

Internship Report

Title: Performing a Basic Audit of Your AWS Environment (SPL-73)

Company: Internee.pk

Internship Duration: July- September

Intern: Ammad Aziz

1. Introduction

The purpose of this audit is to evaluate the security posture of AWS resources, focusing on **IAM permissions, EC2 security groups, VPC configurations, CloudWatch monitoring, and CloudTrail logs**.

This aligns with the industry best practices of **governance, compliance, and risk management** in cloud infrastructure.

2. Objectives

By the end of this audit, the following were achieved:

- Reviewed **user permissions** in AWS IAM.
 - Captured **audit evidence** using IAM Policy Simulator.
 - Analyzed **security group rules** for EC2 instances.
 - Reviewed **Amazon VPC configurations, subnets, and NACLs**.
 - Monitored **CloudWatch metrics** and alarms.
 - Reviewed **CloudTrail logs** stored in Amazon S3.
-

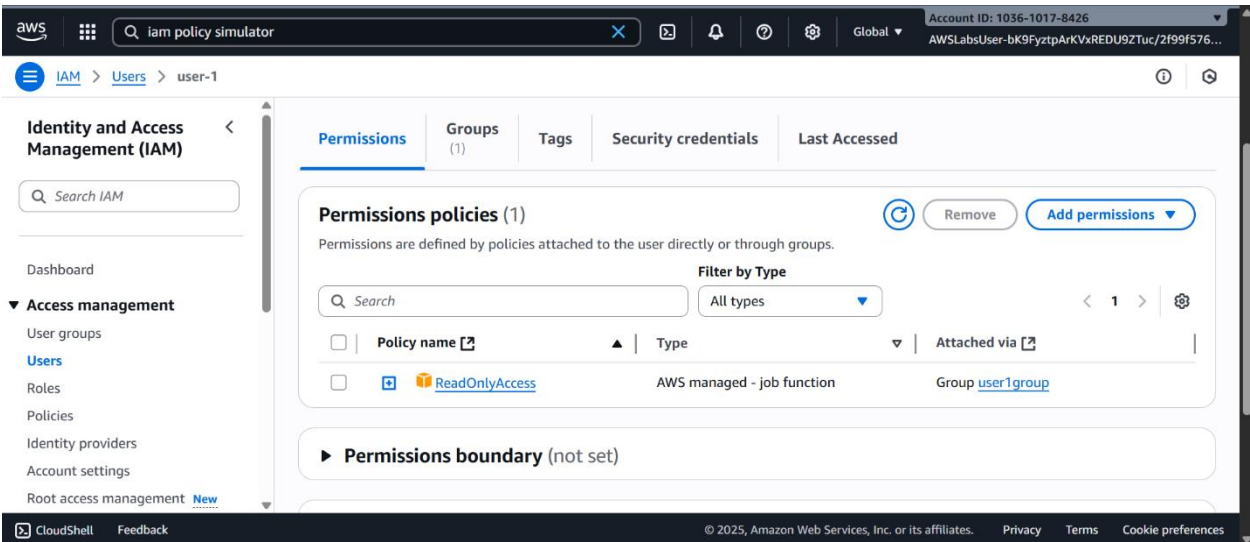
3. Methodology

The audit was performed using the **AWS Management Console** in a lab environment. Each service was analyzed step by step, and screenshots were taken as evidence for compliance.

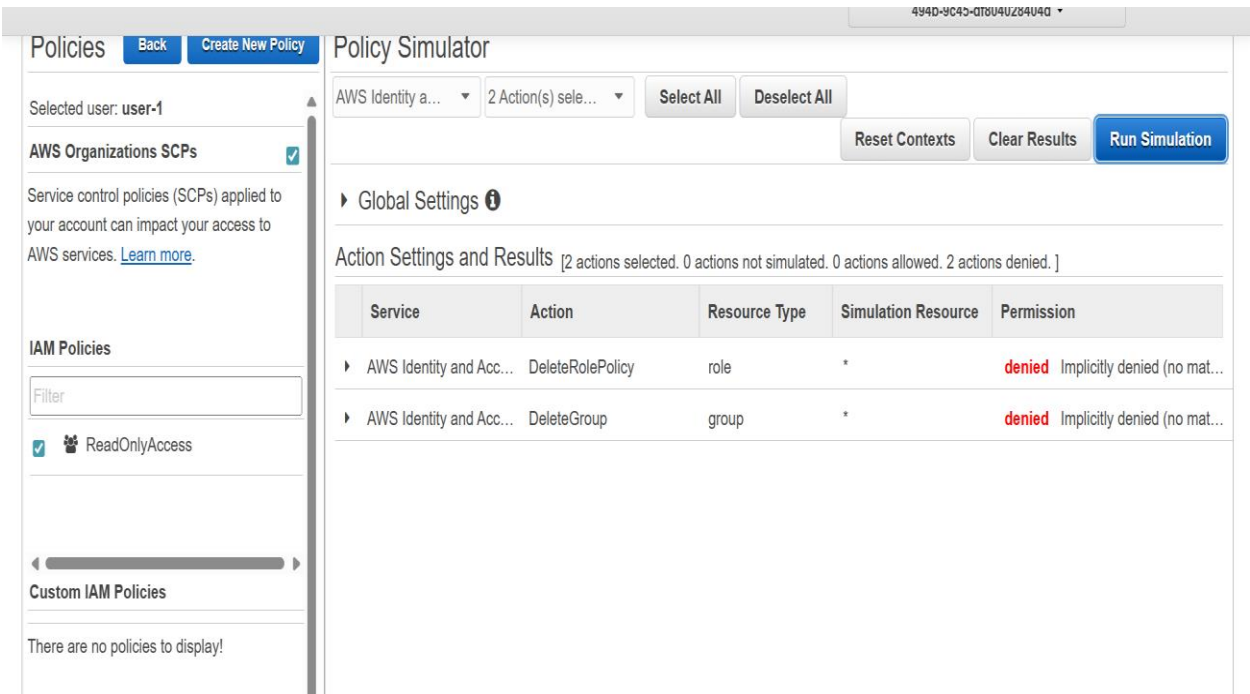
4. Findings

4.1 IAM User Permissions Audit

- Reviewed user-1 under IAM → Users.
- Permissions assigned via **ReadOnlyAccess** policy.



- Policy Simulator Results:
 - DeleteGroup → **Denied**
 - DeleteRolePolicy → **Denied**

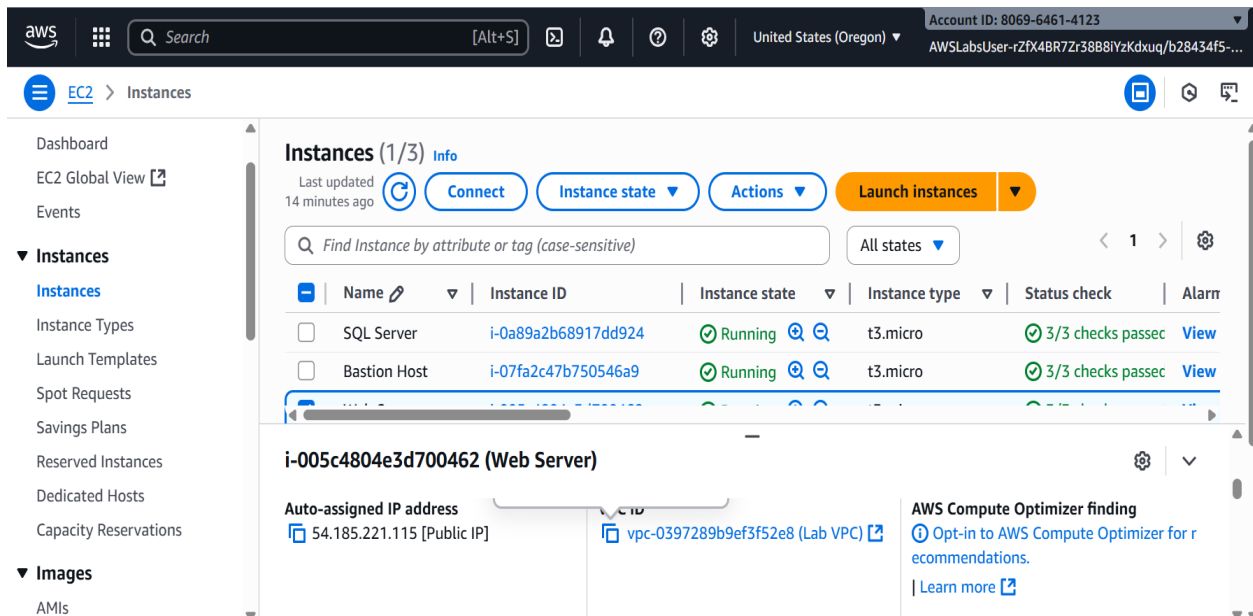


-  This confirms that **least privilege access** is enforced.

4.2 Security Groups Audit


WebServerSG

- Inbound rules allow:
 - **HTTP/HTTPS (80/443)** restricted to 10.10.10.0/24.
 - **RDP (3389)** allowed only via BastionSG.




-  Security-hardened design; not open to the internet.

BastionSG

- Acts as a **jump box** for secure remote access.
- Inbound rules:
 - **SSH (22)** and **RDP (3389)** allowed only from 10.10.10.0/24.
-  Restricts administrative access to a private management network.

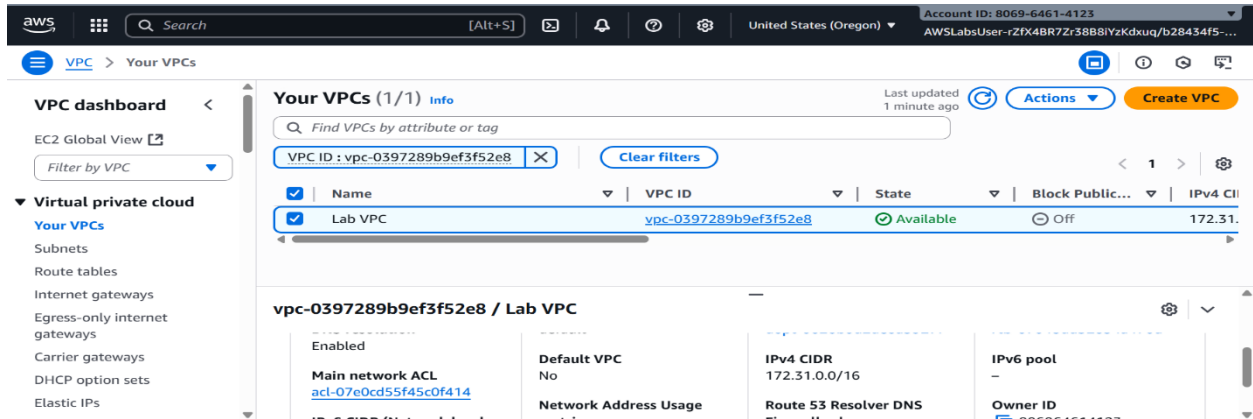
SQLSG

- Inbound traffic allowed only from WebServerSG.
- Outbound rules restricted to application-specific flows.

-  Prevents direct database exposure.

4.3 VPC Configuration Audit

- **VPC ID** verified with the running EC2 instances.



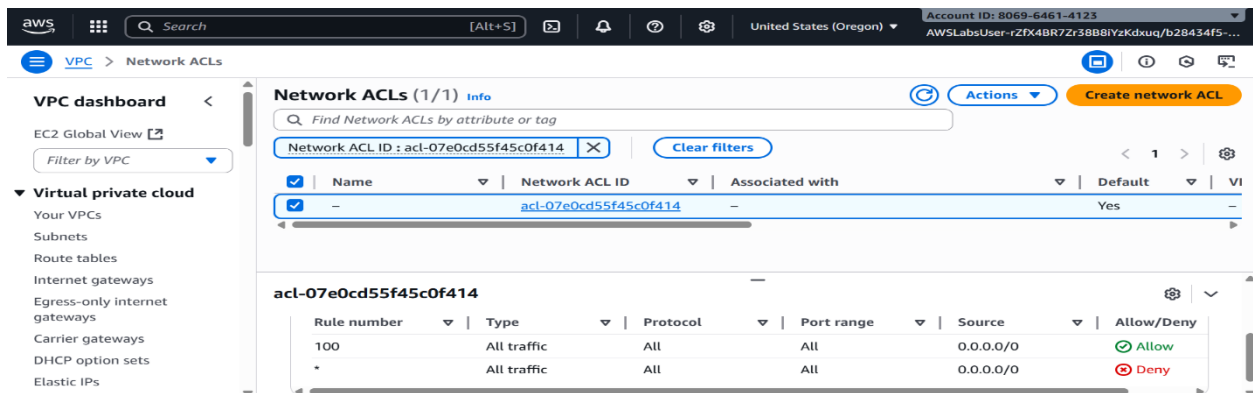
The screenshot shows the AWS VPC console interface. The left sidebar contains the 'VPC dashboard' and 'Virtual private cloud' sections. The main content area displays 'Your VPCs (1/1)' with a table listing VPCs. The selected VPC is 'Lab VPC' with ID 'vpc-0397289b9ef3f52e8'. Below the table, the configuration for 'vpc-0397289b9ef3f52e8 / Lab VPC' is shown, including details like 'Enabled', 'Main network ACL', 'Default VPC', 'IPv4 CIDR', 'IPv6 pool', and 'Owner ID'.

✓	Name	VPC ID	State	Block Public...	IPv4 CIDR
✓	Lab VPC	vpc-0397289b9ef3f52e8	Available	Off	172.31.0.0/16

vpc-0397289b9ef3f52e8 / Lab VPC

- Enabled
- Main network ACL: [acl-07e0cd55f45c0f414](#)
- Default VPC: No
- IPv4 CIDR: 172.31.0.0/16
- IPv6 pool: -
- Network Address Usage: -
- Route 53 Resolver DNS: -
- Owner ID: [8069-6461-4123](#)

- **NACL Rules:**
 - Reviewed Inbound & Outbound policies.
 - Ensures **explicit protocol-level control** for subnets.

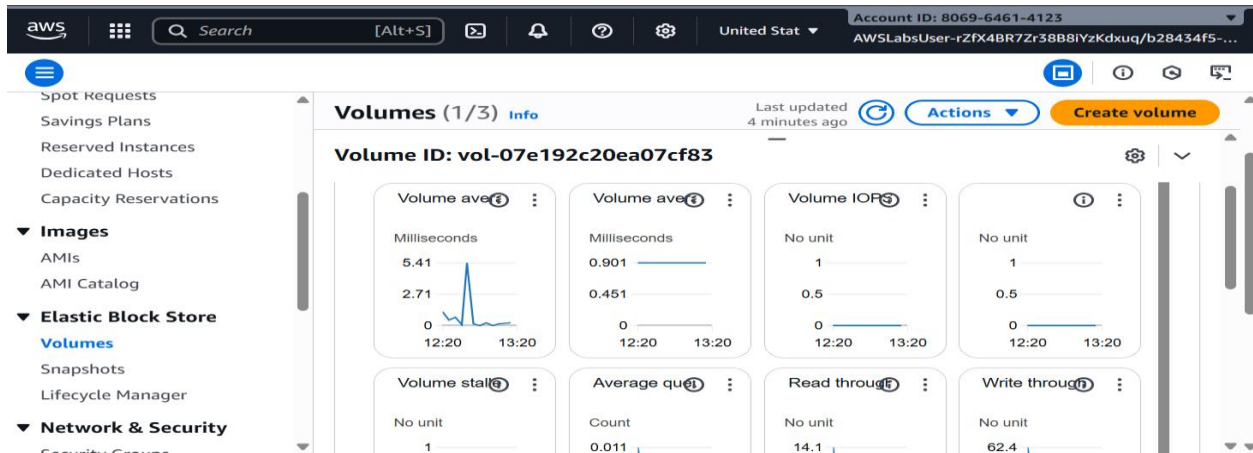


The screenshot shows the AWS VPC console interface for Network ACLs. The left sidebar contains the 'VPC dashboard' and 'Virtual private cloud' sections. The main content area displays 'Network ACLs (1/1)' with a table listing Network ACLs. The selected Network ACL is 'acl-07e0cd55f45c0f414'. Below the table, the configuration for 'acl-07e0cd55f45c0f414' is shown, including details like 'Rule number', 'Type', 'Protocol', 'Port range', 'Source', and 'Allow/Deny'.

✓	Name	Network ACL ID	Associated with	Default	VI
✓	-	acl-07e0cd55f45c0f414	-	Yes	-

acl-07e0cd55f45c0f414

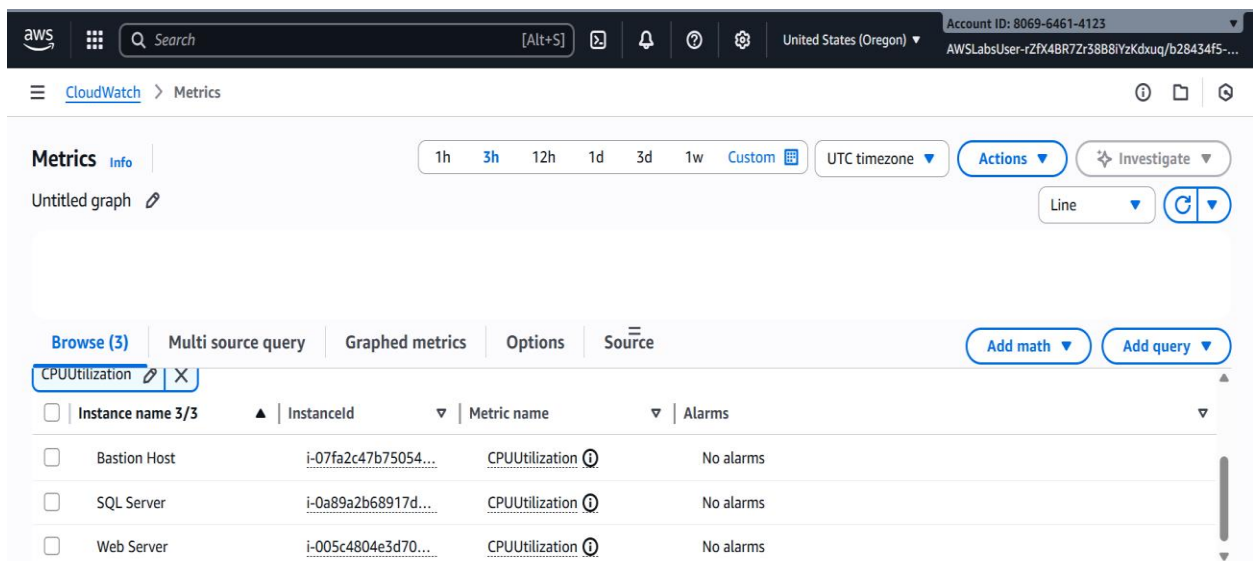
Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

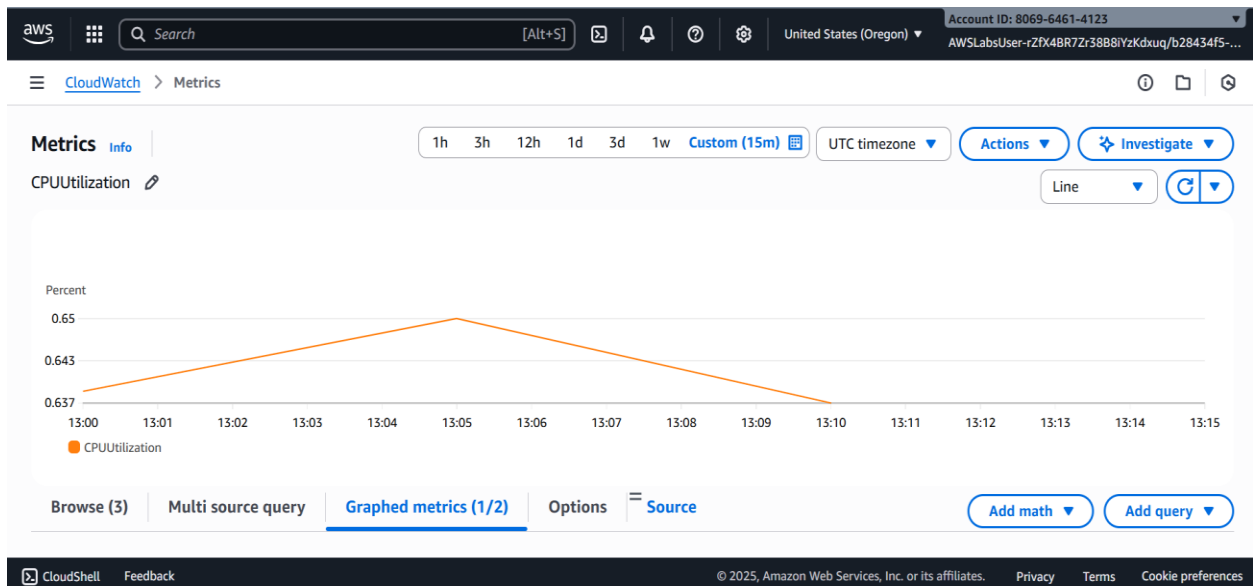



- ☒ Network segmentation enforced.

4.4 CloudWatch Metrics and Alarms

- Metrics observed: **CPU Utilization, Disk I/O.**
- EC2 instance performance reviewed.
- EBS volume monitoring enabled under **Monitoring tab**.





-  Provides real-time operational visibility.

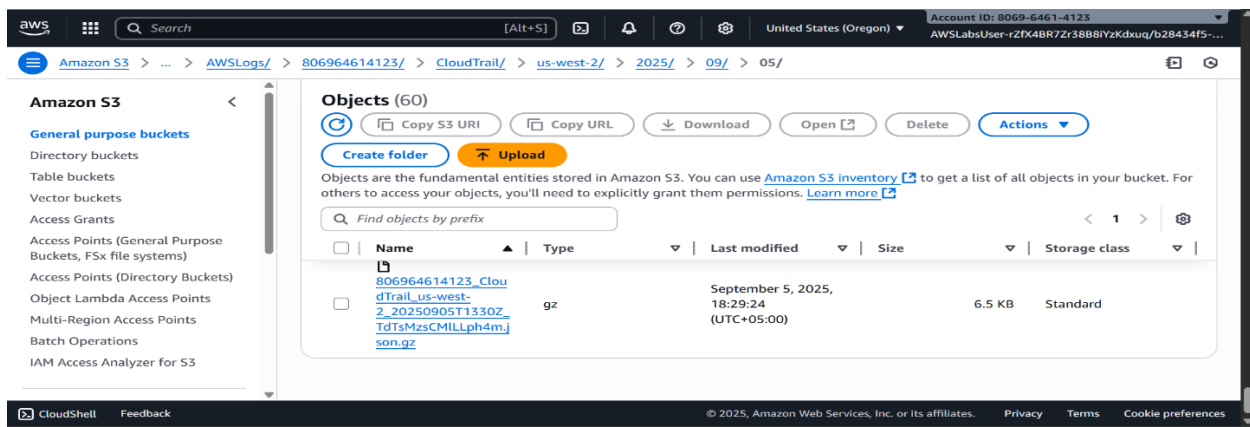
4.5 CloudTrail Logs Audit

- **CloudTrail Trail (LabCloudTrail)** stores logs in S3 bucket (spl73logs).

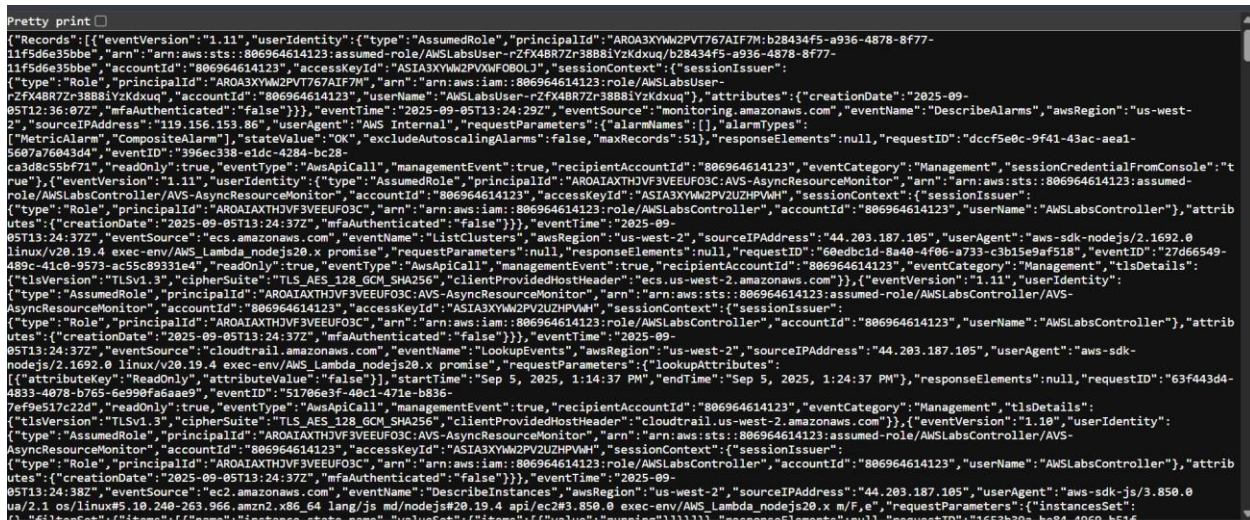
The screenshot shows the AWS CloudTrail console. The top navigation bar includes the AWS logo, a search bar, and account information (Account ID: 8069-6461-4123, AWS Labs User). The main header shows 'CloudTrail > Trails > arn:aws:cloudtrail:us-west-2:806964614123:trail/LabCloudTrail'. The left sidebar has 'CloudTrail' selected. The main content area displays the details of the 'LabCloudTrail'. The 'General details' section shows the following information:

Trail logging	Trail log location	Log file validation	SNS notification delivery
Logging	spl73logs-us-west-2-558507269/AWSLogs/806964614123	Disabled	Disabled
Trail name	LabCloudTrail	Last file validation delivered	Last SNS notification
Multi-region trail	No	-	-
Apply trail to my organization	Not enabled	Log file SSE-KMS encryption	Not enabled
		Not enabled	

Below the 'General details' section, there is a 'CloudWatch Logs' section with an 'Edit' button.



- Logs reviewed in **JSON format** → includes API calls and events.



-  Ensures traceability for auditing and compliance.

5. Audit Evidence

Screenshots were captured for:


- IAM user permissions & policy simulator.
- Security Group inbound/outbound rules.
- VPC + NACL configuration.
- CloudWatch metrics for EC2/EBS.
- CloudTrail logs from S3.

(All evidence stored in screenshots/ folder).

6. Conclusion

The AWS Security Audit confirmed that:

- IAM policies enforce **least privilege**.
- Security groups follow **restricted access principles**.
- VPC and NACL provide **network segmentation**.
- CloudWatch ensures **monitoring & alerting**.
- CloudTrail maintains **accountability & traceability**.

 Overall, the AWS environment demonstrates **strong adherence to cloud security best practices**.

7. Recommendations

- Enable **MFA for all IAM users**.
- Regularly review and rotate **IAM access keys**.
- Configure **CloudWatch alarms** for anomalies.
- Automate compliance checks with **AWS Config**.
- Enable **S3 bucket encryption + versioning** for CloudTrail logs.