# AWS Config

Complete Theory & Implementation Guide

**📚 Table of Contents**

* [Theory Foundation](#theory-foundation)
* [AWS Config Architecture](#aws-config-architecture)
* [Personal Learning Notes](#personal-learning-notes)
* [Complete Implementation Journey](#implementation-journey)
* [Integration Analysis](#integration-analysis)
* [Enterprise Applications](#enterprise-applications)
* [Troubleshooting & Lessons Learned](#troubleshooting)
* [Day Review Summary](#day-review)

## Theory Foundation

**What is AWS Config?**

**AWS Config = AWS Configuration Management and Compliance Service**

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources continuously. Think of it as your **"configuration compliance detective"** that never sleeps - it watches every resource change and immediately evaluates whether those changes comply with your security and governance policies.

### The Business Problem AWS Config Solves

Organizations face critical challenges that manual processes cannot solve at scale:

#### 1. Configuration Drift Crisis

* **Problem:** Resources slowly deviate from approved security baselines
* **Real Impact:** A secure EC2 instance gradually becomes vulnerable as developers modify security groups, open ports, change IAM policies
* **Business Cost:** 90% of cloud breaches involve configuration errors
* **Why Config Solves This:** Continuous monitoring catches drift immediately, not during quarterly audits

#### 2. Compliance Automation Necessity

* **Problem:** Manual compliance checking is error-prone, expensive, and doesn't scale
* **Real Impact:** Auditors spend weeks manually checking thousands of resources
* **Business Cost:** Failed audits, regulatory penalties, audit firm costs
* **Why Config Solves This:** Automated rule evaluation provides real-time compliance status

#### 3. Change Investigation Requirements

* **Problem:** When security incidents occur, teams need to understand "what changed when"
* **Real Impact:** Security teams spend days investigating configuration history
* **Business Cost:** Extended incident response times, unclear root causes
* **Why Config Solves This:** Complete configuration history with timeline

## AWS Config Architecture

### How Config Actually Works

### 

### Core Components Deep Dive

#### 1. Configuration Recorder (The "What to Watch" Engine)

**Purpose:** Defines which AWS resources Config monitors and how frequently

**Recording Options**

* **All Supported Resources:** Monitor everything AWS Config can track (recommended)
* **Specific Resource Types:** Only monitor selected services (EC2, S3, IAM, etc.)
* **Global Resources:** IAM users, roles, policies (recorded once globally, not per region)

**Why This Matters for Security:**

* **Complete Visibility:** "All supported" ensures new AWS services are automatically monitored
* **Global Resource Tracking:** IAM changes affect all regions, must be captured centrally
* **Resource Relationships:** Config maps dependencies (VPC → Subnet → Instance → Security Group)

#### 2. Configuration Items (CIs) - The "Resource Snapshots"

**Definition:** Point-in-time snapshot of a resource's complete configuration state

**What's Captured in Each CI:**

* **Resource Identification:** Type, ID, name, region, account
* **Configuration Data:** All resource properties and settings
* **Relationships:** Connected resources and dependencies
* **Metadata:** Creation time, configuration capture time, resource status
* **Change History:** Previous configurations for comparison

#### 3. Delivery Channel (The "Where to Store" Engine)

**Purpose:** Defines where Config stores configuration data and snapshots

**Storage Destinations:**

* **S3 Bucket (Required):** Primary storage for all configuration data
* **SNS Topic (Optional):** Real-time notifications for configuration changes

#### 4. Config Rules (The "Compliance Evaluation" Engine)

**Purpose:** Automated evaluation of resource configurations against compliance requirements

**AWS Managed Rules (Pre-built by AWS)**

* s3-bucket-public-read-prohibited: Ensures S3 buckets don't allow public read
* encrypted-volumes: Verifies EBS volumes are encrypted
* iam-user-mfa-enabled: Checks if IAM users have MFA enabled
* root-access-key-check: Ensures root account doesn't have access keys

**Compliance States:**

* **COMPLIANT:** Resource meets rule requirements
* **NON\_COMPLIANT:** Resource violates rule requirements
* **NOT\_APPLICABLE:** Rule doesn't apply to this resource type
* **INSUFFICIENT\_DATA:** Not enough information to evaluate

## Implementation Analysis & Technical Insights

### Authentication Strategy Evaluation

During the implementation phase, comprehensive analysis was conducted on AWS CLI authentication methods, leading to the selection of an optimal MFA approach:

#### Approach 1: Manual MFA Token Management

# Step 1: Get MFA session token manually

aws sts get-session-token --profile admin-base --serial-number arn:aws:iam::733366527973:mfa/device-1 --token-code 123456

# Step 2: Manually update credentials file with temporary credentials

# Step 3: Set profile to use those temporary credentials

set AWS\_PROFILE=temp-mfa-profile

#### Approach 2: Automated Role Assumption (Selected Method)

# Just set the profile - AWS CLI handles MFA automatically

$env:AWS\_PROFILE= “admin-mfa”

aws sts get-caller-identity

# AWS CLI prompts for MFA automatically

**Configuration File Implementation**

[profile admin-mfa] role\_arn = arn:aws:iam::733366527973:role/AdminRole-MFA source\_profile = admin-base mfa\_serial = arn:aws:iam::733366527973:mfa/device-1 region = us-east-1

**Behind-the-scenes Process Flow:**

1. Command execution: aws sts get-caller-identity
2. AWS CLI reads admin-mfa profile configuration
3. AWS CLI recognizes role assumption requirement with MFA
4. AWS CLI automatically executes: aws sts assume-role
5. AWS CLI prompts for MFA code input
6. AWS CLI obtains and caches temporary credentials
7. Command executes with authenticated credentials

### S3 Security Architecture Analysis

Through comprehensive S3 bucket implementation, several critical enterprise security concepts were mastered and validated:

#### Bucket Types and Use Cases

##### General Purpose Bucket

* Multi-AZ storage with high durability
* Supports multiple storage classes (Standard, IA, Glacier)
* Ideal for compliance data requiring cross-region replication

##### Directory Bucket (S3 Express One Zone)

* Single AZ deployment for ultra-low latency
* Optimized for high-performance workloads
* Not suitable for compliance data requiring durability

#### Object Ownership Security Models

**ACLs Disabled (Recommended for Enterprise)**

Bucket owner maintains ownership of all objects regardless of uploader. Access control managed exclusively through bucket policies and IAM policies, providing centralized security management.

**ACLs Enabled (Legacy Compatibility)**

More complex model where objects can be owned by uploaders. Requires careful ACL management and can lead to security gaps in enterprise environments.

#### Block Public Access Settings Analysis

The implementation included all four critical public access protection layers:

1. **Block public access through new ACLs:** Prevents future ACL modifications enabling public access
2. **Block public access through any ACLs:** Ignores existing public ACLs
3. **Block public access through new policies:** Prevents new bucket policies with public access
4. **Block public and cross-account access through any policies:** Comprehensive policy-based protection

#### Encryption Strategy Selection

**SSE-S3 (Selected for Cost)**

* AWS managed keys
* No additional cost
* Sufficient for most compliance requirements

**SSE-KMS (Advanced Control)**

* Customer managed keys
* Enhanced audit capabilities
* Key rotation control

**DSSE-KMS (Maximum Security)**

* Dual-layer encryption
* Compliance-heavy environments
* Defense in depth strategy

### CloudTrail Integration Architecture

#### Service-Specific Bucket Policy Requirements

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "Statement1",

"Effect": "Allow",

"Principal": {

"Service":"cloudtrail.amazonaws.com"

},

"Action": [

"s3:GetBucketAcl"

],

"Resource": "arn:aws:s3:::cloudtrail-logs-733366527973-training"

},

{

"Sid": "Statement2",

"Effect": "Allow",

"Principal": {

"Service":"cloudtrail.amazonaws.com"

},

"Action": [

"s3:PutObject"

],

"Resource": "arn:aws:s3:::cloudtrail-logs-733366527973-training/\*",

"Condition": {

"StringEquals": {

"s3:x-amz-acl": "bucket-owner-full-control"

}

}

}

]

}

**Permission Analysis Deep Dive**

**GetBucketAcl Permission:** CloudTrail validates bucket ownership and access permissions before writing logs, ensuring proper authorization chain.

**PutObjectAcl Condition:** CloudTrail sets ACLs on log files ensuring bucket owner maintains full control over all audit data, preventing privilege escalation.

## Complete Implementation Journey

### Day 2 Implementation Timeline

**1**

**IAM Service Role Creation**

**Implementation Approach:**

* Created AwsConfig-service-role via AWS Console
* Applied trust policy restricting access to config.amazonaws.com service
* Attached AWS managed ConfigRole policy for service permissions

##### Trust Policy Configuration

# Trust policy content saved as config-trust-policy.json

{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "config.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }

##### Role Verification Commands

# Verify IAM role creation and policies

aws iam get-role --role-name AwsConfig-service-role

aws iam list-attached-role-policies --role-name AwsConfig-service-role

##### Security Analysis

The trust policy restricts role assumption to AWS Config service only, preventing privilege escalation and ensuring least privilege access.

**2**

**S3 Bucket Security Architecture**

**Implementation Steps:**

* Created config-compliance-data-733366527973 bucket
* Applied all four public access block protections
* Implemented service-specific bucket policy

##### Bucket Creation

# Create dedicated S3 bucket for Config data

aws s3 mb s3://config-compliance-data-733366527973 --region us-east-1

##### Security Controls Implementation

# Apply comprehensive public access block aws s3api put-public-access-block \ --bucket config-compliance-data-733366527973 \ --public-access-block-configuration "BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true" \ --profile admin-mfa

##### Service-Specific Bucket Policy

# Bucket policy content saved as config-bucket-policy.json

"Version": "2012-10-17",

"Statement": [

{

"Sid": "Statement1",

"Effect": "Allow",

"Principal": {

"Service":"cloudtrail.amazonaws.com"

},

"Action": [

"s3:GetBucketAcl"

],

"Resource": "arn:aws:s3:::cloudtrail-logs-733366527973-training"

},

{

"Sid": "Statement2",

"Effect": "Allow",

"Principal": {

"Service":"cloudtrail.amazonaws.com"

},

"Action": [

"s3:PutObject"

],

"Resource": "arn:aws:s3:::cloudtrail-logs-733366527973-training/\*",

"Condition": {

"StringEquals": {

"s3:x-amz-acl": "bucket-owner-full-control"

}

}

}

]

}

##### Security Verification

# Verify public access block configuration

aws s3api get-public-access-block \ --bucket config-compliance-data-733366527973 \ --profile admin-mfa

# Verify bucket policy application

aws s3api get-bucket-policy \ --bucket config-compliance-data-733366527973 \ --profile admin-mfa

**3-5**

**Configuration Recorder and Delivery Channel**

**Implementation Achievements:**

* **Configuration Recorder:** default recorder monitoring all resource types
* **Global Resources:** IAM resources included for complete security coverage
* **No Exclusions:** Removed AWS's default IAM exclusion for cost savings
* **Delivery Channel:** 24-hour snapshot frequency for cost efficiency
* **Recording Status:** Active since 15:42 IST on August 14, 2025

##### Configuration Recorder Verification

# Verify configuration recorder setup

aws configservice describe-configuration-recorders --profile admin-mfa

# Check recorder status

aws configservice describe-configuration-recorder-status --profile admin-mfa

##### Delivery Channel Verification

# Verify delivery channel configuration aws configservice describe-delivery-channels --profile admin-mfa

##### Data Flow Validation

# Check Config data flow to S3 aws s3 ls s3://config-compliance-data-733366527973/AWSLogs/733366527973/Config/ --recursive --profile admin-mfa

##### Expected Status Indicators

* "recording": true
* "lastStatus": "SUCCESS"
* "lastStartTime": Shows activation timestamp
* ConfigWritabilityCheckFile confirms Config can write to bucket

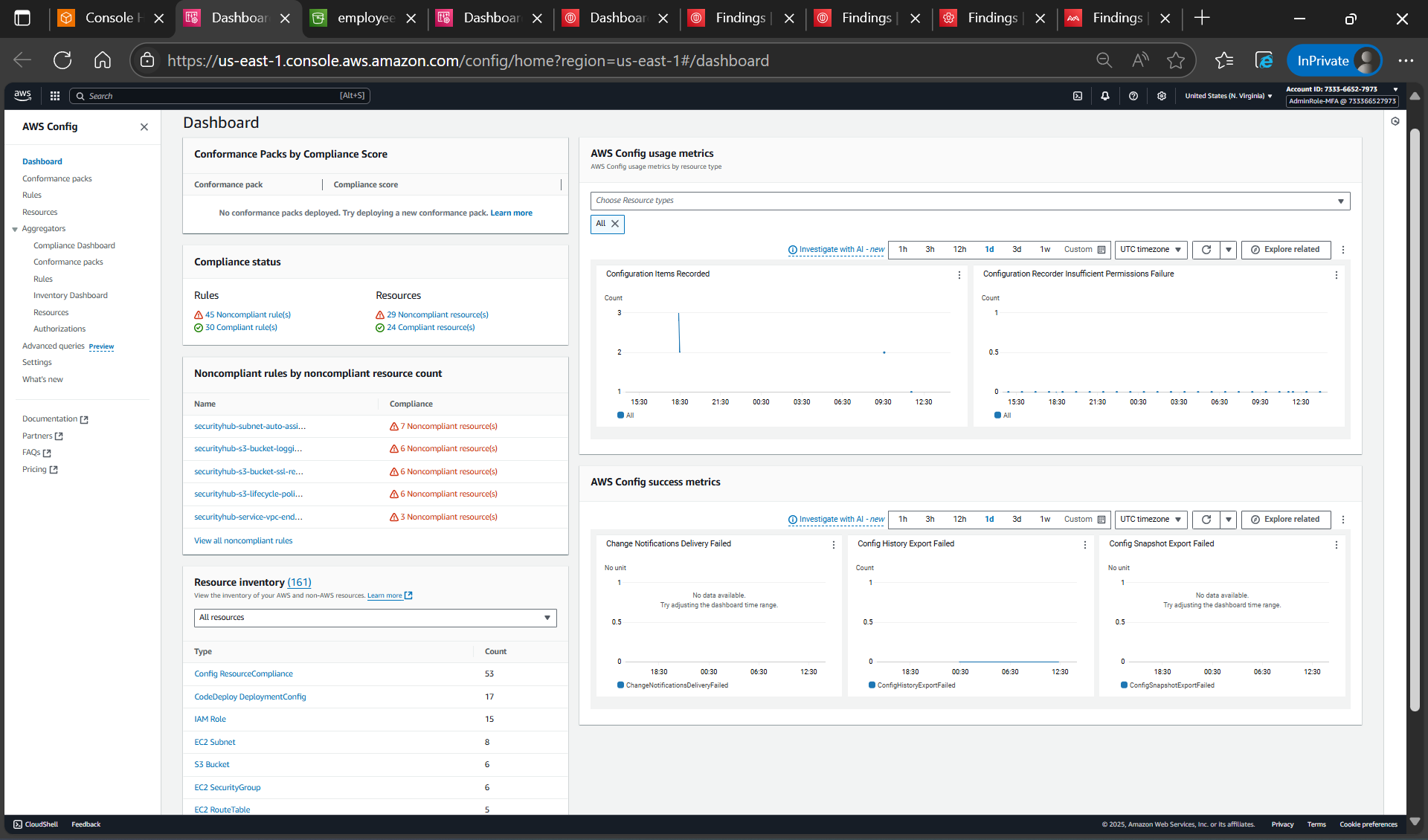


Figure 2.1: AWS Config Dashboard showing active configuration recording with comprehensive resource discovery.

Demonstrates Config service operational status.

**6**

**Compliance Rule Implementation and Testing**

##### S3 Public Access Compliance Rule Creation

# Create mandatory S3 public access compliance rule

aws configservice put-config-rule \ --config-rule '{ "ConfigRuleName": "s3-bucket-public-read-prohibited", "Description": "Checks that S3 buckets do not allow public read access", "Source": { "Owner": "AWS", "SourceIdentifier": "S3\_BUCKET\_PUBLIC\_READ\_PROHIBITED" }, "Scope": { "ComplianceResourceTypes": ["AWS::S3::Bucket"] } }' \ --profile admin-mfa

##### Rule Verification

# Verify rule creation

aws configservice describe-config-rules --config-rule-names s3-bucket-public-read-prohibited --profile admin-mfa

# Check compliance status

aws configservice get-compliance-details-by-config-rule \ --config-rule-name s3-bucket-public-read-prohibited \ --profile admin-mfa

# Check discovered resources

aws configservice get-discovered-resource-counts --profile admin-mfa

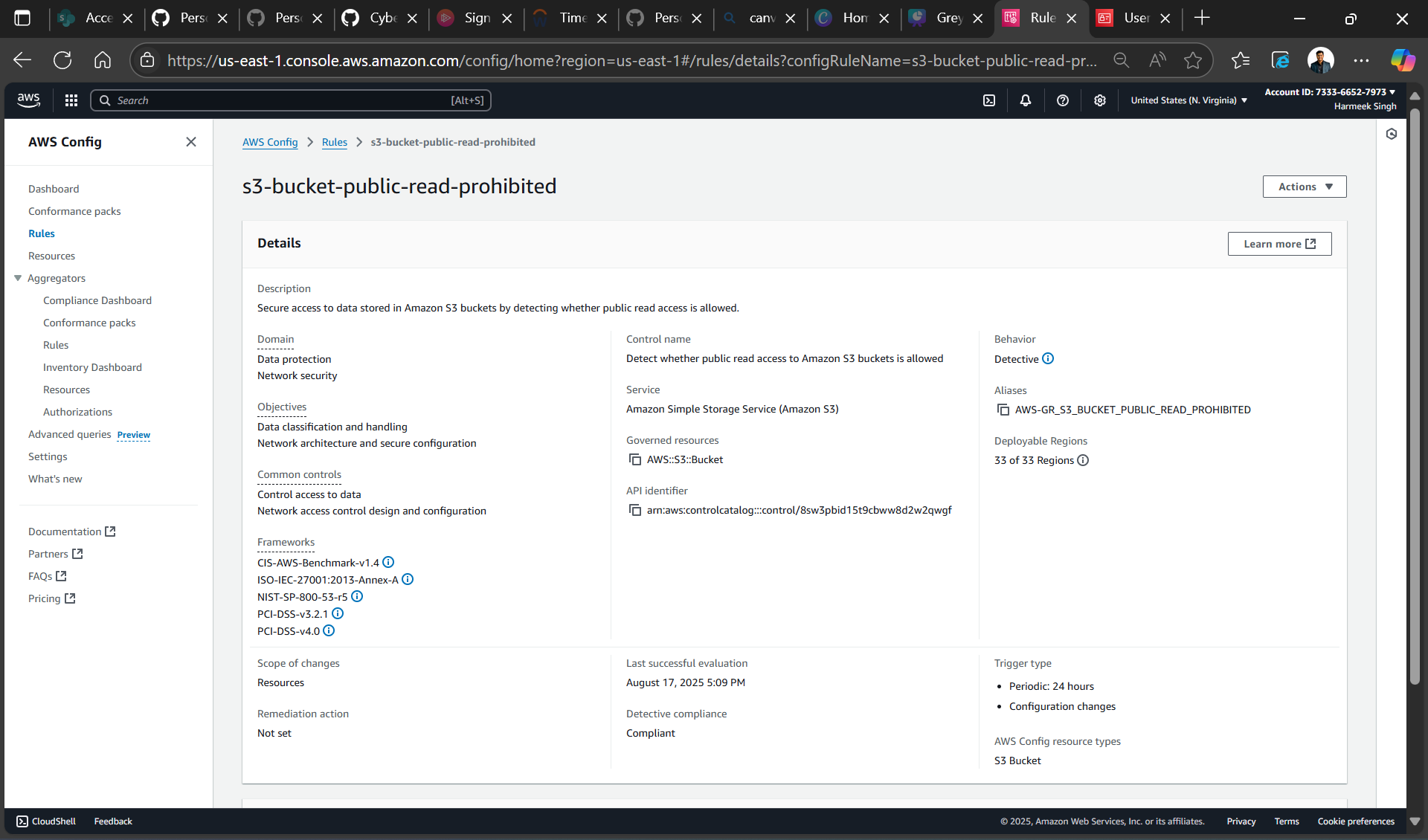


Figure 2.2: AWS managed Config rule for S3 public access compliance with automated evaluation.

Shows compliance automation implementation

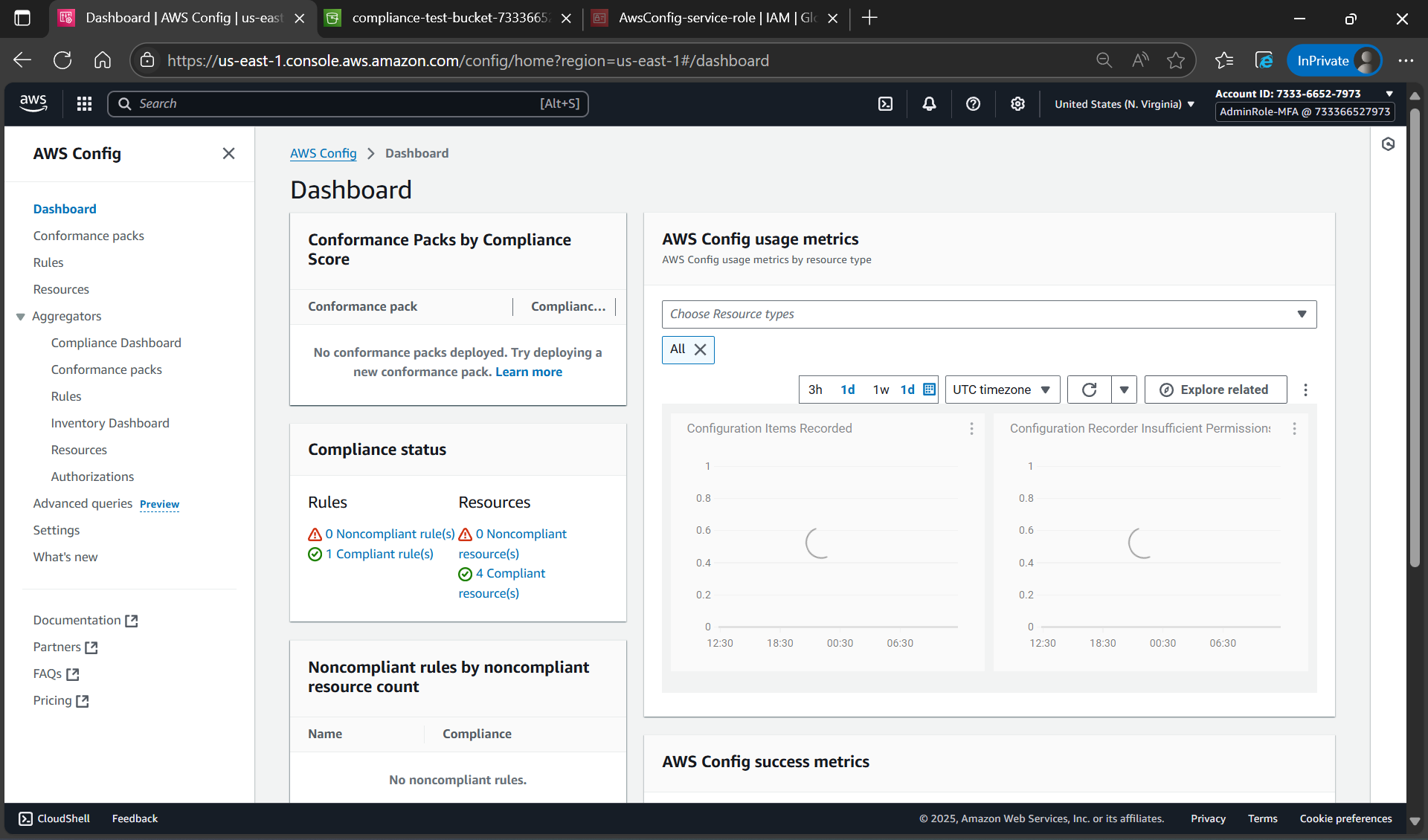


Figure 2.3a: Baseline compliance status showing all S3 buckets meeting security requirements.

Shows initial compliant state.

##### Compliance Testing Workflow

# Create test bucket for compliance testing

aws s3 mb s3://compliance-test-bucket-733366527973 --region us-east-1 --profile admin-mfa

# Remove public access block to allow policy testing

aws s3api delete-public-access-block \ --bucket compliance-test-bucket-733366527973 \ --profile admin-mfa

# Apply public bucket policy (creates compliance violation)

# Policy content saved as violation-bucket-policy.json

{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": "\*", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::compliance-test-bucket-733366527973/\*" } ] }

# Apply the violation policy

aws s3api put-bucket-policy \ --bucket compliance-test-bucket-733366527973 \ --policy file://violation-bucket-policy.json \ --profile admin-mfa

# Force immediate rule evaluation

aws configservice start-config-rules-evaluation \ --config-rule-names s3-bucket-public-read-prohibited \ --profile admin-mfa

# Check for non-compliant resources

aws configservice get-compliance-details-by-config-rule \ --config-rule-name s3-bucket-public-read-prohibited \ --compliance-types NON\_COMPLIANT \ --profile admin-mfa

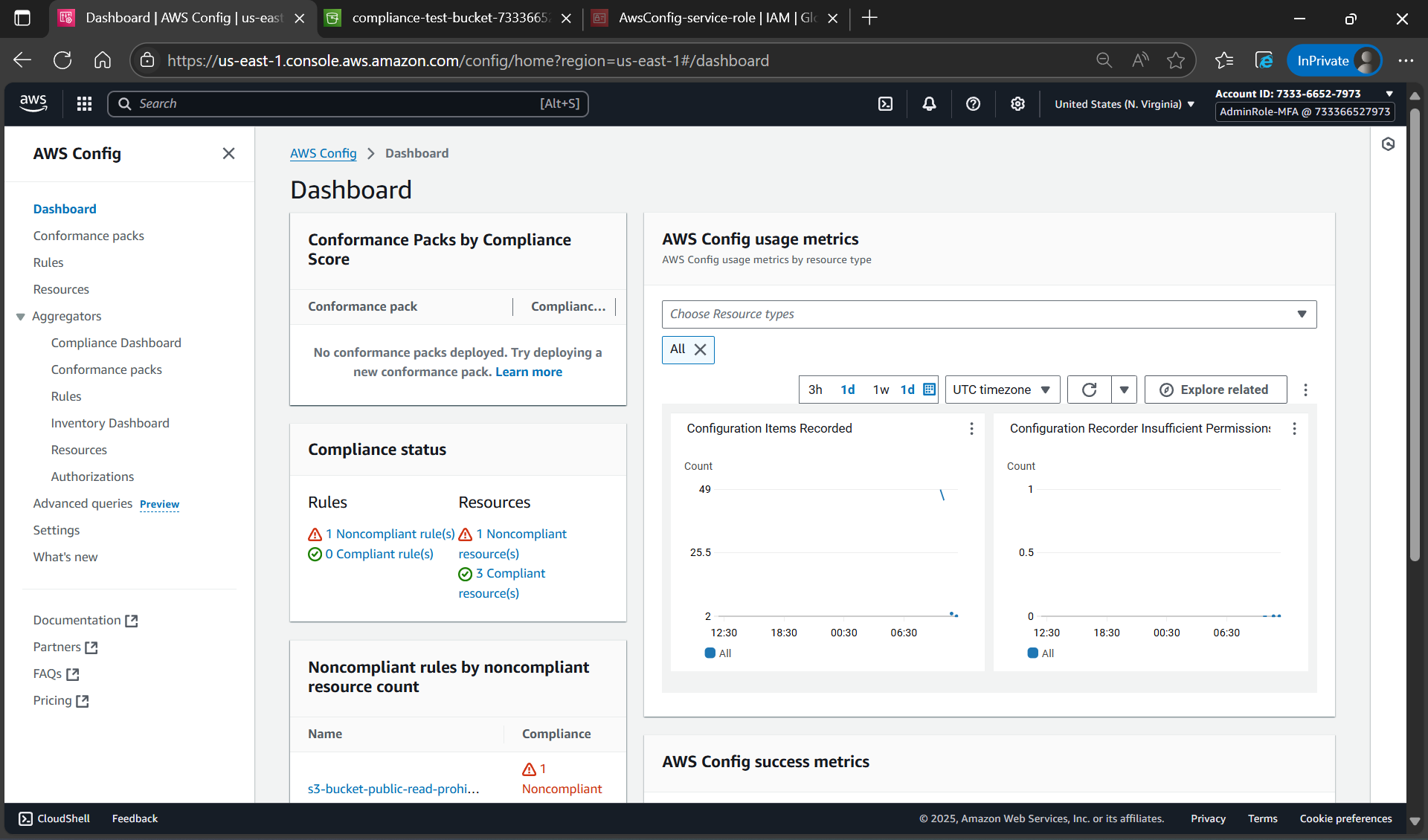


Figure 2.3b: Config rule detecting policy violation in real-time with automated compliance evaluation.

Demonstrates violation detection capability.

##### Remediation and Compliance Restoration

# Remove public bucket policy to restore compliance

aws s3api delete-bucket-policy \ --bucket compliance-test-bucket-733366527973 \ --profile admin-mfa

# Restore public access block protection

aws s3api put-public-access-block \ --bucket compliance-test-bucket-733366527973 \ --public-access-block-configuration "BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true" \ --profile admin-mfa

# Trigger rule re-evaluation after remediation

aws configservice start-config-rules-evaluation \ --config-rule-names s3-bucket-public-read-prohibited \ --profile admin-mfa

# Verify compliance restoration

aws configservice get-compliance-details-by-config-rule \ --config-rule-name s3-bucket-public-read-prohibited \ --profile admin-mfa

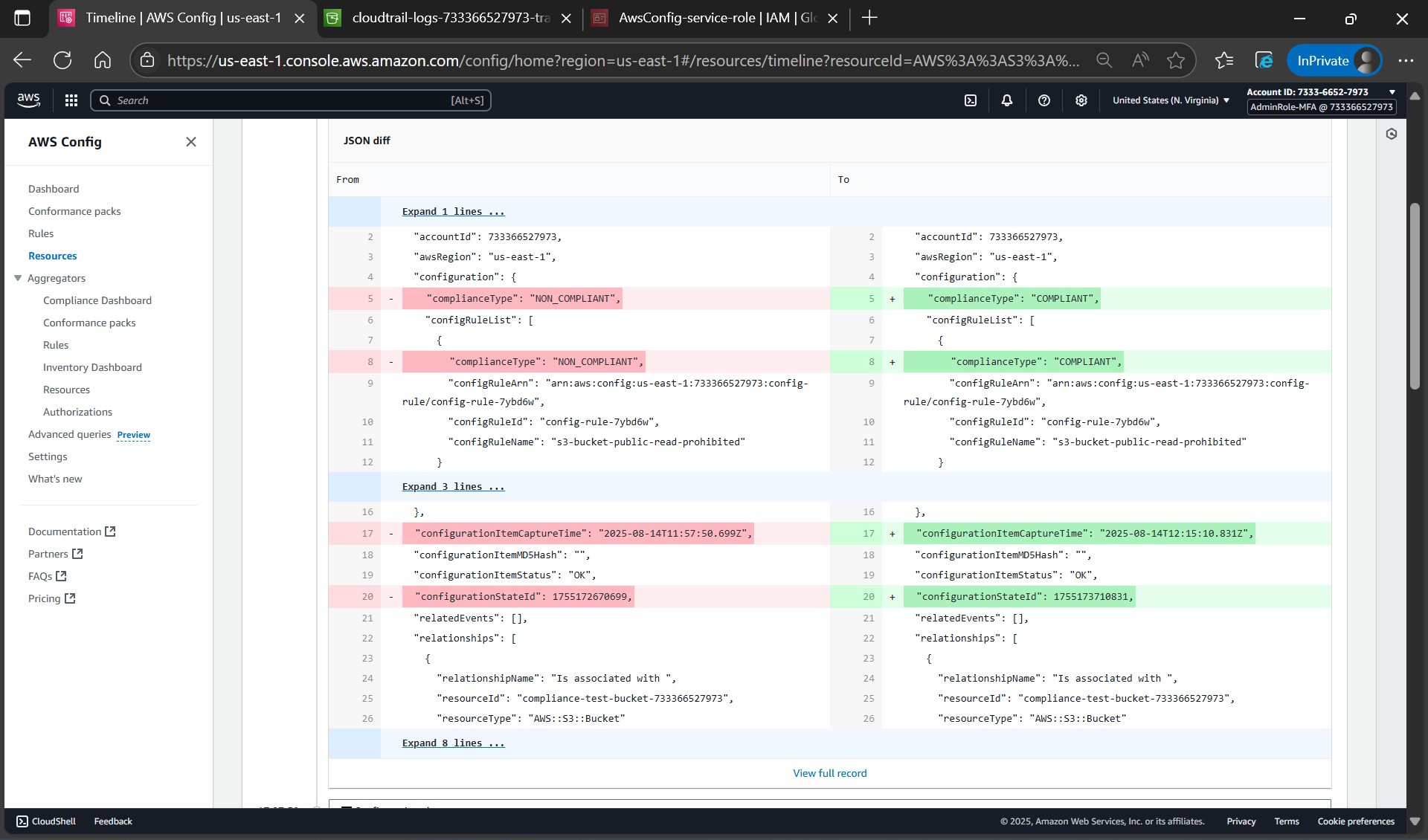


Figure 2.3c: Successful remediation with all resources returned to compliant status

Purpose: Shows remediation validation

##### Testing Results Summary

1. **Created test bucket:** compliance-test-bucket-733366527973
2. **Applied public policy:** Using violation-bucket-policy.json
3. **Detected violation:** Config rule identified NON\_COMPLIANT status
4. **Remediated violation:** Removed public policy
5. **Verified restoration:** All buckets returned to COMPLIANT status

**7**

**CloudTrail Integration Validation**

##### CloudTrail Log Analysis

# Download CloudTrail logs for integration analysis

aws s3 sync s3://cloudtrail-logs-733366527973-training/AWSLogs/733366527973/CloudTrail/us-east-1/2025/08/14/ ./cloudtrail-logs/ --profile admin-mfa

# Search for Config service events in CloudTrail

findstr /S /I "configservice" cloudtrail-logs\\*.json

# Search for Config rule creation events

findstr /S /I "PutConfigRule" cloudtrail-logs\\*.json

# Search for rule evaluation triggers

findstr /S /I "StartConfigRulesEvaluation" cloudtrail-logs\\*.json

# Search for compliance testing events

findstr /S /I "PutBucketPolicy" cloudtrail-logs\\*.json findstr /S /I "DeleteBucketPolicy" cloudtrail-logs\\*.json

# Search for test bucket events

findstr /S /I "compliance-test-bucket" cloudtrail-logs\\*.json

##### Config Data Analysis

# Download Config data for analysis

aws s3 sync s3://config-compliance-data-733366527973/AWSLogs/733366527973/Config/us-east-1/ ./config-data/ --profile admin-mfa

# Search for S3 bucket configuration items

findstr /S /I "AWS::S3::Bucket" config-data\\*.json

# Search for specific bucket configurations

findstr /S /I "compliance-test-bucket-733366527973" config-data\\*.json

**Integration Evidence Discovered:**

* **Config Rule Creation:** PutConfigRule events at 11:17:45Z
* **Service Operations:** Config service role assumptions
* **Compliance Evaluations:** PutEvaluations with rule results
* **Bucket Policy Testing:** Complete violation/remediation workflow
* **Configuration Data:** 1,411-byte S3 bucket ConfigHistory file

## Integration Analysis

### Critical Integration: How Config Builds on CloudTrail

Since you have CloudTrail active from Day 1, Config leverages this foundation:

**CloudTrail Provides**

* **WHO:** Which user/role made the change
* **WHEN:** Exact timestamp of the API call
* **WHAT API:** Which specific AWS API was invoked
* **SOURCE:** IP address, user agent, request parameters

**Config Adds**

* **BEFORE STATE:** What the resource looked like before the change
* **AFTER STATE:** What the resource looks like after the change
* **RELATIONSHIPS:** How this resource connects to other resources
* **COMPLIANCE:** Whether the new state violates any rules

**Combined Power**

**Complete audit story = Actor + Action + Timeline + Configuration Impact + Compliance Status**

### Your Actual Integration Evidence

From your CloudTrail analysis, we found:

* **11:17:45Z:** You created the S3 compliance rule
* **11:55:01Z:** Applied public bucket policy (violation creation)
* **12:14:16Z:** Removed bucket policy (remediation)
* **12:16:43Z:** Config evaluated compliance status
* **Complete Timeline:** Every action logged with full context

## Enterprise Applications

### Compliance Framework Mapping

**SOX (Sarbanes-Oxley) Compliance**

**Requirement:** Section 404 - Internal Controls Over Financial Reporting

**Config Value:**

* Automated monitoring of IT general controls
* Continuous assessment of system configurations
* Historical evidence of control effectiveness

**PCI DSS (Payment Card Industry)**

**Requirement:** 11.5 - Deploy file-integrity monitoring or change-detection software

**Config Value:**

* Real-time configuration change detection
* Compliance with security configuration standards
* Automated validation of security controls

**HIPAA (Health Insurance Portability)**

**Requirement:** Administrative Safeguards - Security Management Process

**Config Value:**

* Continuous monitoring of security configurations
* Automated compliance assessment
* Audit trail of configuration changes

### Real-World Use Cases

#### Use Case 1: Financial Services Client

**Challenge**

SOX compliance requires quarterly attestation of IT controls

**Config Solution**

Automated compliance monitoring reduces manual audit effort from weeks to hours

**Business Value**

$500K annual audit cost reduction, faster compliance certification

#### Use Case 2: Healthcare Organization

**Challenge**

HIPAA requires continuous security monitoring of patient data systems

**Config Solution**

Real-time alerting on security configuration changes

**Business Value**

Immediate incident response, regulatory compliance assurance

#### Use Case 3: Multi-Account Enterprise

**Challenge**

Consistent security policies across 50+ AWS accounts

**Config Solution**

Centralized compliance monitoring with AWS Organizations integration

**Business Value**

Unified security posture, reduced compliance overhead

## Troubleshooting & Lessons Learned

### Major Issues Encountered and Resolved

**Issue 1: File Path and JSON Management**

**Problems Faced:**

* no such file or directory: config-trust-policy.json
* Multiple malformed put-config-rule attempts
* JSON policy formatting errors

**Solutions Learned:**

* Create JSON files in working directory before CLI commands
* Validate JSON syntax before applying policies
* Use file-based approach for complex configurations

**Issue 2: S3 Bucket Security Restrictions**

**Problem:** The Bucket does not allow ACLs

**Root Cause:** Modern S3 buckets have enhanced security defaults

**Solution:** Use bucket policies instead of ACLs for compliance testing

**Implementation:** Created violation-bucket-policy.json for testing

**Issue 3: Windows File Path Limitations**

**Problem:** Config data downloads failing due to long paths

**Error:** [Errno 22] Invalid argument

**Solution:** Use S3 API list-objects-v2 for metadata analysis

**Alternative:** Analyze file existence and sizes without downloading

**Issue 4: AWS Policy Case Sensitivity**

**Problem:** BlockPublicACLs vs BlockPublicAcls parameter validation failure

**Solution:** Exact parameter names required in AWS CLI

**Learning:** Always reference AWS documentation for precise syntax

### Best Practices Developed

* **File Organization:** Keep policy files organized and verify existence
* **Security Testing:** Use bucket policies rather than ACLs for testing
* **Verification Steps:** Verify each phase before proceeding
* **Error Handling:** Use specific commands to validate configurations
* **Alternative Methods:** Have backup approaches for Windows limitations
* **JSON Validation:** Always validate JSON before applying
* **Sequential Implementation:** Follow phase-by-phase for clarity

## Day Review Summary

### Technical Achievements

#### Infrastructure Implemented

* **Complete AWS Config Service:** All components configured and operational
* **Enterprise Security:** MFA-enforced access with role-based permissions
* **Automated Compliance:** Real-time rule evaluation and violation detection
* **Audit Integration:** CloudTrail + Config complete audit trail
* **Data Protection:** Encrypted S3 storage with service-only access

### Readiness for Day 3

**Foundation Established**

* CloudTrail capturing all AWS API activity
* Config monitoring all resource configurations
* Compliance rules actively evaluating security policies
* Complete audit trail for security investigations

### Final Reflection

**Day 2 Transformation Achievement**

The AWS environment underwent a complete transformation from basic audit logging (CloudTrail) to comprehensive compliance monitoring (Config). The implementation established:

1. **Complete Configuration Visibility:** Every AWS resource monitored continuously with real-time change detection
2. **Automated Compliance:** Rules evaluating security policies in real-time with immediate violation detection
3. **Complete Audit Capability:** Combined CloudTrail + Config forensic analysis providing WHO, WHAT, WHEN, and COMPLIANCE STATUS
4. **Enterprise Foundation:** Production-ready infrastructure for Security Hub centralization and GuardDuty threat detection

### Knowledge Transfer and Documentation

#### Implementation Deliverables

* Complete CLI command reference with tested commands
* Compliance framework mapping for SOX, PCI DSS, and HIPAA
* Integration validation methodology for audit trail verification
* Error resolution procedures for common AWS CLI challenges

**Continuous Improvement Insights**

* **File Management:** Organized policy file structure prevents CLI execution errors
* **Security Testing:** Bucket policy-based testing more reliable than ACL-based approaches
* **Verification Workflows:** Phase-by-phase validation ensures implementation integrity
* **Alternative Approaches:** Multiple methods for data analysis accommodate platform limitations

**AWS Config - Complete Theory & Implementation Guide**

Cyber & Risk Consulting Training | Day 2 |