

# Project: Automation Compliance framework

GitHub repo: <https://github.com/Mithra1995/aws-compliance-automation-framework.git>

## Project Objective:

To develop an end-to-end compliance solution that:

1. Detects non-compliance using AWS Config.
2. Automatically remediates using SSM Automation Documents.
3. Sends alerts via SNS and stores logs in S3/CloudWatch.
4. Produces weekly reports for auditing.

## AWS Services Used:

Service	Purpose
<b>AWS Config</b>	Rule-based compliance checks
<b>SSM Automation Docs</b>	Runbook-based remediation
<b>Amazon SNS</b>	Real-time alerts
<b>CloudWatch Logs</b>	Store execution and remediation logs
<b>AWS CloudTrail</b>	Audit trail of all changes
<b>IAM</b>	Fine-grained permissions for remediation execution
<b>Amazon S3</b>	Store compliance reports
<b>AWS Organizations</b> <i>(Optional)</i>	Cross-account policy enforcement

## Automation flow diagram

## Automation Flow Diagram

plaintext

 Copy  Edit

```
AWS Config (rules + recorder)
  |
  ↓
Detect Non-compliance
  |
  ↓
Trigger Lambda or SSM Automation
  |
  ↓
Remediate + Notify via SNS
  |
  ↓
Log in CloudWatch + CloudTrail
```



### **Step by step Implementation:**

#### EC2 Required Tags

1. Resource Type: AWS::EC2::Instance
2. Flow:
  - a. AWS Config managed rule detects non-compliance
  - b. EventBridge rule triggers SSM Automation to apply missing tags

Step 1: create AWS config record for EC2 tags

The screenshot shows the AWS Config console interface. On the left, there is a navigation sidebar with links like Conformance packs, Rules, Resources, Aggregators, Compliance Dashboard, and more. A section titled "Settings" is currently selected. Below it are links for Documentation, Partners, FAQs, and Pricing. At the bottom of the sidebar are CloudShell and Feedback buttons.

The main content area displays configuration details:

- Record specific resource types.**
- Recorded resource types (2)**

Resource types	Frequency
AWS EC2 Instance	Continuous
AWS EC2 SecurityGroup	Continuous
- Governance**

IAM role for AWS Config  
AWSServiceRoleForConfig
- Amazon CloudWatch Events rule**

AWS Config sends detailed information about the configuration changes and notifications to Amazon CloudWatch Events. To create rules, visit the [Step 1: Create Rule](#) page in the Amazon CloudWatch Events console.

At the bottom right of the main content area, there are links for © 2025, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

## Step 2: SNS notification subscription

AWS Notification - Subscription Confirmation Inbox

**AWS Notifications** <no-reply@sns.amazonaws.com>  
to me ▾

You have chosen to subscribe to the topic:  
**arn:aws:sns:us-east-1:382828593676:config-topic**

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):  
[Confirm subscription](#)

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please

[Reply](#) [Forward](#) [Smileys](#)

aws.us-east-1.amazonaws.com/confirmation.html?TopicArn=arn:aws:sns:us-east-1:382828593676:config-topic&Token=2336412f37fb687f5d51e6e2425a8a58770f195...

**Subscription confirmed!**

You have successfully subscribed.

Your subscription's id is:  
**arn:aws:sns:us-east-1:382828593676:config-topic:a0a8e76b-63b4-41e5-9b5e-8064c71e261d**

If it was not your intention to subscribe, [click here to unsubscribe](#).

### Step 3: create AWS config rules for EC2 tags

The screenshot shows the AWS Config Rules page. The left sidebar has a 'Rules' section expanded, showing options like Compliance Dashboard, Conformance packs, Rules, Inventory Dashboard, Resources, Authorizations, Advanced queries (with a 'Preview' link), Settings, and What's new. The main content area is titled 'Rules' and contains a table header with columns: Name, Remediation action, Type, Enabled evaluation..., and Detective compliance. A message 'No rules found.' is displayed, along with a prominent orange 'Add rule' button.

The screenshot shows the 'Configure rule' step of the rule creation wizard. The left sidebar shows 'Step 1: Specify rule type' (selected), 'Step 2: Configure rule' (current), and 'Step 3: Review and create'. The main content area is titled 'Configure rule' and says 'Customize any of the following fields'. It has a 'Details' section with a 'Name' field containing 'required-tags' and a 'Description - optional' field containing 'Checks whether your resources have the tags that you specify.' Below it is a 'Managed rule name' field with 'REQUIRED\_TAGS' entered. The top navigation bar includes AWS logo, search bar, [Alt+S] key, notifications, United States (N. Virginia) region, and user Mithra @ 3828-2859-3676.

Screenshot of the AWS Config Rule Parameters configuration screen.

**Parameters**

Rule parameters define attributes that your resources must adhere to for compliance with the rule. Example attributes include a required tag or a specified S3 bucket. **Optional** parameters that are not valid, such as missing a key or a value, will not be saved.

Key	Value
tag1Key	Environment
tag2Key	Owner

**Add another row** **Remove**

**Rule tags - optional**

Screenshot of the AWS Config Rule creation review screen.

**Review and create**

Review this rule before adding it to your account

**Step 1** [Specify rule type](#)

**Step 2** [Configure rule](#)

**Step 3** [Review and create](#)

**Details**

Rule name required-tags	Managed rule name REQUIRED_TAGS
Description Checks whether your resources have the tags that you specify.	

**Evaluation mode**

Proactive evaluation Disabled	Detective evaluation Enabled
Trigger type • When configuration changes	Resource types ACM Certificate, AutoScaling AutoScalingGroup

[CloudShell](#) [Feedback](#)

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Step 4: by default the EC2 instance don't have tags(Environment and Owner ) so the AWS config rule become NON-COMPLIANT

**EC2**

- Instances
  - Instances
  - Instance Types
  - Launch Templates
  - Spot Requests
  - Savings Plans
  - Reserved Instances
  - Dedicated Hosts
  - Capacity Reservations
- Images
  - AMIs
  - AMI Catalog

**Auto-assigned IP address**: 54.80.232.120 [Public IP]

**VPC ID**: vpc-031a9b3b1dcc0a13e

**IAM Role**: -

**IMDSv2**: Required

**Subnet ID**: subnet-0355fb975989646d0

**Operator**: -

**Instance ARN**: arn:aws:ec2:us-east-1:382828593676:instance/i-07e10e4a978b93c68

**AWS Compute Optimizer finding**: Opt-in to AWS Compute Optimizer for recommendations.

**Auto Scaling Group name**: -

**Managed**: false

**Tags**

Key	Value
Name	ec2tags

**AWS Config**

- Dashboard
- Conformance packs
- Rules**
- Resources
- Aggregators
  - Compliance Dashboard
  - Conformance packs
  - Rules
  - Inventory Dashboard
  - Resources
  - Authorizations
- Advanced queries [Preview](#)
- Settings
- What's new

**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.

Name	Remediation action	Type	Enabled evaluation...	Detective compliance
ec2_required-tags	AddMissingEC2Tags	AWS managed	DETECTIVE	⚠ 1 Noncompliant ...
restricted-ssh	RevokePublicSSHAc...	AWS managed	DETECTIVE	🟢 Compliant

```

{
  "evaluationResult": {
    "evaluationResultIdentifier": {
      "evaluationResultQualifier": {
        "configRuleName": "restricted-ssh",
        "resourceType": "AWS::EC2::SecurityGroup",
        "resourceId": "sg-04bb7176a0828f577",
        "evaluationMode": "DETECTIVE"
      },
      "resourceEvaluationId": null,
      "orderingTimestamp": "2025-07-25T04:11:02.693Z"
    },
    "complianceType": "NON_COMPLIANT",
    "resultRecordedTime": "2025-07-25T04:11:31.135Z",
    "configRuleInvokedTime": "2025-07-25T04:11:30.919Z",
    "annotation": null,
    "resultToken": null
  },
  "oldEvaluationResult": {
    "evaluationResultIdentifier": {
      "evaluationResultQualifier": {
        "configRuleName": "restricted-ssh",
        "resourceType": "AWS::EC2::SecurityGroup",
        "resourceId": "sg-04bb7176a0828f577",
        "evaluationMode": "DETECTIVE"
      },
      "resourceEvaluationId": null,
      "orderingTimestamp": "2025-07-25T03:57:53.980Z"
    }
  }
}

```

Step 5: Now add the Eventbridge rule to trigger Auto-remediation , so it will trigger when there is change in status to NON-COMPLIANT

**Amazon EventBridge > Rules > TriggerSSMOnTagViolation**

<b>Description</b> Trigger SSM when EC2 missing required tags	<b>Rule ARN</b> arn:aws:events:us-east-1:382828593676:rule/TriggerSSMOnTagViolation	<b>Event bus ARN</b> arn:aws:events:us-east-1:382828593676:event-bus/default
--	--	---

**Event pattern** **Edit**

```

1 {
  "source": ["aws.config"],
  "detail-type": ["Config Rules Compliance Change"],
  "detail": {
    "configRuleName": ["ec2_required-tags"],
    "resourceType": ["AWS::EC2::Instance"],
    "newEvaluationResult": [
      {"complianceType": ["NON_COMPLIANT"]}
    ]
  }
}

```

**Targets**

**Monitoring**

**Tags**

**Event pattern Info**

**Copy**

**Input transformer**

**Input path**

```

1 {
2   "instanceId": "$.detail.resourceId"
3 }

```

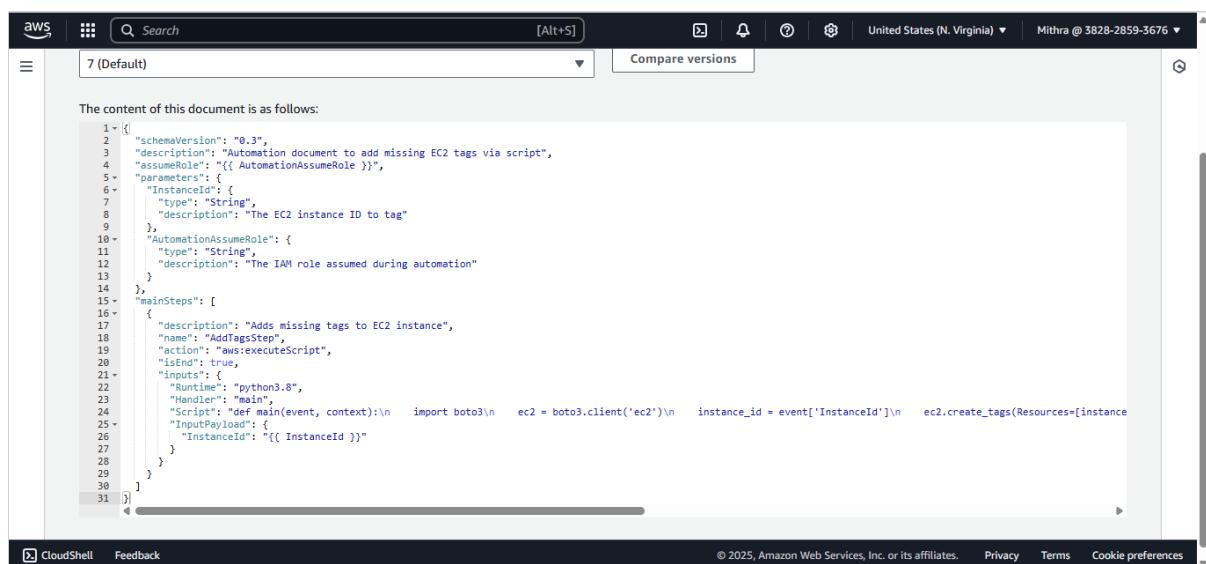
**Input template**

```

1 {
2   "InstanceId": "<instanceId>"
3 }
4

```

## Step 6: Now create the custom runbook for Auto remediation



The content of this document is as follows:

```

1 {
2   "schemaVersion": "0.3",
3   "description": "Automation document to add missing EC2 tags via script",
4   "assumeRole": "{{ AutomationAssumeRole }}",
5   "parameters": {
6     "InstanceId": {
7       "type": "String",
8       "description": "The EC2 instance ID to tag"
9     },
10    "AutomationAssumeRole": {
11      "type": "String",
12      "description": "The IAM role assumed during automation"
13    }
14  },
15  "mainSteps": [
16    {
17      "description": "Adds missing tags to EC2 instance",
18      "action": "AddTagsStep",
19      "inputs": {
20        "Runtime": "python3.8",
21        "Handler": "main",
22        "Script": "def main(event, context):\n    import boto3\n    ec2 = boto3.client('ec2')\n    instance_id = event['InstanceId']\n    ec2.create_tags(Resources=[instance_id],\n                    Tags=[{\n                        'Key': 'Name',\n                        'Value': 'Auto Tagged'\n                    }])"
23      }
24    }
25  ]
31 }

```

Step 7: once the auto remediation starts we can see the progress in Automation history

The screenshot shows the AWS Systems Manager Automation history page. At the top, there are tabs for 'Executions' (which is selected), 'Integrations', and 'Preferences'. Below this, a section titled 'Automation executions' displays a table of completed executions. The table has columns for 'Execution ID', 'Runbook name', 'Status', 'Start time', and 'End time'. One execution is listed:

Execution ID	Runbook name	Status	Start time	End time
85f5b4cc-a713-4fff-9f2e-0c2246f505ed	AddMissingEC2Tags	Success	Fri, 25 Jul 2025 04:25:13 GMT	Fri, 25 Jul 2025 04:25:17 GMT

Step 8: And now we can see the tags added to EC2 instance

The screenshot shows the AWS EC2 Instances details page for an instance with ID i-07e10e4a978b93c68. The left sidebar shows navigation links for EC2, Instances, Images, and other services. The main pane displays instance details under 'Subnet ID' (subnet-0355fb97598964d0) and 'Instance ARN' (arn:aws:ec2:us-east-1:382828593676:instance/i-07e10e4a978b93c68). A 'Tags' tab is selected at the bottom, showing the following tags:

Key	Value
Environment	Production
Name	ec2tags
Owner	OpsTeam

Step 9: And now the NON- COMPLIANT will move to COMPLIANT

Rules				
Filter by compliance status				
<a href="#">All</a> ▾				
◀ 1 ▶ ⚙				
Name	Remediation action	Type	Enabled evaluation...	Detective compliance
<a href="#">ec2_required-tags</a>	AddMissingEC2Tags	AWS managed	DETECTIVE	 Compliant
<a href="#">restricted-ssh</a>	RevokePublicSSHAc...	AWS managed	DETECTIVE	 Compliant

Step 10 : Got an SNS notification also for COMPLIANT status

```
    "Configuration.Tags.0": {  
        "previousValue": null,  
        "updatedValue": {  
            "key": "Environment",  
            "value": "Production"  
        },  
        "changeType": "CREATE"  
    },  
    ...  
    "key": "Environment",  
    "value": "Production"  
},  
{  
    "key": "Name",  
    "value": "ec2tags"  
},  
{  
    "key": "Owner",  
    "value": "OpsTeam"  
}  
]  
...  
"Owner": "OpsTeam",
```

```
 "resourceType": "AWS::EC2::Instance",
 "resourceId": "i-07e10e4a978b93c68",
 "awsRegion": "us-east-1",
 "newEvaluationResult": {
     "evaluationResultIdentifier": {
         "evaluationResultQualifier": {
             "configRuleName": "ec2_required-tags",
             "resourceType": "AWS::EC2::Instance",
             "resourceId": "i-07e10e4a978b93c68",
             "evaluationMode": "DETECTIVE"
         },
         "resourceEvaluationId": null,
         "orderingTimestamp": "2025-07-25T04:27:26.026Z"
     },
     "complianceType": "COMPLIANT",
     "resultRecordedTime": "2025-07-25T04:27:56.756Z",
     "configRuleInvokedTime": "2025-07-25T04:27:56.613Z",
     "annotation": null,
     "resultToken": null
 },
 "oldEvaluationResult": {
     "evaluationResultIdentifier": {
```

## Security Group SSH Open Access

- Resource Type: AWS::EC2::SecurityGroup
- Flow:
  - AWS Config managed rule detects non-compliance
  - EventBridge rule triggers SSM Automation remediation

Step 1: create AWS config rule for EC2 security group

AWS Config > Rules > Add rule

Step 1 Specify rule type

Step 2 Configure rule

Step 3 Review and create

## Configure rule

Customize any of the following fields

**Details**

**Name**  
A unique name for the rule. 128 characters max. No special characters or spaces.

**Description - optional**  
Describe what the rule evaluates and how to fix resources that don't comply.

**Managed rule name**

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Runs when there are changes to your specified AWS resources

Runs on the frequency that you choose

**Scope of changes**  
Choose when evaluations will occur.

All changes  
When any resource recorded by AWS Config is created, changed, or deleted

Resources  
When any resource that matches the specified type, or the type plus identifier, is created, changed, or deleted

Tags  
When any resource with the specified tag is created, changed, or deleted

**Resources**  
This rule can be triggered only when the recorded resources are created, edited, or deleted. Specify the resources to record by editing the Settings page.

Resource category: All resource categories

Resource type: Multiple selected

AWS EC2 SecurityGroup

Resource identifier - optional

Frequency: 24 hours

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Screenshot of the AWS Lambda Function Configuration page for a CloudWatch Metrics Filter Rule.

Rule name	restricted-ssh	Managed rule name	INCOMING_SSH_DISABLED
Description	Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.		
<b>Evaluation mode</b>			
Proactive evaluation	Disabled	Detective evaluation	Enabled
Trigger type	<ul style="list-style-type: none"> <li>When configuration changes</li> <li>Periodic</li> </ul>	Frequency	24 hours
Scope of changes	Resources	Resource types	EC2 SecurityGroup
Resource identifier			

Buttons at the bottom: Cancel, Previous, Save.

Step 2: Get the security group with 0.0.0.0/0 and it should move with NON-COMPLIANT

Screenshot of the AWS EC2 Security Groups page showing the configuration of a security group named "sg-04bb7176a0828f577 - default".

**Details:**

- Security group name: default
- Security group ID: sg-04bb7176a0828f577
- Description: default VPC security group
- VPC ID: vpc-031a9b3b1dcc0a13e
- Owner: 382828593676
- Inbound rules count: 2 Permission entries
- Outbound rules count: 1 Permission entry

**Inbound rules (2):**

Name	Security group r...	IP version	Type	Protocol	Port range	Source
-	sgr-09bf5a1c0976ac...	IPv4	HTTP	TCP	80	0.0.0.0/0
-	sgr-0b04aeab7758e...	IPv4	SSH	TCP	22	0.0.0.0/0

The screenshot shows the AWS Config Rules page. The left sidebar has 'Rules' selected. The main content area displays a table of rules. One rule is listed:

Name	Remediation action	Type	Enabled evaluation...	Detective compliance
restricted-ssh	Not set	AWS managed	DETECTIVE	⚠️ 1 Noncompliant ...

A status bar at the bottom indicates '1 Noncompliant ...'.

### Step 3: Got an email for NON-COMPLIANT

The screenshot shows an email message body containing JSON data. The JSON object represents a non-compliant evaluation result for a security group named 'restricted-ssh'. The key fields include:

- `"evaluationResultIdentifier": {`
- `"evaluationResultQualifier": {`
- `"configRuleName": "restricted-ssh",`
- `"resourceType": "AWS::EC2::SecurityGroup",`
- `"resourceId": "sg-04bb7176a0828f577",`
- `"evaluationMode": "DETECTIVE"`
- `},`
- `"resourceEvaluationId": null,`
- `"orderingTimestamp": "2025-07-29T18:58:37.359Z"`
- `},`
- `"complianceType": "NON_COMPLIANT",`
- `"resultRecordedTime": "2025-07-29T18:59:09.890Z",`
- `"configRuleInvokedTime": "2025-07-29T18:59:09.709Z",`
- `"annotation": null,`
- `"resultToken": null`
- `},`
- `"oldEvaluationResult": null,`
- `"notificationCreationTime": "2025-07-29T18:59:10.751Z",`
- `"messageType": "ComplianceChangeNotification",`
- `"recordVersion": "1.0"`
- `}`

## Step 4: Now create the Eventbridge rule to trigger NON-COMPLIANT

The screenshot shows the AWS EventBridge Rules page. On the left, there's a sidebar with links like Dashboard, Developer resources (Learn, Sandbox, Quick starts), Buses (Event buses, Rules, Global endpoints, Archives, Replays), Pipes (Pipes), and Scheduler (Schedules). The main area shows a rule named 'TriggerSecurityGroupRemediation'. It has a description: 'Triggers SSM Automation when SG is non-compliant'. The Rule ARN is arn:aws:events:us-east-1:382828593676:rule/TriggerSecurityGroupRemediation. The Event bus ARN is arn:aws:events:us-east-1:382828593676:event-bus/default. Below this, there are tabs for Event pattern, Targets, Monitoring, and Tags. The Event pattern tab is selected, showing a JSON snippet:

```
1 {
2   "source": ["aws.config"],
3   "detail-type": ["Config Rules Compliance Change"],
4   "detail": {
5     "messageType": ["ComplianceChangeNotification"],
6     "configRuleName": ["restricted-ssh"],
7     "newEvaluationResult": [
8       "complianceType": ["NON_COMPLIANT"]
9     ]
10   }
11 }
```

There's also a 'Copy' button.

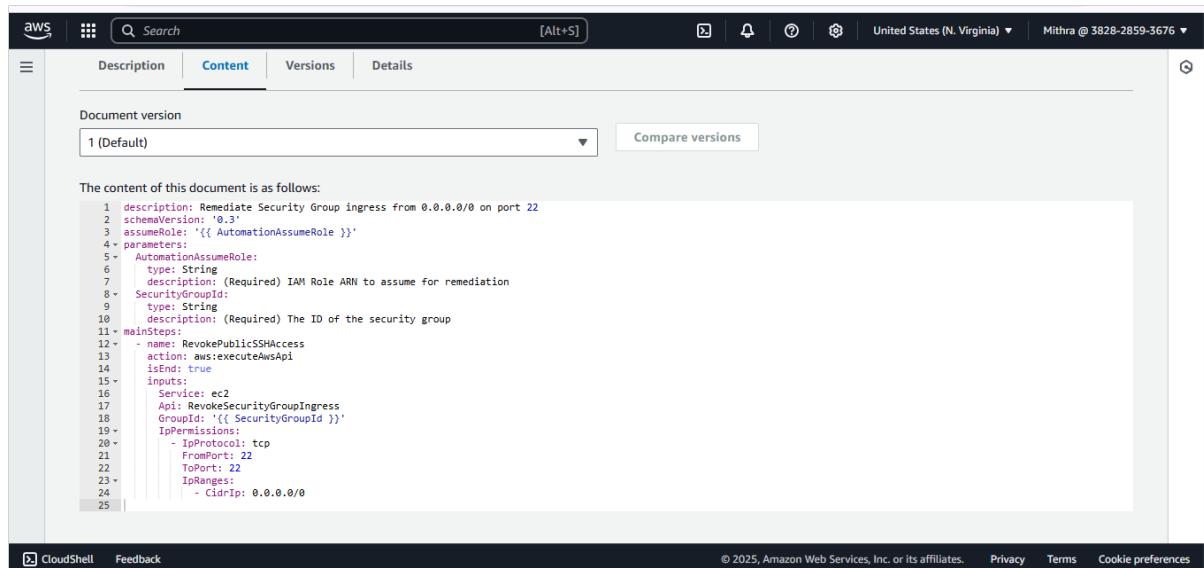
The screenshot shows the 'Input transformer' configuration dialog. It has two sections: 'Input path' and 'Input template'. The 'Input path' section contains the following JSON:

```
1 {
2   "resourceId": "$.detail.resourceId"
3 }
```

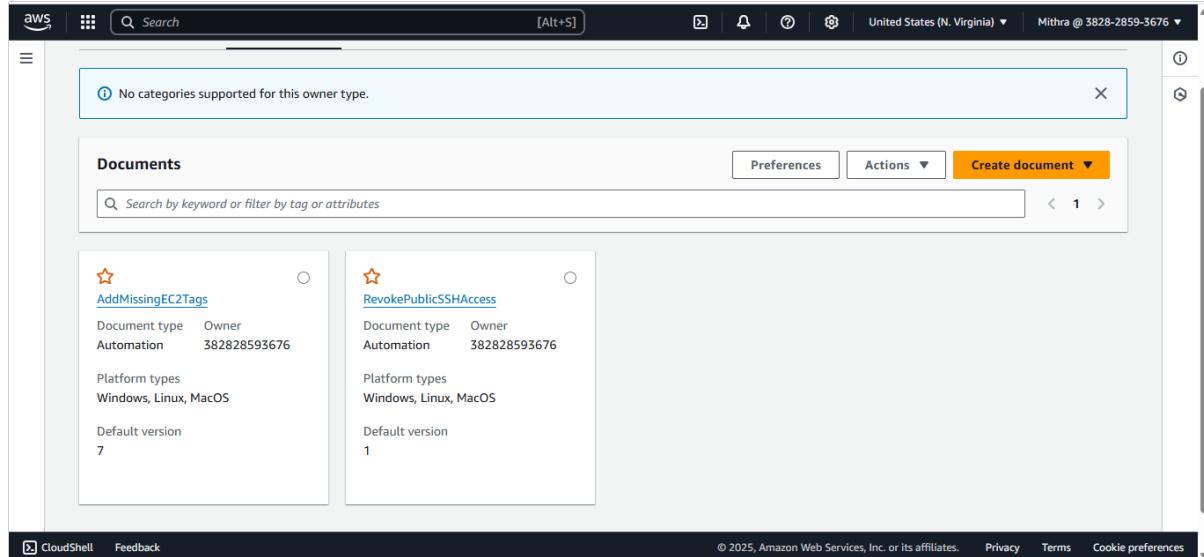
The 'Input template' section contains the following JSON:

```
1 {
2   "AutomationAssumeRole": "arn:aws:iam::382828593676:role/SSMAutomationExecutor",
3   "SecurityGroupId": "<resourceId>"
4 }
5
```

## Step 5: Create the Custom SSM document for auto remediation



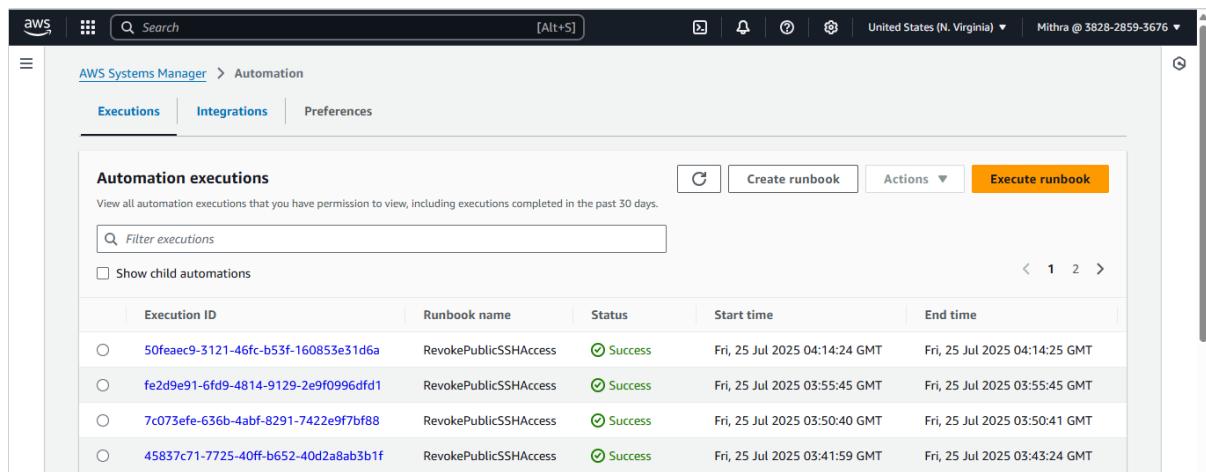
```
1 description: Remediate Security Group ingress from 0.0.0.0/0 on port 22
2 schemaVersion: '0.3'
3 assumeRole: '{{ AutomationAssumeRole }}'
4 parameters:
5   AutomationAssumeRole:
6     type: String
7     description: (Required) IAM Role ARN to assume for remediation
8   SecurityGroupId:
9     type: String
10    description: (Required) The ID of the security group
11  mainSteps:
12    - name: RevokePublicSSHAcess
13      action: aws:executeAwsApi
14      inputs: true
15      inputs:
16        Service: ec2
17        Api: RevokeSecurityGroupIngress
18        GroupId: '{{ SecurityGroupId }}'
19        IpPermissions:
20          - IpProtocol: tcp
21            FromPort: 22
22            ToPort: 22
23            IpRanges:
24              - CidrIp: 0.0.0.0/0
25
```



No categories supported for this owner type.

Documents	Actions	Create document	
<a href="#">AddMissingEC2Tags</a> Document type Owner Automation 382828593676 Platform types Windows, Linux, MacOS Default version 7	<a href="#">Preferences</a>	<a href="#">Actions</a>	<a href="#">Create document</a>
<a href="#">RevokePublicSSHAcess</a> Document type Owner Automation 382828593676 Platform types Windows, Linux, MacOS Default version 1	<a href="#">Preferences</a>	<a href="#">Actions</a>	<a href="#">Create document</a>

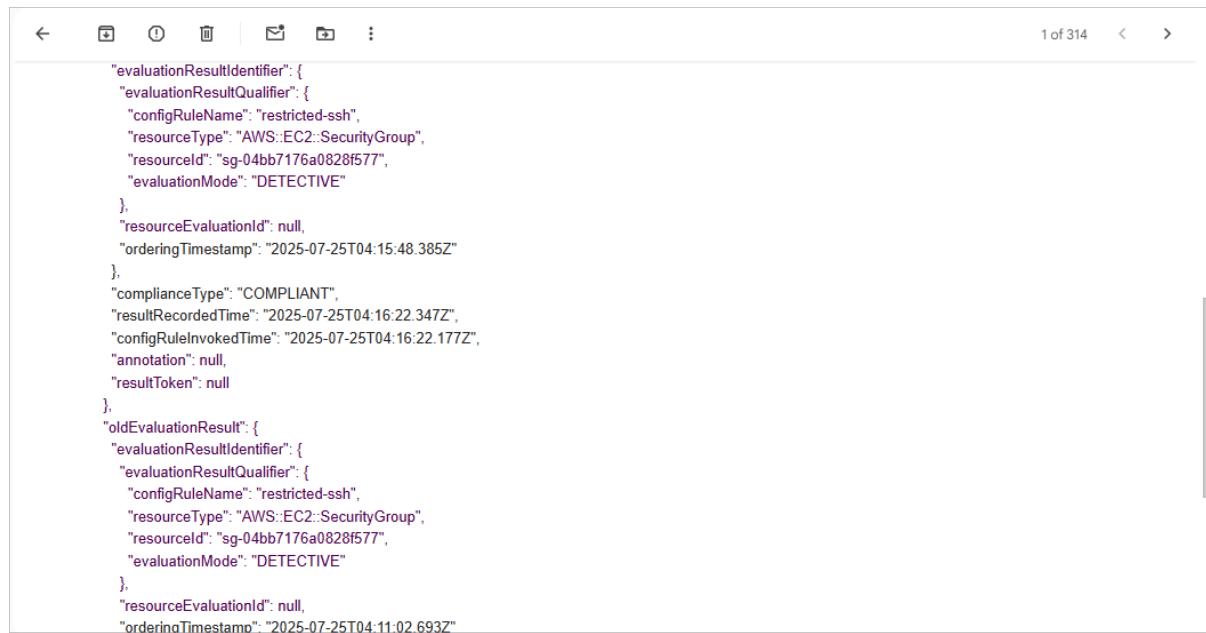
Step 6: Now the SSH public access will get removed and the config rule will move it to COMPLIANT



The screenshot shows the AWS Systems Manager Automation executions page. At the top, there's a navigation bar with the AWS logo, a search bar, and account information for 'United States (N. Virginia)' and 'Mithra @ 3828-2859-3676'. Below the navigation is a breadcrumb trail: AWS Systems Manager > Automation. The main content area has tabs for 'Executions' (selected), 'Integrations', and 'Preferences'. A large heading 'Automation executions' is followed by a sub-header: 'View all automation executions that you have permission to view, including executions completed in the past 30 days.' There's a 'Filter executions' input field and a pagination control showing page 1 of 2. A checkbox for 'Show child automations' is checked. A table lists four automation executions:

Execution ID	Runbook name	Status	Start time	End time
50feac9-3121-46fc-b53f-160853e31d6a	RevokePublicSSHAcess	Success	Fri, 25 Jul 2025 04:14:24 GMT	Fri, 25 Jul 2025 04:14:25 GMT
fe2d9e91-6fd9-4814-9129-2e9f0996dfd1	RevokePublicSSHAcess	Success	Fri, 25 Jul 2025 03:55:45 GMT	Fri, 25 Jul 2025 03:55:45 GMT
7c073efe-636b-4abf-8291-7422e9f7bf88	RevokePublicSSHAcess	Success	Fri, 25 Jul 2025 03:50:40 GMT	Fri, 25 Jul 2025 03:50:41 GMT
45837c71-7725-40ff-b652-40d2a8ab3b1f	RevokePublicSSHAcess	Success	Fri, 25 Jul 2025 03:41:59 GMT	Fri, 25 Jul 2025 03:43:24 GMT

At the bottom right of the table are 'Actions' and 'Execute runbook' buttons.



The screenshot shows a detailed view of a CloudTrail event. At the top, there are standard browser controls (back, forward, refresh, etc.) and a page number '1 of 314'. The main content is a JSON-formatted log entry:

```
{
  "evaluationResultIdentifier": {
    "evaluationResultQualifier": {
      "configRuleName": "restricted-ssh",
      "resourceType": "AWS::EC2::SecurityGroup",
      "resourceId": "sg-04bb7176a0828f577",
      "evaluationMode": "DETECTIVE"
    },
    "resourceEvaluationId": null,
    "orderingTimestamp": "2025-07-25T04:15:48.385Z"
  },
  "complianceType": "COMPLIANT",
  "resultRecordedTime": "2025-07-25T04:16:22.347Z",
  "configRuleInvokedTime": "2025-07-25T04:16:22.177Z",
  "annotation": null,
  "resultToken": null
},
"oldEvaluationResult": {
  "evaluationResultIdentifier": {
    "evaluationResultQualifier": {
      "configRuleName": "restricted-ssh",
      "resourceType": "AWS::EC2::SecurityGroup",
      "resourceId": "sg-04bb7176a0828f577",
      "evaluationMode": "DETECTIVE"
    },
    "resourceEvaluationId": null,
    "orderingTimestamp": "2025-07-25T04:11:02.693Z"
  }
}
```

The screenshot shows the AWS EC2 Security Groups console. On the left, a navigation sidebar includes sections for Images, Elastic Block Store, Network & Security, and Load Balancing. The main content area displays the details of a security group named "sg-04bb7176a0828f577 - default". The "Details" section shows the security group name, ID, owner, and VPC ID. Below this, tabs for Inbound rules, Outbound rules, Sharing, VPC associations, and Tags are present. The Inbound rules table lists one rule: "sgr-09bf5a1c0976ac949" (Security group rule ID), IPv4 (IP version), HTTP (Type), TCP (Protocol), and port 80. The footer contains links for CloudShell, Feedback, and various AWS terms.

The screenshot shows the AWS Config Rules console. The left sidebar includes sections for Dashboard, Conformance packs, Rules, Resources, Aggregators, Compliance Dashboard, Conformance packs, Rules, Inventory Dashboard, Resources, Authorizations, Advanced queries, Settings, and What's new. The main content area shows the "Rules" page with a table of rules. The table columns are Name, Remediation action, Type, Enabled evaluation..., and Detective compliance. Two rules are listed: "ec2\_required-tags" (Remediation action: AddMissingEC2Tags, Type: AWS managed, Detective: DETECTIVE, Status: Noncompliant) and "restricted-ssh" (Remediation action: RevokePublicSSHAccess, Type: AWS managed, Detective: DETECTIVE, Status: Compliant). A "Filter by compliance status" dropdown is set to "All". The footer contains links for Documentation, CloudShell, Feedback, and various AWS terms.

## S3 Bucket Public Access Blocked

- Resource Type: AWS::S3::Bucket
- Flow:
  - AWS Config managed rule detects non-compliance
  - EventBridge rule triggers Lambda function

- o Lambda writes to CloudWatch Logs

Step 1: Create AWS config rule with custom lambda function and default all the buckets will have public access enabled , so the config rule is COMPLIANT

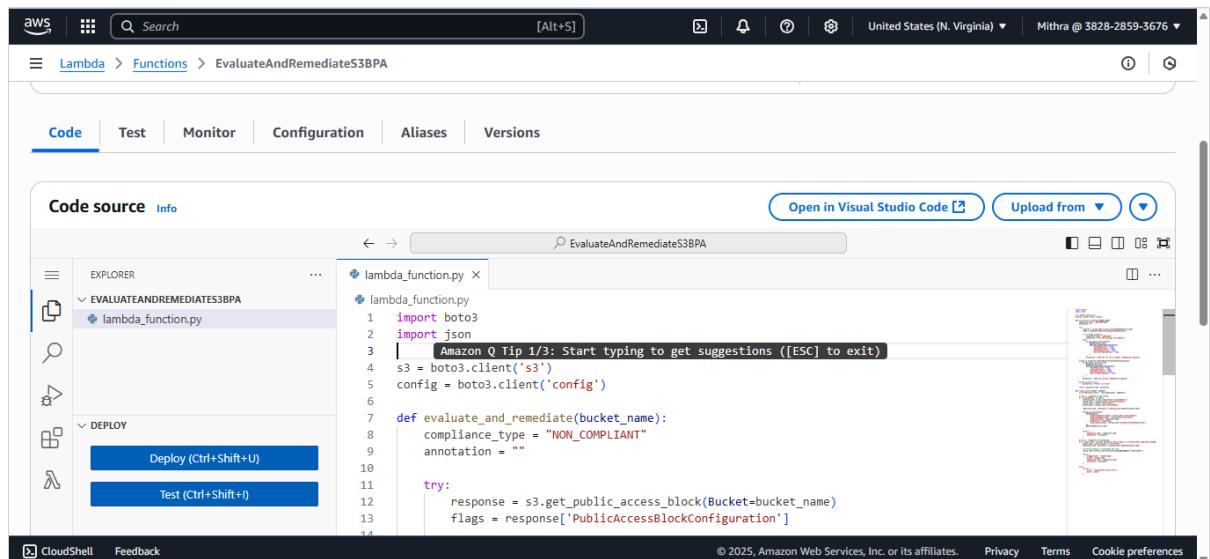
The screenshot shows the AWS Config Rules page. On the left, there's a sidebar with navigation links like Dashboard, Conformance packs, Rules (which is selected), Resources, Aggregators, and more. The main content area is titled "Rules" and contains a table of rules. The table has columns for Name, Remediation action, Type, Enabled evaluation..., and Detective compliance. There are two rows:

Name	Remediation action	Type	Enabled evaluation...	Detective compliance
restricted-ssh	Not set	AWS managed	DETECTIVE	-
s3bucketBPA	Not set	Custom Lambda	DETECTIVE	Compliant

The screenshot shows the details for the s3bucketBPA rule. At the top, it says "1:382828593676:config-rule/config-rule-a05qpk" and "July 27, 2025 12:12 AM". To the right, it lists "Scope of changes", "Resources", and "Resource types S3 Bucket". Below this, there's a section titled "Resources in scope" with a table. The table has columns for ID, Type, Status, Annotation, and Compliance. It lists five S3 buckets, all of which are marked as "Compliant".

ID	Type	Status	Annotation	Compliance
aws-cloudtrail-logs-38...	S3 Bucket	-	All BPA settings are en...	Compliant
config-bucket-382828...	S3 Bucket	-	All BPA settings are en...	Compliant
elasticbeanstalk-us-ea...	S3 Bucket	-	All BPA settings are en...	Compliant
lambda triggers 3 bucke...	S3 Bucket	-	All BPA settings are en...	Compliant
myncplbucke encryptio...	S3 Bucket	-	All BPA settings are en...	Compliant

## Step 2: Create the Lambda function for Evaluating AWS config rule



The screenshot shows the AWS Lambda console interface. In the top navigation bar, the path is Lambda > Functions > EvaluateAndRemediateS3BPA. Below the navigation, there are tabs for Code, Test, Monitor, Configuration, Aliases, and Versions. The Code tab is selected. The main area is titled "Code source" and contains an "Info" tab. On the left, there's an "EXPLORER" sidebar with a tree view showing a folder named "EVALUATEANDREMEDIES3BPA" containing a file "lambda\_function.py". Below the tree, there are "DEPLOY" buttons for "Deploy (Ctrl+Shift+U)" and "Test (Ctrl+Shift+I)". On the right, the code editor displays the following Python script:

```
lambda_function.py
import boto3
import json
s3 = boto3.client('s3')
config = boto3.client('config')
def evaluate_and_remediate(bucket_name):
    compliance_type = "NON_COMPLIANT"
    annotation = ""
try:
    response = s3.get_public_access_block(Bucket=bucket_name)
    flags = response['PublicAccessBlockConfiguration']
```

Below the code editor, a large preview window shows the full code for "lambda\_function.py". The code is identical to the one above, but it includes additional lines 14 through 22, which are partially visible at the bottom of the editor.

```
4 s3 = boto3.client('s3')
5 config = boto3.client('config')
6
7 def evaluate_and_remediate(bucket_name):
8     compliance_type = "NON_COMPLIANT"
9     annotation = ""
10
11     try:
12         response = s3.get_public_access_block(Bucket=bucket_name)
13         flags = response['PublicAccessBlockConfiguration']
14
15         if all(flags.values()):
16             compliance_type = "COMPLIANT"
17             annotation = "All BPA settings are enabled."
18         else:
19             s3.put_public_access_block(
20                 Bucket=bucket_name,
21                 PublicAccessBlockConfiguration={
```

Step 3: create Eventbridge rule will trigger when AWS config rule become NON-Compliant and choose the target as lambda function

The screenshot shows the AWS EventBridge Rules page. A rule named "TriggerRemediationOnNonCompliance" is selected. The "Event pattern" tab is active, displaying the following JSON code:

```
1 {
2   "source": ["aws.config"],
3   "detail-type": ["Config Rules Compliance Change"],
4   "detail": {
5     "configRuleName": ["s3bucketBPA"],
6     "newEvaluationResult": {
7       "complianceType": ["NON_COMPLIANT"]
8     }
9   }
10 }
```

A "Copy" button is located below the event pattern code.

The screenshot shows the AWS EventBridge Rules page. The same rule "TriggerRemediationOnNonCompliance" is selected. The "Targets" tab is active, showing a single target:

Details	Target Name	Type	ARN	Input	Role
EvaluateAndRemediateS3BPA	EvaluateAndRemediateS3BPA	Lambda function	arn:aws:lambda:us-east-1:382828593676:function:EvaluateAndRemediateS3BPA	Matched event	Amazon_EventBridge_Invoke_Lambda_923332369

Below the table, there are input fields for "Input to target" (set to "Matched event"), "Additional parameters" (set to "--"), and "Dead-letter queue (DLQ)" (set to "-").

Step 4: Now test the full flow by disabling the S3 public access

Amazon S3 > Buckets > lambdatrigger3bucket-ncpl1 > Edit Block public access (bucket settings)

**Block public access (bucket settings)**

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

**Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

**Cancel** **Save changes**

Amazon S3 > Buckets > lambdatrigger3bucket-ncpl1

**Block public access (bucket settings)**

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

**Block all public access**  
⚠ Off  
► Individual Block Public Access settings for this bucket

**Bucket policy**

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

No policy to display.

**Edit** **Delete** **Copy**

© 2025, Amazon Web Services, Inc. or its affiliates. **Privacy** **Terms** **Cookie preferences**

Step 5: Now the config rule become NON-COMPLIANT

Primary	Promotions	Social	Updates
□ ★ AWS Notifications 4	[AWS Config:us-east-1] Config Rules Evaluation Started for Account 382828593676 - { "awsAcc...		
□ ★ AWS Notifications 2	[AWS Config:us-east-1] AWS::S3::Bucket lambdatriggers3bucket-ncpl1 is NON_COMPLIANT wi...		
□ ★ AWS Notifications 2	[AWS Config:us-east-1] AWS::S3::Bucket lambdatriggers3bucket-ncpl1 Updated in A... <span style="float: right;">[ ] [ ]</span>		

```

    "configRuleName": "s3bucketBPA",
    "resourceType": "AWS::S3::Bucket",
    "resourceId": "lambdatriggers3bucket-ncpl1",
    "evaluationMode": "DETECTIVE"
},
"resourceEvaluationId": null,
"orderingTimestamp": "2025-07-27T04:25:38.000Z"
},
"complianceType": "NON_COMPLIANT",
"resultRecordedTime": "2025-07-27T04:26:11.438Z",
"configRuleInvokedTime": "2025-07-27T04:26:09.787Z",
"annotation": "BPA was not fully enabled. Remediation applied.",
"resultToken": null
},
"oldEvaluationResult": {
    "evaluationResultIdentifier": {
        "evaluationResultQualifier": {

```

Step 6: Now we can see the public access got enabled after auto remediation

Amazon S3

General purpose buckets

Directory buckets

Table buckets

Vector buckets [Preview](#)

Access Grants

Access Points (General Purpose Buckets, FSx file systems)

Access Points (Directory Buckets)

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

CloudShell Feedback

Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#). [View analyzer for us-east-1](#)

Block public access (bucket settings)

Block all public access

On

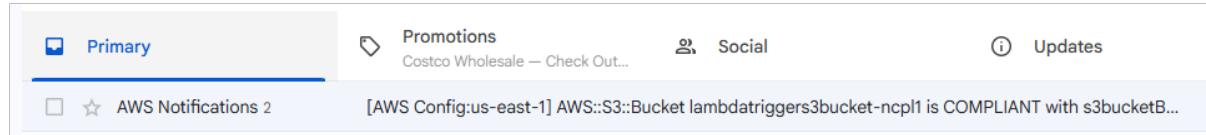
Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts.

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 7: Now we can see the config rule become COMPLIANT



Primary

Promotions

Social

Updates

AWS Notifications 2

[AWS Config:us-east-1] AWS::S3::Bucket lambdatriggers3bucket-ncpl1 is COMPLIANT with s3bucketB...

The screenshot shows an email from AWS Config containing two JSON objects representing evaluation results. The first object is for a configuration rule named 's3bucketBPA' on an AWS::S3::Bucket resource. It includes details like the evaluation mode (DETECTIVE), ordering timestamp, and annotation stating 'All BPA settings are enabled.' The second object is for the same rule on the same resource, with a slightly different ordering timestamp.

```

{
  "evaluationResultIdentifier": {
    "evaluationResultQualifier": {
      "configRuleName": "s3bucketBPA",
      "resourceType": "AWS::S3::Bucket",
      "resourceId": "lambda triggers 3 bucket-ncpl1",
      "evaluationMode": "DETECTIVE"
    },
    "resourceEvaluationId": null,
    "orderingTimestamp": "2025-07-27T02:45:18.000Z"
  },
  "complianceType": "COMPLIANT",
  "resultRecordedTime": "2025-07-27T02:45:49.183Z",
  "configRuleInvokedTime": "2025-07-27T02:45:48.910Z",
  "annotation": "All BPA settings are enabled.",
  "resultToken": null
},
{
  "oldEvaluationResult": {
    "evaluationResultIdentifier": {
      "evaluationResultQualifier": {
        "configRuleName": "s3bucketBPA",
        "resourceType": "AWS::S3::Bucket",
        "resourceId": "lambda triggers 3 bucket-ncpl1",
        "evaluationMode": "DETECTIVE"
      },
      "resourceEvaluationId": null,
      "orderingTimestamp": "2025-07-26T01:22:58.000Z"
    }
  }
}

```

The screenshot shows the AWS Config Rules page. The left sidebar navigation bar includes links for Dashboard, Conformance packs, Rules (which is selected and highlighted in blue), Resources, Aggregators, Compliance Dashboard, Conformance packs, Rules, Inventory Dashboard, Resources, Authorizations, Advanced queries (with a preview link), Settings, and What's new. The main content area displays a table of rules. The table has columns for Name, Remediation action, Type, Enabled evaluation status, and Detective compliance status. Two rules are listed: 'restricted-ssh' (Type: AWS managed, Detective compliance: -) and 's3bucketBPA' (Type: Custom Lambda, Detective compliance: Compliant). A filter dropdown at the top of the table is set to 'All'. Action buttons include View details, Edit rule, Actions (with a dropdown arrow), and Add rule.

Name	Remediation action	Type	Enabled evaluation...	Detective compliance
restricted-ssh	Not set	AWS managed	DETECTIVE	-
s3bucketBPA	Not set	Custom Lambda	DETECTIVE	Compliant

Step 8: CloudWatch logs also captured with lambda function

Screenshot of the AWS CloudWatch Log streams page. The left sidebar shows 'CloudWatch' and 'AI Operations'. The main area displays 'Log streams (9)' with a search bar and filter options. One log stream is listed:

Log stream	Last event time
2025/07/26/[LATEST]bb4929f1a21b4e2ab5f74610790782d9	2025-07-27 00:26:15 (UTC-04:00)

Screenshot of the AWS CloudWatch Log events page. The left sidebar shows 'CloudWatch', 'AI Operations' (with 'Overview' selected), 'Logs', 'Log groups', and 'Log Anomalies'. The main area displays 'Log events' with a search bar and filter options. Events are listed by timestamp:

Timestamp	Message
2025-07-27T00:26:10.020-04:00	INIT_START Runtime Version: python:3.13.v50 Runtime Version ARN: arn:aws:lambda:us-east-1::runtime:83a0b2...
2025-07-27T00:26:10.463-04:00	START RequestId: 8f9c1eb8-9f02-491a-b00f-262a0dbf809c Version: \$LATEST
2025-07-27T00:26:10.464-04:00	Received event: {

Screenshot of the AWS CloudTrail Event history page. The left sidebar shows 'CloudTrail', 'Event history' (selected), 'Lake', 'Trails', and 'Settings'. The main area displays 'Event history (50+)' with a search bar and filter options. Events are listed by event name and time:

Event name	Event time	User name
PutEvaluations	July 27, 2025, 00:28:16 (UTC-04:00)	EvaluateAndRemediateS3BPA
PutEvaluations	July 27, 2025, 00:26:50 (UTC-04:00)	EvaluateAndRemediateS3BPA
PutEvaluations	July 27, 2025, 00:26:47 (UTC-04:00)	EvaluateAndRemediateS3BPA
PutEvaluations	July 27, 2025, 00:26:45 (UTC-04:00)	EvaluateAndRemediateS3BPA
PutEvaluations	July 27, 2025, 00:26:44 (UTC-04:00)	EvaluateAndRemediateS3BPA
PutEvaluations	July 27, 2025, 00:26:42 (UTC-04:00)	EvaluateAndRemediateS3BPA
CreateLogStream	July 27, 2025, 00:26:17 (UTC-04:00)	EvaluateAndRemediateS3BPA

# CloudTrail Logging Compliance

- Resource Type: AWS::CloudTrail::Trail
- Flow:
  - AWS Config Rule (Lambda evaluation)
  - Detects non-compliance
  - EventBridge triggers SSM Automation
  - Logs actions to CloudWatch Logs and CloudTrail Logs

Step 1: Create Cloud trail and provide name as "TestTrail"

The screenshot shows the AWS CloudTrail Trails page. On the left, there's a navigation sidebar with options like Dashboard, Event history, Insights, Lake, and Trails. The 'Trails' section is selected. The main area is titled 'Trails' and contains a table with the following data:

Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	Cloud Watch Logs log group	Status
TestTrail	US East (N. Virginia)	Yes	arn:aws:cloudtrail:us-east-1:382828593676:trail/TestTrail	Disabled	No	aws-cloudtrail-logs-382828593676-ed40fb43	-	-	Logging

At the top right of the table, there are buttons for 'Copy events to Lake', 'Delete', and 'Create trail'. The status column for the 'TestTrail' row shows 'Logging' with a green checkmark.

Step 3: Create AWS config rule with custom lambda function and it will become COMPLIANT

The screenshot shows the AWS Config console with a modal dialog titled "Enable CloudTrail Logging". The dialog contains parameters for the remediation task:

Key	Value	Description
AutomationAssumeRole	arn:aws:iam::382828593676:role/SSMAutomationExecutionRole	(Required) The ARN of the role that allows Automation to assume it.
TrailName	TestTrail	(Required) The name of the CloudTrail trail to remediate.

Below the parameters, there is a section titled "Resources in scope" which lists two resources:

ID	Type	Status	Annotation	Compliance
TestTrail	CloudTrail Trail	<span>✓ Action executed successfully</span>	CloudTrail logging is enabled	<span>Compliant</span>
arn:aws:cloudtrail:us-east-1:...	CloudTrail Trail	-	Logging enabled	<span>Compliant</span>

Step 4: Now create Eventbridge rule and choose target as SSM for Automatic remediation

The screenshot shows the "Event pattern" tab of an AWS Lambda function configuration. The event pattern is defined as follows:

```
1 {
2   "source": ["aws.config"],
3   "detail-type": ["Config Rules Compliance Change"],
4   "detail": {
5     "newEvaluationResult": {
6       "complianceType": ["NON_COMPLIANT"]
7     },
8     "configRuleName": ["cloudtrailcompliancetrigger"]
9   }
10 }
```

Below the event pattern, there is a "Copy" button.

The screenshot shows the 'Targets' tab selected in the CloudWatch Events console. A single target, 'EnableCloudTrailLogging', is listed. The target is of type 'Systems Manager Automation' and uses an 'Input transformer'. It is associated with a role named 'Amazon\_EventBridge\_Invoke\_Start\_Automation\_Execution\_1743623051'. Below the table, there are sections for 'Input to target', 'Additional parameters', and 'Dead-letter queue (DLQ)'.

## Step 5: Create SSM runbook for automatic remediation

The screenshot shows the 'Content' tab of an AWS Systems Manager Automation document named 'EnableCloudTrailLogging'. The document version is set to '1 (Default)'. The content of the document is a JSON script for enabling CloudTrail logging. The script includes parameters like 'AutomationAssumeRole', 'TrailName', and 'Inputs' which specify the CloudTrail trail name and the API action to start logging.

```

1 schemaVersion: '0.3'
2 description: Starts CloudTrail logging for a given trail name to remediate NON_COMPLIANT status detected by AWS Config.
3 assumeRole: '{{ AutomationAssumeRole }}'
4-
5 parameters:
6   AutomationAssumeRole:
7     type: String
8     description: (Required) The ARN of the role that allows Automation to perform the actions.
9   TrailName:
10    type: String
11    description: (Required) The name of the CloudTrail trail to enable logging.
12  mainSteps:
13    - description: Enables logging for the CloudTrail trail.
14      name: StartCloudTrailLogging
15      action: aws:executeAwsApi
16      isEnd: true
17    inputs:
18      Service: cloudtrail
19      Api: StartLogging
20      Name: '{{ TrailName }}'
21
  
```

## Step 6: Now manually test the CloudTrail by disabling the logging

The screenshot shows the AWS CloudTrail console with the 'Trails' section selected. A single trail, 'TestTrail', is displayed. The 'General details' section shows the following configuration:

Setting	Value
Trail logging	Off
Trail name	TestTrail
Multi-region trail	Yes
Apply trail to my organization	Not enabled
Trail log location	aws-cloudtrail-logs-382828593676-ed40fb43/AWSLogs/382828593676
Last log file delivered	July 28, 2025, 12:05:55 (UTC-04:00)
Log file validation	Disabled
SNS notification delivery	Disabled
Log file SSE-KMS encryption	Not enabled
Last SNS notification	-

The 'CloudWatch Logs' section indicates 'No CloudWatch Logs log groups' and 'CloudWatch Logs is not configured for this trail'. There are 'Edit' buttons for both sections.

The screenshot shows the AWS CloudTrail console with the 'Trails' section selected. The 'Trails' table lists one trail, 'TestTrail', with the following details:

Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	Cloud Watch Logs log group	Status
TestTrail	US East (N. Virginia)	Yes	arn:aws:cloudtrail:us-east-1:382828593676:trail/TestTrail	Disabled	No	aws-cloudtrail-logs-382828593676-ed40fb43	-	-	Off

There are 'Copy events to Lake' and 'Create trail' buttons at the top right of the table area. The bottom of the screen shows standard AWS navigation links like CloudShell and Feedback.

Step 8: Now config rule changed to NON-COMPLIANT

1 of 380 < >

[AWS Config:us-east-1] AWS::CloudTrail::Trail TestTrail is NON\_COMPLIANT with cloudtrailcomplianc... [Inbox](#)

AWS Notifications 1:41 AM (10 hours ago) ☆  
View the Timeline for this Resource in AWS Config Management Console: <https://console.aws.amazon.com/config/home?region=us-east-1#/timeline/AWS::CloudT...>

AWS Notifications 2:24 AM (9 hours ago) ☆  
"resultRecordedTime": "2025-07-28T06:24:00.012Z", "configRuleInvokedTime": "2025-07-28T06:23:57.044Z", "oldEvaluationResult": { "complianceType": "COMPLIANT", "annotation": "CloudTrail logging is disabled." }, "resourceType": "AWS::CloudTrail::Trail", "resourceId": "TestTrail", "evaluationMode": "DETECTIVE", "orderingTimestamp": "2025-07-28T06:24:00.012Z", "complianceType": "NON\_COMPLIANT", "resultRecordedTime": "2025-07-28T16:07:50.466Z", "configRuleInvokedTime": "2025-07-28T16:07:49.725Z", "annotation": "CloudTrail logging is disabled.", "resultToken": null, "oldEvaluationResult": { "evaluationResultIdentifier": { "evaluationResultQualifier": { "configRuleName": "cloudtrailcompliancetrigger", "resourceType": "AWS::CloudTrail::Trail", "resourceId": "TestTrail", "evaluationMode": "DETECTIVE" } }, "resourceEvaluationId": null, "orderingTimestamp": "2025-07-28T04:22:25.000Z" }

AWS Notifications 3:18 AM (8 hours ago) ☆  
"resultRecordedTime": "2025-07-28T07:18:57.905Z", "configRuleInvokedTime": "2025-07-28T07:15:41.424Z", "resultRecordedTime": "2025-07-28T06:52:13.445Z", "complianceType": "NON\_COMPLIANT", "annotation": "CloudTrail logging is disabled.", "resultToken": null, "oldEvaluationResult": { "evaluationResultIdentifier": { "evaluationResultQualifier": { "configRuleName": "cloudtrailcompliancetrigger", "resourceType": "AWS::CloudTrail::Trail", "resourceId": "TestTrail", "evaluationMode": "DETECTIVE" } }, "resourceEvaluationId": null, "orderingTimestamp": "2025-07-28T04:22:25.000Z" }

AWS Notifications 12:07 PM (0 minutes ago) ☆ ☺ ↶ ⋮  
to me  
View the Timeline for this Resource in AWS Config Management Console:  
<https://console.aws.amazon.com/config/home?region=us-east-1#/timeline/AWS::CloudTrail::Trail/TestTrail?time=2025-07-28T04:22:25.000Z>

New Compliance Change Record:

```
{}
```

```
< > ⓘ 🗑️ 📎 📥 ⋮

"resourceType": "AWS::CloudTrail::Trail",
"resourceId": "TestTrail",
"evaluationMode": "DETECTIVE"
},
"resourceEvaluationId": null,
"orderingTimestamp": "2025-07-28T04:22:25.000Z"
},
"complianceType": "NON_COMPLIANT",
"resultRecordedTime": "2025-07-28T16:07:50.466Z",
"configRuleInvokedTime": "2025-07-28T16:07:49.725Z",
"annotation": "CloudTrail logging is disabled.",
"resultToken": null
},
"oldEvaluationResult": {
"evaluationResultIdentifier": {
"evaluationResultQualifier": {
"configRuleName": "cloudtrailcompliancetrigger",
"resourceType": "AWS::CloudTrail::Trail",
"resourceId": "TestTrail",
"evaluationMode": "DETECTIVE"
}
},
"resourceEvaluationId": null,
"orderingTimestamp": "2025-07-28T04:22:25.000Z"
}
```

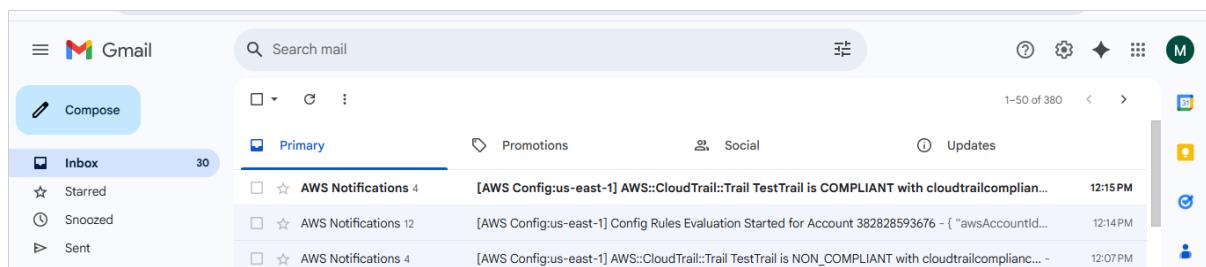
The screenshot shows the AWS Config console. On the left, the navigation pane includes 'Dashboard', 'Conformance packs', 'Rules' (selected), 'Resources', 'Aggregators', 'Compliance Dashboard', 'Conformance packs', 'Rules', 'Inventory Dashboard', 'Resources', 'Authorizations', 'Advanced queries', 'Settings', and 'What's new'. Below these are links for 'Documentation', 'CloudShell', and 'Feedback'. The main content area is titled 'Parameters' and lists two entries: 'AutomationAssumeRole' with value 'arn:aws:iam::382828593676:role/SSMAutomationExecutionRole' and 'TrailName' with value 'TestTrail'. Below this is a section titled 'Resources in scope' with a table showing three CloudTrail trails: 'arn:aws:cloudtrail:us-east-1:123456789012:trail/EC2TagComplianceTrail', 'EC2TagComplianceTrail', and 'TestTrail'. The 'EC2TagComplianceTrail' and 'TestTrail' rows show a status of 'Noncompliant' with a warning icon. The bottom of the page includes copyright information and links for 'Privacy', 'Terms', and 'Cookie preferences'.

Step 9: Now the eventbridge rule will trigger and execute the SSM document

The screenshot shows the AWS Systems Manager Automation console. The top navigation bar includes 'Search' and 'United States (N. Virginia)'. The main content area is titled 'Automation executions' and displays a table of completed executions. The table columns are 'Execution ID', 'Runbook name', 'Status', 'Start time', and 'End time'. Five entries are listed:

Execution ID	Runbook name	Status	Start time	End time
0f9d7bac-673b-49bb-ad09-d9a34a9b3406	EnableCloudTrailLogging	Success	Mon, 28 Jul 2025 16:10:23 GMT	Mon, 28 Jul 2025 16:10:24 GMT
cd9b0807-d99f-43e2-8d02-52e8ed6e6327	EnableCloudTrailLogging	Success	Mon, 28 Jul 2025 16:10:03 GMT	Mon, 28 Jul 2025 16:10:04 GMT
3637716c-6021-4b2d-8bfc-9c16937bc38e	EnableCloudTrailLogging	Success	Mon, 28 Jul 2025 16:04:09 GMT	Mon, 28 Jul 2025 16:04:10 GMT
cbffbecc9-b062-46ba-8d08-62f2685588ac	EnableCloudTrailLogging	Success	Mon, 28 Jul 2025 16:01:03 GMT	Mon, 28 Jul 2025 16:01:04 GMT
0d3bda59-f71b-4b64-af8a-8f0cf234ef24	EnableCloudTrailLogging	Success	Mon, 28 Jul 2025 07:21:33 GMT	Mon, 28 Jul 2025 07:21:34 GMT

Step 10: Now we the config rule changed to COMPLIANT



The screenshot shows the AWS Config console with the following details:

- Left Sidebar (AWS Config)**:
  - Dashboard
  - Conformance packs
  - Rules** (selected)
  - Resources
  - Aggregators
    - Compliance Dashboard
    - Conformance packs
    - Rules
    - Inventory Dashboard
    - Resources
    - Authorizations
  - Advanced queries [Preview](#)
  - Settings
  - What's new- Top Bar**: EnableCloudTrailLogging [Alt+S]
- Central Content Area**:
  - Parameters** table:

Key	Value	Description
AutomationAssumeRole	arn:aws:iam::382828593676:role/SSMAutomationExecutionRole	(Required) The ARN of the role that allows Automation to assume it.
TrailName	TestTrail	(Required) The name of the CloudTrail trail to remediate.
  - Resources in scope** table:

ID	Type	Status	Annotation	Compliance
TestTrail	CloudTrail Trail	<span>✓ Action executed successfully</span>	CloudTrail logging is enabled	<span>Compliant</span>
arn:aws:cloudtrail:us-e...	CloudTrail Trail	-	Logging enabled	<span>Compliant</span>