

## **CLCT 4011 - AWS Security**

---

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

---

### **Assignment (30 points)**

#### **Complete AWS Academy Lab Project - Cloud Security Builder: Securing and Monitoring Resources with AWS**

Paste screenshot of the AWS Management Console after completing each task.

##### **Phase 1: Securing data in Amazon S3**

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

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS S3 buckets page. At the top, there is a success message: "Successfully created bucket 'data-bucket-072bb568623da1871'". Below this, there is a table listing three buckets:

Name	AWS Region	Creation date
<a href="#">data-bucket-072bb568623da1871</a>	US East (N. Virginia) us-east-1	August 16, 2025, 22:40:59 (UTC-04:00)
<a href="#">s3-inventory-072bb568623da1871</a>	US East (N. Virginia) us-east-1	August 16, 2025, 22:26:42 (UTC-04:00)
<a href="#">s3-objects-access-log-072bb568623da1871</a>	US East (N. Virginia) us-east-1	August 16, 2025, 22:26:42 (UTC-04:00)

Below the table, there are two cards: "Account snapshot" and "External access summary".

**Account snapshot** (Info) Updated daily: Storage Lens provides visibility into storage usage and activity trends.

**External access summary - new** (Info) Updated daily: External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

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

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS S3 console interface. On the left, a sidebar titled "Amazon S3" lists various services under "General purpose buckets". The main area displays the properties of an object named "myfile.txt.txt" located in the bucket "data-bucket3-072bb568623da1871". The "Properties" tab is selected. Key details shown include:

- Owner:** awslabscOw6790608t1700619383
- AWS Region:** US East (N. Virginia) us-east-1
- Last modified:** August 16, 2025, 23:22:26 (UTC-04:00)
- Size:** 0 B
- Type:** txt
- Key:** myfile.txt.txt

On the right, there are links to "S3 URI", "Amazon Resource Name (ARN)", "Entity tag (Etag)", and "Object URL". The "Permissions" and "Versions" tabs are also visible. A yellow box highlights the "Account ID" in the top right corner of the browser window.

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS S3 console interface. At the top right, the account ID '9040-2554-2188' is circled in yellow. In the center, under the 'Objects' tab, there is a red box highlighting an error message: 'Insufficient permissions to list objects'. The message explains that after permissions are updated, the user should refresh the page. Below this, there is a 'Diagnose with Amazon CloudWatch Logs' button. The left sidebar lists various AWS services like General purpose buckets, Storage Lens, and CloudShell.

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

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS S3 console. The top navigation bar includes the AWS logo, search bar, account information (Account ID: 9040-2554-2188, vclabs/user4299732=Elvin\_Hatamov), and region (United States (N. Virginia)). The left sidebar under 'Amazon S3' has a 'General purpose buckets' section with links for Directory buckets, Table buckets, Vector buckets, Access Grants, Access Points (General Purpose Buckets, FSx file systems), Access Points (Directory Buckets), Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. It also includes a link to Block Public Access settings for this account and a 'Storage Lens' section with a 'Dashboards' link. The main content area shows a green success message: 'Successfully edited Bucket Versioning' with a note to configure lifecycle rules. Below this is the bucket name 'data-bucket3-072bb568623da1871' with an 'Info' link. A navigation bar below the bucket name includes 'Objects', 'Metadata', 'Properties' (which is selected), 'Permissions', 'Metrics', and 'Man'. The 'Bucket overview' section displays the AWS Region (US East (N. Virginia) us-east-1), Amazon Resource Name (ARN) (arn:aws:s3:::data-bucket3-072bb568623da1871), and Creation date (August 16, 2025, 23:21:45 (UTC-04:00)). The 'Bucket Versioning' section contains a descriptive text about versioning and a blue 'Edit' button. At the bottom, there are links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS S3 console for a specific bucket. At the top, there's a green success message: "Successfully edited server access logging." Below this, the "Server access logging" section is displayed. It includes a status summary: "No archive configurations" and "No configurations to display." A "Create configuration" button is present. To the right, there's an "Edit" button. Further down, the "AWS CloudTrail data events (0)" section is shown, with a "Configure in CloudTrail" button. The bottom of the page features a dark footer bar with links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

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

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS S3 console with the path: Amazon S3 > Buckets > data-bucket3-072bb568623da1871 > Management > Inventory configurations. A green success message box contains two items: "Inventory successfully created" (with a note about delivery time) and "Bucket policy successfully created" (with a "View policy" link). Below this, the "Inventory configurations" table lists one entry:

Name	Status	Scope	Destination	Frequency	Last export	Format
Inventory	Enabled	Entire bucket	s3://s3-inve...	Daily	-	Apache Par...

### Task 1.4: Confirm that versioning works as intended

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows a web browser window with the AWS S3 interface. The URL is [Amazon S3 > Buckets > data-bucket3-072bb568623da1871 > customers.csv](#). The file 'customers.csv' is selected, and its properties are shown: General purpose buckets, Directory buckets, Table buckets, Properties, Permissions, and Versions. The file is saved to the user's PC. Below the S3 interface is a Microsoft Excel window displaying the same 'customers.csv' data. The Excel ribbon shows tabs for File, Home, Insert, Draw, Page Layout, Formulas, Data, Review, View, Automate, Help, and Acrobat. The Home tab is selected, showing various formatting tools like font, alignment, and styles. A warning message at the top of the Excel window says: "POSSIBLE DATA LOSS Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file format." The Excel table has columns: CustomerID, First Name, Last Name, Join Date, Street, Add, City, State, and Phone. The data is as follows:

	CustomerID	First Name	Last Name	Join Date	Street	Add	City	State	Phone
1	1	Alejandro	Rosalez	12/12/201	123 Main	S	AnyTown	MD	301-555-0158
2	2	Jane	Doe	10/5/2014	456 State	S	Anywhere	WA	360-555-0163
3	xxxxxx								
4	3	John	Stiles	9/20/2016	1980 8th	S	Nowhere	NY	914-555-0122
5	4	Li	Juan	6/29/2011	1323 22nd	S	Anytown	NY	914-555-0149
6									
7									
8									
9									

Document Recovery: Excel has recovered the following files. Save the ones you wish to keep.

- June\_2025\_Statement (ver... Version created from the last... 2025-07-09 3:49 PM)
- June\_2025\_Statement.xlsx... Version created last time the

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

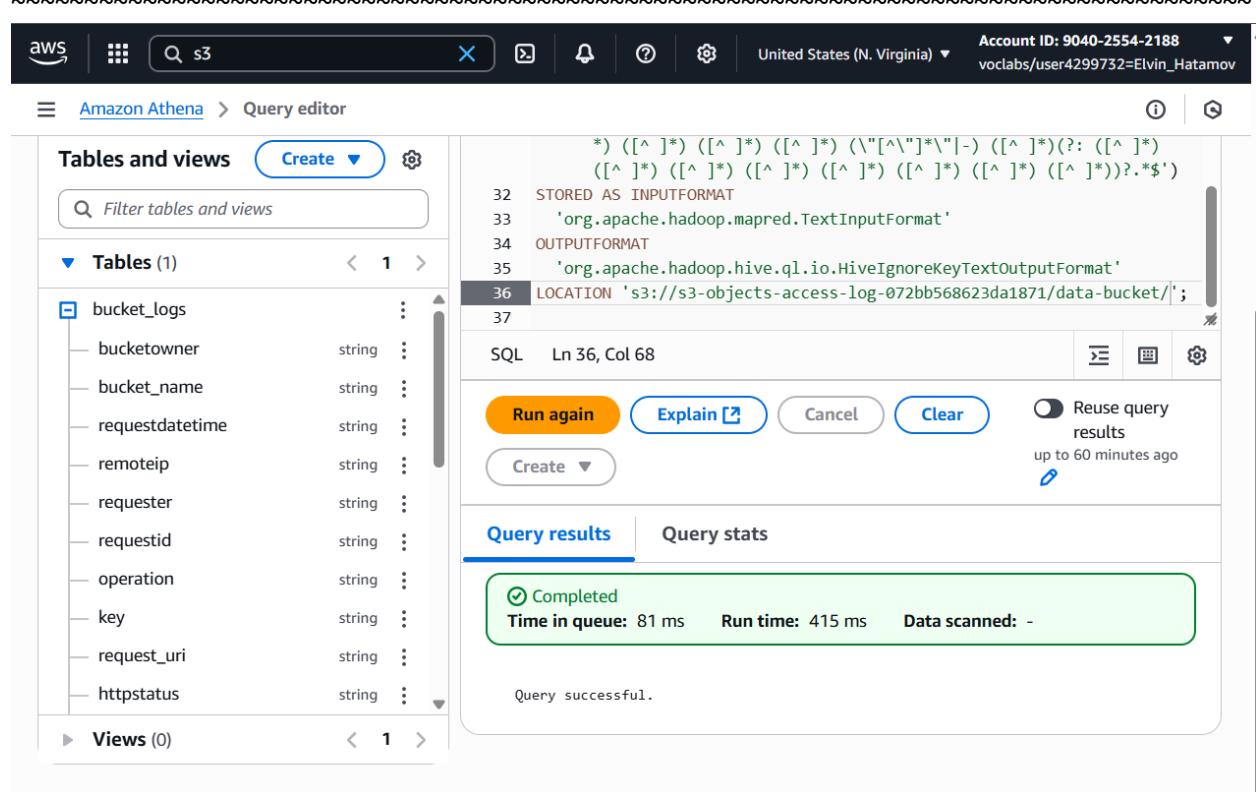
The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with 'Amazon S3' navigation. Under 'General purpose buckets', several options like 'Directory buckets', 'Table buckets', etc., are listed. Below this is a section for 'Block Public Access settings for this account'. Under 'Storage Lens', there's a 'Dashboards' link. At the bottom of the sidebar are links for 'CloudShell', 'Feedback', 'Privacy', 'Terms', and 'Cookie preferences'. The main content area is titled 'Objects' and contains a table header with columns: Name, Type, Last modified, Size, Storage class. A red box highlights an error message: 'Insufficient permissions to list objects. After you or your AWS administrator has updated your permissions to allow the s3>ListBucket action, refresh the page. Learn more about Identity and access management in Amazon S3.' There's also a 'Diagnose with Amazon CloudWatch Metrics' link.

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

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025



The screenshot shows the Amazon Athena Query editor interface. The top navigation bar includes the AWS logo, a search bar with 's3', and account information: Account ID: 9040-2554-2188, vclabs/user4299732=Elvin\_Hatamov. The main area is divided into two panes. The left pane displays the 'Tables and views' section, listing one table: 'bucket\_logs'. The table schema includes columns: bucketowner (string), bucket\_name (string), requestdatetime (string), remoteip (string), requester (string), requestid (string), operation (string), key (string), request\_uri (string), and httpstatus (string). The right pane shows the query code in the SQL tab:

```
* ) ([^ ]*) ([^ ]*) ([^ ]*) (\\"[^"]*\\") (-) ([^ ]*)(?: ([^ ]*)  
([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*))?.*$')  
32 STORED AS INPUTFORMAT  
33 'org.apache.hadoop.mapred.TextInputFormat'  
34 OUTPUTFORMAT  
35 'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'  
36 LOCATION 's3://s3-objects-access-log-072bb568623da1871/data-bucket/';  
37  
SQL Ln 36, Col 68
```

Below the code, there are buttons for 'Run again', 'Explain', 'Cancel', and 'Clear'. A checkbox for 'Reuse query results' is checked, with a note indicating it was used up to 60 minutes ago. The 'Query results' tab is selected, showing a green box with 'Completed' status and performance metrics: Time in queue: 81 ms, Run time: 415 ms, Data scanned: -. The message 'Query successful.' is displayed at the bottom.

### Cost assessment to secure Amazon S3

### Phase 2: Securing VPCs

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

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS VPC Details page for a VPC named "vpc-00dbc03e174e4e327 / LabVPC". The page is divided into several sections: "Details", "Resource map", and "CIDRs", "Flow logs", "Tags", and "Integrations".

**Details**

VPC ID	State	Block Public Access	DNS hostnames
vpc-00dbc03e174e4e327	Available	Off	Enabled
DNS resolution	Tenancy	DHCP option set	Main route table
Enabled	default	dopt-0ebda216723b66b24	rtb-0b52431fb94a12424
Main network ACL	Default VPC	IPv4 CIDR	IPv6 pool
acl-02cf9d80e99371d12	No	10.1.0.0/16	-
IPv6 CIDR (Network border group)	Network Address	Route 53 Resolver DNS Firewall rule groups	Owner ID
-	Usage metrics	-	904025542188

**Resource map**

This section shows a map of the VPC structure, indicating the VPC and its associated Subnets (1).

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS VPC Route tables page. The left sidebar is titled "VPC dashboard" and includes sections for EC2 Global View, Virtual private cloud (Your VPCs, Subnets, Route tables), Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, and NAT gateways. The main content area is titled "Route tables (3)" and shows a table with the following data:

Route table ID	Explicit subnet assoc...	Edge associations	Main	VPC
<a href="#">rtb-0b52431fb94a12424</a>	-	-	Yes	<a href="#">vpc</a>
<a href="#">rtb-0a056571ad0a16872</a>	-	-	Yes	<a href="#">vpc</a>
<a href="#">rtb-0b00e2b9d4673f2de</a>	-	-	Yes	<a href="#">vpc</a>

Below the table, there is a section titled "Select a route table".

### Task 2.2: Create a VPC flow log

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS VPC dashboard with the URL [https://aws.amazon.com/vpc/details/flow-logs/fl-03dcf868a3da7793a](#). A green success message box at the top right states: "Successfully created flow log for the following resource: vpc-00dbc03e174e4e327". The main table displays the details of the flow log "fl-03dcf868a3da7793a / LabVPCFlowLogs".

Details			
Flow Log ID <a href="#">fl-03dcf868a3da7793a</a>	Destination Type cloud-watch-logs	Traffic Type ALL	File Format —
Name <a href="#">LabVPCFlowLogs</a>	Destination Name <a href="#">LabVPCFlowLogs</a>	Max Aggregation Interval 1 minute	Hive Compatible Partitions —
State <a href="#">Active</a>	IAM Role <a href="#">arn:aws:iam::904025542188:role/VPCFlowLogsRole</a>	Log Format Default	Partition Logs —
Creation Time Sunday, August 17, 2025 at 01:23:05 EDT	Cross Account IAM Role —		

Below the table, there are "Tags" and "Integrations" tabs. The footer includes links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences, along with the copyright notice: "© 2025, Amazon Web Services, Inc. or its affiliates."

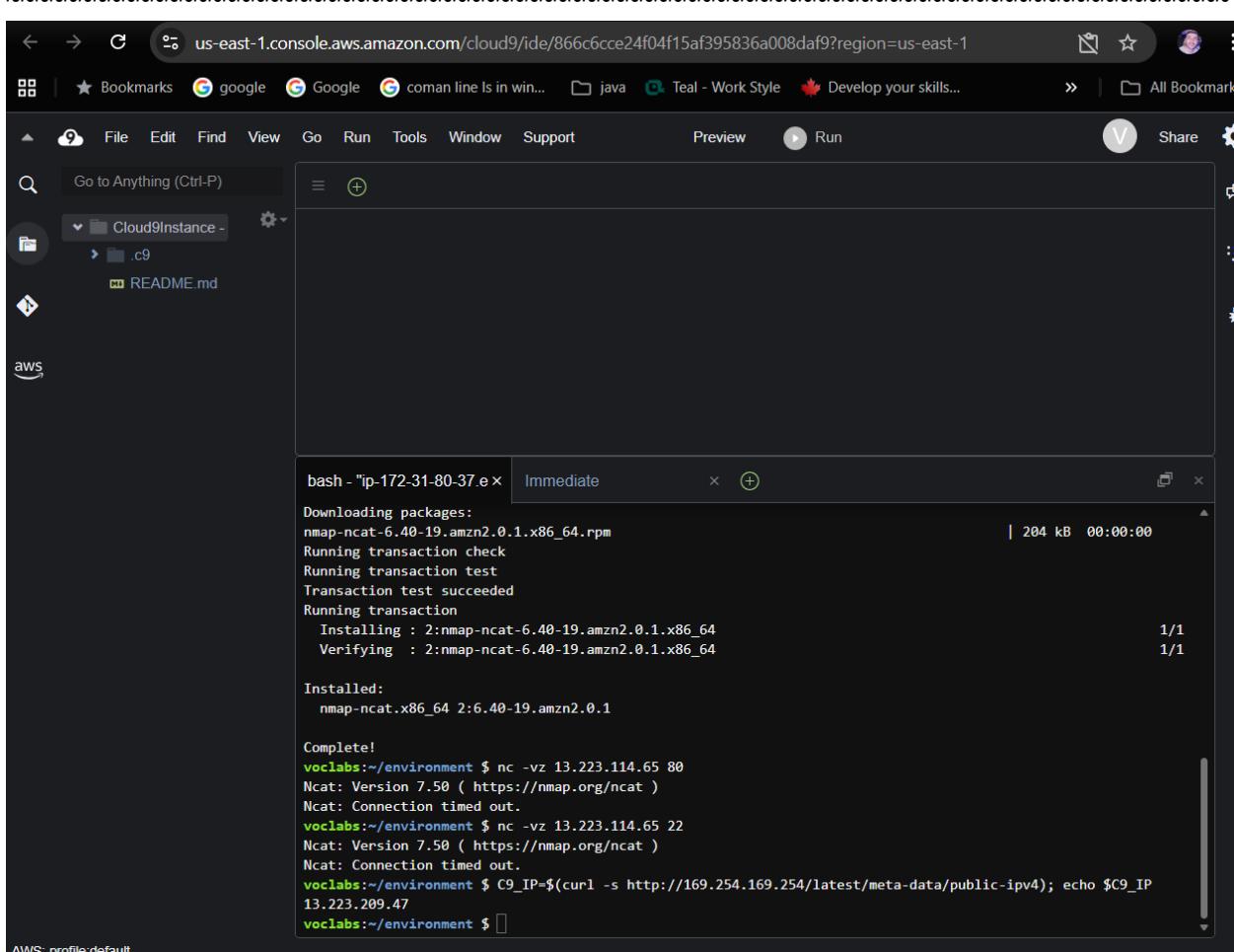
**Task 2.3: Access the WebServer instance from the internet and review VPC flow logs in CloudWatch**

## CLCT 4011 - AWS Security

---

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025



The screenshot shows a Cloud9 IDE interface with a terminal window open. The terminal window title is "bash - \*ip-172-31-80-37.e.x". The output of the terminal shows the following steps:

```
bash - *ip-172-31-80-37.e.x Immediate × +  
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!  
vclabs:/environment $ nc -vz 13.223.114.65 80  
Ncat: Version 7.50 ( https://nmap.org/ncat )  
Ncat: Connection timed out.  
vclabs:/environment $ nc -vz 13.223.114.65 22  
Ncat: Version 7.50 ( https://nmap.org/ncat )  
Ncat: Connection timed out.  
vclabs:/environment $ C9_IP=$(curl -s http://169.254.169.254/latest/meta-data/public-ipv4); echo $C9_IP  
13.223.209.47  
vclabs:/environment $
```

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS CloudWatch Log Groups interface. The left sidebar navigation includes CloudWatch, Favorites and recents, Dashboards, AI Operations, Alarms, Logs (with Log groups selected), Metrics, Application Signals (APM), GenAI Observability (Preview), and Network Monitoring. The main content area displays 'Log events' for the log group 'eni-0f070f25b5afdd19a-all'. A search bar at the top allows filtering by timestamp (Clear, 1m, 30m) and message. Below the search bar, a table lists log events with columns for Timestamp and Message. The table contains 14 rows of log entries, each starting with a timestamp from 2025-08-17T05:23:24.000Z and followed by a unique identifier and log details.

Timestamp	Message
2025-08-17T05:23:24.000Z	2 904025542188 eni-0f070f25b5afdd19a 35.203.210.64 10.1.3.4 52522 18354 6 1 44 1755408204 1755408260 REJECT OK
	2 904025542188 eni-0f070f25b5afdd19a 35.203.210.64 10.1.3.4 52522 18354 6 1 44 1755408204 1755408260 REJECT OK
2025-08-17T05:23:24.000Z	2 904025542188 eni-0f070f25b5afdd19a 35.203.211.125 10.1.3.4 54564 3580 6 1 44 1755408204 1755408260 REJECT OK
2025-08-17T05:23:24.000Z	2 904025542188 eni-0f070f25b5afdd19a 162.216.149.168 10.1.3.4 54858 9648 6 1 44 1755408204 1755408260 REJECT OK
2025-08-17T05:23:24.000Z	2 904025542188 eni-0f070f25b5afdd19a 35.203.210.251 10.1.3.4 49430 9383 6 1 44 1755408204 1755408260 REJECT OK
2025-08-17T05:23:24.000Z	2 904025542188 eni-0f070f25b5afdd19a 198.235.24.146 10.1.3.4 56631 5985 6 1 44 1755408204 1755408260 REJECT OK
2025-08-17T05:23:24.000Z	2 904025542188 eni-0f070f25b5afdd19a 205.210.31.3 10.1.3.4 56032 3388 6 1 44 1755408204 1755408260 REJECT OK
2025-08-17T05:23:24.000Z	2 904025542188 eni-0f070f25b5afdd19a 35.203.211.26 10.1.3.4 49674 50998 6 1 44 1755408204 1755408260 REJECT OK
2025-08-17T05:23:24.000Z	2 904025542188 eni-0f070f25b5afdd19a 20.65.194.105 10.1.3.4 41395 3389 6 1 52 1755408204 1755408260 REJECT OK
2025-08-17T05:23:24.000Z	2 904025542188 eni-0f070f25b5afdd19a 147.185.133.20 10.1.3.4 50754 2222 6 1 44 1755408204 1755408260 REJECT OK
2025-08-17T05:24:26.000Z	2 904025542188 eni-0f070f25b5afdd19a 162.216.149.71 10.1.3.4 56714 4083 6 1 44 1755408266 1755408320 REJECT OK

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

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025



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

[ec2-user@webserver ~]$ ^[[200~ping -c 3 www.amazon.com
bash: $'E[200~ping': command not found
[ec2-user@webserver ~]$ ping -c 3 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (3.162.97.237) 56(84) bytes of data.
64 bytes from server-3-162-97-237.iad61.r.cloudfront.net (3.162.97.237): icmp_seq=1 ttl=250 time=0.354 ms
64 bytes from server-3-162-97-237.iad61.r.cloudfront.net (3.162.97.237): icmp_seq=2 ttl=250 time=0.395 ms
64 bytes from server-3-162-97-237.iad61.r.cloudfront.net (3.162.97.237): icmp_seq=3 ttl=250 time=0.397 ms

--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.354/0.382/0.397/0.019 ms
[ec2-user@webserver ~]$ 
```

i-01c5879f13b67c3c4 (WebServer)

PublicIPs: 13.223.114.65 PrivateIPs: 10.1.3.4

CloudShell Feedback Privacy Terms Cookie preferences

© 2025, Amazon Web Services, Inc. or its affiliates.

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS EC2 Security Groups interface. The top navigation bar includes the AWS logo, search bar, and account information: Account ID: 9040-2554-2188, vclabs/user4299732=Elvin\_Hatamov. The main title is "sg-072c6ccc48ac9d817 - WebServerSecurityGroup". On the left, a sidebar lists categories: Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. The "Network & Security" section is expanded, showing Security Groups, Elastic IPs, Placement Groups, Key Pairs, and Network Interfaces. The "Load Balancing" section is also expanded, showing Load Balancers, Target Groups, and Trust Stores. The "Auto Scaling" section is collapsed. The main content area displays the security group details: Owner (904025542188), Inbound rules count (4 Permission entries), and Outbound rules count (1 Permission entry). Below this, the "Inbound rules" tab is selected, showing four rules:

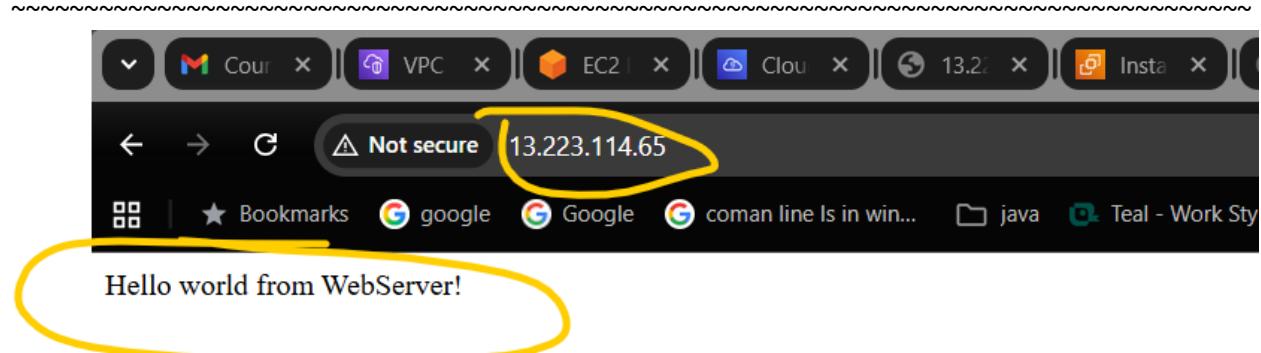
Security group rule ID	IP version	Type	Protocol
sgr-0c836e1e96dab680c	IPv4	SSH	TCP
sgr-089525127b3ff52fc	IPv4	SSH	TCP
sgr-0063b4640525f4bf9	IPv4	HTTP	TCP
sgr-06bfc3d2f9a92c31c	IPv4	Custom TCP	TCP

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

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025



A screenshot of the AWS VPC Network ACLs console. The left sidebar shows "VPC dashboard" and "Virtual private cloud" sections. The main area shows a success message: "You have successfully updated inbound rules for acl-02cf9d80e99371d12". A table details the Network ACL settings:

Network ACL ID	Associated with	Default	VPC ID
acl-02cf9d80e99371d12	subnet-Odea121c32680a4c5 / WebServerSubnet	Yes	vpc-00dbc03e174e4e327 / LabVPC
Owner	904025542188		

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

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

### Task 2.6: Review Network Firewall VPC and its associated resources

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS VPC dashboard with the following details:

**VPC dashboard** (Left sidebar):

- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections
- Route servers [New](#)

**Virtual private cloud** (Left sidebar):

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections
- Route servers [New](#)

**Security** (Left sidebar):

- Network ACLs
- CloudShell Feedback
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections
- Route servers [New](#)

**Network ACLs** (Left sidebar):

- Security groups

**PrivateLink and Lattice** (Left sidebar):

- Getting started [Updated](#)
- Endpoints [Updated](#)
- Endpoint services
- Service networks [Updated](#)

**Main network ACL** (VPC dashboard):

- Enabled
- Default
- Default VPC
- No
- IPv4 CIDR: 10.0.0/16
- IPv6 CIDR: -
- Network Address Usage metrics: Disabled
- Route 53 Resolver DNS Firewall rule groups: -
- Main route table: rtb-0b00e2b9d4673f2de
- IPv6 pool: -
- Owner ID: 904025542188

**Resource map** (VPC dashboard):

- Subnets (2): Subnets within this VPC
- us-east-1a
  - FirewallSubnet
  - WebServer2Subnet
- Route tables (1): Route network traffic to resources
- rtb-0b00e2b9d4673f2de
- Network Connections (1): Connections to other networks
- NetworkFirewallIG

**acl-0006fd9f5056587bf** (Network ACLs detail view):

**Details**

Network ACL ID: acl-0006fd9f5056587bf	Associated with: 2 Subnets	Default: Yes	VPC ID: vpc-0ec015fe0effea374 / NetworkFirewallVPC
Owner: 904025542188			

**Inbound rules (2)**

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

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS EC2 Security Groups console. On the left, there's a navigation sidebar with options like Dashboard, EC2 Global View, Events, Instances, Images, and Elastic Block Store. The main panel displays the details for a security group named "sg-059494b82bb50055b - WebServer2SecurityGroup". Under the "Details" section, it shows the security group name, ID, owner, and counts for inbound and outbound rules. Below this, the "Inbound rules" tab is selected, showing three entries:

Security group rule ID	IP version	Type	Protocol	Port range	Source
sgr-0955eec5595934c9a	IPv4	Custom TCP	TCP	8080	0.0.0.0/0
sgr-05e167344671ffb6c	IPv4	SSH	TCP	22	0.0.0.0/0
sgr-064653c888da8d546	IPv4	HTTP	TCP	80	0.0.0.0/0

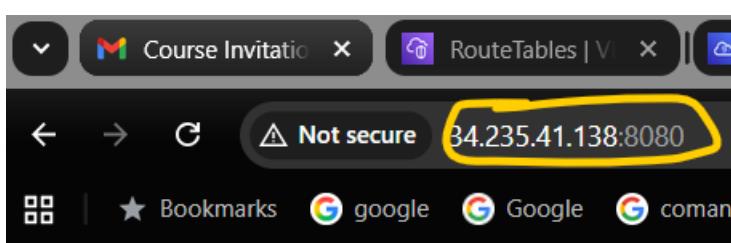
At the bottom of the page, there's a footer with links to CloudShell, Feedback, and various AWS services. The browser window below shows a self-signed SSL certificate warning for the IP address 34.235.41.138.

Hello world from WebServer2!

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025



### Task 2.7: Create a network firewall

A screenshot of the AWS Network Firewall Policies page. The left sidebar shows navigation options like Endpoint services, Service networks (Updated), Lattice services, Resource configurations (New), Resource gateways (New), Target groups, DNS firewall (Rule groups, Domain lists), and Network Firewall (Firewalls, Firewall policies). The Firewall policies section is currently selected. The main content area shows a table for a single Firewall Policy named "FirewallPolicy". The table includes columns for Details (Name: FirewallPolicy, Description: -, ARN: arn:aws:network-firewall:us-east-1:904025542188:firewall-policy/FirewallPolicy, Use count: 0, Stream exception policy: Drop, Status: Active), Customer managed key (Key type: AWS owned key), and Policy variables (HOME\_NET variable override values: -).

### Task 2.8: Create route tables

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS VPC dashboard with the 'Route tables' section selected. A green success message at the top right states: 'Updated routes for rtb-08d48d37e837284db / Firewall-Route-Table successfully'. The main panel displays the details for the route table 'rtb-08d48d37e837284db / Firewall-Route-Table'. The 'Routes' tab is active, showing two routes:

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-0b2ad99d71fa11cba	Active	No	Create Route
10.1.0.0/16	local	Active	No	Create Route Table

### Task 2.9: Configure logging for the network firewall

The screenshot shows the AWS CloudWatch Logs interface. The left sidebar is collapsed. The main area shows log events for the log stream 'log\_stream\_created\_by\_aws\_to\_validate\_log\_delivery\_subscriptions'. One event is visible in the log table:

Timestamp	Message
2025-08-17T06:52:05.033Z	Permissions are set correctly to allow AWS CloudWatch Logs to write into your logs while creating a...

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

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

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

### Phase 3: Securing AWS resources by using AWS KMS

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

The screenshot shows the AWS KMS console interface. On the left, there's a navigation sidebar with options like 'Key Management Service (KMS)', 'AWS managed keys', 'Customer managed keys' (which is selected), and 'Custom key stores'. The main content area displays a success message: 'Successfully enabled automatic key rotation' for a key with the ID 'fda80d6c-196b-4a9b-a118-db848f2b5968'. This key has an alias 'MyKMSKey' and an ARN starting with 'arn:aws:kms:us-east-1:904025542188:key/fda80d6c-196b-4a9b-a118-db848f2b5968'. The 'General configuration' section also shows the status as 'Enabled', a creation date of 'Aug 17, 2025 14:58 EDT', and a 'Regionality' of 'Single Region'. Below this, there are tabs for 'Key policy', 'Cryptographic configuration', 'Tags', 'Key material and rotations', and 'Aliases'. The 'Key policy' tab is active, showing a table for 'Key administrators' with one entry: 'vclabs'. There's a checkbox next to the entry that is checked, with the label 'Allow key administrators to delete this key'. At the bottom of the page, there are links for 'CloudShell', 'Feedback', '© 2025, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

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

The screenshot shows the AWS KMS Key configuration page for a key named `fda80d6c-196b-4a9b-a118-db848f2b5968`. The left sidebar shows navigation options like 'Key Management Service (KMS)', 'Customer managed keys', and 'Custom key stores'. The main area has tabs for 'General configuration' and 'Key policy'. The 'Key policy' tab is active, displaying the following JSON code:

```
40 "Sid": "Allow use of the key",
41 "Effect": "Allow",
42 "Principal": {
43     "AWS": [
44         "arn:aws:iam::904025542188:role/voclabs",
45         "arn:aws:iam::904025542188:user/sofia"
46     ]
47 },
48 "Action": [
49     "kms:Encrypt",
50     "kms:Decrypt",
51     "kms:ReEncrypt*",
52     "kms:GenerateDataKey*",
53     "kms:DescribeKey"
54 ],
55 "Resource": "*"
56 },
```

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS IAM Policies page with the following details:

**Policy details:**

- Type: Customer managed
- Creation time: August 16, 2025, 22:26 (UTC-04:00)
- Edited time: August 16, 2025, 22:26 (UTC-04:00)
- ARN: arn:aws:iam::904025542188:policy/PolicyForFinancialAdvisors

**Permissions:**

This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose Show remaining. [Learn more](#)

**Permissions defined in this policy:**

Service	Access level	Resource	Request type
KMS	Limited: Read, Write	All resources	None
S3	Limited: List, Read, Write	BucketName  string like  All	None

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

# CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows two stacked screenshots of the AWS S3 console. The top screenshot displays the 'loan-data.csv' object details. A yellow circle highlights the object name 'loan-data.csv' in the main list. Another yellow circle highlights the 'Account ID: 9040-2554-2188' in the top right corner of the browser window. The bottom screenshot shows the 'Edit server-side encryption' configuration page for the same object. A yellow circle highlights the 'Encryption key ARN' field, which contains the value 'arn:aws:kms:us-east-1:904025542188:key/fda80d8c-19d0-4a9b-a118-d8b84f82b968'. Both screenshots are taken from a Windows 10 desktop environment.

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

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS CloudWatch Metrics Insights interface. A query is being run against the AWS Lambda metric stream. The results table displays data for various Lambda functions, including their ARN, function name, memory size, and execution duration. One row is expanded to show detailed metrics like吞吐量 (Throughput), 延迟 (Latency), and 成功调用数 (Successful calls).

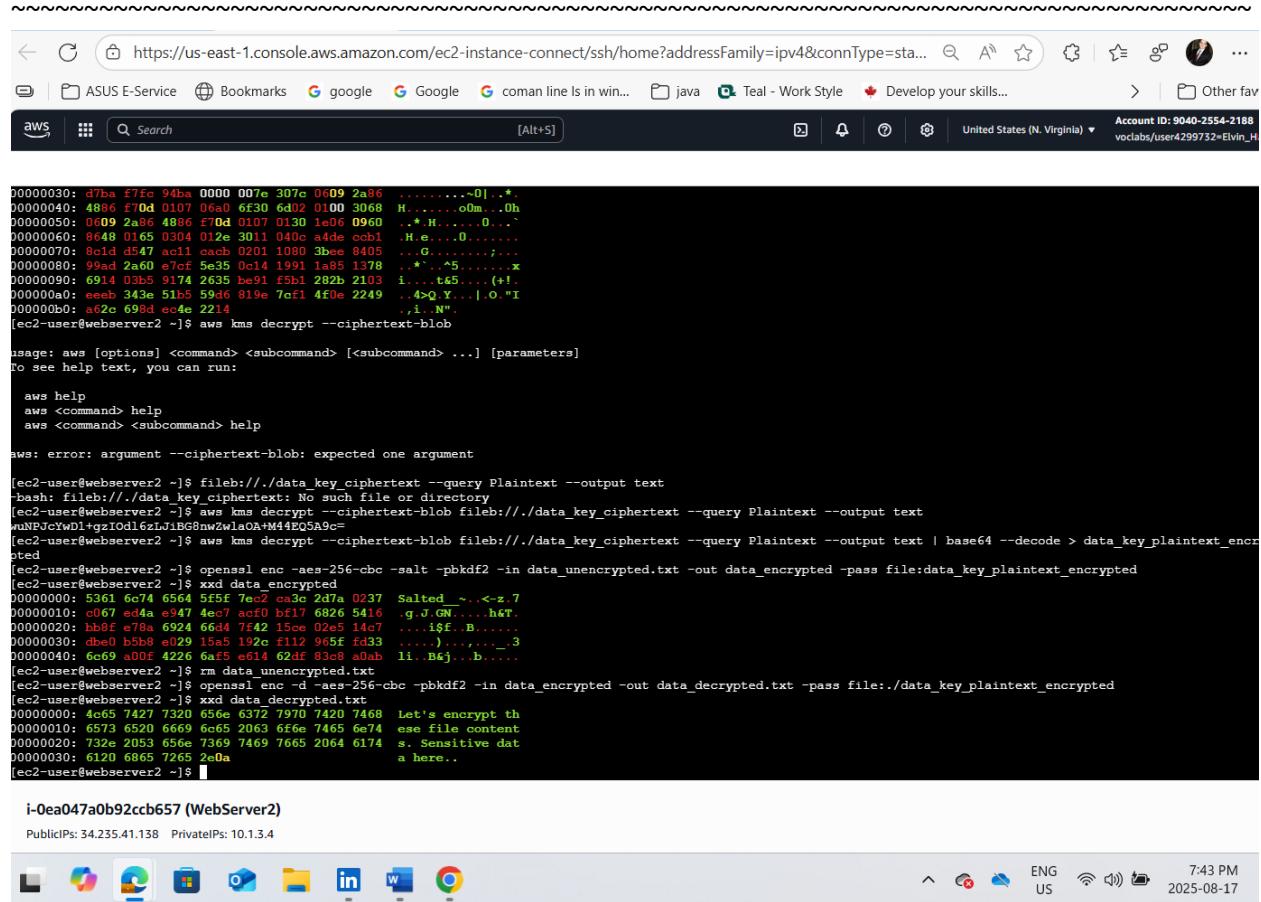
ARN	Function Name	Memory Size (MB)	Execution Duration (ms)	吞吐量 (Throughput)	延迟 (Latency)	成功调用数 (Successful calls)
arn:aws:lambda:us-east-1:123456789012:function:my-lambda	my-lambda	128	100	1000	100	1000
arn:aws:lambda:us-east-1:123456789012:function:another-lambda	another-lambda	128	150	1000	100	1000
arn:aws:lambda:us-east-1:123456789012:function:third-lambda	third-lambda	128	200	1000	100	1000

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

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025



The screenshot shows a terminal window with the following content:

```
00000030: d7ba f7fc 94ba 0000 007e 307c 0609 2a86 .....~0|.*.
00000040: 4886 f70d 0107 06a0 6f30 6d02 0100 3068 H.....oM..0h
00000050: 0609 2a86 4886 f70d 0107 0130 1e06 0960 ..*H.....0...
00000060: 8648 0165 0304 012e 3011 040c adde ccb1 ..H.e.....0...
00000070: 8c1d d547 ac11 cach 0201 1080 3bee 8405 ..G.....;...
00000080: 99ad 2a60 e7cf 5e35 0c14 1991 1a85 1378 ..*..^5.....x
00000090: 6914 03b5 9174 2635 be91 f5b1 282b 2103 i...t45.....(+!
000000a0: eeeb 343e 51b5 59d6 819e 7ef1 4f0e 2249 ..4-Q.Y....|.O."I
000000b0: a62c 698d ec4e 2214 i...N".
[ec2-user@webserver2 ~]$ aws kms decrypt --ciphertext-blob

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

aws help
aws <command> help
aws <command> <subcommand> help

aws: error: argument --ciphertext-blob: expected one argument

[ec2-user@webserver2 ~]$ fileb:///data/key_ciphertext --query Plaintext --output text
-bash: fileb:///data/key_ciphertext: No such file or directory
[ec2-user@webserver2 ~]$ aws kms decrypt --ciphertext-blob fileb:///data/key_ciphertext --query Plaintext --output text
wUNPcvxWdl+gzIdlgzLj1B6GnwZwlaOa+M44EQ5AQ9c=
[ec2-user@webserver2 ~]$ aws kms decrypt --ciphertext-blob fileb:///data/key_ciphertext --query Plaintext --output text | base64 --decode > data_key_plaintext_encrypted
[ec2-user@webserver2 ~]$ openssl enc -aes-256-cbc -salt -pbkdf2 -in data_unencrypted.txt -out data_encrypted -pass file:data_key_plaintext_encrypted
[ec2-user@webserver2 ~]$ xxd data_encrypted
00000000: 5361 6c74 6564 5f5f 7e2c ca3c 2d7a 0237 Salted ~.-<-z.7
00000010: c067 ed4a e947 4ec7 acf0 bf17 6826 5416 g.J.GN.....h&T.
00000020: bb8f e78a 6924 66d4 7f42 15c0 02e5 14c7 ..i$#.B.....
00000030: dbe0 b588 e029 15a5 192c f112 9e5e fd33 ..)....._.-_.3
00000040: 6c69 a00f 422a 6af5 e614 62df 83cb a0ab 11.Bkj...b.....
[ec2-user@webserver2 ~]$ rm data.unencrypted.txt
[ec2-user@webserver2 ~]$ openssl enc -d -aes-256-cbc -pbkdf2 -in data_encrypted -out data_decrypted.txt -pass file:/data/key_plaintext_encrypted
[ec2-user@webserver2 ~]$ xxd data_decrypted.txt
00000000: 4c65 7427 7320 656e 6372 7970 7420 7468 Let's encrypt th
00000010: 6573 6520 6669 6c65 2063 6f6e 7465 6e74 ese file content
00000020: 732e 2053 656e 7369 7469 7665 2064 6174 s. Sensitive dat
00000030: 6120 6865 7265 2e0a a here..
[ec2-user@webserver2 ~]$ 
```

i-0ea047a0b92ccb657 (WebServer2)  
PublicIPs: 34.235.41.138 PrivateIPs: 10.1.3.4

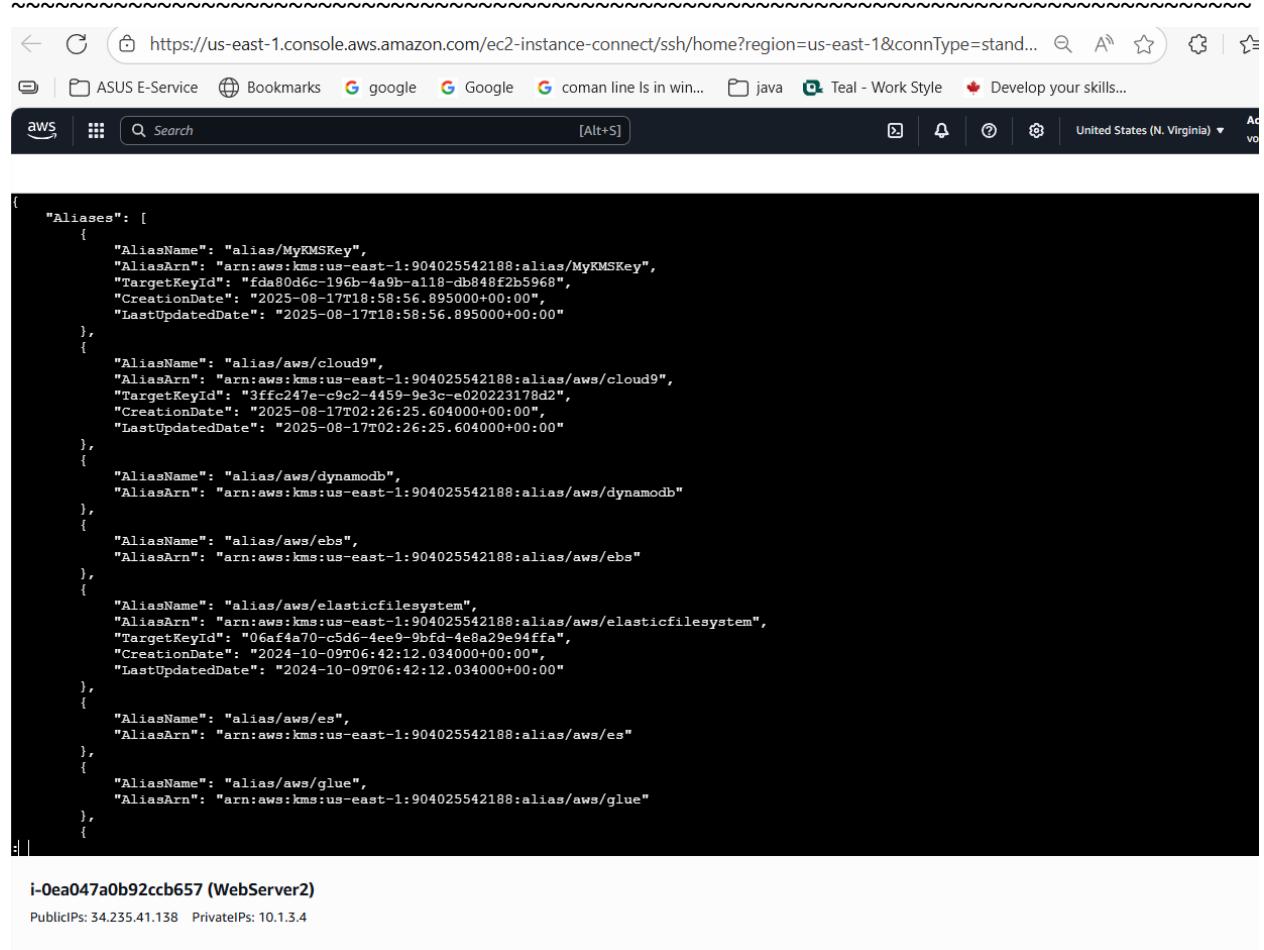


### Task 3.6: Use AWS KMS to encrypt a Secrets Manager secret

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025



A screenshot of a web browser window titled "aws" showing the AWS KMS Alias list. The URL in the address bar is <https://us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh/home?region=us-east-1&connType=stand...>. The page displays a JSON array of aliases, each with fields like AliasName, AliasArn, TargetKeyId, CreationDate, and LastUpdatedDate. The aliases listed are: MyKMSKey, aws/cloud9, aws/dynamodb, aws/ebs, aws/elasticfilesystem, aws/es, and aws/glue. At the bottom of the page, it shows the instance ID i-0ea047a0b92ccb657 (WebServer2) and its public IP 34.235.41.138.

```
{
  "aliases": [
    {
      "AliasName": "alias/MyKMSKey",
      "AliasArn": "arn:aws:kms:us-east-1:904025542188:alias/MyKMSKey",
      "TargetKeyId": "fda80d6c-196b-4a9b-a118-db848f2b5968",
      "CreationDate": "2025-08-17T18:58:56.895000+00:00",
      "LastUpdatedDate": "2025-08-17T18:58:56.895000+00:00"
    },
    {
      "AliasName": "alias/aws/cloud9",
      "AliasArn": "arn:aws:kms:us-east-1:904025542188:alias/aws/cloud9",
      "TargetKeyId": "3ffc247e-c9c2-4459-9e3c-e020223178d2",
      "CreationDate": "2025-08-17T02:26:25.604000+00:00",
      "LastUpdatedDate": "2025-08-17T02:26:25.604000+00:00"
    },
    {
      "AliasName": "alias/aws/dynamodb",
      "AliasArn": "arn:aws:kms:us-east-1:904025542188:alias/aws/dynamodb"
    },
    {
      "AliasName": "alias/aws/ebs",
      "AliasArn": "arn:aws:kms:us-east-1:904025542188:alias/aws/ebs"
    },
    {
      "AliasName": "alias/aws/elasticfilesystem",
      "AliasArn": "arn:aws:kms:us-east-1:904025542188:alias/aws/elasticfilesystem",
      "TargetKeyId": "06af4a70-c5d6-4ee9-9bfd-4e8a29e94ffa",
      "CreationDate": "2024-10-09T06:42:12.034000+00:00",
      "LastUpdatedDate": "2024-10-09T06:42:12.034000+00:00"
    },
    {
      "AliasName": "alias/aws/es",
      "AliasArn": "arn:aws:kms:us-east-1:904025542188:alias/aws/es"
    },
    {
      "AliasName": "alias/aws/glue",
      "AliasArn": "arn:aws:kms:us-east-1:904025542188:alias/aws/glue"
    }
  ]
}
```

i-0ea047a0b92ccb657 (WebServer2)  
Public IPs: 34.235.41.138 Private IPs: 10.1.3.4

### Cost assessment for using AWS KMS

### Phase 4: Monitoring and logging

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

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

The screenshot shows the AWS CloudTrail console interface. At the top, there is a green success message: "Trail successfully created". Below it, a blue info message says: "You can now enrich CloudTrail events with additional information by adding resource tags and IAM global keys in CloudTrail Lake. [Learn more](#)". The main section is titled "Trails" and contains a table with one row of data. The columns are: Name, Home region, Multi-region trail, ARN, Insights, Organization trail, S3 bucket, Log file prefix, Cloud Watch Logs log group, and Status. The data row shows: "data-bucket-reads-writes", "US East (N. Virginia)", "Yes", "arn:aws:cloudtrail:us-east-1:904025542188:trail/data-bucket-reads-writes", "Disabled", "No", "cloudtrail-logs-072bb568623da1871", "-", "-", and "Logging". There are buttons for "Copy events to Lake", "Delete", and "Create trail".

Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	Cloud Watch Logs log group	Status
<a href="#">data-bucket-reads-writes</a>	US East (N. Virginia)	Yes	arn:aws:cloudtrail:us-east-1:904025542188:trail/data-bucket-reads-writes	Disabled	No	cloudtrail-logs-072bb568623da1871	-	-	<input checked="" type="checkbox"/> Logging

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS CloudTrail Event history interface. On the left, there's a sidebar with navigation links like Dashboard, Event history, Insights, Lake (with sub-links for Dashboards, Query, Event data stores, Integrations, Trails), Settings, Pricing, Documentation, Forums, and FAQs. The main content area has a header with a search bar, account information (Account ID: 9040-2554-2188, voclabs/user4299752=Elvin\_Hatamov), and a message about enriching CloudTrail events with resource tags and IAM global keys.

**Event history (1/5) Info**

Event history shows you the last 90 days of management events.

Lookup attributes:

Read-only	Q false	Filter by date and time	Clear filter		
<input checked="" type="checkbox"/> Event name	Event time	User name	Event source	Resource type	Resource name
<input checked="" type="checkbox"/> <a href="#">UpdateInstanceInfor...</a>	August 17, 2025, 19:57:41 (UTC...)	i-0151d4fd4a9298...	ssm.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">EnvironmentTokenSu...</a>	August 17, 2025, 19:57:04 (UTC...)	-	cloud9.amazonaws.co...	-	-

1 / 5 events selected

**Compare event details** Info

Select 2-5 events to compare their details.

Event properties | Event 1 X

Event name	<a href="#">UpdateInstanceInformation</a>
Event ID	Oce8d7f4-943d-4ee5-8b92-40880dda28cc
Event time	August 17, 2025, 19:57:41 (UTC-04:00)
User name	i-0151d4fd4a9298467
AWS access key	ASIA5E7A7BYWHOPJG5N2
Event source	ssm.amazonaws.com
Request ID	1f4f732b-ea17-4c91-b970-b1051048a406

**CLCT 4011 - AWS Security**

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS Athena Query Editor interface. The top navigation bar includes links for 'ASUS E-Service', 'Bookmarks', 'Google', 'coman line ls in win...', 'java', 'Teal - Work Style', and 'Develop your skills...'. On the right, it displays 'Account ID: 9040-2554-2188' and 'voclabs/user4299732=Elvin\_Hatamov'. The main area shows a query named 'Query 1' with the following SQL code:

```
1 -- SELECT eventtime, eventname, eventsource, useridentity.arn
2 -- FROM "cloudtrail_logs_cloudtrail_logs_072bb568623da1871"
3 -- ORDER BY eventtime DESC
4 -- LIMIT 25;
5 SELECT eventtime, useridentity.principalid, requestparameters, eventname
6 FROM "cloudtrail_logs_cloudtrail_logs_072bb568623da1871"
7 WHERE
8     eventname IN ('PutObject') AND
9     requestparameters LIKE '%customer-data.csv%'
10 limit 10;
```

Below the code, the status bar indicates 'SQL Ln 5, Col 1'. At the bottom, there are buttons for 'Run again', 'Explain', 'Cancel', 'Clear', and 'Create'. To the right, a toggle switch for 'Reuse query results up to 60 minutes ago' is shown. The 'Query results' tab is selected, displaying a green bar with 'Completed' status and metrics: 'Time in queue: 141 ms', 'Run time: 892 ms', and 'Data scanned: 365.50 KB'. The results table has a single row with columns 'principalid' and 'requestparameters'. The 'requestparameters' column contains the value: '["X-Amz-Date": "20250817T235839Z", "bucketName": "data-bucket3-072bb568623da1871", "X-Amz-Algorithm": "AWS4-HMAC-SHA256", "x-amz-acl": "bucket-owner-full-control"]'.

Amazon Athena > Query editor [Alt+5]

United States (N. Virginia) Account ID: 9800-1234-5678 user@prod#2993733.us-east-1.amazonaws.com

```
1 -- SELECT eventtime, eventname, eventsource, useridentity.arn
2 FROM "cloudtrail_logs".cloudtrail_log_0206088023dd871
3 -- ORDER BY eventtime DESC
4 -- LIMIT 25;
5
6 -- SELECT eventtime, useridentity.principalId, requestparameters, eventname
7 FROM "cloudtrail_logs".cloudtrail_log_0206088223dd871
8
9 -- WHERE
10 --   eventname IN ("PutObject") AND
11 --   requestparameters LIKE "%Customer-data.csv%"
12 --   [left 10]
13 -- SELECT eventname, eventtime AS ts, useridentity.arn AS principal_arn, sourceIPAddress AS ip, userAgent AS browser
14 -- FROM "default"."cloudtrail_log".cloudtrail_log_07200560622da1071 WHERE eventsource='*.amazonaws.com' AND eventname IN ('GetObject','HeadObject') AND lower(json_extract_scalar(json_parse(requestparameters),'$.key')) LIKE '%Customer-data.csv%' AND (errorcode IS NULL OR errorcode='')
15 ORDER BY ts DESC LIMIT 25;
```

SQL Ln 12, Col 311

Run again Explain Cancel Clear Create ▾

Recall query results up to 60 minutes ago

Query results Query stats

Completed Time in queue: 101 ms Run time: 1.064 sec Data scanned: 451.66 KB

Copy Download results CSV

Results [3]

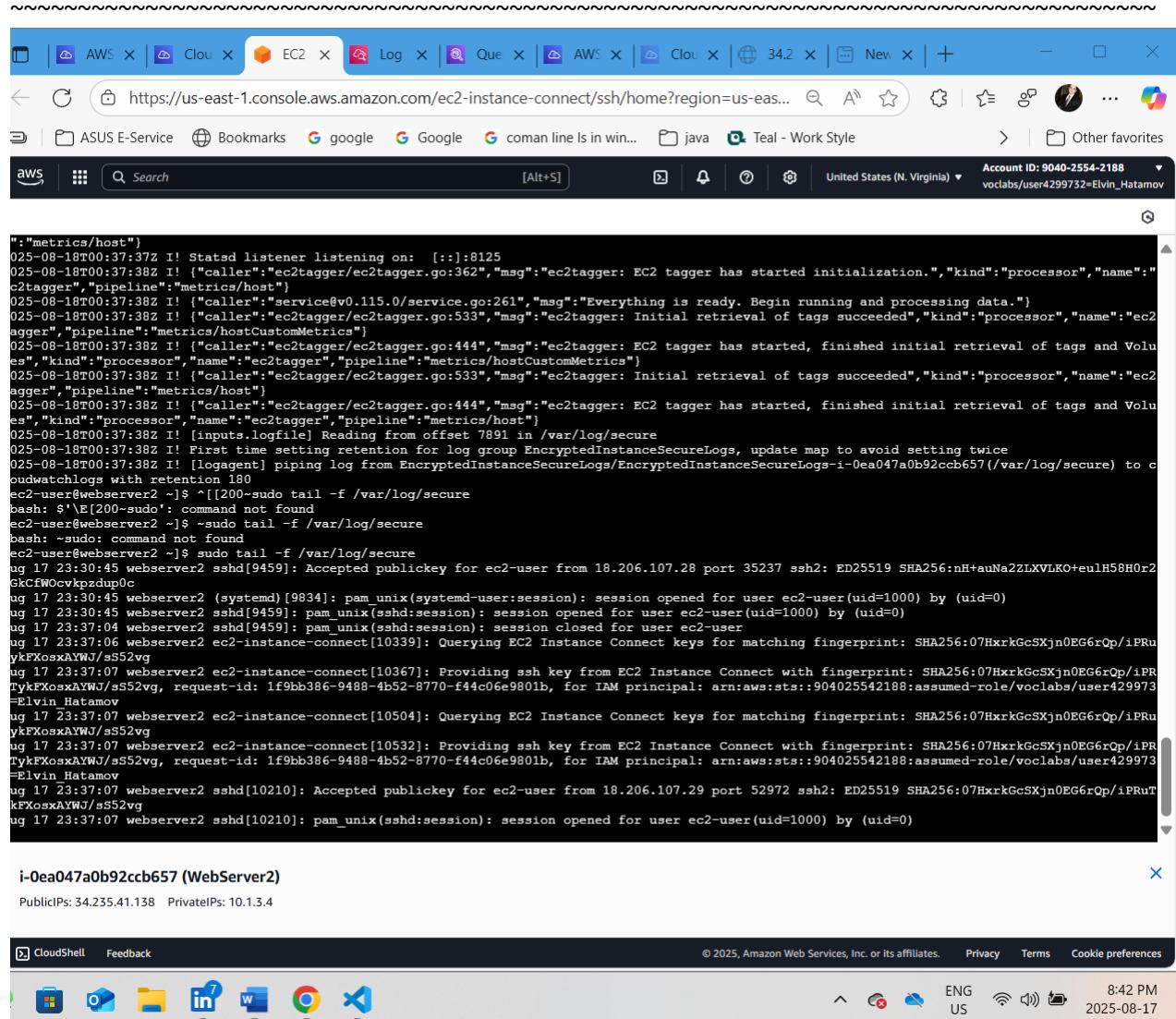
#	ts	principal_arn	ip	browser
1	2025-08-17 23:59:30.000 UTC	arn:aws:sts::904025542188:assumed-role/vocabUser:user2499732@voin_Hatamov	142.188.245.128	[Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36 Edg/140.0.0.0]
2	2025-08-17 23:59:30.000 UTC	arn:aws:sts::904025542188:assumed-role/vocabUser:user2499732@voin_Hatamov	142.188.245.128	[Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36 Edg/140.0.0.0]
3	2025-08-17 23:59:30.000 UTC	arn:aws:sts::904025542188:assumed-role/vocabUser:user2499732@voin_Hatamov	142.188.245.128	[Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36 Edg/140.0.0.0]

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

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025



```
":metrics/host")
025-08-18T00:37:37Z I! Statsd listener listening on: [::]:8125
025-08-18T00:37:38Z I! {"caller":"ec2tagger/ec2tagger.go:362","msg":"ec2tagger: EC2 tagger has started initialization.","kind":"processor","name":"ec2tagger","pipeline":"metrics/host"}
025-08-18T00:37:38Z I! {"caller":"service@v0.115.0/service.go:261","msg":"Everything is ready. Begin running and processing data."}
025-08-18T00:37:38Z I! {"caller":"ec2tagger/ec2tagger.go:533","msg":"ec2tagger: Initial retrieval of tags succeeded","kind":"processor","name":"ec2tagger","pipeline":"metrics/hostCustomMetrics"}
025-08-18T00:37:38Z I! {"caller":"ec2tagger/ec2tagger.go:444","msg":"ec2tagger: EC2 tagger has started, finished initial retrieval of tags and Volumes","kind":"processor","name":"ec2tagger","pipeline":"metrics/hostCustomMetrics"}
025-08-18T00:37:38Z I! {"caller":"ec2tagger/ec2tagger.go:533","msg":"ec2tagger: Initial retrieval of tags succeeded","kind":"processor","name":"ec2tagger","pipeline":"metrics/host"}
025-08-18T00:37:38Z I! {"caller":"ec2tagger/ec2tagger.go:444","msg":"ec2tagger: EC2 tagger has started, finished initial retrieval of tags and Volumes","kind":"processor","name":"ec2tagger","pipeline":"metrics/host"}
025-08-18T00:37:38Z I! [inputs.logfile] Reading from offset 7891 in /var/log/secure
025-08-18T00:37:38Z I! First time setting retention for log group EncryptedInstanceSecureLogs, update map to avoid setting twice
025-08-18T00:37:38Z I! [logagent] piping log from EncryptedInstanceSecureLogs/EncryptedInstanceSecureLogs-i-0ea047a0b92ccb657(/var/log/secure) to cloudwatchlogs with retention 180
ec2-user@webserver2 ~]$ [[200+sudo tail -f /var/log/secure
bash: $'\E[200~': command not found
ec2-user@webserver2 ~]$ sudo tail -f /var/log/secure
bash: ~sudo: command not found
ec2-user@webserver2 ~]$ sudo tail -f /var/log/secure
ug 17 23:30:45 webserver2 sshd[9459]: Accepted publickey for ec2-user from 18.206.107.28 port 35237 ssh2: ED25519 SHA256:nH+auNa2ZLXVLKO+eulH58H0r2GkCFeWcckpzdu0c
ug 17 23:30:45 webserver2 (systemd)[9834]: pam_unix(systemd-user:session): session opened for user ec2-user(uid=1000) by (uid=0)
ug 17 23:30:45 webserver2 sshd[9459]: pam_unix(sshd:session): session opened for user ec2-user(uid=1000) by (uid=0)
ug 17 23:37:04 webserver2 sshd[9459]: pam_unix(sshd:session): session closed for user ec2-user
ug 17 23:37:06 webserver2 ec2-instance-connect[10339]: Querying EC2 Instance Connect keys for matching fingerprint: SHA256:07HxrkGcSXjn0EG6rQp/iPrUyxFosxAYWj/sS52vg
ug 17 23:37:07 webserver2 ec2-instance-connect[10367]: Providing ssh key from EC2 Instance Connect with fingerprint: SHA256:07HxrkGcSXjn0EG6rQp/iPrTykFxsxAYWj/sS52vg, request-id: lf9bb386-9488-4b52-8770-f44c06e9801b, for IAM principal: arn:aws:sts::904025542188:assumed-role/voclabs/user429973=Elvin_Hatamov
ug 17 23:37:07 webserver2 ec2-instance-connect[10504]: Querying EC2 Instance Connect keys for matching fingerprint: SHA256:07HxrkGcSXjn0EG6rQp/iPrUyxFosxAYWj/sS52vg
ug 17 23:37:07 webserver2 ec2-instance-connect[10532]: Providing ssh key from EC2 Instance Connect with fingerprint: SHA256:07HxrkGcSXjn0EG6rQp/iPrTykFxsxAYWj/sS52vg, request-id: lf9bb386-9488-4b52-8770-f44c06e9801b, for IAM principal: arn:aws:sts::904025542188:assumed-role/voclabs/user429973=Elvin_Hatamov
ug 17 23:37:07 webserver2 sshd[10210]: Accepted publickey for ec2-user from 18.206.107.29 port 52972 ssh2: ED25519 SHA256:07HxrkGcSXjn0EG6rQp/iPrUtkFxsxAYWj/sS52vg
ug 17 23:37:07 webserver2 sshd[10210]: pam_unix(sshd:session): session opened for user ec2-user(uid=1000) by (uid=0)
```

i-0ea047a0b92ccb657 (WebServer2)

Public IPs: 34.235.41.138 Private IPs: 10.1.3.4



**CLCT 4011 - AWS Security**

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS CloudWatch Log Groups interface. The left sidebar contains navigation links for CloudShell, Feedback, CloudWatch Metrics, Application Signals (APM), Network Monitoring, and Insights. The main content area displays a list of log events under the heading "Log events". The log entries are timestamped and show messages related to EC2 Instance Connect key queries and ssh key provisionings.

Timestamp	Message
Aug 17 23:37:06	webserver2 ec2-instance-connect[10339]: Querying EC2 Instance Connect keys for matching fingerprint: SHA256:07HxrkGcSXjn0EG6rqp/iPRUtykFxosXAYW/s552vg
2025-08-18T00:36:31.047Z	Aug 17 23:37:07 webserver2 ec2-instance-connect[10367]: Providing ssh key from EC2 Instance Connect with fingerprint: SHA256:07HxrkGcSXjn0EG6rqp/iPRUtykFxosXAYW/s552vg, request-id: if9bb386-9488-4b52-8778-f44c06e0e801b, for IAM principal: arn:aws:sts::904025542188:assumed-role/voclabs/user4299732=Elvin_Hatamov
2025-08-18T00:36:31.047Z	Aug 17 23:37:07 webserver2 ec2-instance-connect[10504]: Querying EC2 Instance Connect keys for matching fingerprint: SHA256:07HxrkGcSXjn0EG6rqp/iPRUtykFxosXAYW/s552vg
2025-08-18T00:36:31.047Z	Aug 17 23:37:07 webserver2 ec2-instance-connect[10532]: Providing ssh key from EC2 Instance Connect with fingerprint: SHA256:07HxrkGcSXjn0EG6rqp/iPRUtykFxosXAYW/s552vg, request-id: if9bb386-9488-4b52-8778-f44c06e0e801b, for IAM principal: arn:aws:sts::904025542188:assumed-role/voclabs/user4299732=Elvin_Hatamov
2025-08-18T00:36:31.047Z	Aug 17 23:37:07 webserver2 sshd[10210]: Accepted publickey for ec2-user from 18.206.107.29 port 52972 s...
2025-08-18T00:36:35.513Z	Aug 17 23:37:07 webserver2 sshd[10210]: pam_unix(sshd:session): session opened for user ec2-user(uid=10...)
Aug 17 23:37:07	webserver2 sshd[10210]: pam_unix(sshd:session): session opened for user ec2-user(uid=1000) by (uid=0)

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

## CLCT 4011 - AWS Security

---

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025



Simple Notification Service

### Subscription confirmed!

You have successfully subscribed.

Your subscription's id is:

arn:aws:sns:us-east-  
1:904025542188:Not\_valid\_users\_exceeding\_limit:12355174-5274-4a16-a9b9-  
44b4843498d3

If it was not your intention to subscribe, [click here to unsubscribe](#).

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows a web browser window with the following details:

- AWS CloudWatch Alarms:** The user is viewing the "Alarms" section. There is one alarm listed:

Name	State	Last state update (UTC)	Conditions
Not valid users exceeding limit on EncryptedInstance	Insufficient data	2025-08-18 00:52:51	NotValidUsers >= 5 for 1 datapoints within 1 day
- AWS Notification - Subscription Confirmation:** An email from AWS Notifications (no-reply@sns.amazonaws.com) to the user. The subject is "AWS Notification - Subscription Confirmation". The message body contains:

You have chosen to subscribe to the topic:  
**arn:aws:sns:us-east-1:904025542188:Not\_valid\_users\_exceeding\_limit**

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):  
[Confirm subscription](https://sns.us-east-1.amazonaws.com/?SubscriptionArn=arn:aws:sns:us-east-1:904025542188:Not_valid_users_exceeding_limit)

## CLCT 4011 - AWS Security

---

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS CloudWatch Alarms interface. On the left, there's a navigation sidebar with sections like AI Operations, Alarms (which has 1 item), Logs, Metrics, Application Signals (APM), Network Monitoring, and Insights. The main area is titled "Alarms (1)" and displays a single alarm named "Not valid users exceeding limit on EncryptedInstance". The alarm status is "OK", it was last updated on "2025-08-18 00:58:33", and the condition is "NotValidUsers >= 5 for 1 datapoints within 1 day". There's also a note saying "Actions enable". The top right of the screen shows account information: "Account ID: 9040-2554-vocabls/user4299732=El". The bottom right shows system status: "ENG US", "9:08 PM", and the date "2025-08-17".

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

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS S3 console with the bucket 'compliance-bucket-072bb568623da1871' selected. The 'Permissions' tab is active. A success message 'Successfully edited Object Ownership.' is displayed. The 'Block public access (bucket settings)' section shows 'On' for 'Block all public access'. The 'Bucket policy' section notes that public access is blocked due to bucket settings. The AWS taskbar at the bottom shows various open applications and the date/time '2025-08-17 9:14 PM'.

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

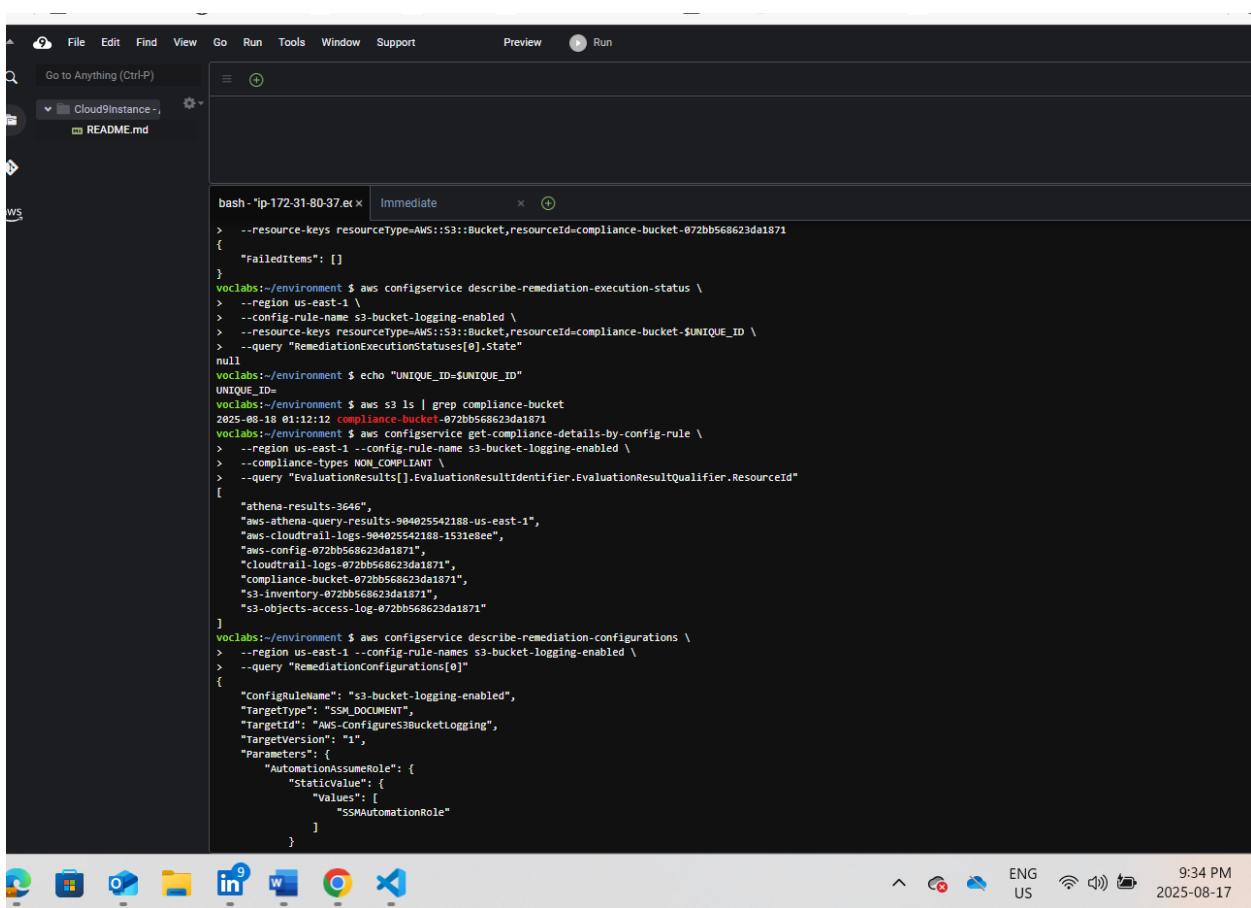
Term: SUMMER 2025

The screenshot shows the AWS Config Dashboard. On the left, a sidebar lists navigation options like Conformance packs, Rules, Resources, Aggregators, and Compliance Dashboard. The main area displays the 'Conformance Packs by Compliance Score' section, which indicates 'No conformance packs deployed. Try deploying a new conformance pack.' Below this is the 'Compliance status' section, which shows 0 Noncompliant rule(s) and 0 Compliant rule(s) for both Rules and Resources. The 'Noncompliant rules by noncompliant resource count' section shows 'No noncompliant rules.' On the right, there are two line charts under 'AWS Config usage metrics': 'Configuration Items Recorded' and 'Configuration Recorder Insufficient Permissions'. Both charts show no data available for the selected time range (1d). At the bottom, there's a 'AWS Config success metrics' section with three charts: 'Change Notifications Deli...', 'Config History Export Fail', and 'Config Snapshot Export F...'. The status bar at the bottom right shows the date and time as 2025-08-17 9:16 PM.

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025



The screenshot shows a terminal window with several AWS CLI commands run in an environment. The commands are related to AWS Config and CloudTrail logs.

```
bash -i p-172-31-80-37.ex x | Immediate x
> --resource-keys resourceType=AWS::S3::Bucket,resourceId=compliance-bucket-072bb568623da1871
{
  "FailedItems": []
}
voclabs:~/environment $ aws configservice describe-remediation-execution-status \
> --region us-east-1 \
> --config-rule-name s3-bucket-logging-enabled \
> --resource-keys resourceType=AWS::S3::Bucket,resourceId=compliance-bucket-$UNIQUE_ID \
> --query "RemediationExecutionStatuses[0].state"
null
voclabs:~/environment $ echo "UNIQUE_ID=$UNIQUE_ID"
UNIQUE_ID=
voclabs:~/environment $ aws s3 ls | grep compliance-bucket
2025-08-18 01:12:12 compliance-bucket-072bb568623da1871
voclabs:~/environment $ aws configservice get-compliance-details-by-config-rule \
> --region us-east-1 --config-rule-name s3-bucket-logging-enabled \
> --compliance-types NON_COMPLIANT \
> --query "EvaluationResults[].EvaluationResultIdentifier.EvaluationResultQualifier.ResourceId"
[
  "athena-results-3646",
  "aws-athena-query-results-904025542188-us-east-1",
  "aws-cloudtrail-logs-984025542188-1531e8ec",
  "aws-config-072bb568623da1871",
  "cloudtrail-logs-072bb568623da1871",
  "compliance-bucket-072bb568623da1871",
  "s3-inventory-072bb568623da1871",
  "s3-objects-access-log-072bb568623da1871"
]
voclabs:~/environment $ aws configservice describe-remediation-configurations \
> --region us-east-1 --config-rule-names s3-bucket-logging-enabled \
> --query "RemediationConfigurations[0]"
{
  "ConfigRuleName": "s3-bucket-logging-enabled",
  "TargetType": "SSM_DOCUMENT",
  "TargetId": "AWS-ConfiguresS3BucketLogging",
  "TargetVersion": "1",
  "Parameters": {
    "AutomationAssumeRole": {
      "StaticValue": {
        "Values": [
          "SSMAutomationRole"
        ]
      }
    }
  }
}
```

The terminal window is part of a larger desktop environment. The taskbar at the bottom shows various icons for Microsoft Office applications (Word, Excel, PowerPoint) and social media (LinkedIn). The system tray indicates the date and time as 2025-08-17 9:34 PM, and shows battery status, signal strength, and language settings (ENG US).

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

The screenshot shows the AWS Config console interface. On the left, there's a navigation sidebar with links like Dashboard, Conformance packs, Rules, Resources, Aggregators, and Documentation. The main area has a form for creating a new configuration rule, with fields for GranteeEmailAddress, GranteeId, GranteeType, GranteeUri, TargetBucket, TargetObjectKeyPartitionDataSource, TargetObjectKeyPrefix, and TargetPrefix. Below this is a section titled "Resources in scope" with a dropdown set to "Noncompliant". A table lists several S3 buckets, each with a status column indicating they are non-compliant. At the bottom of the page, there are links for CloudShell, Feedback, and various legal and preference links.

### Cost assessment for monitoring and logging

It cost a small amount of money under 1 dollar.

## CLCT 4011 - AWS Security

Student Name: ELVIN HATAMOV  
Student ID: 101150598

Term: SUMMER 2025

We can check it from cloudwatch metrics,

