AWS Config: Track, Assess & Maintain Compliance in AWS!

Overview

AWS **Config** is a fully managed service that enables **continuous monitoring, assessment, and compliance management** of AWS resources. It records and evaluates changes to your AWS environment, helping you **detect misconfigurations, troubleshoot operational issues, and maintain security best practices.**

With AWS Config, you can:

- **Track Configuration Changes** – Capture historical and real-time changes to AWS resources.
- **Ensure Compliance** – Enforce policies using pre-defined and custom compliance rules.
- **Audit and Troubleshoot** – Identify unauthorized changes and analyze issues efficiently.
- **Automate Remediation** – Integrate with AWS Systems Manager and Lambda to enforce corrective actions.

By leveraging AWS Config, organizations can strengthen **security posture, regulatory compliance, and operational governance** in their cloud environments.

Step 1: Setup AWS Config

Select Recording Method

Choose a **Recording Strategy**:

- **All resource types with customizable overrides**
- **Specific resource types**

Data Governance

- Assign an **IAM role for AWS Config** to grant permissions.

Delivery Method

- Choose an **Amazon S3 bucket** to store configuration history and snapshots.

Click **Next** to proceed.

Step 2: Configure Rules

AWS **Managed Rules** help enforce compliance and best practices.

Example Rule for EC2:

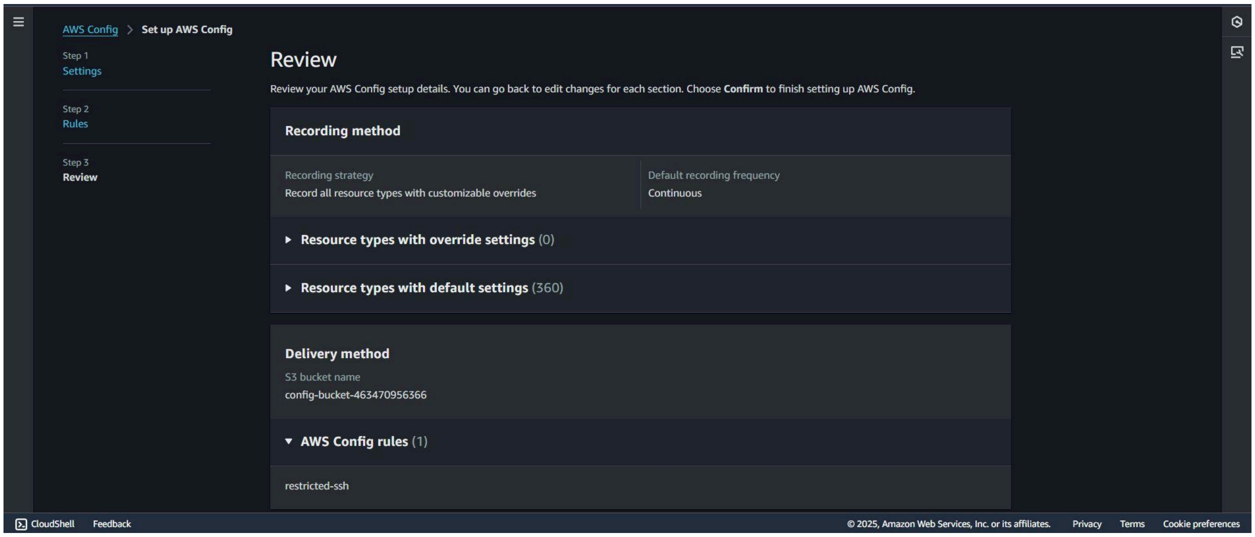
- **Name:** `restricted-ssh`
- **Label:** EC2
- **Supported Evaluation Mode:** Detective
- **Description:** Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.

You can add multiple rules in a single setup.

Click **Next** to proceed.

Step 3: Review & Confirm

Once setup is complete



Review

Review your AWS Config setup details. You can go back to edit changes for each section. Choose **Confirm** to finish setting up AWS Config.

Recording method

Recording strategy
Record all resource types with customizable overrides

Default recording frequency
Continuous

▸ **Resource types with override settings** (0)

▸ **Resource types with default settings** (360)

Delivery method

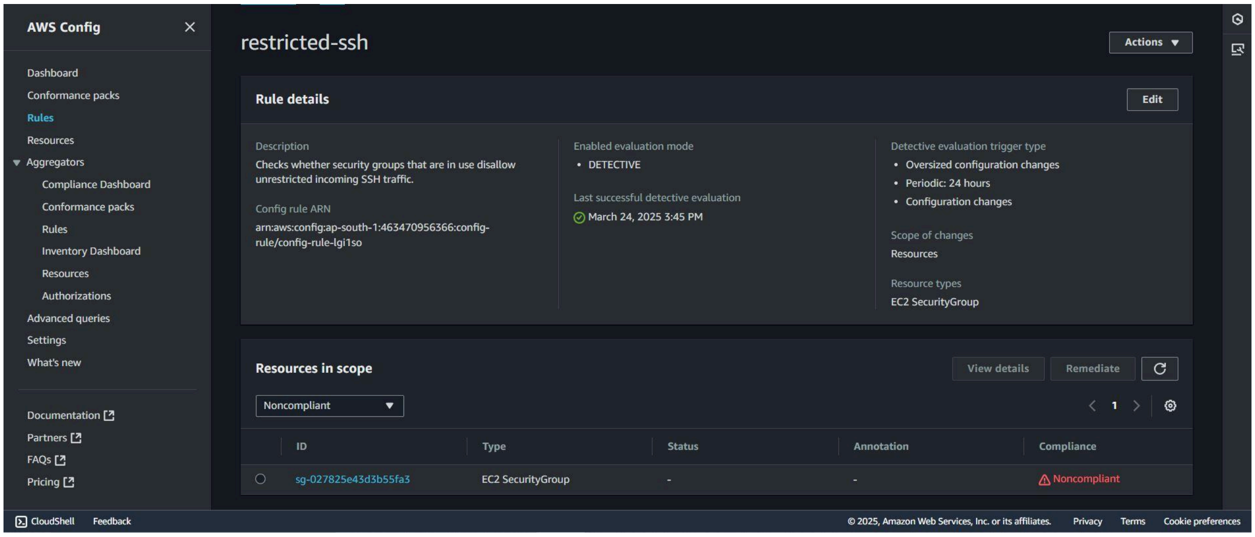
S3 bucket name
config-bucket-463470956366

▾ **AWS Config rules** (1)

restricted-ssh

Once setup is complete you can the resources that are compliant or not on “Dashboard” or at “Rules ” page :

1. Navigate to the **Rules** tab in AWS Config.
2. View the **Security Groups** that are **Non-Compliant** with the `restricted-ssh` rule under the **Resources in Scope** table.



restricted-ssh

Rule details

Description
Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.

Config rule ARN
arn:aws:config:ap-south-1:463470956366:config-rule/config-rule-lgi1so

Enabled evaluation mode
- DETECTIVE

Last successful detective evaluation
✓ March 24, 2025 3:45 PM

Detective evaluation trigger type
- Oversized configuration changes
- Periodic: 24 hours
- Configuration changes

Scope of changes
Resources

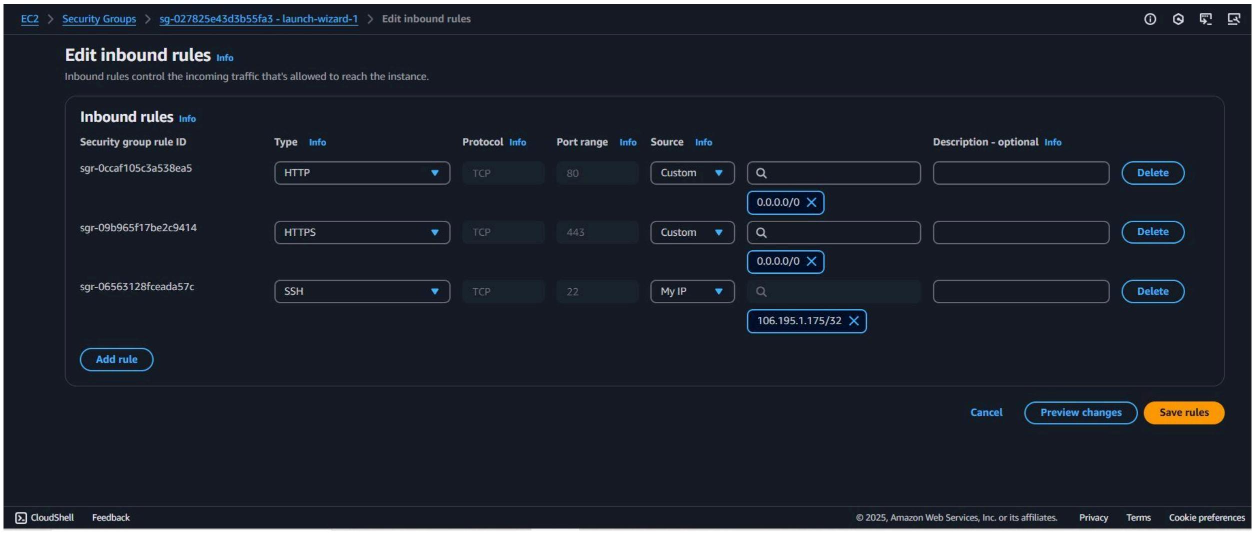
Resource types
EC2 SecurityGroup

Resources in scope

	ID	Type	Status	Annotation	Compliance
○	sg-027825e43d3b55fa3	EC2 SecurityGroup	-	-	⚠ Noncompliant

Step 4: Take Necessary Actions

1. Click on the **non-compliant resource**.
2. Select **Manage Resource** to take corrective actions.
3. Modify the **Security Group** settings:
    - Set the **Source** to **Your IP** by selecting "My IP" in the **Source** field for Type **-** SSH.
4. Save the resource.



EC2 > Security Groups > sg-027825e43d3b55fa3 - launch-wizard-1 > Edit inbound rules

Edit inbound rules Info

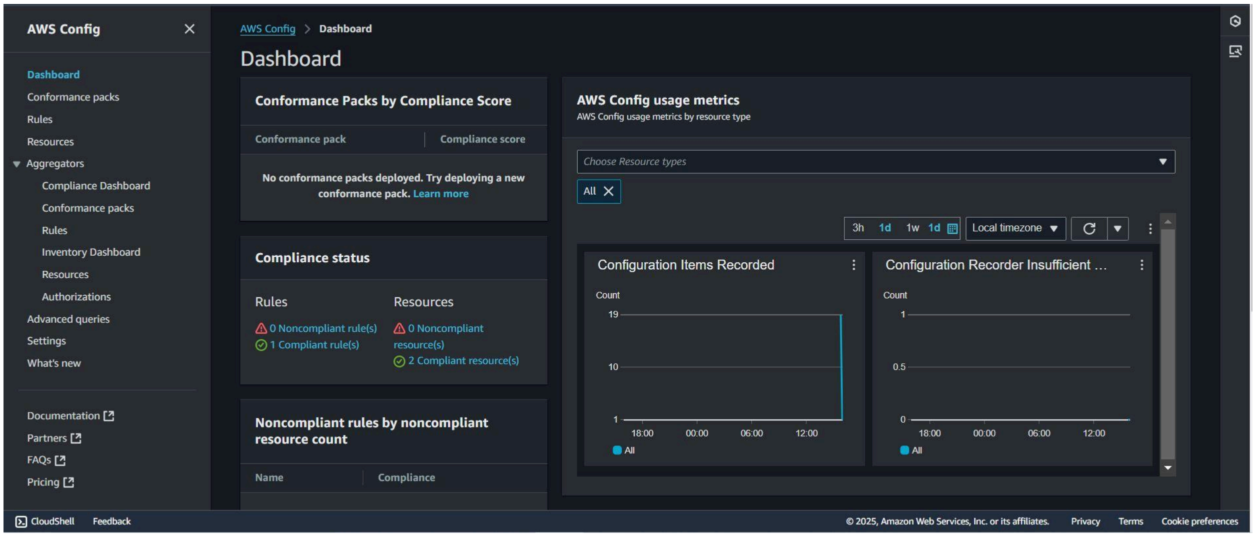
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info
sgr-0ccaf105c3a538ea5	HTTP	TCP	80	Custom	0.0.0.0/0	
sgr-09b965f17be2c9414	HTTPS	TCP	443	Custom	0.0.0.0/0	
sgr-06563128fceada57c	SSH	TCP	22	My IP	106.195.1.175/32	

Verification

- Check the **AWS Config Dashboard** to confirm that the resource is now **compliant**.



AWS Config > Dashboard

Dashboard

Conformance Packs by Compliance Score

Conformance pack	Compliance score

No conformance packs deployed. Try deploying a new conformance pack. Learn more

Compliance status

Rules	Resources
⚠ 0 Noncompliant rule(s) ✓ 1 Compliant rule(s)	⚠ 0 Noncompliant resource(s) ✓ 2 Compliant resource(s)

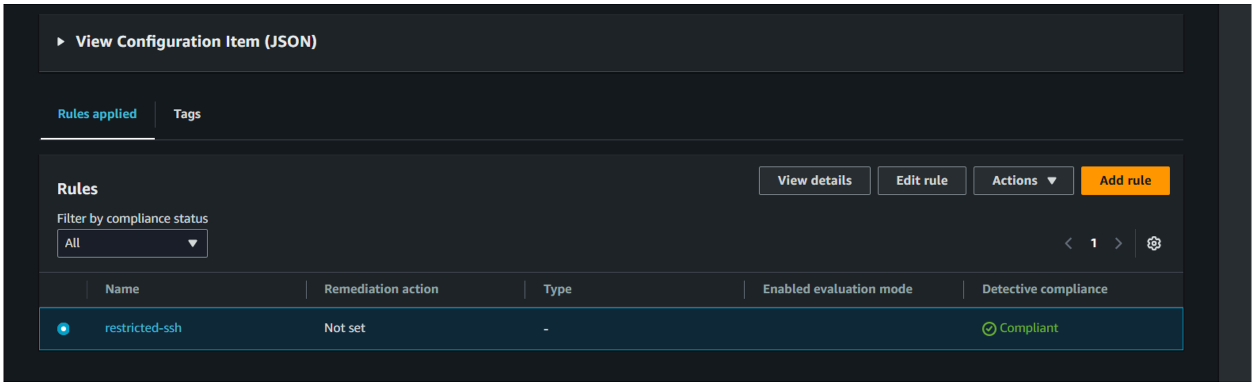
Noncompliant rules by noncompliant resource count

Name	Compliance

AWS Config usage metrics

AWS Config usage metrics by resource type

Choose Resource types: All



Rules

	Name	Remediation action	Type	Enabled evaluation mode	Detective compliance
●	restricted-ssh	Not set	-		✓ Compliant

Additional compliance rules can be added later as needed by clicking “Add Rule”.

Benefits of AWS Config

✅ **Continuous Monitoring** – Tracks changes to AWS resources in real time.
✅ **Continuous Assessment** – Ensures compliance with security policies.
✅ **Change Management** – Logs and audits modifications to AWS resources.
✅ **Operational Troubleshooting** – Identifies misconfigurations and remediates issues quickly.

AWS Config is a must-have for ensuring security, compliance, and operational excellence in AWS! Have you implemented AWS Config in your environment? Let’s discuss! 🚀

#AWS #AWSConfig #CloudSecurity #Compliance #Monitoring #DevOps #CloudEngineering #Security