

# **AWS config- Research and Development Report**

A brief research and practical report on AWS Config's core features, compliance use cases, and resource monitoring in a sandbox environment



Submitted by: Neety H Maharjan

Submitted to: Desh Deepak Dhobi

Course: Cloud Computing

Organization: Genese Solution

Date: August 31, 2025

## **Table of Contents**

1. Introduction
2. What is AWS Config?
3. Problems AWS Config Solves
4. Core Functionalities
5. Use Cases
6. AWS Config Pricing Overview
7. Limitations of AWS Config
8. Practical Implementation in AWS Sandbox
  - Step 1: Enable AWS Config
  - Step 2: View Resource Configurations
  - Step 3: Add Compliance Rule
  - Step 4: Compliance Dashboard
9. Future Scope of AWS Config
10. Conclusion
11. References

## **1. Introduction**

In cloud environments, resources are constantly being created, modified, or deleted. Tracking these changes manually is difficult and can lead to compliance and security risks. AWS Config is a service that continuously records the configurations of AWS resources, monitors compliance, and provides a history of changes over time.

This report explores what AWS Config is, the problems it solves, its core functionalities, and practical implementation in the AWS sandbox environment.

## **2. What is AWS Config?**

AWS Config is a fully managed service that provides a detailed view of the configuration of AWS resources in an account. It continuously monitors resources, tracks configuration changes, and evaluates them against compliance rules.

It works like a CCTV system for AWS infrastructure, where every change is tracked and recorded for visibility, auditing, and governance.

### **3. Problems AWS Config Solves**

- Ensures compliance and governance.
- Provides auditing and security with a history of resource changes.
- Supports troubleshooting by identifying “what changed.”
- Improves change management with accountability of resource states.

## **4. Core Functionalities**

1. Configuration Recording
2. Configuration History & Timeline
3. Compliance Rules (Managed & Custom)
4. Automated Remediation
5. Compliance Dashboard
6. Integration with other AWS services (CloudTrail, Security Hub, Control Tower)

## **5. Use Cases**

- Financial Sector – PCI-DSS compliance checks.
- Healthcare – HIPAA compliance through IAM and S3 monitoring.
- Enterprises – Tracking IAM and security group changes.
- DevOps Teams – Enforcing governance in CI/CD pipelines.

## **6. AWS Config Pricing Overview**

- Charged per configuration item recorded.
- Charged per rule evaluation.
- Conformance packs add extra charges.
- In free-tier/sandbox, usage is low and cost is minimal.



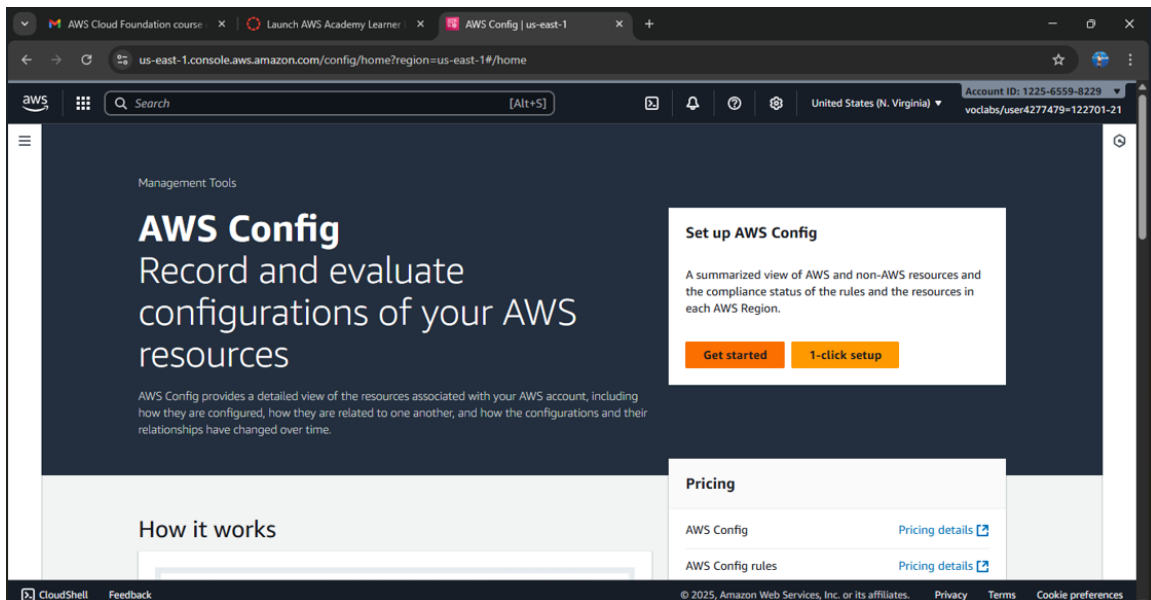
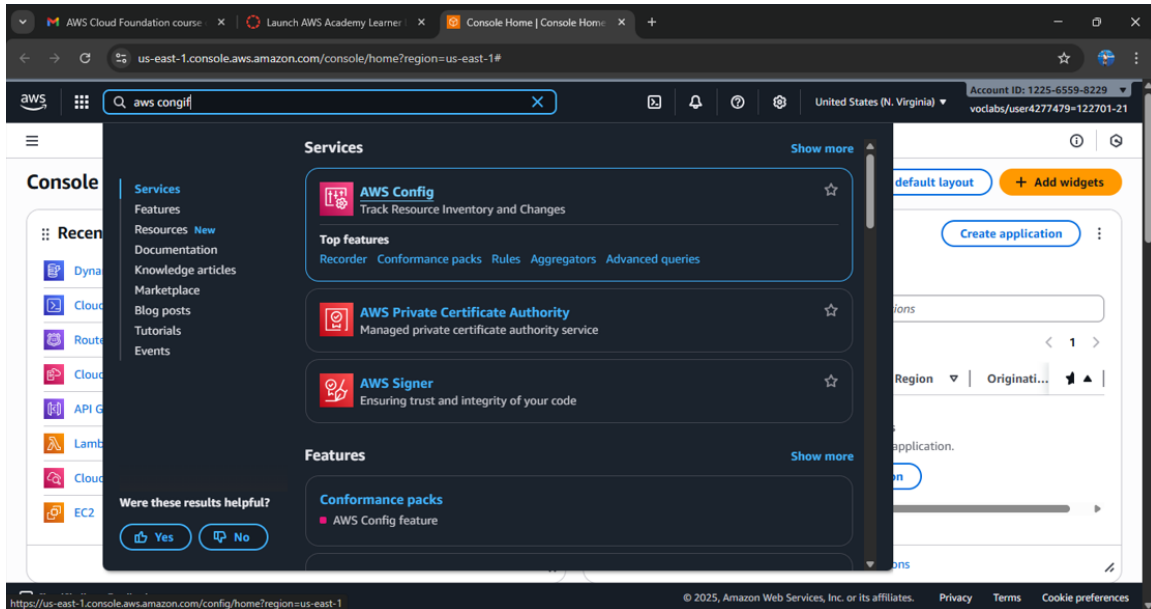
## **7. Limitations of AWS Config**

- Detects issues but does not prevent misconfigurations.
- Evaluations are not always instant.
- Can become costly with many resources and rules.

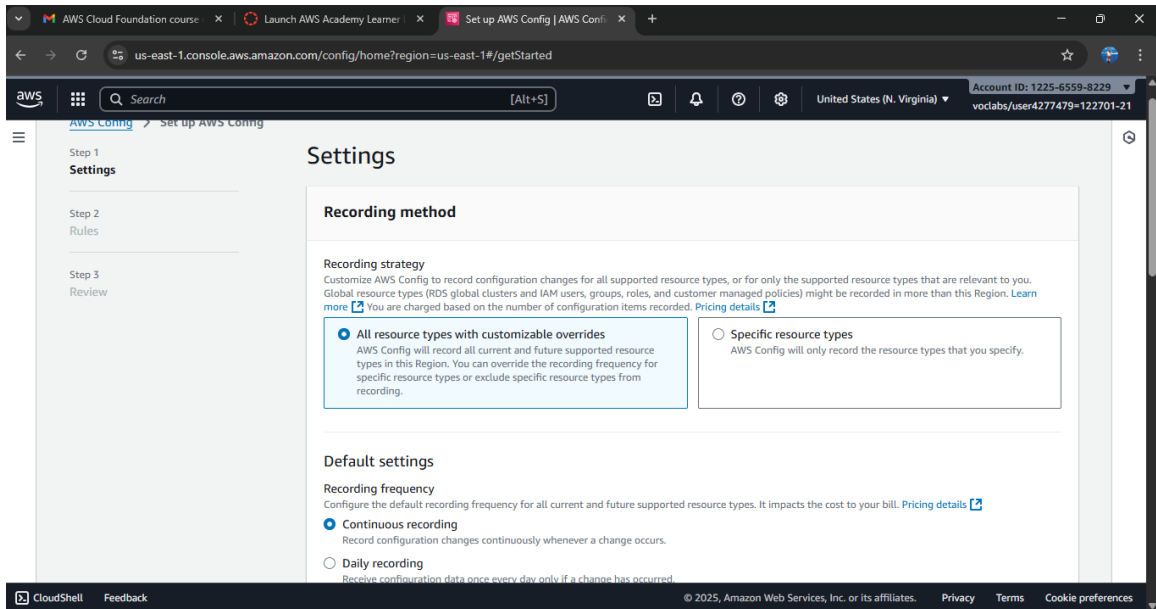
## 8. Practical Implementation in AWS Sandbox

### Step 1: Enable AWS Config

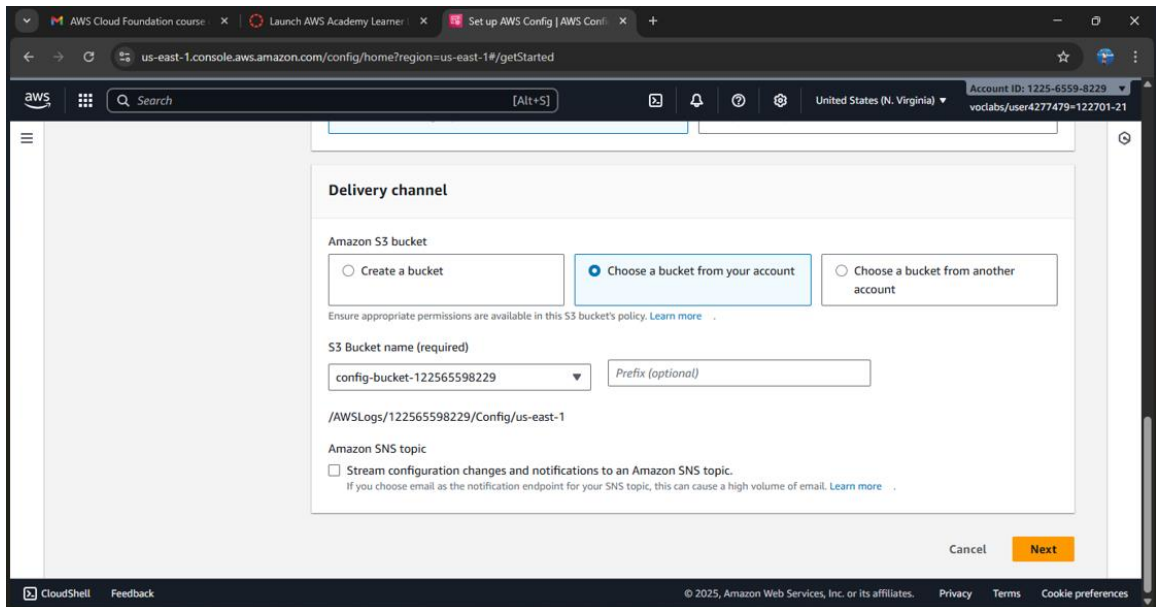
- Opened AWS Config → Clicked Get Started.



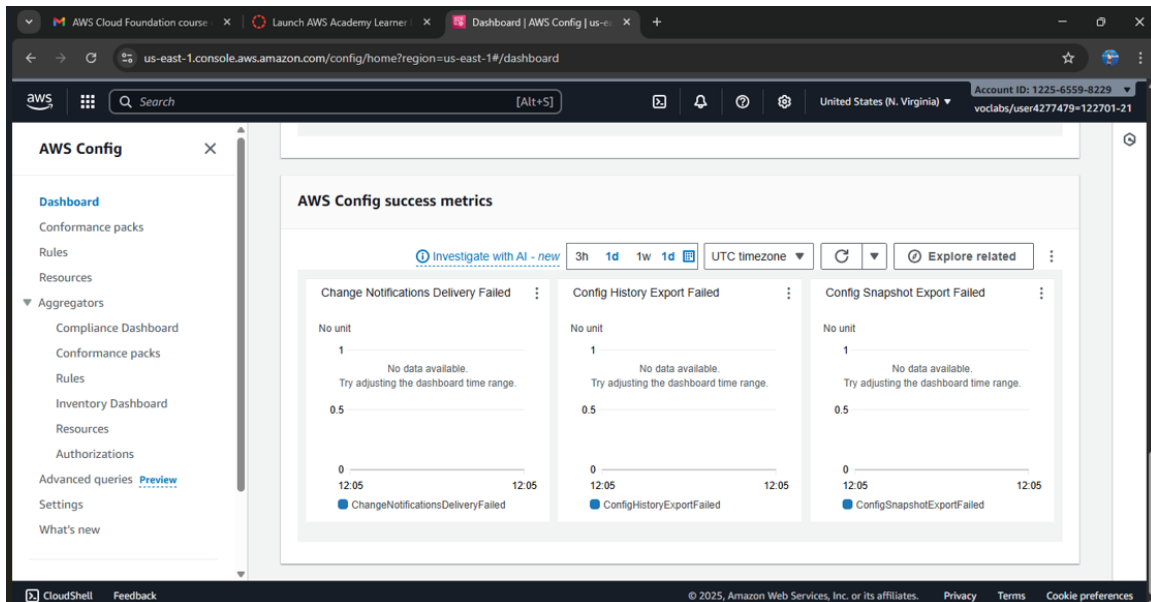
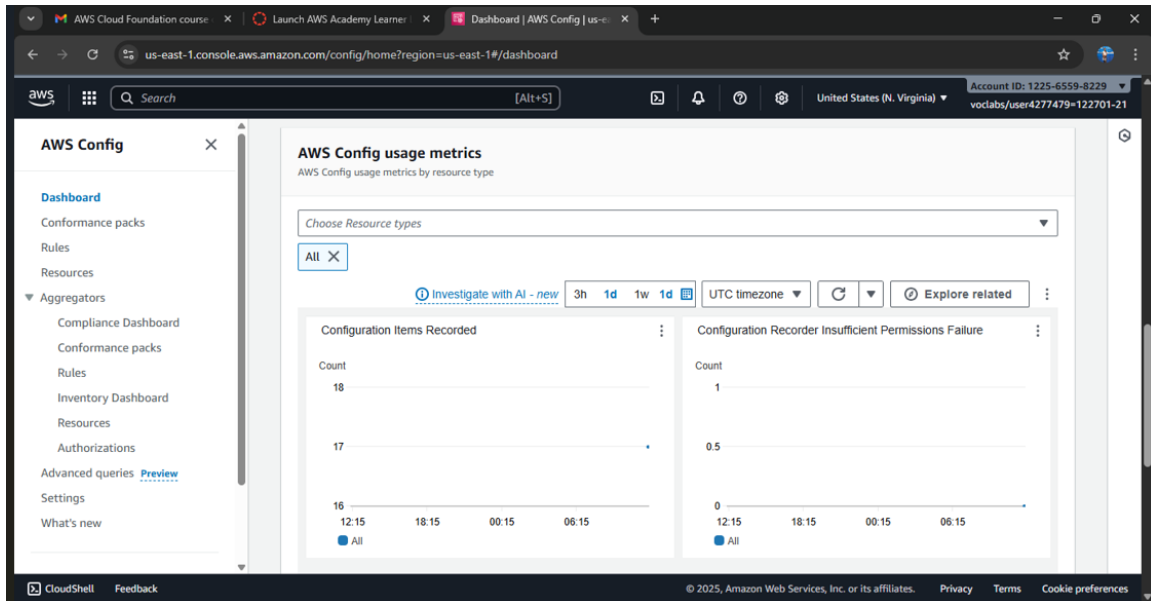
- Selected Record all resources.



- Configured an S3 bucket to store configuration data.



- Enabled recording.



## Step 2: View Resource Configurations

- Checked Resources tab.
- Opened EC2 instance → Viewed configuration timeline.

The screenshot displays the AWS Config console interface. The left-hand navigation pane includes links to Dashboard, Conformance packs, Rules, Resources, and Aggregators. The 'Resources' section is expanded, showing options like Compliance Dashboard, Conformance packs, Rules, Inventory Dashboard, Resources, Authorizations, Advanced queries, Settings, and What's new. The main content area is titled 'Timeline' and provides a description of the resource timeline. Below this, the 'General details' section shows the Resource ID as 'i-0e6d8194eb664e562', the Resource type as 'AWS::EC2::Instance', and the Resource name as '-'. The 'Events' section features a filter for 'All event types' and a date range set to '2025/08/31'. A timeline for 'August 31, 2025' shows two events: a 'Configuration change' at 12:47:12 and a 'CloudTrail Event' at 12:44:57. The bottom of the page includes a footer with '© 2025, Amazon Web Services, Inc. or its affiliates.' and links for Privacy, Terms, and Cookie preferences.

**AWS Config**

Dashboard  
Conformance packs  
Rules  
**Resources**  
▼ Aggregators  
Compliance Dashboard  
Conformance packs  
Rules  
Inventory Dashboard  
Resources  
Authorizations  
Advanced queries [Preview](#)  
Settings  
What's new

### Timeline

The resource timeline allows you to view all the configuration items captured over time for a specific resource and the compliance status changes. For accurate reporting on the compliance status, you must record the AWS Config ResourceCompliance resource type.

**General details**

Resource ID	Resource type	Resource name
i-0e6d8194eb664e562	AWS::EC2::Instance	-

**Events**  
All times are in Asia/Katmandu (UTC+05:45)

End date: 2025/08/31  Event type: All event types ▼

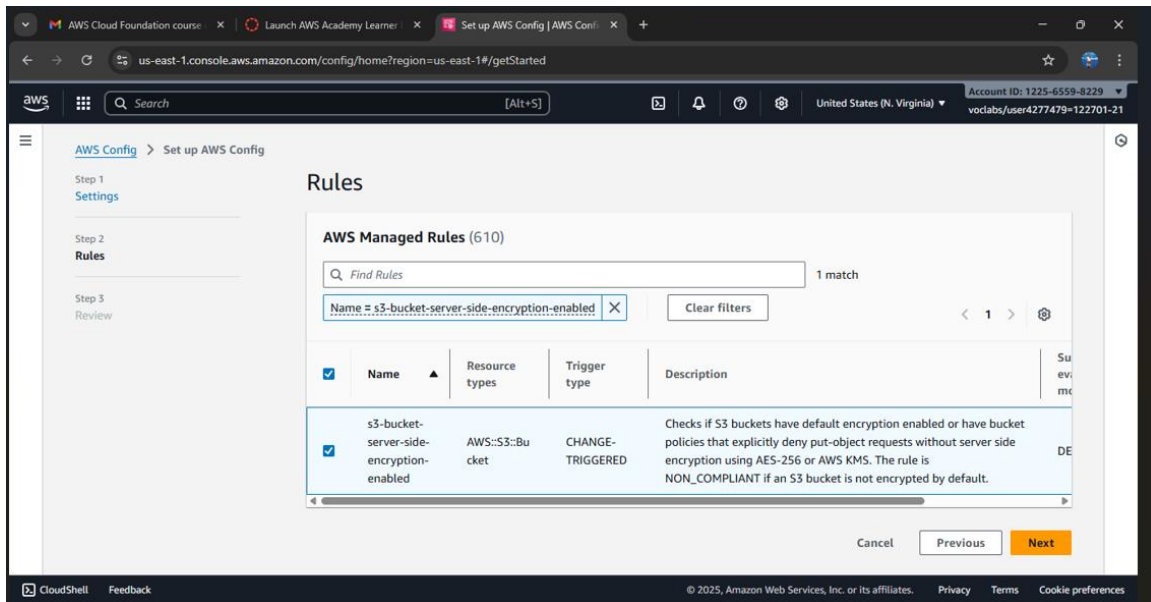
**August 31, 2025**

- 12:47:12 ☐ Configuration change
- 12:44:57 ☒ CloudTrail Event

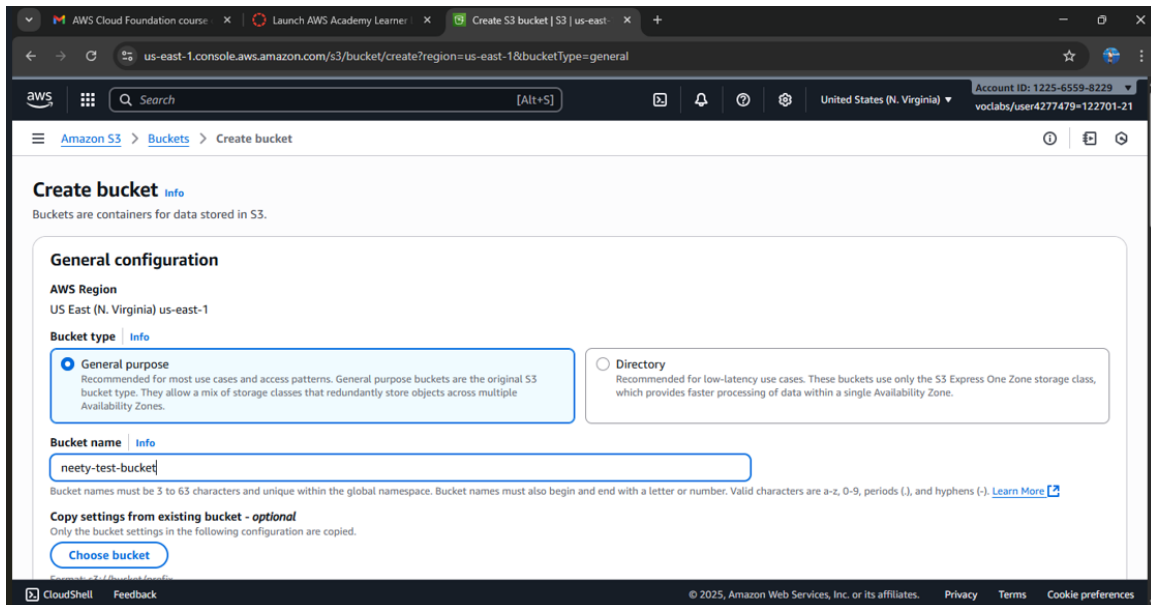
© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

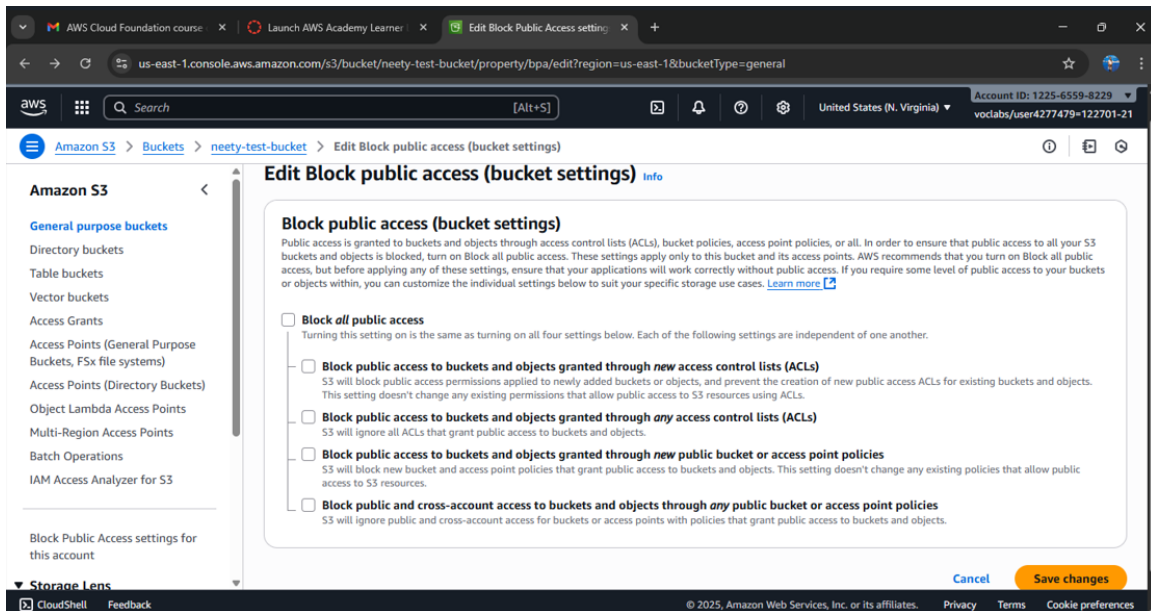
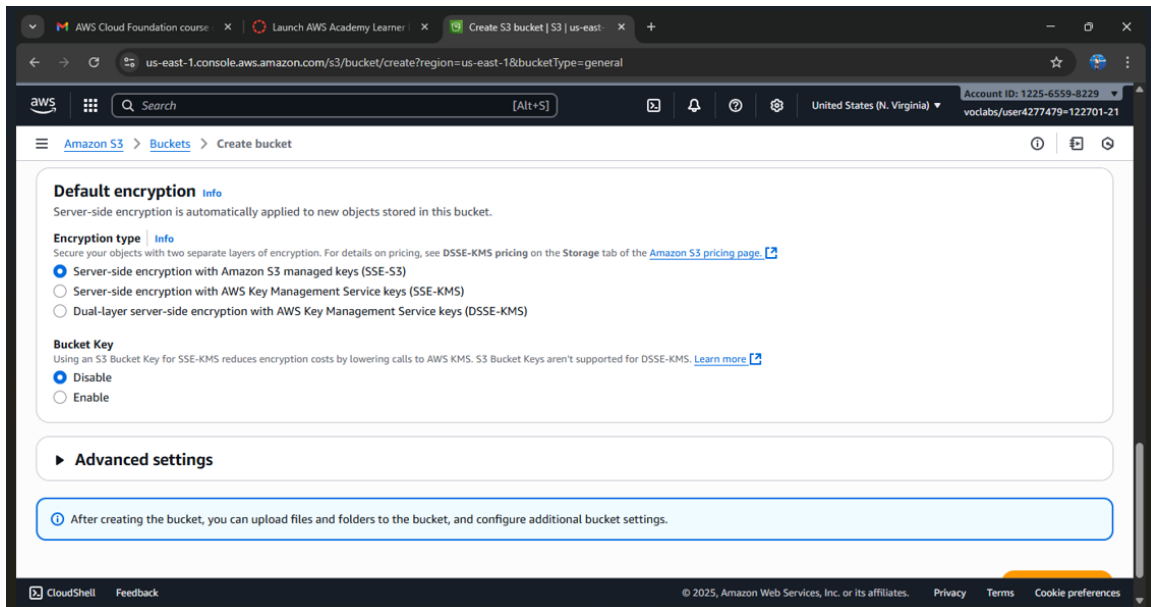
### Step 3: Add Compliance Rule

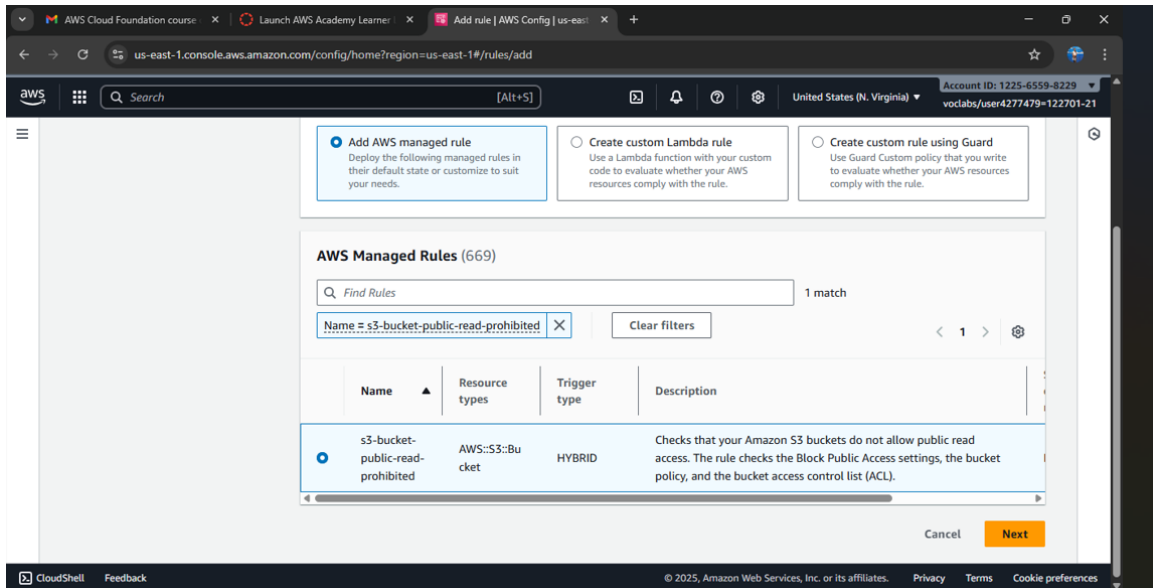
- Added rule s3-bucket-server-side-encryption-enabled.



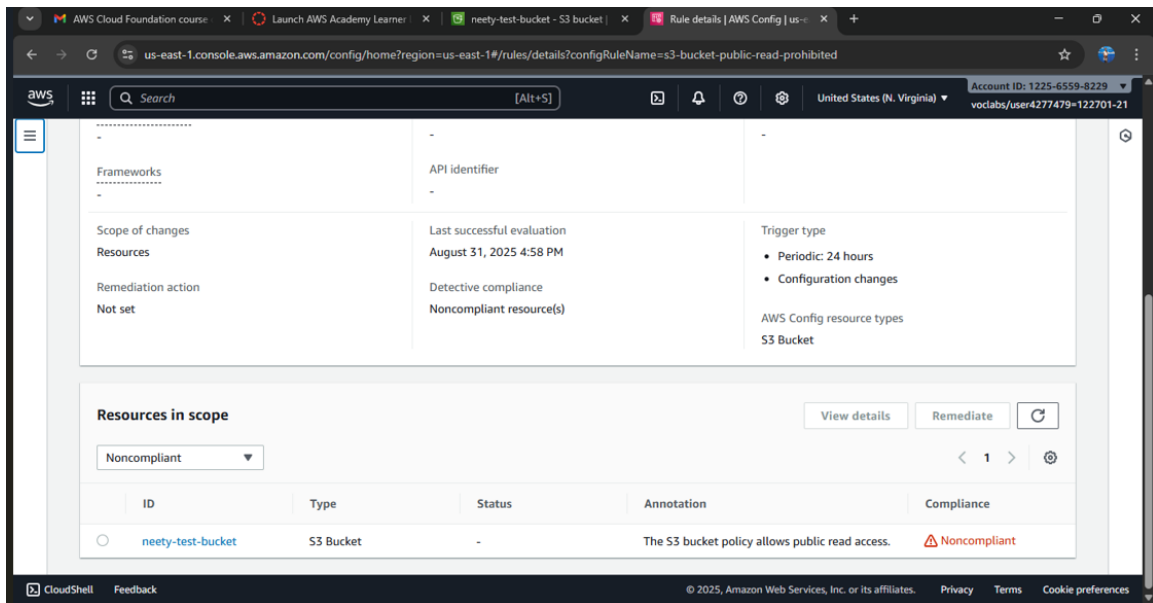
- Created a public S3 bucket for testing.







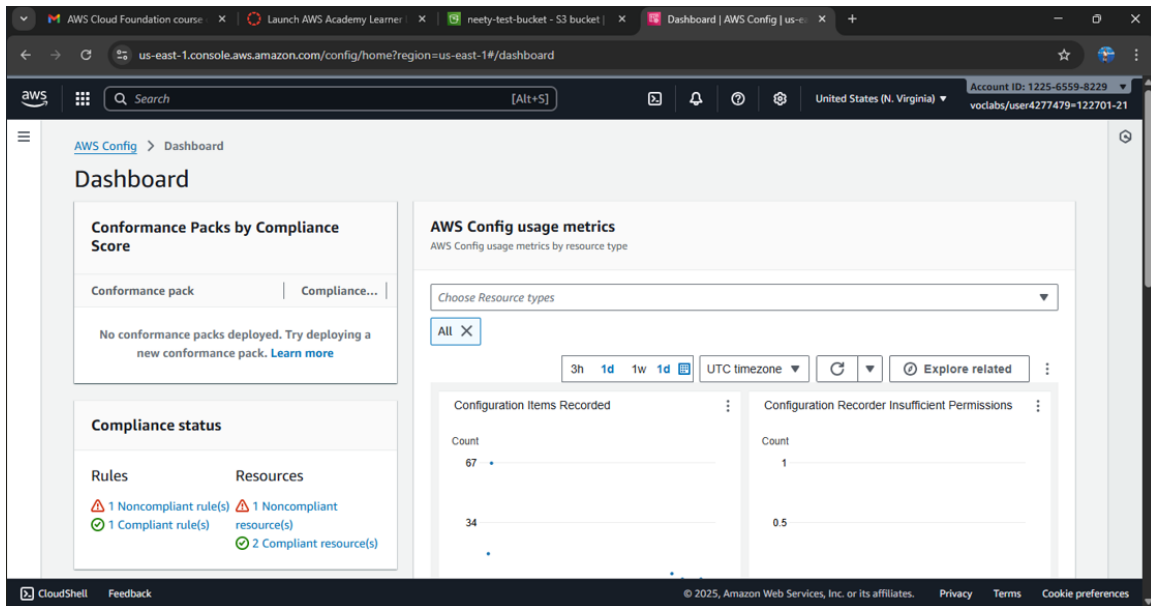
- AWS Config marked it Non-compliant.





## Step 4: Compliance Dashboard

### - Viewed dashboard



The screenshot shows the AWS Config Compliance Dashboard in the us-east-1 region. The dashboard provides an overview of compliance status and usage metrics.

**Compliance Packs by Compliance Score**

Compliance pack	Compliance...
No compliance packs deployed. Try deploying a new compliance pack. <a href="#">Learn more</a>	

**Compliance status**

Rules	Resources
1 Noncompliant rule(s)	1 Noncompliant resource(s)
1 Compliant rule(s)	2 Compliant resource(s)

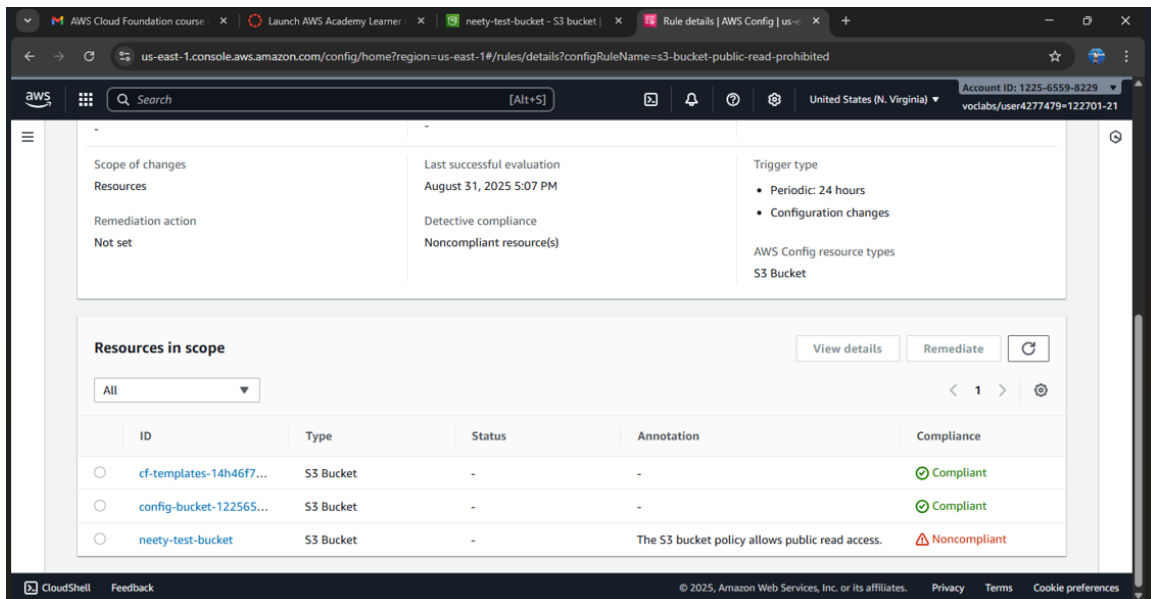
**AWS Config usage metrics**

AWS Config usage metrics by resource type

Choose Resource types:

3h 1d 1w 1d UTC timezone [Explore related](#)

Configuration Items Recorded	Configuration Recorder Insufficient Permissions
Count: 67	Count: 1
34	0.5



The screenshot shows the details of a specific AWS Config rule, 's3-bucket-public-read-prohibited', in the us-east-1 region.

**Scope of changes**  
Resources

**Remediation action**  
Not set

**Last successful evaluation**  
August 31, 2025 5:07 PM

**Detective compliance**  
Noncompliant resource(s)

**Trigger type**

- Periodic: 24 hours
- Configuration changes

**AWS Config resource types**  
S3 Bucket

**Resources in scope**

[View details](#) [Remediate](#)

1

ID	Type	Status	Annotation	Compliance
cf-templates-14h46f7...	S3 Bucket	-	-	Compliant
config-bucket-122565...	S3 Bucket	-	-	Compliant
neety-test-bucket	S3 Bucket	-	The S3 bucket policy allows public read access.	Noncompliant

## **9. Future Scope of AWS Config**

- AI-driven anomaly detection.
- Deeper integration with Security Hub.
- Possible multi-cloud governance support.

## **10. Conclusion**

AWS Config ensures compliance, governance, and visibility in cloud environments by continuously monitoring resource configurations. It provides history, compliance checks, and remediation options.

Through the sandbox practice, I enabled AWS Config, tracked resource changes, applied a compliance rule, and tested non-compliance. The results confirmed how AWS Config simplifies governance and enhances security in AWS.

## **11. References**

1. AWS Config – Official Documentation:

<https://docs.aws.amazon.com/config/>

2. AWS Config Pricing: <https://aws.amazon.com/config/pricing/>

3. AWS Config Features & Use Cases:

<https://aws.amazon.com/config/features/>

