot 1: Log streams tab

- Log streams (0)**: No log streams found.
- Filter log streams or try prefix search**: Search bar with dropdown for "Exact match" and "Show expired".
- Last event time**: Placeholder text "There are no log streams."

Screenshot 2: Anomaly detection tab

- Anomaly detection**: Configure button.
- Stored bytes**: Value "-".

Screenshot 3: Metric filters tab

- Metric filters (0)**: No metric filters defined.
- Create metric filter**: Button.

Common UI Elements:

- CloudWatch Sidebar**: Alarms, Logs, Log groups, Favorites and recents.
- Top Bar**: Search, [Alt+S], N. Virginia, vclabs/user3630557=gaurav.sharma2@georgebrown.ca @ 9026-2588...
- Bottom Bar**: CloudShell, Feedback, Search, various icons, ENG US, 5:06 PM, 2024-12-12.

AWS-Cloud-Security-Project

The image displays three sequential screenshots of the AWS CloudWatch Metrics Filter creation interface.

Screenshot 1: Step 3 - Review and create

This screen shows the final step of creating a metric filter. It includes:

- Filter name:** Not valid users
- Filter pattern:** "Invalid user"
- Enable metric filter on transformed logs:** A checkbox is checked, with a note: "When enabled, metric filter will be applied to transformed logs. When disabled, metric filter will be applied to original logs."
- Metric details:** Shows the metric namespace "secure" and the metric name "NotValidUsers".

Screenshot 2: Step 2: Metric

This screen shows the configuration of the metric. It includes:

- Assign metric:** Fields include:
 - Filter name: Not valid users
 - Metric name: NotValidUsers
 - Metric namespace: secure
 - Applied on transformed logs: A dropdown menu showing "-" (selected)
 - Metric value: 1
 - Default value: 0
 - Unit: Count
- Buttons:** Cancel, Previous, Create metric filter (highlighted in orange), and a green checkmark icon.

Screenshot 3: Final Step Confirmation

This screen shows the confirmation of the metric filter creation. It includes:

- The same metric configuration as Screenshot 2.
- Buttons:** Cancel, Previous, Create metric filter (highlighted in orange), and a green checkmark icon.

AWS-Cloud-Security-Project

The screenshots show the AWS CloudWatch Create alarm wizard in three stages:

- Step 1: Set threshold condition**

Whenever NotValidUsers is...
Define the alarm condition.

Greater > threshold
 Greater/Equal \geq threshold
 Lower/Equal \leq threshold
 Lower < threshold

than...
Define the threshold value.
5
Must be a number

Additional configuration

Cancel Next
- Step 2: Add name and description**

Step 2 Configure actions
Step 3 Add name and description
Step 4 Preview and create

Name and description

Alarm name
Not valid users exceeding limit on EncryptedInstance

Alarm description - optional [View formatting guidelines](#)

Edit **Preview**

This is an H1
double asterisks will produce strong character
This is [an example](https://example.com/) inline link.

Up to 1024 characters (0/1024)

Info Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.
- Step 3: Add name and description**

Notification
When In alarm, send a notification to "Not_valid_users_exceeding_limit"

Step 3: Add name and description

Name and description

Name
Not valid users exceeding limit on EncryptedInstance

Description
-

Edit

Cancel Previous **Create alarm**

AWS-Cloud-Security-Project

The image displays three vertically stacked screenshots of the AWS CloudWatch Metrics Insights interface.

Screenshot 1: Log Analysis Rules

This screenshot shows a list of log analysis rules:

Rule Name	Log Type	Type	Description
rds-logging-enabled	RDS, Database Logs	DETECTIVE	Checks if respective logs of Amazon Relational Database Service (Amazon RDS) are enabled. The rule is NON_COMPLIANT if any types are not enabled.
s3-bucket-logging-enabled	S3	DETECTIVE, PROACTIVE	Checks if logging is enabled for your S3 buckets. The rule is NON_COMPLIANT if logging is not enabled.
waf-classic-logging-enabled	WAF, WAFClassic, Logging, WebACL	DETECTIVE	Checks if logging is enabled on AWS WAF classic global web control lists (web ACLs). The rule is NON_COMPLIANT for a global web ACL, if it does not have logging enabled.
wafv2-logging-enabled	WAFv2, Logging, WebACL	DETECTIVE	Checks if logging is enabled on AWS WAFv2 regional and global access control lists (web ACLs). The rule is NON_COMPLIANT if logging is enabled but the logging destination does not match the value of the parameter.

Screenshot 2: Resource Types with Override Settings

This screenshot shows the configuration of recording strategies for different AWS resources:

Resource Type	Recording Strategy	Default Recording Frequency
All Resource Types	Record all resource types with customizable overrides	Continuous

Screenshot 3: Resource Types with Default Settings

This screenshot shows the default recording settings for various AWS IAM entities:

Resource Type	Override
AWS IAM Policy	Exclude from recording
AWS IAM User	Exclude from recording
AWS IAM Role	Exclude from recording
AWS IAM Group	Exclude from recording

AWS-Cloud-Security-Project

The screenshots show the AWS CloudWatch Metrics Insights interface, specifically the 'Create new metric filter' wizard.

Screenshot 1: Step 1 - Filter definition

Delivery method: S3 bucket name
compliance-bucket-unique

Screenshot 2: Step 2 - AWS Config rules

s3-bucket-logging-enabled

Screenshot 3: Step 3 - AWS Managed Rules

AWS Managed Rules (498) search results for s3-bucket-logging-enabled:

Name	Labels	Supported evaluation mode	Description
s3-bucket-logging-enabled	S3	DETECTIVE, PROACTIVE	Checks if logging is enabled for your S3 buckets. The rule is NON_COMPLIANT if logging is not enabled.

Cancel Previous Confirm

AWS-Cloud-Security-Project

The image consists of three vertically stacked screenshots of the AWS Config console, all taken from the same browser session.

Screenshot 1: Resources in scope

This screenshot shows a list of non-compliant resources. The table has columns for ID, Type, Status, and Annotation. The resources listed are:

ID	Type	Status	Annotation
athena-results-752895	S3 Bucket	-	-
aws-config-05c2dbc75fe1d7e55	S3 Bucket	-	-
cloudtrail-logs-05c2dbc75fe1d7e55	S3 Bucket	-	-
compliance-bucket-unique	S3 Bucket	-	-
s3-inventory-05c2dbc75fe1d7e55	S3 Bucket	-	-
s3-objects-access-log-05c2dbc75fe1d7e55	S3 Bucket	-	-

Screenshot 2: Rule details - s3-bucket-logging-enabled

This screenshot shows the details of the 's3-bucket-logging-enabled' rule. The rule description states: "Checks if logging is enabled for your S3 buckets. The rule is NON_COMPLIANT if logging is not enabled." The rule is set to DETECTIVE evaluation mode. The last successful evaluation was on December 12, 2024, at 5:41 PM. The rule ARN is arn:aws:config:us-east-1:902625889566:config-rule/config-rule-xrbit. The rule is associated with S3 Bucket resources.

Screenshot 3: Rule details - s3-bucket-logging-enabled (continued)

This screenshot is a continuation of the rule details page, showing the same information as the second screenshot. It includes the rule description, evaluation mode, last successful evaluation, rule ARN, and resource types.

AWS-Cloud-Security-Project

The image consists of three vertically stacked screenshots from the AWS Management Console.

Screenshot 1: AWS CloudTrail Configuration (Step 1)

This screenshot shows the "CloudTrail Configuration" page. A modal dialog is open, prompting for configuration details:

- GrantedPermission: Full control
- GranteeType: CanonicalUser
- GranteeEmailAddress: (optional)
- GranteeId: (optional)
- GranteeUri: (optional)
- AutomationAssumeRole: SSMAutomationRole (highlighted in blue)
- TargetObjectKeyPartitionDataSource: (optional)
- TargetObjectKeyPrefix: (optional)

At the bottom right of the modal are "Cancel" and "Save changes" buttons.

Screenshot 2: AWS CloudTrail Configuration (Step 2)

This screenshot shows the "CloudTrail Configuration" page after saving the changes. A green success message box is displayed:

Success! s3-bucket-logging-enabled has been updated.

The URL shown is [AWS Config > Rules > s3-bucket-logging-enabled](#).

Screenshot 3: AWS Config Rule Details

This screenshot shows the "s3-bucket-logging-enabled" rule details in the AWS Config console.

Rule details:

Description	Enabled evaluation mode	Detective evaluation trigger type
Checks if logging is enabled for your S3 buckets. The rule is NON_COMPLIANT if logging is not enabled.	• DETECTIVE	• Oversized configuration changes • Configuration changes
Config rule ARN	Last successful detective evaluation	Scope of changes
arn:aws:config:us-east-1:902625889566:config-rule/config-rule-xrbbit	December 12, 2024 5:41 PM	Resources
		Resource types
		S3 Bucket

- **Question: In this lab, does your use of CloudTrail, CloudWatch, and AWS Config security features result in additional cost in the account? If so, how much do you estimate that it will cost?**

Cost Structure:

- **Management events (read/write) within a single region are free for the first copy.**
- **Additional copies and data events (e.g., S3 or Lambda function invocations) are charged.**

AWS-Cloud-Security-Project

- **Estimated Cost:**
 - If you enable only management events and have a moderate amount of activity, the cost might be \$0.
 - If you log data events, the cost is \$0.10 per 100,000 events.

2. CloudWatch

- **Cost Structure:**
 - Log ingestion: \$0.50 per GB of log data ingested.
 - Log storage: \$0.03 per GB per month.
 - Custom metrics: \$0.30 per metric per month.
 - Alarms: \$0.10 per alarm per month.
 - **Estimated Cost:**
 - For the metric filter and alarm in this lab, the cost might be ~\$0.40 (one custom metric and one alarm for a month).
 - Additional log ingestion costs depend on the volume of logs generated, which could add ~\$1–\$5 if logs are moderate in size.

3. AWS Config

- **Cost Structure:**
 - \$0.003 per configuration item recorded.
 - Managed rules are charged at \$2 per rule per region per month.
 - Remediation actions are not directly charged but could incur costs if they invoke other services.
 - **Estimated Cost:**
 - For recording resources and one managed rule (e.g., s3-bucket-logging-enabled), the monthly cost might be ~\$2–\$3, depending on the number of resources recorded.

Total Estimated Cost

AWS-Cloud-Security-Project

- If the lab is run over a short period (e.g., a few hours), the costs would be minimal, perhaps under \$1–\$5.
- If these configurations remain active for a full month, the estimated cost would be ~\$5–\$10, depending on the volume of logs, resources recorded by AWS Config, and usage of managed rules.