Configuration Monitoring and Compliance Enforcement on AWS

1. Problem Statement

A regulated enterprise required continuous monitoring of AWS configurations to maintain compliance standards. Manual configuration reviews were inefficient and prone to oversight. A centralized compliance monitoring and automated remediation framework was needed.

I implemented this framework to ensure cloud resources comply with security and regulatory requirements aligned with CIS, NIST, and ISO 27001 standards.

The solution uses AWS-native services to provide continuous monitoring, automated remediation, and audit-ready reporting.

2. Objectives

The primary objectives were to:

- Enforce security and configuration standards
- Preventing insecure resource deployment
- Detect configuration drift
- Automate remediation
- Support audit and compliance reporting
- Improve governance and accountability

3. Compliance Monitoring Architecture

The compliance framework was built using:

- AWS Config
- Amazon EventBridge
- AWS Lambda
- AWS Security Hub
- Amazon CloudWatch

All supported resources are continuously recorded and evaluated against defined rules.

4. EBS Encryption Compliance Control

4.1 Control Overview

All Amazon EBS volumes must be encrypted at rest to protect sensitive data.

4.2 Compliance Requirements

- CIS AWS Foundations Benchmark
- NIST SP 800-53 (SC-12, SC-28)
- ISO/IEC 27001 (A.10.1)

4.3 AWS Config Implementation

The AWS-managed rule encrypted-volumes was enabled to monitor EBS encryption.

EBS encryption by default was enabled at the account level.

4.4 Compliance Testing

Attempts to create unencrypted volumes were blocked, confirming preventive enforcement.

4.5 Remediation Strategy

Preventive controls were prioritized.

For legacy volumes, snapshots were encrypted and migrated.

Status: Compliant

5. S3 Public Access Compliance Control

5.1 Control Overview

All S3 buckets must be protected from public access.

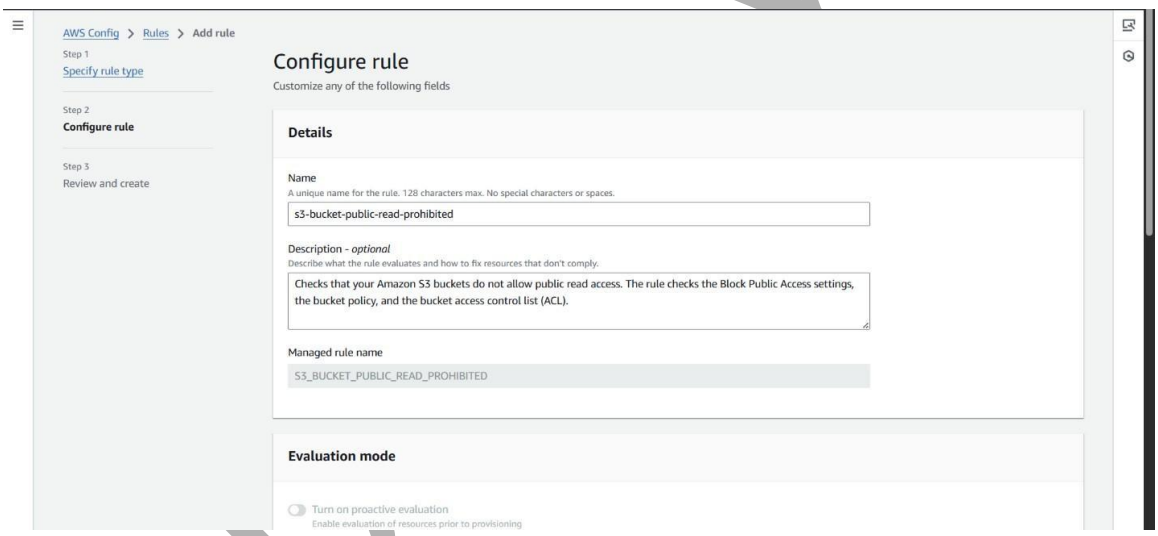
5.2 Compliance Requirements

- CIS AWS Foundations Benchmark
- NIST SP 800-53 (AC-3, AC-6)
- ISO/IEC 27001 (A.9)

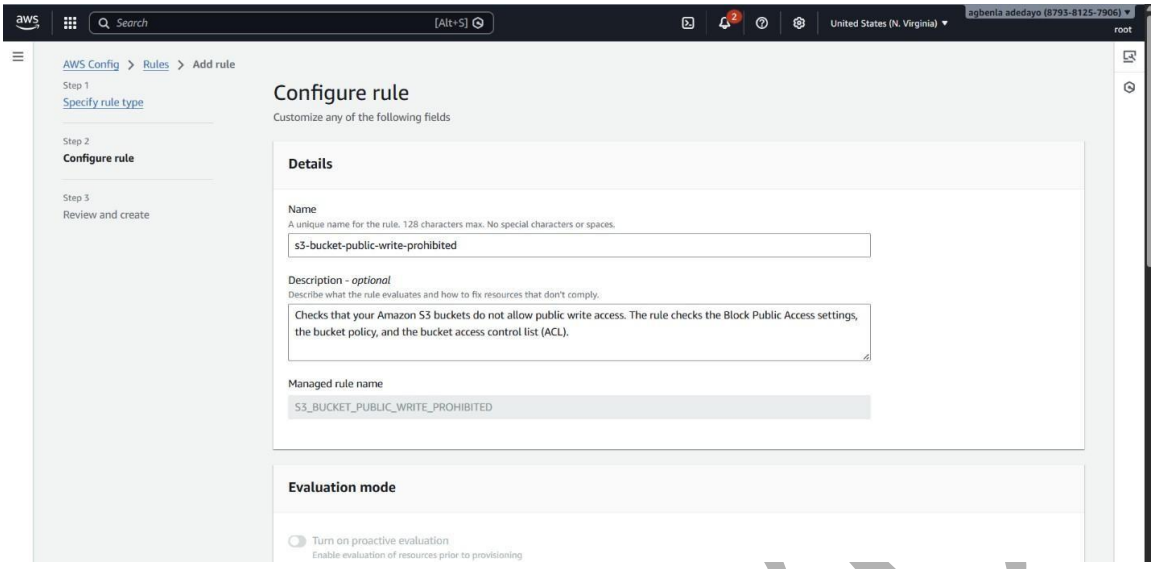
5.3 AWS Config Implementation

Managed rules enabled:

- s3-bucket-public-read-prohibited

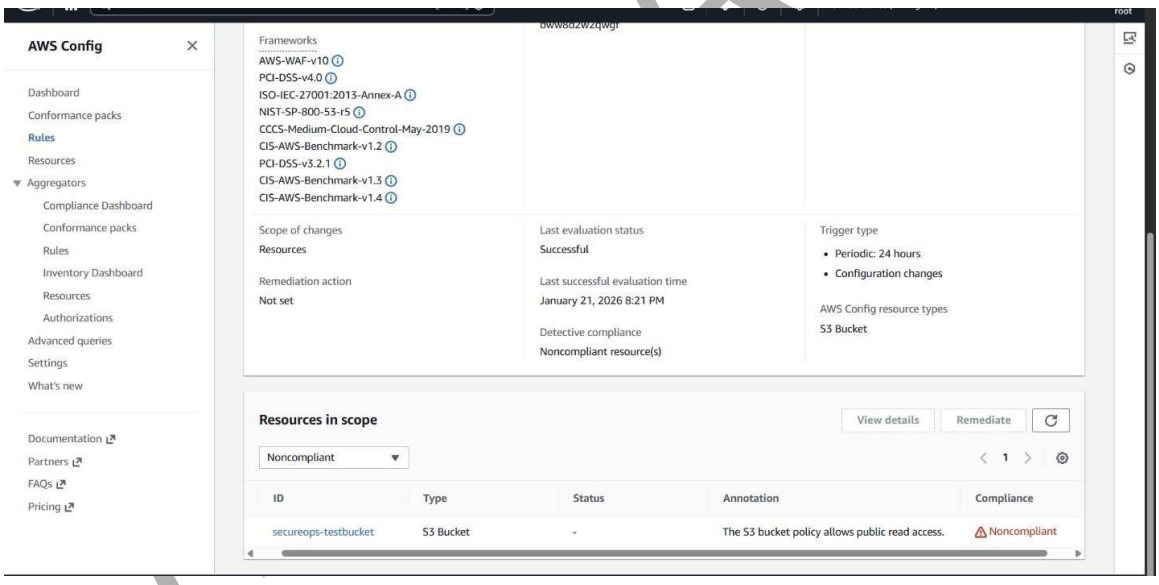


- s3-bucket-public-write-prohibited



5.4 Compliance Testing

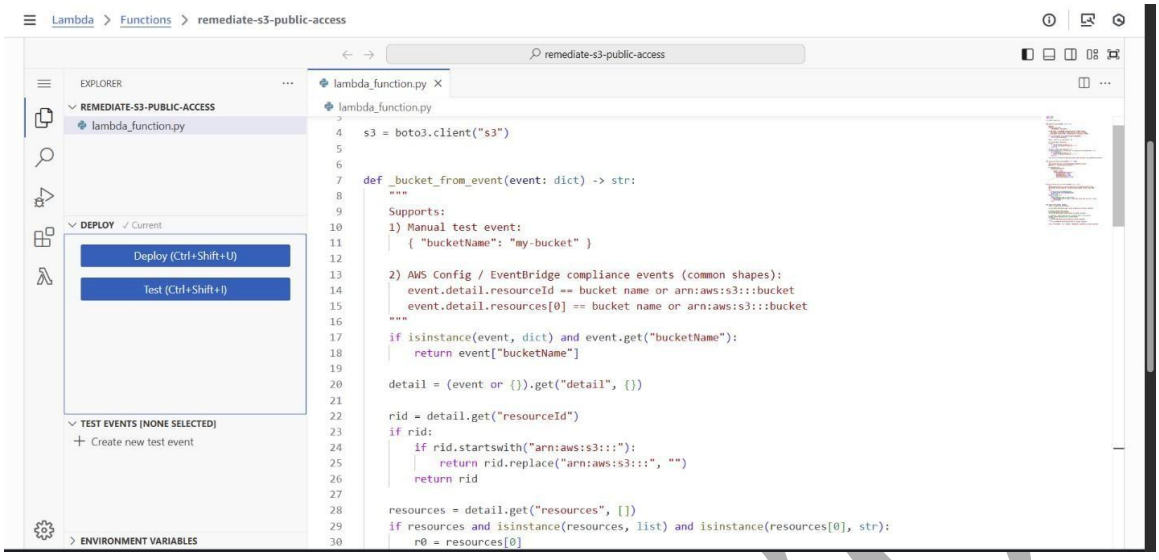
Public access was introduced intentionally and detected successfully.



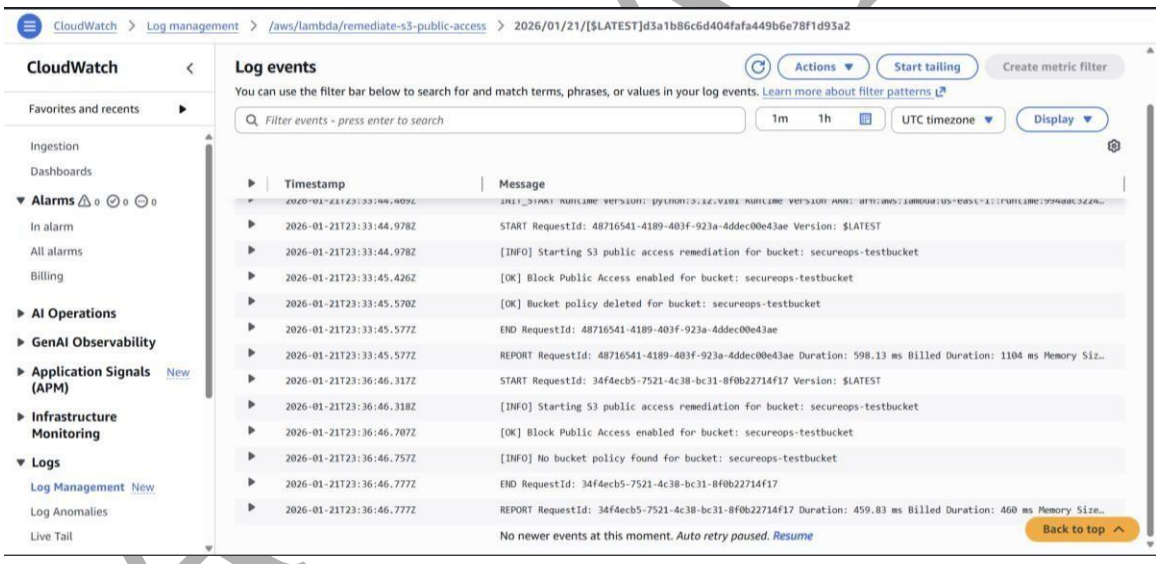
5.5 Automated Remediation

A Lambda-based remediation workflow was implemented using EventBridge.

The function:



- Enables Block Public Access
- Removes insecure policies
- Logs actions to CloudWatch



Status: Compliant (Automated Remediation)

6. Account-Level Preventive Controls

Account-level S3 Block Public Access and EBS encryption by default were reviewed and enforced.

These controls prevent misconfigurations before deployment.

7. Compliance Mapping and Alignment

Controls were mapped to major frameworks:

- CIS AWS Foundations
- NIST SP 800-53
- ISO/IEC 27001

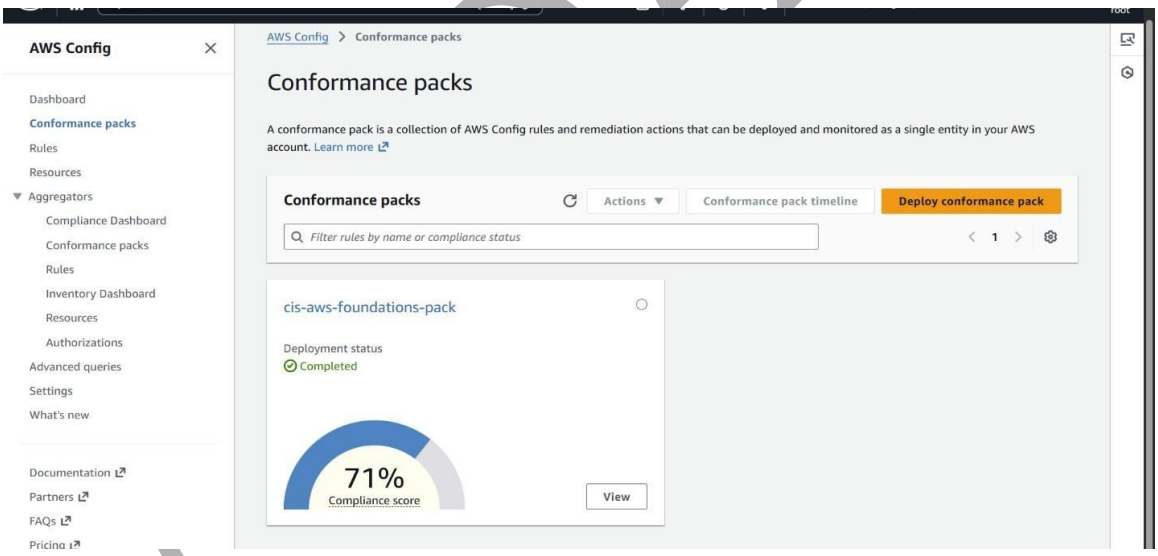
Preventive, detective, and corrective controls were implemented.

8. Conformance Pack Deployment

An AWS Config CIS conformance pack was deployed.

The pack automatically evaluated multiple security controls.

Dashboards provided visibility into compliance posture.



9. Automated Remediation Framework

Compliance change events trigger EventBridge rules.

Lambda functions perform corrective actions.

Manual procedures were defined as fallback.

10. Governance and Documentation

All compliance rules, workflows, and remediation processes were documented.

Documentation supports:

- Regulatory audits
- Internal reviews
- Incident investigations
- Knowledge transfer

11. Reporting and Visibility

AWS Config dashboards and Security Hub were used for reporting.

Reports include:

- Compliance status
- Violations
- Remediation progress

Reports are reviewed regularly.

12. Testing and Validation

Controls were validated using intentional misconfigurations:

- Public S3 buckets
- Disabled encryption
- Policy changes

Violations were detected and remediated automatically.

13. Outcomes and Impact

This implementation delivered:

- Continuous compliance monitoring
- Reduced configuration drift
- Automated remediation
- Improved governance
- Audit-ready reporting
- Reduced regulatory risk

14. Conclusion

I designed and implemented an enterprise-grade compliance monitoring and enforcement framework on AWS.

Through continuous evaluation, automated remediation, and governance controls, this solution ensures secure, compliant, and well-governed cloud operations.