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:

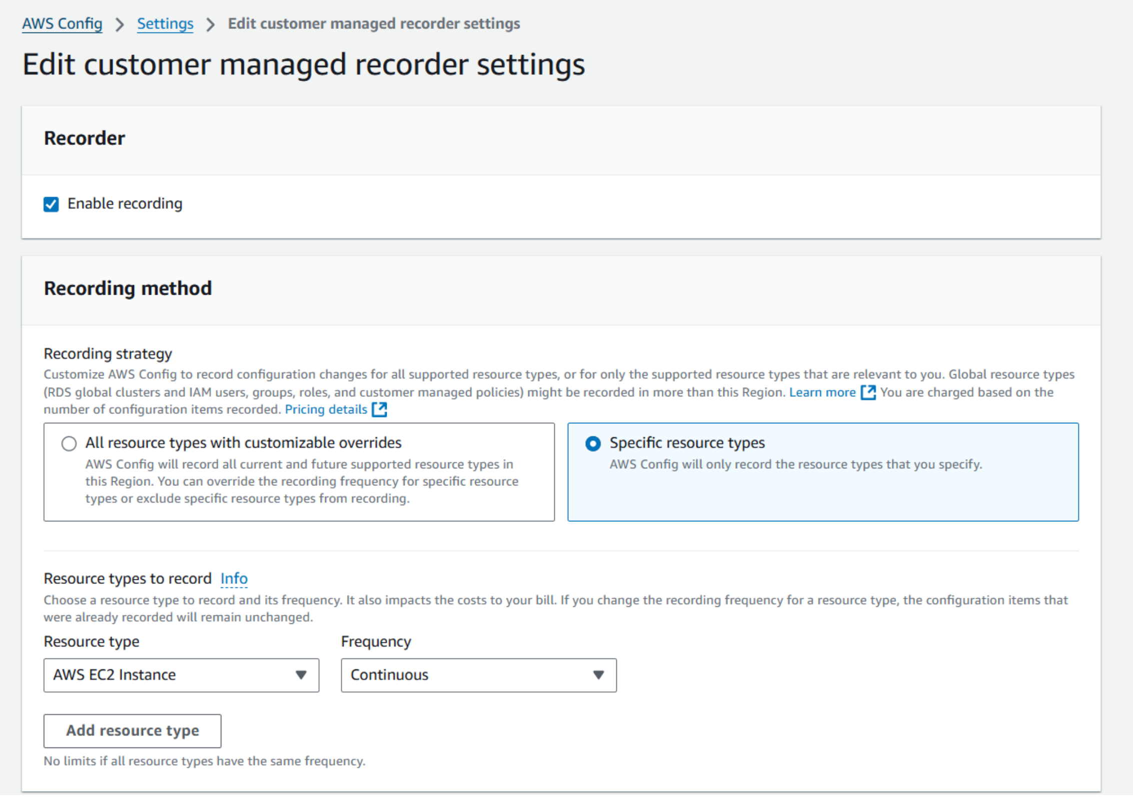
- **Get Started**
- **1-Click Setup**

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)



AWS Config > Settings > Edit customer managed recorder settings

Edit customer managed recorder settings

Recorder

☑ Enable recording

Recording method

Recording strategy

Customize AWS Config to record configuration changes for all supported resource types, or for only the supported resource types that are relevant to you. Global resource types (RDS global clusters and IAM users, groups, roles, and customer managed policies) might be recorded in more than this Region. Learn more You are charged based on the number of configuration items recorded. Pricing details

○ All resource types with customizable overrides
AWS Config will record all current and future supported resource types in this Region. You can override the recording frequency for specific resource types or exclude specific resource types from recording.

● Specific resource types
AWS Config will only record the resource types that you specify.

Resource types to record Info

Choose a resource type to record and its frequency. It also impacts the costs to your bill. If you change the recording frequency for a resource type, the configuration items that were already recorded will remain unchanged.

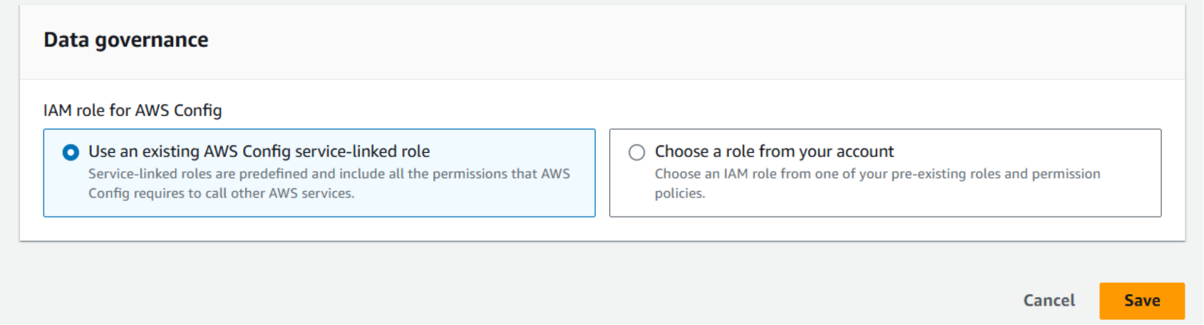
Resource type: AWS EC2 Instance

Frequency: Continuous

Add resource type

No limits if all resource types have the same frequency.

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



Data governance

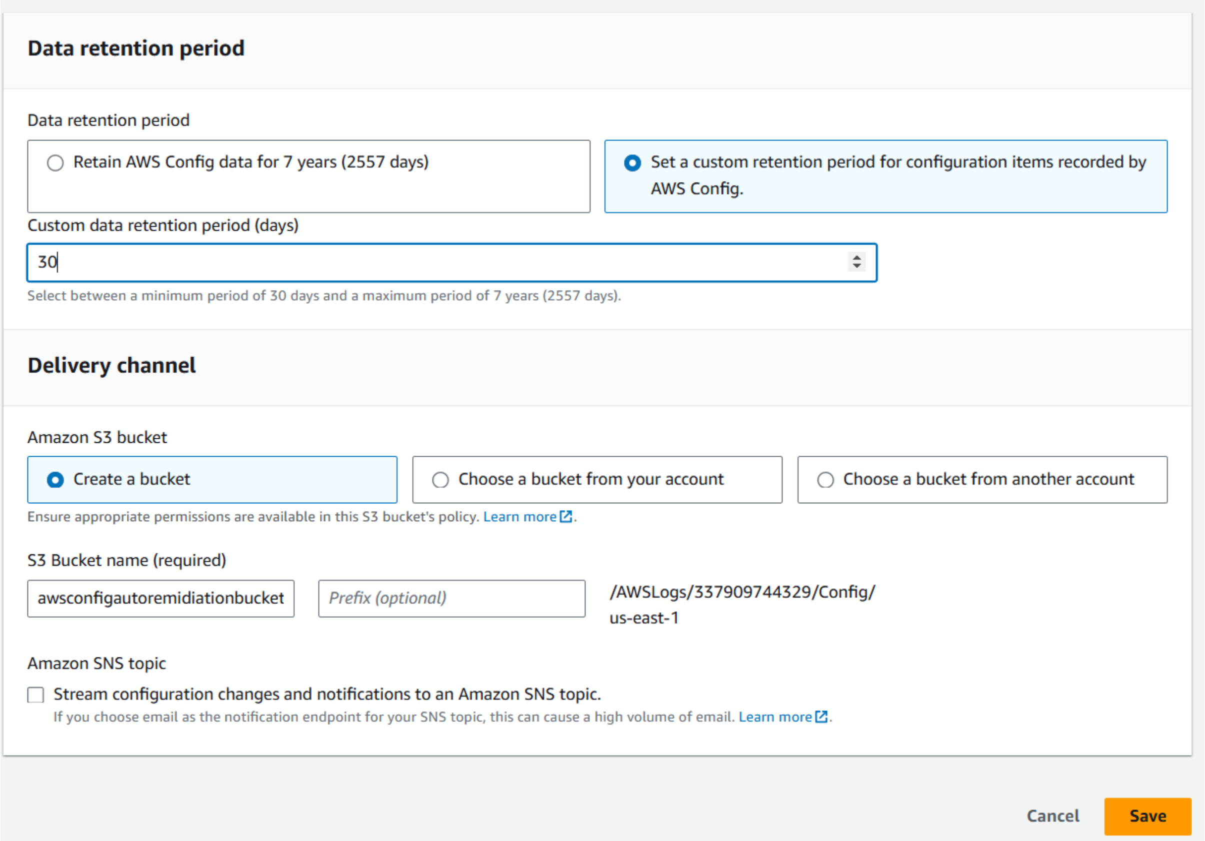
IAM role for AWS Config

● Use an existing AWS Config service-linked role
Service-linked roles are predefined and include all the permissions that AWS Config requires to call other AWS services.

○ Choose a role from your account
Choose an IAM role from one of your pre-existing roles and permission policies.

Delivery Method:

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



Data retention period

Data retention period

○ Retain AWS Config data for 7 years (2557 days)

● Set a custom retention period for configuration items recorded by AWS Config.

Custom data retention period (days)

30

Select between a minimum period of 30 days and a maximum period of 7 years (2557 days).

Delivery channel

Amazon S3 bucket

● Create a bucket ○ Choose a bucket from your account ○ Choose a bucket from another account

Ensure appropriate permissions are available in this S3 bucket's policy. Learn more

S3 Bucket name (required)

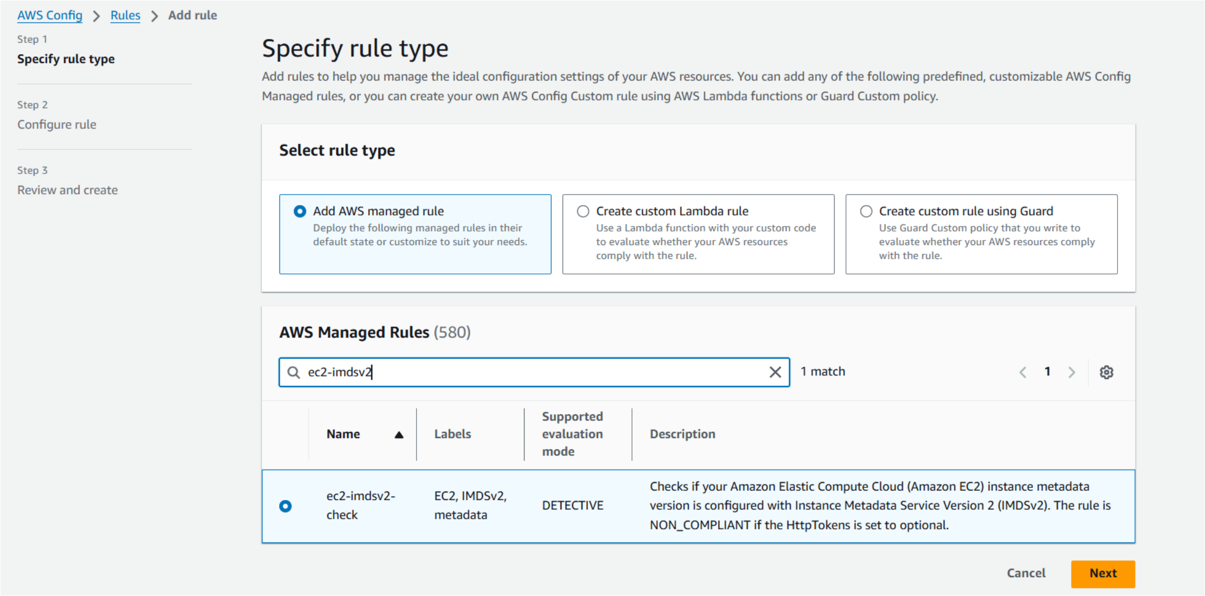
awsconfigautoremidiationbucket | Prefix (optional) | /AWSLogs/337909744329/Config/us-east-1

Amazon SNS topic

□ Stream configuration changes and notifications to an Amazon SNS topic.
If you choose email as the notification endpoint for your SNS topic, this can cause a high volume of email. Learn more

Step 3: Selecting AWS Config Rules

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



AWS Config > Rules > Add rule

Step 1
Specify rule type

Step 2
Configure rule

Step 3
Review and create

Specify rule type

Add rules to help you manage the ideal configuration settings of your AWS resources. You can add any of the following predefined, customizable AWS Config Managed rules, or you can create your own AWS Config Custom rule using AWS Lambda functions or Guard Custom policy.

Select rule type

● Add AWS managed rule
Deploy the following managed rules in their default state or customize to suit your needs.

○ Create custom Lambda rule
Use a Lambda function with your custom code to evaluate whether your AWS resources comply with the rule.

○ Create custom rule using Guard
Use Guard Custom policy that you write to evaluate whether your AWS resources comply with the rule.

AWS Managed Rules (580)

ec2-imdsv2 — 1 match

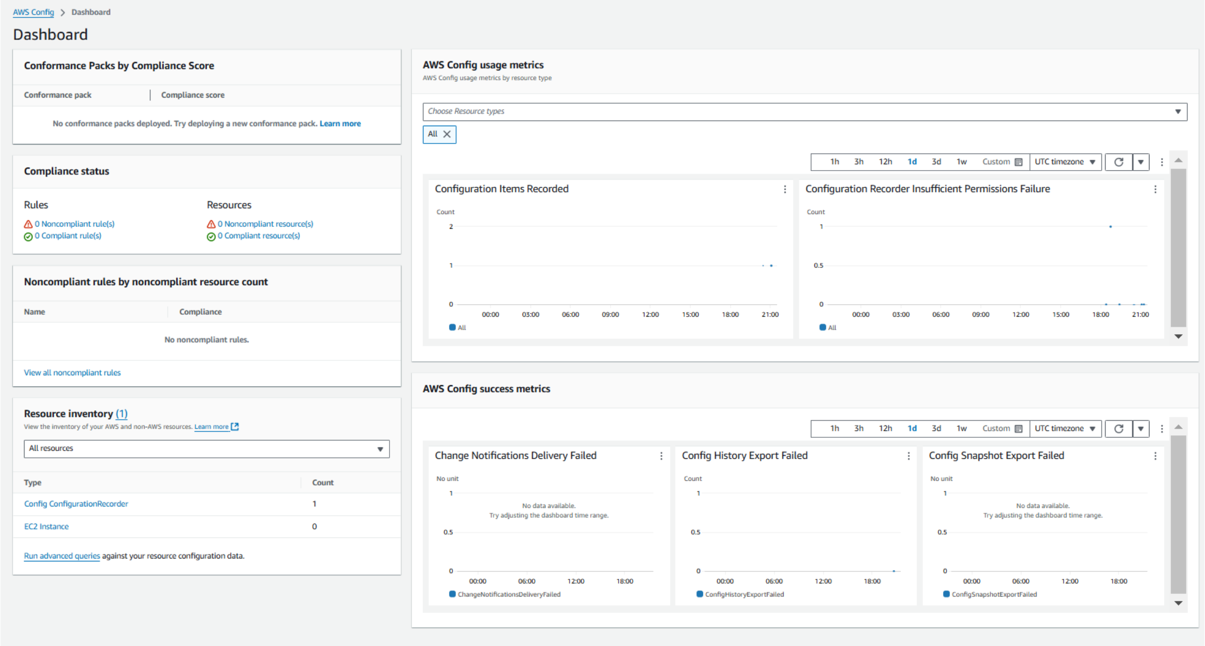
	Name	Labels	Supported evaluation mode	Description
●	ec2-imdsv2-check	EC2, IMDSv2, metadata	DETECTIVE	Checks if your Amazon Elastic Compute Cloud (Amazon EC2) instance metadata version is configured with Instance Metadata Service Version 2 (IMDSv2). The rule is NON_COMPLIANT if the HttpTokens is set to optional.

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.



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
⚠ 0 Noncompliant rule(s)
✓ 0 Compliant rule(s)

Resources
⚠ 0 Noncompliant resource(s)
✓ 0 Compliant resource(s)

Noncompliant rules by noncompliant resource count

Name	Compliance

No noncompliant rules.

View all noncompliant rules

Resource inventory (1)
View the inventory of your AWS and non-AWS resources. Learn more

All resources

Type	Count
Config ConfigurationRecorder	1
EC2 Instance	0

Run advanced queries against your resource configuration data.

AWS Config usage metrics
AWS Config usage metrics by resource type

Choose Resource types
All

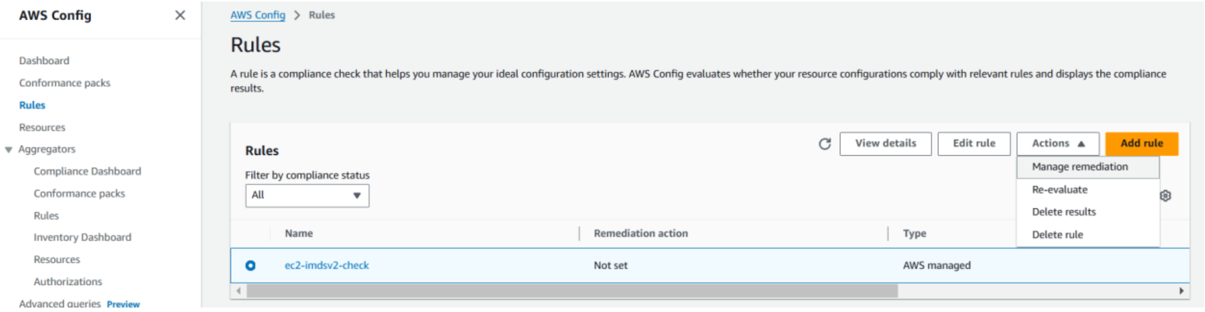
AWS Config success metrics

1h 3h 12h 1d 3d 1w Custom UTC timezone
Configuration Items Recorded
Count
2
1
0
00:00 03:00 06:00 09:00 12:00 15:00 18:00 21:00
All
Configuration Recorder Insufficient Permissions Failure
Count
1
0.5
0
00:00 03:00 06:00 09:00 12:00 15:00 18:00 21:00
All
1h 3h 12h 1d 3d 1w Custom UTC timezone
Change Notifications Delivery Failed
No unit
1
No data available.
Try adjusting the dashboard time range.
0.5
0
00:00 06:00 12:00 18:00
ChangeNotificationsDeliveryFailed
Config History Export Failed
Count
1
0.5
0
00:00 06:00 12:00 18:00
ConfigHistoryExportFailed
Config Snapshot Export Failed
No unit
1
No data available.
Try adjusting the dashboard time range.
0.5
0
00:00 06:00 12:00 18:00
ConfigSnapshotExportFailed

Configuring Remediation

Step 1: Accessing Remediation Actions

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



Rules

A rule is a compliance check that helps you manage your ideal configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and displays the compliance results.

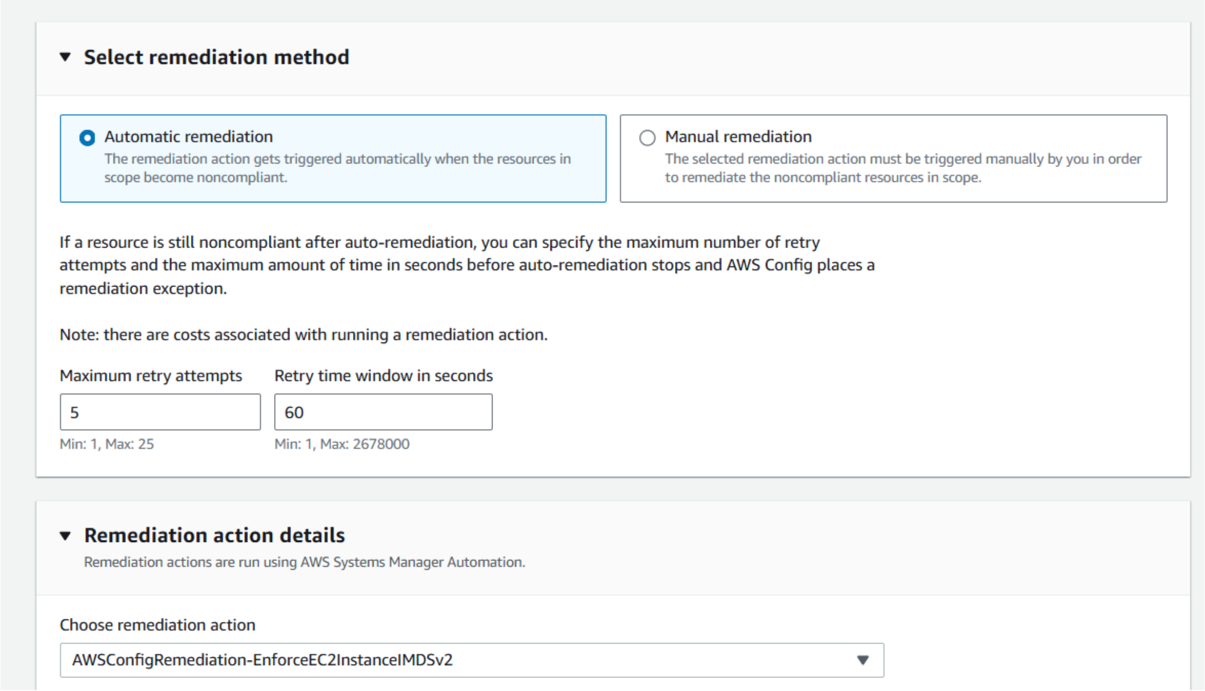
Rules

Filter by compliance status: All

	Name	Remediation action	Type
●	ec2-imdsv2-check	Not set	AWS managed

Step 2: Setting Remediation Parameters

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



▼ Select remediation method

● Automatic remediation
The remediation action gets triggered automatically when the resources in scope become noncompliant.

○ Manual remediation
The selected remediation action must be triggered manually by you in order to remediate the noncompliant resources in scope.

If a resource is still noncompliant after auto-remediation, you can specify the maximum number of retry attempts and the maximum amount of time in seconds before auto-remediation stops and AWS Config places a remediation exception.

Note: there are costs associated with running a remediation action.

Maximum retry attempts: 5
Min: 1, Max: 25

Retry time window in seconds: 60
Min: 1, Max: 2678000

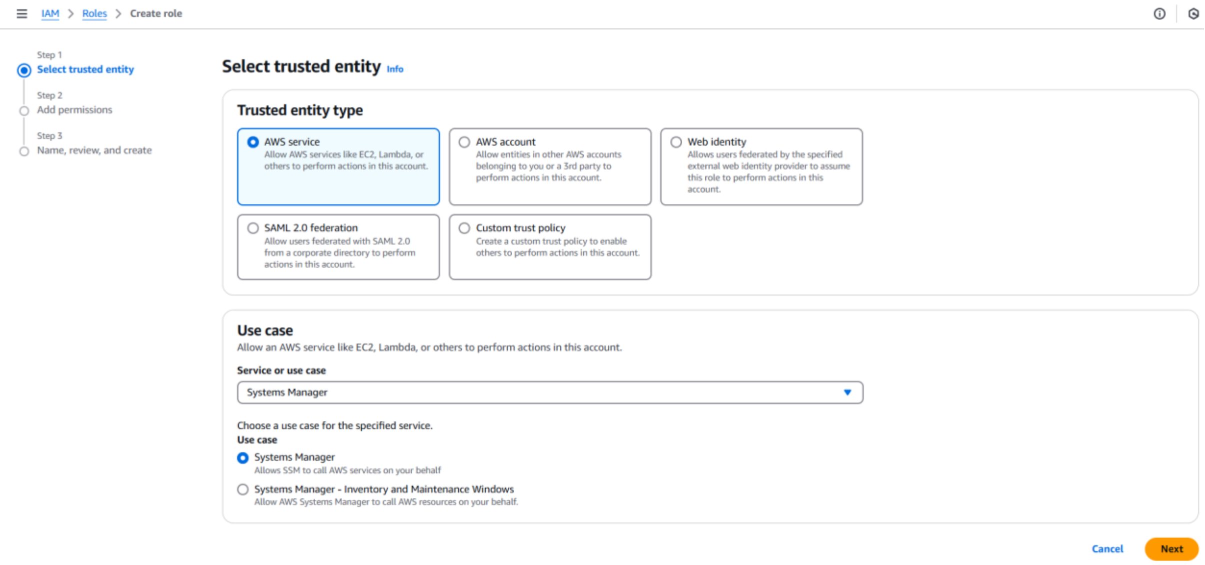
▼ Remediation action details

Remediation actions are run using AWS Systems Manager Automation.

Choose remediation action: AWSConfigRemediation-EnforceEC2InstanceIMDSv2 ▼

Step 3: Creating an IAM Role for Remediation

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



IAM > Roles > Create role

Step 1
● Select trusted entity

Step 2
○ Add permissions

Step 3
○ Name, review, and create

Select trusted entity Info

Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

Systems Manager ▼

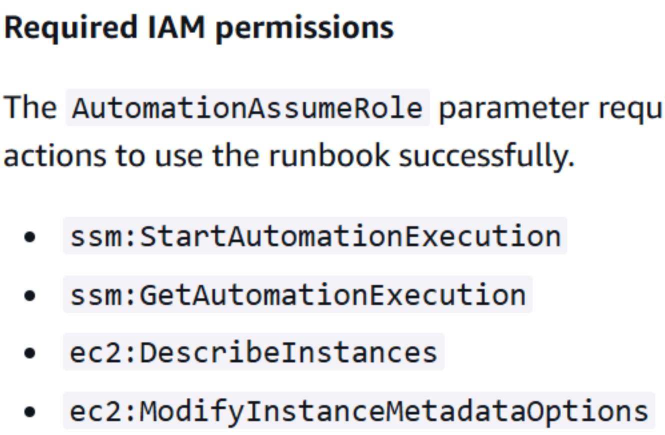
Choose a use case for the specified service.

Use case

● Systems Manager
Allows SSM to call AWS services on your behalf

○ Systems Manager - Inventory and Maintenance Windows
Allow AWS Systems Manager to call AWS resources on your behalf.

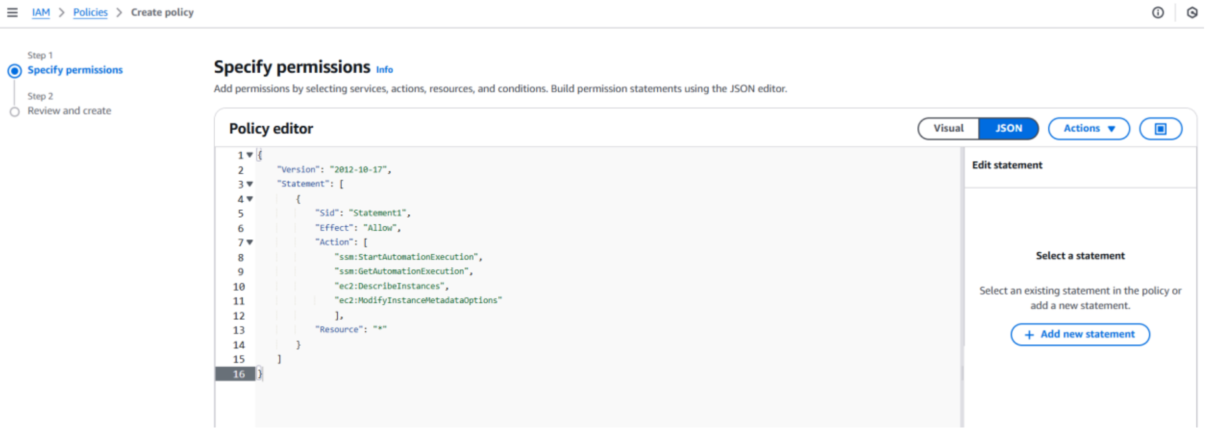
- Create a new policy with required permissions:



Required IAM permissions

The `AutomationAssumeRole` parameter requires the following actions to use the runbook successfully.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeInstances`
- `ec2:ModifyInstanceMetadataOptions`



IAM > Policies > Create policy

Step 1
● Specify permissions

Step 2
○ Review and create

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

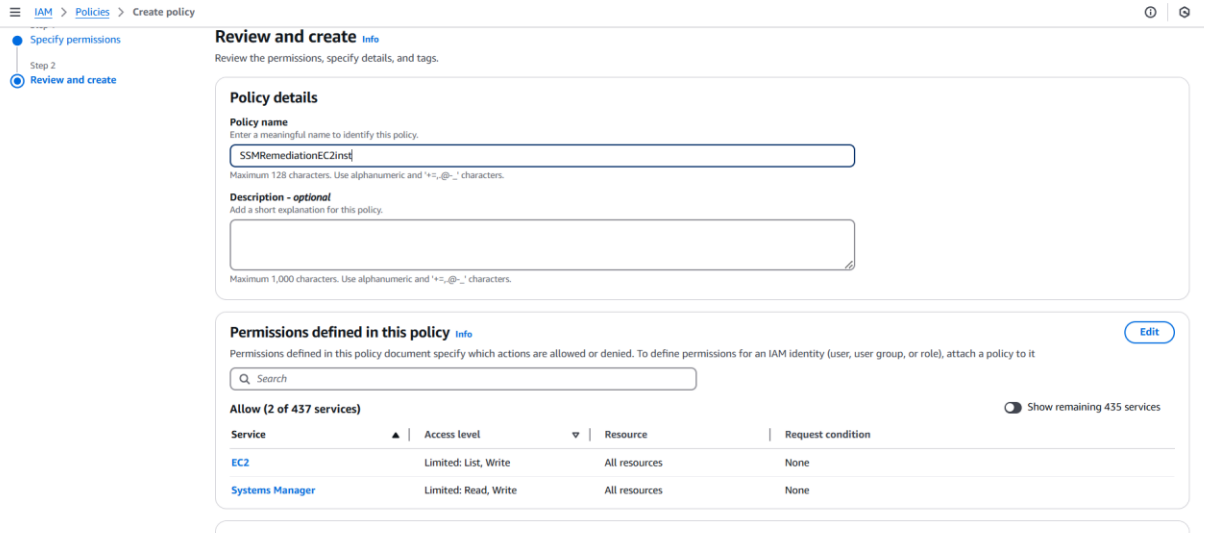
Policy editor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution",
                "ssm:GetAutomationExecution",
                "ec2:DescribeInstances",
                "ec2:ModifyInstanceMetadataOptions"
            ],
            "Resource": "*"
        }
    ]
}
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.



Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.
SSMRemediationEC2inst
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

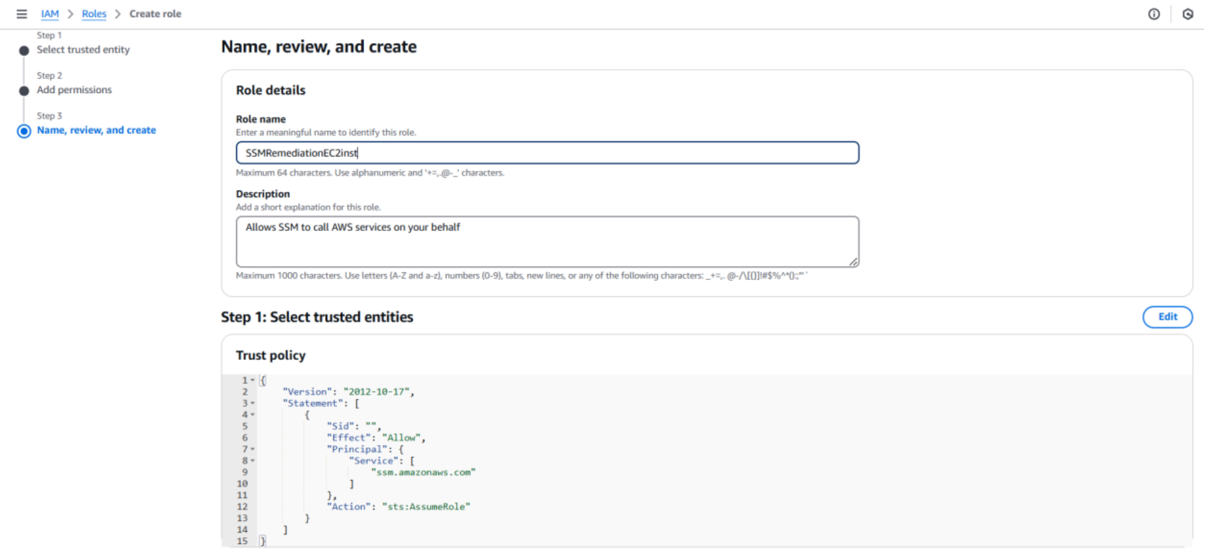
Description - *optional*
Add a short explanation for this policy.
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (2 of 437 services)

Service	Access level	Resource	Request condition
EC2	Limited: List, Write	All resources	None
Systems Manager	Limited: Read, Write	All resources	None



Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
SSMRemediationEC2inst
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

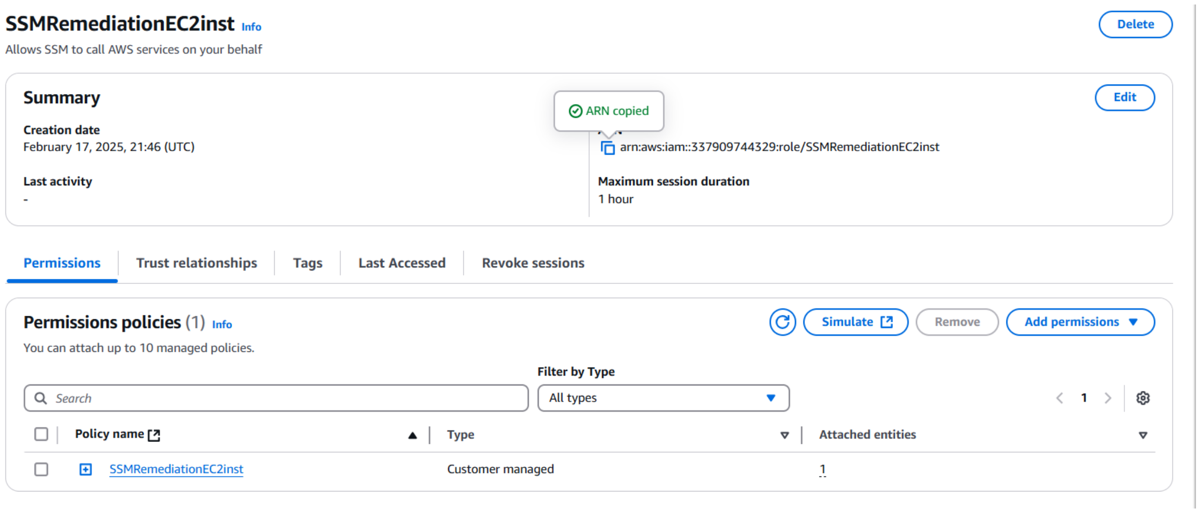
Description
Add a short explanation for this role.
Allows SSM to call AWS services on your behalf
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/\[{}]!#$%^*();:"'`

Step 1: Select trusted entities

Trust policy

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

- 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.



SSMRemediationEC2inst Info

Allows SSM to call AWS services on your behalf

Summary

Creation date
February 17, 2025, 21:46 (UTC)

Last activity
-

arn:aws:iam::337909744329:role/SSMRemediationEC2inst

Maximum session duration
1 hour

Permissions policies (1) Info

You can attach up to 10 managed policies.

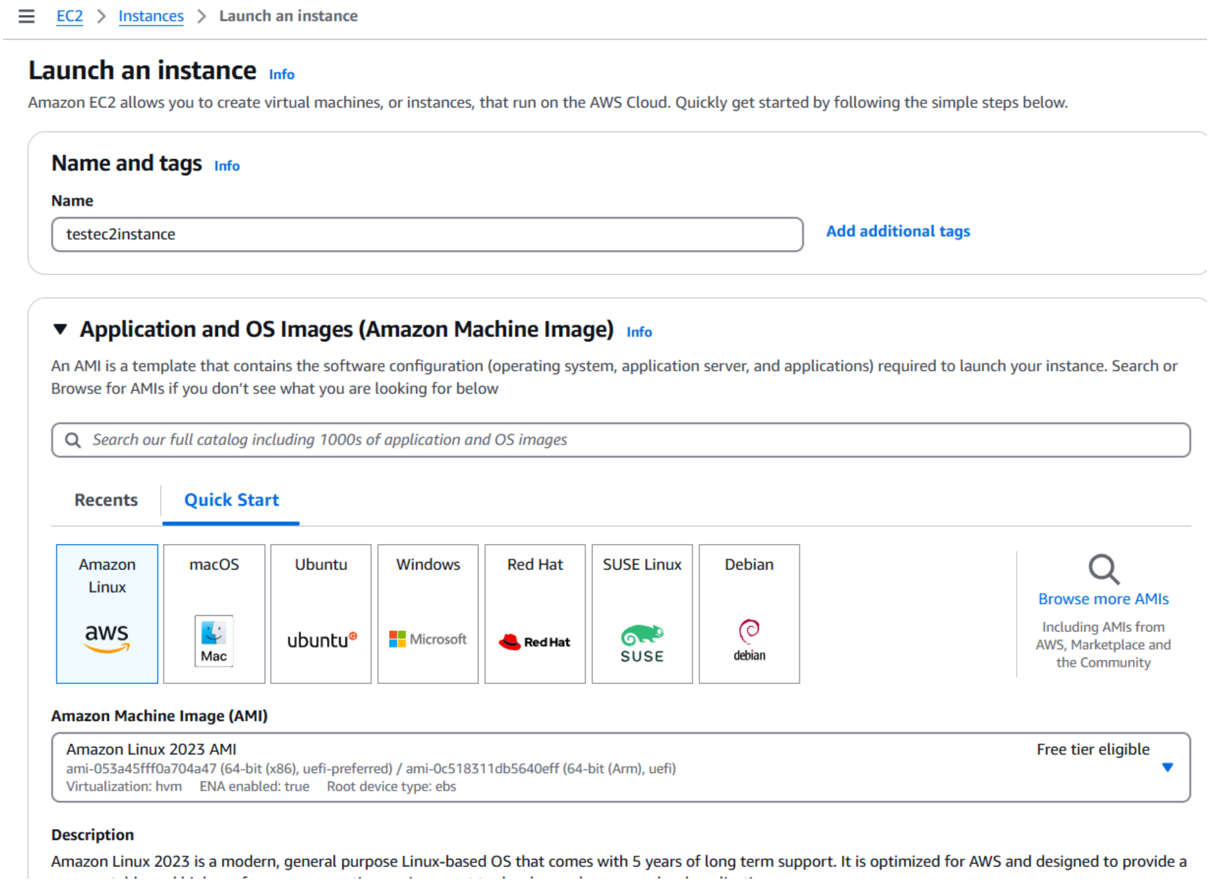
Filter by Type
All types

□	Policy name	Type	Attached entities
□	SSMRemediationEC2inst	Customer managed	1

Launching a Non-Compliant EC2 Instance

Step 1: Launch EC2 Instance

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



EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: testec2instance

Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

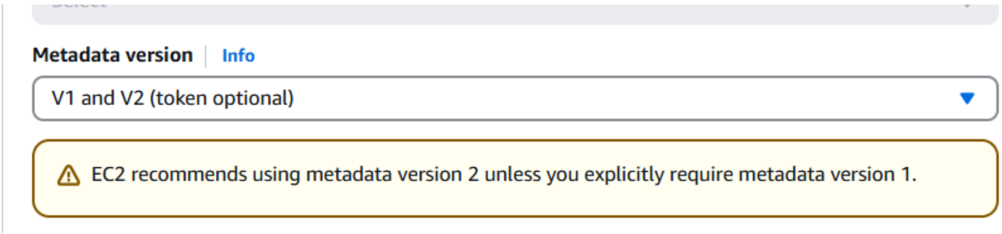
Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible
ami-053a45fff0a704a47 (64-bit (x86), uefi-preferred) / ami-0c518311db5640eff (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a

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



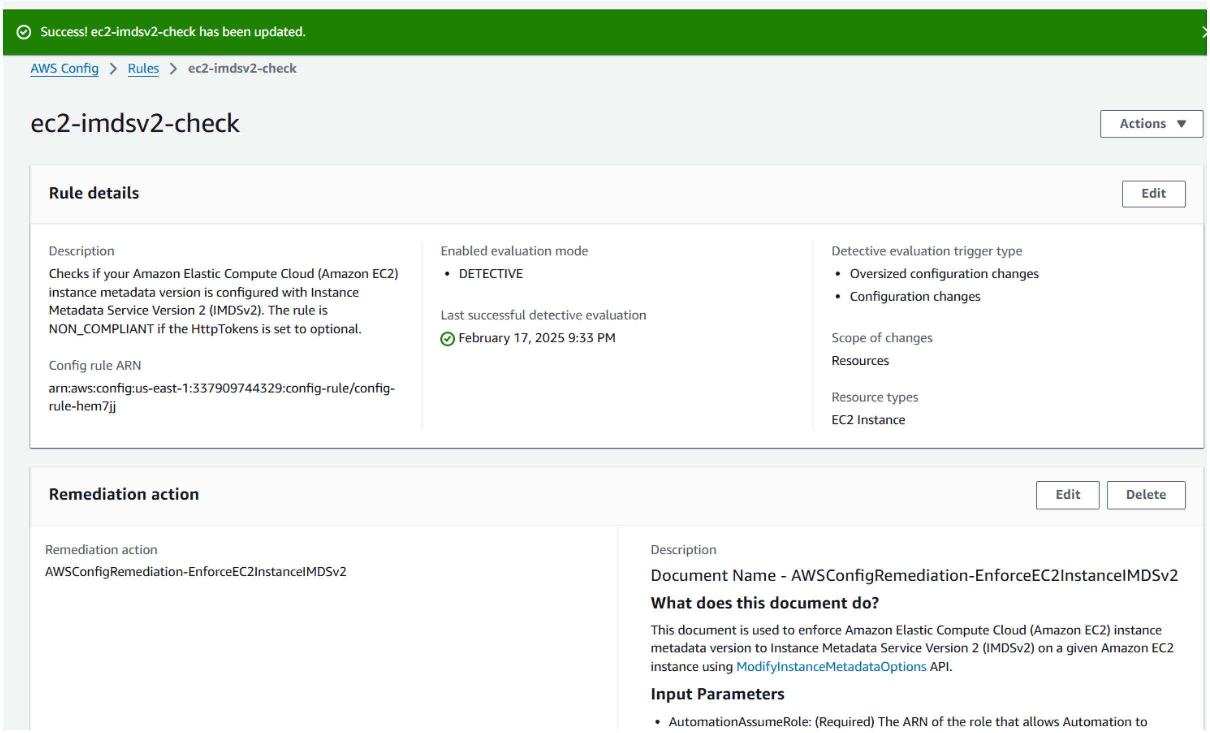
Metadata version Info

V1 and V2 (token optional)

⚠ EC2 recommends using metadata version 2 unless you explicitly require metadata version 1.

Step 2: Checking Noncompliance

- Refresh the **AWS Config Dashboard**.



Success! ec2-imdsv2-check has been updated.

AWS Config > Rules > ec2-imdsv2-check

ec2-imdsv2-check

Rule details

Description

Checks if your Amazon Elastic Compute Cloud (Amazon EC2) instance metadata version is configured with Instance Metadata Service Version 2 (IMDSv2). The rule is NON_COMPLIANT if the HttpTokens is set to optional.

Config rule ARN

arn:aws:config:us-east-1:337909744329:config-rule/config-rule-hem7jj

Enabled evaluation mode

- DETECTIVE

Last successful detective evaluation

✓ February 17, 2025 9:33 PM

Detective evaluation trigger type

- Oversized configuration changes
- Configuration changes

Scope of changes

Resources

Resource types

EC2 Instance

Remediation action

Remediation action

AWSConfigRemediation-EnforceEC2InstanceIMDSv2

Description

Document Name - AWSConfigRemediation-EnforceEC2InstanceIMDSv2

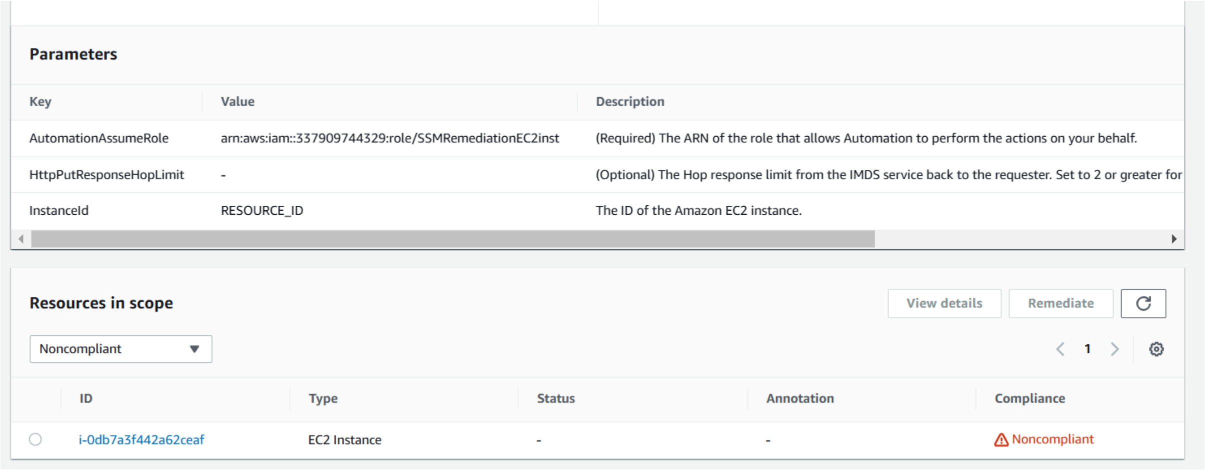
What does this document do?

This document is used to enforce Amazon Elastic Compute Cloud (Amazon EC2) instance metadata version to Instance Metadata Service Version 2 (IMDSv2) on a given Amazon EC2 instance using ModifyInstanceMetadataOptions API.

Input Parameters

- AutomationAssumeRole: (Required) The ARN of the role that allows Automation to

- The instance appears as **Noncompliant**.

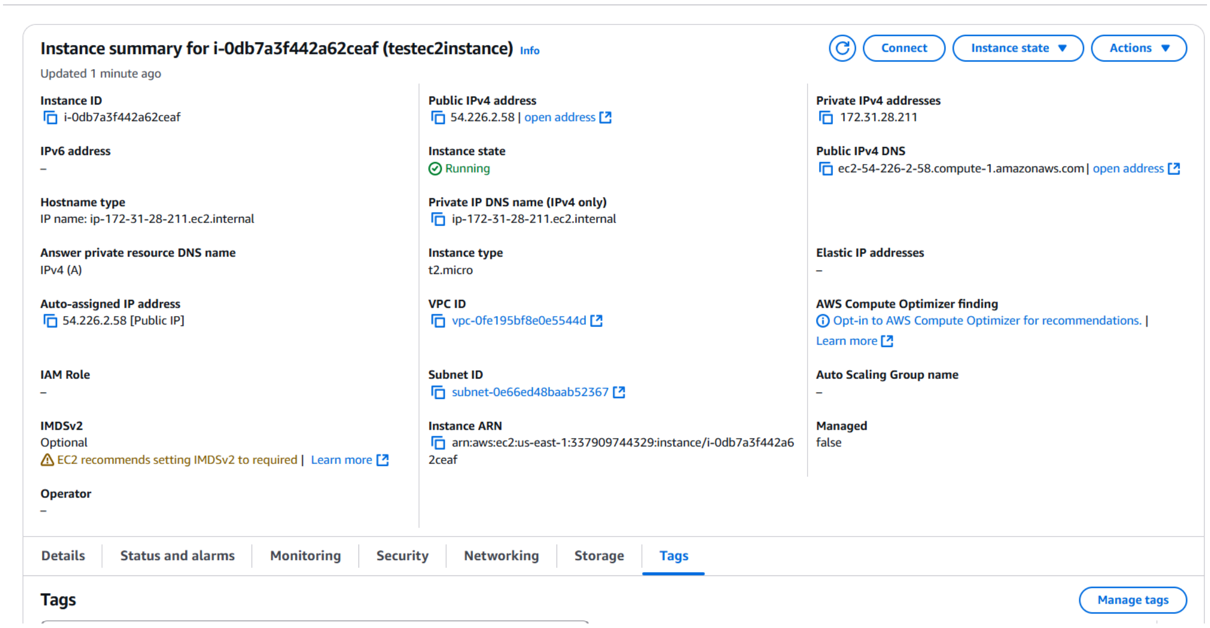


Parameters

Key	Value	Description
AutomationAssumeRole	arn:aws:iam::337909744329:role/SSMRemediationEC2inst	(Required) The ARN of the role that allows Automation to perform the actions on your behalf.
HttpPutResponseHopLimit	-	(Optional) The Hop response limit from the IMDS service back to the requester. Set to 2 or greater for
InstanceId	RESOURCE_ID	The ID of the Amazon EC2 instance.

Resources in scope

	ID	Type	Status	Annotation	Compliance
○	i-0db7a3f442a62ceaf	EC2 Instance	-	-	⚠ Noncompliant



Instance summary for i-0db7a3f442a62ceaf (testec2instance) Info

Updated 1 minute ago

Instance ID
i-0db7a3f442a62ceaf

IPv6 address
–

Hostname type
IP name: ip-172-31-28-211.ec2.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address
54.226.2.58 [Public IP]

IAM Role
–

IMDSv2
Optional
⚠ EC2 recommends setting IMDSv2 to required | Learn more

Operator
–

Public IPv4 address
54.226.2.58 | open address

Instance state
✓ Running

Private IP DNS name (IPv4 only)
ip-172-31-28-211.ec2.internal

Instance type
t2.micro

VPC ID
vpc-0fe195bf8e0e5544d

Subnet ID
subnet-0e66ed48baab52367

Instance ARN
arn:aws:ec2:us-east-1:337909744329:instance/i-0db7a3f442a62ceaf

Private IPv4 addresses
172.31.28.211

Public IPv4 DNS
ec2-54-226-2-58.compute-1.amazonaws.com | open address

Elastic IP addresses
–

AWS Compute Optimizer finding
ⓘ Opt-in to AWS Compute Optimizer for recommendations. | Learn more

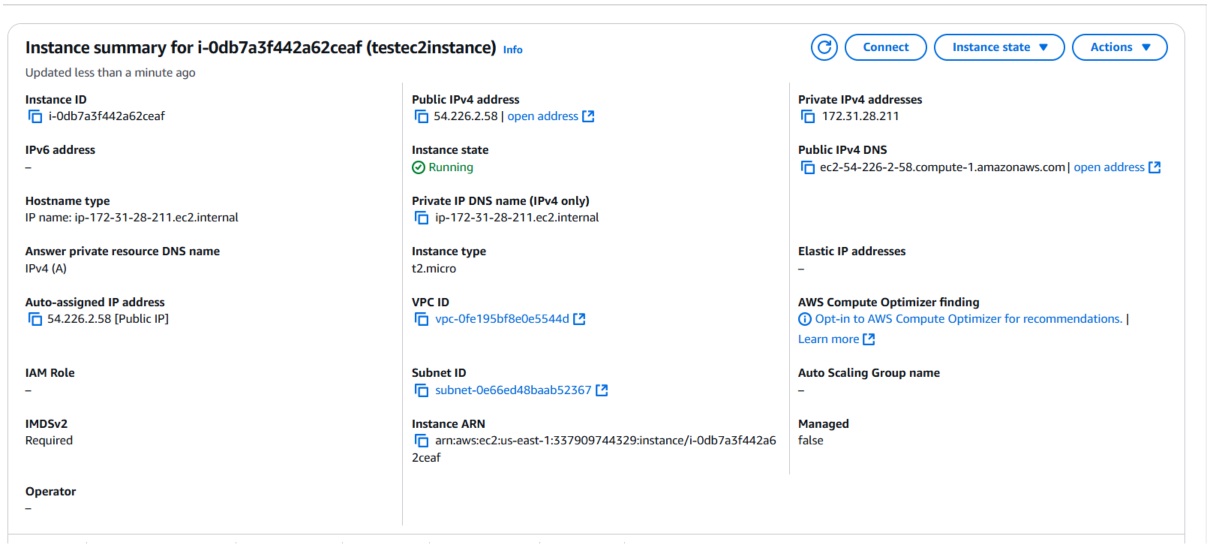
Auto Scaling Group name
–

Managed
false

Tags

Step 3: Verifying Automated Remediation

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



Instance summary for i-0db7a3f442a62ceaf (testec2instance) Info

Updated less than a minute ago

Instance ID
i-0db7a3f442a62ceaf

IPv6 address
–

Hostname type
IP name: ip-172-31-28-211.ec2.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address
54.226.2.58 [Public IP]

IAM Role
–

IMDSv2
Required

Operator
–

Public IPv4 address
54.226.2.58 | open address

Instance state
✓ Running

Private IP DNS name (IPv4 only)
ip-172-31-28-211.ec2.internal

Instance type
t2.micro

VPC ID
vpc-0fe195bf8e0e5544d

Subnet ID
subnet-0e66ed48baab52367

Instance ARN
arn:aws:ec2:us-east-1:337909744329:instance/i-0db7a3f442a62ceaf

Private IPv4 addresses
172.31.28.211

Public IPv4 DNS
ec2-54-226-2-58.compute-1.amazonaws.com | open address

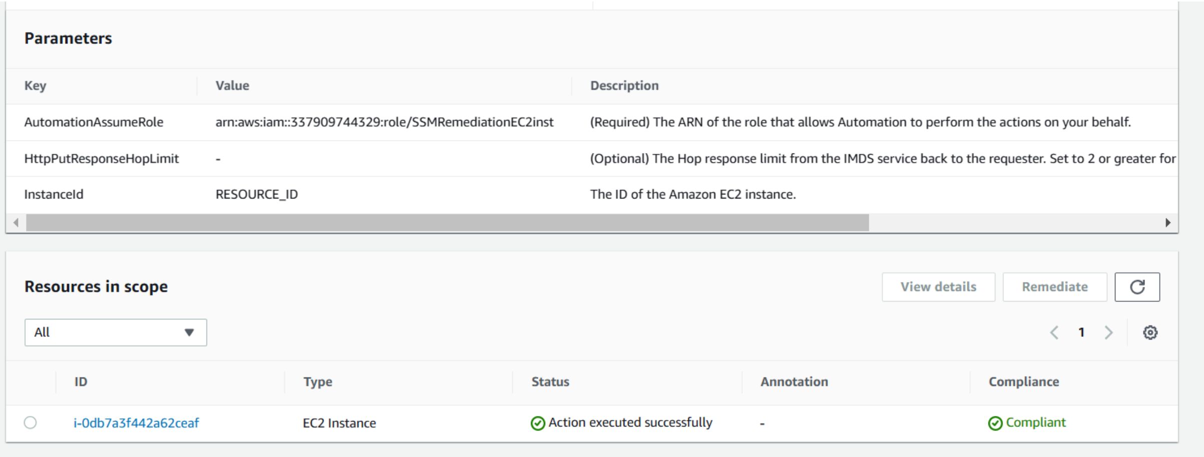
Elastic IP addresses
–

AWS Compute Optimizer finding
ⓘ Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name
–

Managed
false

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



Parameters

Key	Value	Description
AutomationAssumeRole	arn:aws:iam::337909744329:role/SSMRemediationEC2inst	(Required) The ARN of the role that allows Automation to perform the actions on your behalf.
HttpPutResponseHopLimit	-	(Optional) The Hop response limit from the IMDS service back to the requester. Set to 2 or greater for
InstanceId	RESOURCE_ID	The ID of the Amazon EC2 instance.

Resources in scope

	ID	Type	Status	Annotation	Compliance
○	i-0db7a3f442a62ceaf	EC2 Instance	✓ Action executed successfully	-	✓ Compliant

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].