Cloud Security Automation: Fixing Noncompliant Resources with AWS Config & SSM

# Introduction

## What is AWS Config?

AWS Config is a service that provides continuous monitoring and recording of AWS resource configurations. It helps track changes, ensure compliance with policies, and troubleshoot misconfigurations. AWS Config evaluates resources against predefined rules and flags them as **compliant** or **noncompliant** based on their configuration.

**How AWS Config Helps in Security & Compliance**

AWS Config enables organizations to:

* **Monitor Resource Changes:** Track historical and real-time configuration changes.
* **Audit & Ensure Compliance:** Evaluate resources using AWS Config Rules.
* **Troubleshoot & Analyze Security Issues:** Detect security misconfigurations and analyze IAM permissions, security groups, and networking rules.

## Focus of This Documentation

This documentation specifically covers **AWS Config’s remediation feature**, which allows the automatic correction of non-compliant resources using **AWS Systems Manager (SSM) Automation Documents (Runbooks)**. Instead of manual remediation, AWS Config can trigger predefined automation workflows to **fix security misconfigurations, update resource settings, and enforce best practices.**

## What is AWS Systems Manager (SSM)?

AWS Systems Manager (SSM) is a service that helps automate operational tasks across AWS infrastructure. One of its key components is **SSM Automation**, which allows predefined workflows (runbooks) to execute remediation actions when triggered by AWS Config.

By integrating AWS Config with SSM, organizations can **automate compliance enforcement**, reducing manual intervention and ensuring AWS resources remain in a secure and compliant state.

# Remediating Noncompliant Resources with AWS Config

AWS Config allows us to automatically remediate noncompliant resources that AWS Config Rules evaluate. Remediation is applied using AWS Systems Manager (SSM) Automation Documents, which define the corrective actions to be performed on noncompliant AWS resources. We can associate these automation documents with AWS Config rules through the AWS Management Console or APIs.

AWS Config provides a set of **managed automation documents** with predefined remediation actions. Additionally, we can create and associate **custom automation documents** to enforce organization-specific compliance policies.

We can setup **Manual Remediation** or **Automated remediation**, but I’m focusing here on setting up AWS config Automated Remediation with SSM.

## AWS Config Automated Remediation with SSM

AWS Config Automated Remediation with SSM (AWS Systems Manager) enables organizations to automatically fix non-compliant AWS resources when they violate compliance rules. This integration between AWS Config and SSM Automation Documents (runbooks) ensures configuration consistency and security.

### How It Works

**1. AWS Config Monitors Compliance**

AWS Config continuously checks AWS resources against predefined compliance rules (e.g., enforcing IMDSv2 on EC2 instances).

**2. Non-Compliant Resources are Identified**

If a resource does not meet the rule requirements, AWS Config marks it as **Noncompliant**.

**3. AWS Config Triggers a Remediation Action**

When a resource is noncompliant, AWS Config executes an **SSM Automation Document (SSM Runbook)** to remediate the issue.

**4. AWS Systems Manager Fixes the Issue**

The automation runbook performs predefined corrective actions, such as:

* Modifying security groups
* Enforcing encryption
* Updating EC2 instance metadata settings

**5. Verification and Compliance Update**

Once the remediation action is successful, AWS Config re-evaluates the resource and updates its compliance status to **Compliant**.

**Example Use Case: Enforcing IMDSv2 on EC2 Instances**

1. AWS Config detects EC2 instances using IMDSv1.
2. AWS Config triggers an SSM automation runbook (AWSConfigRemediation-EnforceEC2InstanceIMDSv2).
3. SSM modifies the EC2 instance metadata settings to enforce IMDSv2.
4. AWS Config rechecks the instance and updates the compliance status.

### Setting Up Auto Remediation for AWS Config with SSM

**Step 1: Activating AWS Config**

When activating AWS Config, you have two options:

* **Get Started**
* **1-Click Setup**

I’m selecting **Get Started** option for a more detailed setup.

**Step 2: Configuring General and Delivery Method Settings**

**General Settings:**

* **Recording strategy:**
  + Record all current and future resource types supported in this region
  + Record all current and future resource types with exclusions
  + Record specific resource types (Selected for this setup)

A screenshot of a computer

AI-generated content may be incorrect.

* **AWS Config Service Role:**
  + Create AWS Config service-linked role (Recommended if no existing role is available)

A screenshot of a computer

AI-generated content may be incorrect.

**Delivery Method:**

* **S3 Bucket for Log Storage:**
  + Create a new bucket or select an existing one (New bucket created for this setup)

A screenshot of a computer

AI-generated content may be incorrect.

**Step 3: Selecting AWS Config Rules**

* We selected **ec2-imdsv2-check** to enforce IMDSv2.

*A screenshot of a computer

AI-generated content may be incorrect.*

**Reviewing and Confirming Configuration**

* Verify the selected resource types and rules.
* Click **Confirm** to complete setup.

**AWS Config Dashboard Overview**

* Displays compliance status, conformance packs, resource inventory, and usage metrics.

*A screenshot of a computer

AI-generated content may be incorrect.*

### Configuring Remediation

**Step 1: Accessing Remediation Actions**

* Navigate to **Rules** and select **ec2-imdsv2-check**.
* Click on **Actions → Manage remediation**.

A screenshot of a computer

AI-generated content may be incorrect.

**Step 2: Setting Remediation Parameters**

* **Automatic Remediation** selected.
* **Retries:** Default values (5 retries, 60 seconds interval).
* **Remediation Action:** AWSConfigRemediation-EnforceEC2InstanceIMDSv2

A screenshot of a computer

AI-generated content may be incorrect.

**Step 3: Creating an IAM Role for Remediation**

* Navigate to **IAM → Roles → Create Role**.
* Select **AWS Service → Systems Manager**.

A screenshot of a computer

AI-generated content may be incorrect.

* Create a new policy with required permissions:

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

* Assign the policy to the role and copy the ARN.  
  “arn:aws:iam::337909744329:role/SSMRemediationEC2inst”
* Paste the ARN in AWS Config's remediation settings.

A screenshot of a computer

AI-generated content may be incorrect.

### Launching a Non-Compliant EC2 Instance

**Step 1: Launch EC2 Instance**

* Open **EC2 Console → Launch Instance**.
* Select **Amazon Linux AMI**.

A screenshot of a computer

AI-generated content may be incorrect.

* Under **Advanced Details**, set **Metadata version** to V1 and V2 (token optional).

A screenshot of a computer

AI-generated content may be incorrect.

**Step 2: Checking Noncompliance**

* Refresh the **AWS Config Dashboard**.

A screenshot of a computer

AI-generated content may be incorrect.

* The instance appears as **Noncompliant**.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Step 3: Verifying Automated Remediation**

* Refresh the dashboard after a few minutes.
* Instance metadata version is updated to **IMDSv2 Required**.

A screenshot of a computer

AI-generated content may be incorrect.

* AWS Config will eventually mark the instance as **Compliant**.

*A screenshot of a computer

AI-generated content may be incorrect.*

# Key Benefits

* **Automated Compliance:** Reduces manual intervention in enforcing security best practices.
* **Consistency:** Ensures resources maintain compliance across AWS accounts.
* **Security Enhancement:** Automatically fixes security misconfigurations.

# Possible Enhancements & Future Improvements

While this project demonstrates a basic automated remediation setup using AWS Config and SSM, there are several ways to enhance and expand its capabilities:

**1. Multi-Account & Multi-Region Remediation**

* Extend remediation across multiple AWS accounts using **AWS Organizations and AWS Config Aggregators**.
* Implement cross-region AWS Config rules for centralized compliance enforcement.

**2. Custom Remediation Runbooks**

* Instead of using AWS-managed remediation actions, create **custom SSM Automation runbooks** tailored to organizational security policies.
* Example: A custom runbook that automatically reverts unauthorized security group changes.

**3. Security Event Logging & Monitoring**

* Integrate with **AWS Security Hub and AWS CloudTrail** to track remediation actions and security events.
* Send alerts using **Amazon SNS** whenever remediation is triggered.

**4. Remediation for Additional AWS Services**

* Expand automated remediation to other AWS resources such as **IAM policies, S3 bucket permissions, and RDS encryption settings**.

**5. Terraform Automation for Setup**

* Use **Terraform** to automate the provisioning of AWS Config, remediation rules, and IAM roles.
* Example: Terraform script to deploy AWS Config with predefined compliance rules and auto-remediation.

**6. Compliance Reporting & Dashboards**

* Create real-time compliance reports using **Amazon QuickSight** or AWS Lambda to generate compliance summaries.
* Automate monthly compliance audits and send reports via email.

# Cleanup Steps

* Delete AWS Config resources.
* Remove IAM role and policy.
* Terminate the test EC2 instance to avoid charges.

# Conclusion

In conclusion, leveraging AWS Config in combination with AWS Systems Manager (SSM) offers a powerful approach to automating compliance enforcement and security remediation across AWS resources. By continuously monitoring resource configurations and automatically applying remediation actions through predefined runbooks, organizations can ensure that their cloud infrastructure remains secure and compliant with minimal manual intervention. The integration of AWS Config and SSM not only simplifies the management of security misconfigurations but also enhances the overall efficiency and consistency of compliance efforts. This setup, as demonstrated, can effectively automate the correction of noncompliant resources, ensuring a secure and compliant environment within AWS.

# References:

Amazon Web Services, 2025. *AWS Config Documentation*. [online] Available at: <https://docs.aws.amazon.com/config/> [Accessed 17 February 2025].

Amazon Web Services, 2025. *AWS Config: AWS Config Aggregator*. [online] Available at: <https://docs.aws.amazon.com/config/latest/developerguide/config-concepts.html#config-aggregator> [Accessed 17 February 2025].

Amazon Web Services, 2025. *Setting Up AWS Config Automated Remediation*. [online] Available at: <https://docs.aws.amazon.com/config/latest/developerguide/setup-autoremediation.html> [Accessed 17 February 2025].

Amazon Web Services, 2025. *What is AWS Config?*. [online] Available at: <https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html> [Accessed 17 February 2025].

Amazon Web Services, 2025. *AWS Security Hub Overview*. [online] Available at: <https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html> [Accessed 17 February 2025].

Amazon Web Services, 2025. *AWS Systems Manager Automation*. [online] Available at: <https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-automation.html> [Accessed 17 February 2025].

Amazon Web Services, 2025. *AWS Systems Manager Automation Runbooks*. [online] Available at: <https://docs.aws.amazon.com/systems-manager-automation-runbooks/latest/userguide/automation-ref-sys.html> [Accessed 17 February 2025].

Cybr, 2025. *Introduction to AWS Security: Demo - AWS Config Automated Remediation with SSM*. [online] Available at: <https://cybr.com/courses/introduction-to-aws-security/lessons/demo-aws-config-automated-remediation-with-ssm/> [Accessed 17 February 2025].