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

Automation flow diagram

🔄 Automation Flow Diagram

plaintext Copy Edit

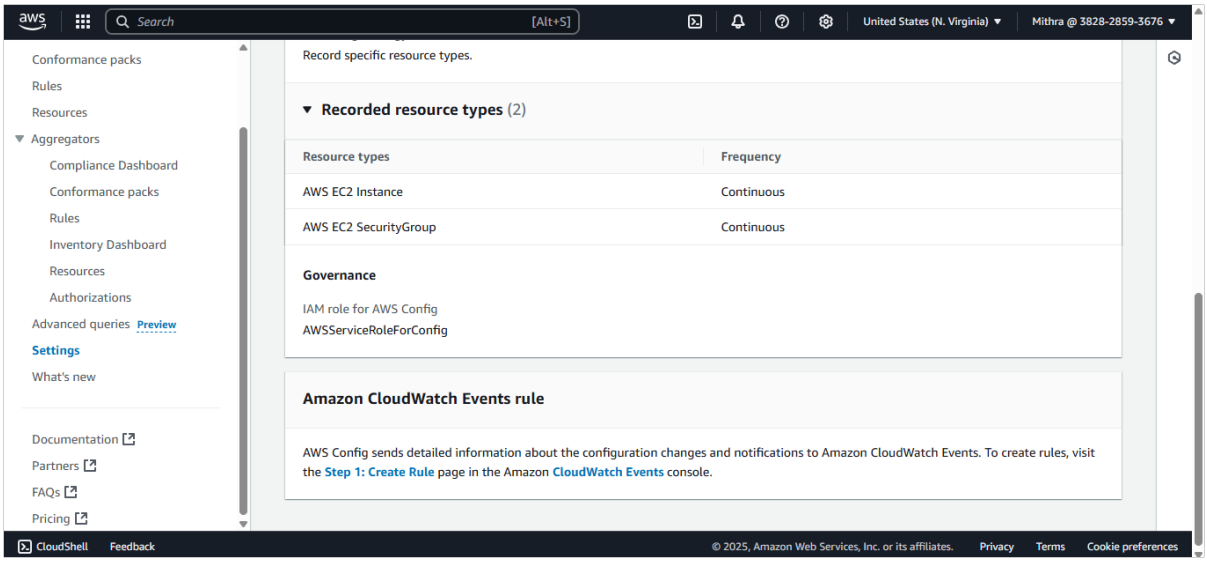
```
AWS Config (rules + recorder)
         |
         ↓
  Detect Non-compliance
         |
         ↓
  Trigger Lambda or SSM Automation
         |
         ↓
   Remediate + Notify via SNS
         |
         ↓
Log in CloudWatch + CloudTrail
```

Step by step Implementation:

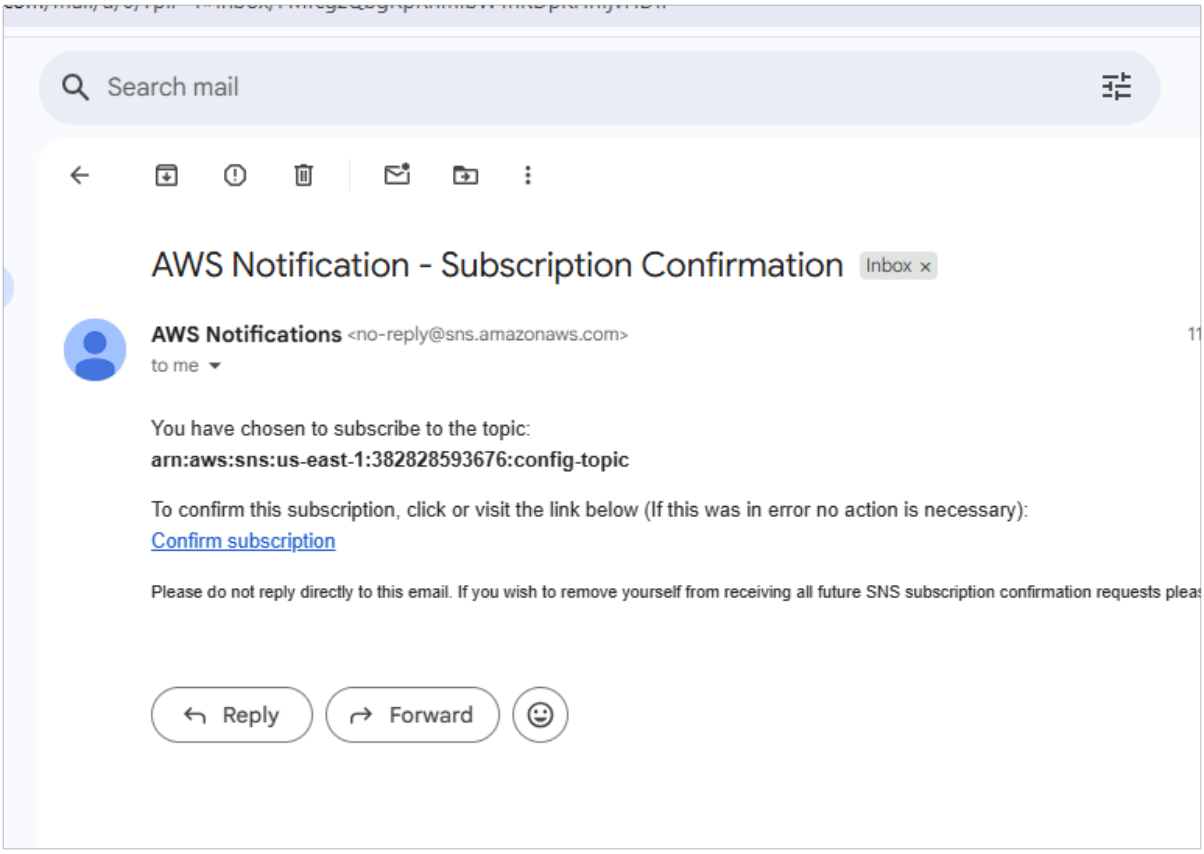
EC2 Required Tags

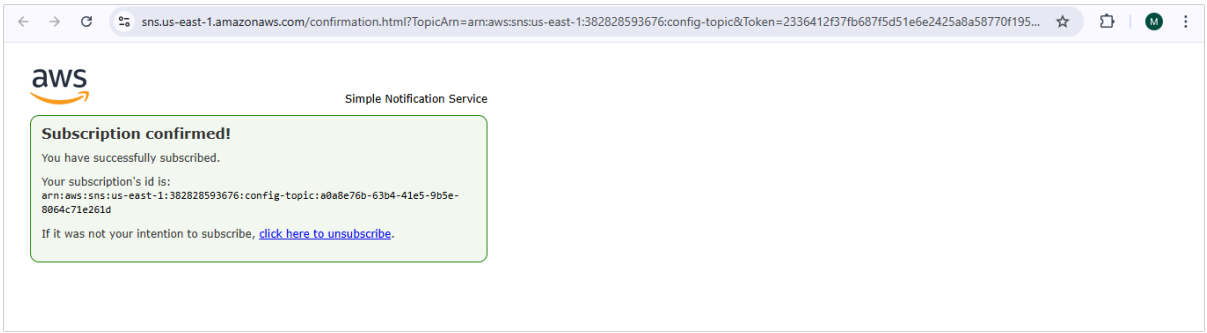
1. Resource Type: `AWS::EC2::Instance`
2. Flow:
    a. AWS Config managed rule detects non-compliance
    b. EventBridge rule triggers SSM Automation to apply missing tags

Step 1: create AWS config record for EC2 tags

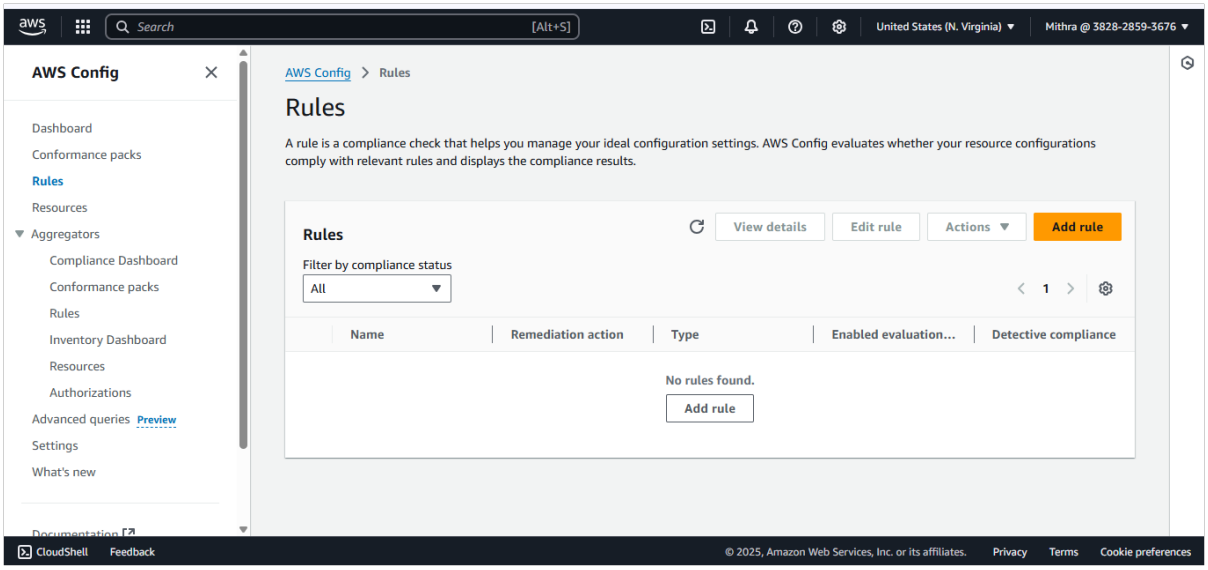


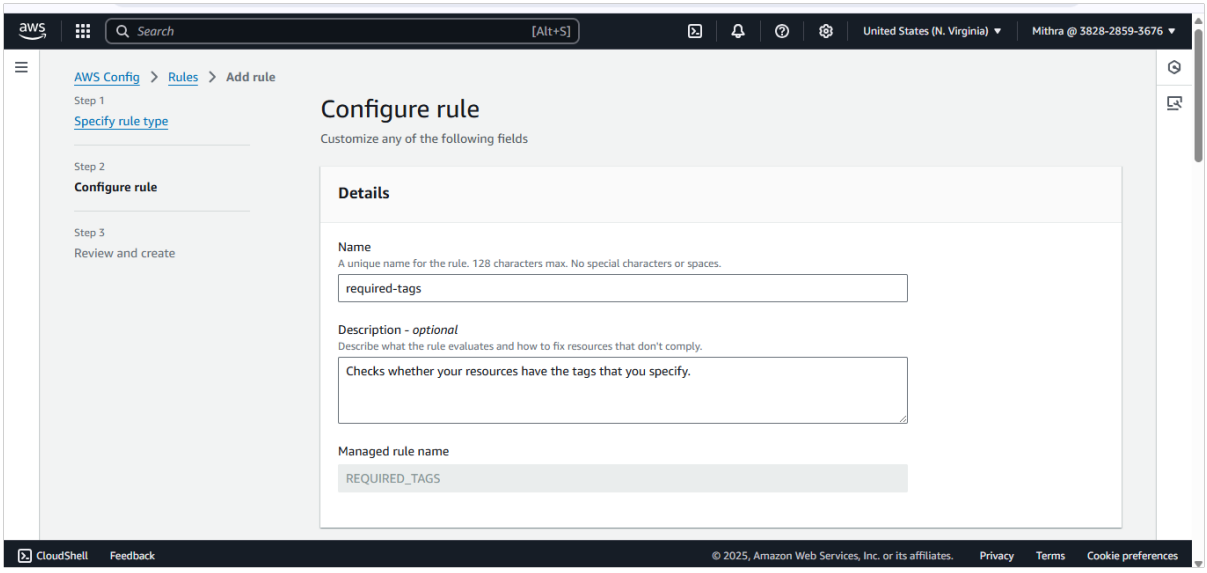
Step 2: SNS notification subscription

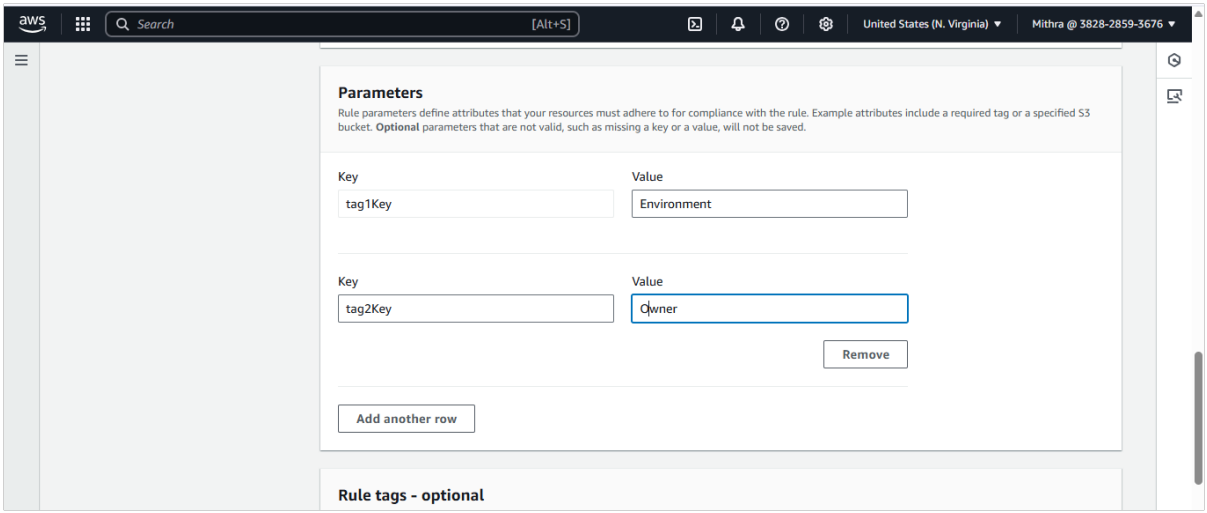

Search mail
AWS Notification - Subscription Confirmation
Inbox ×
AWS Notifications <no-reply@sns.amazonaws.com>
to me
You have chosen to subscribe to the topic:
arn:aws:sns:us-east-1:382828593676:config-topic
To confirm this subscription, click or visit the link below (If this was in error no action 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 pleas
Reply
Forward

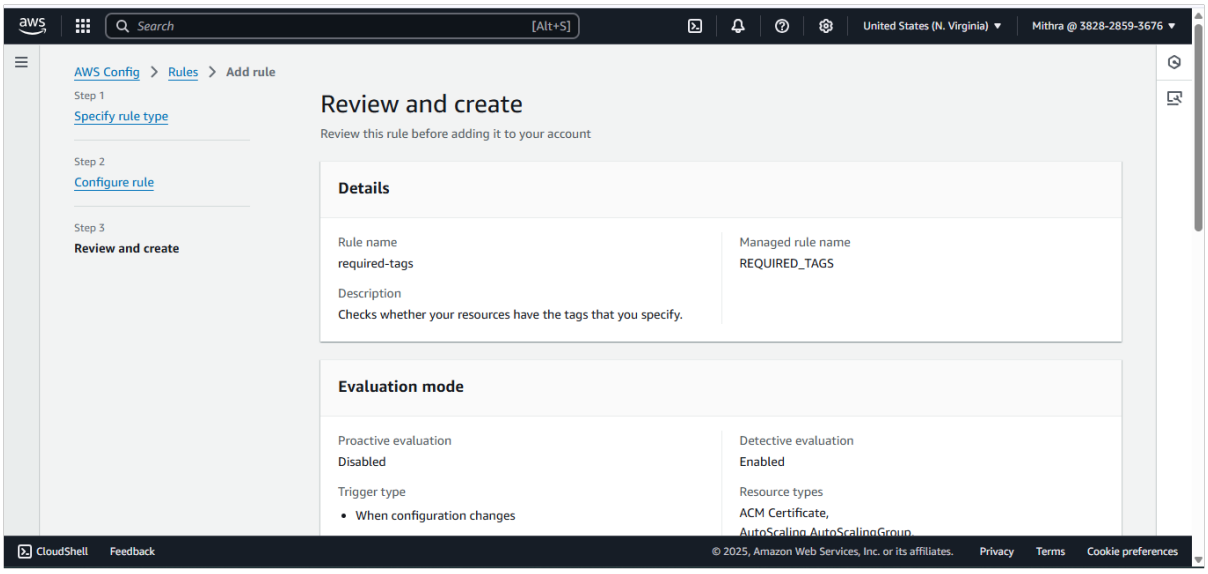

sns.us-east-1.amazonaws.com/confirmation.html?TopicArn=arn:aws:sns:us-east-1:382828593676:config-topic&Token=2336412f37fb687f5d51e6e2425a8a58770f195...
aws
Simple Notification Service
Subscription confirmed!
You have successfully subscribed.
Your subscription's id is:
arn:aws:sns:us-east-1:382828593676:config-topic:a0a8e76b-63b4-41e5-9b5e-8064c71e261d
If it was not your intention to subscribe, click here to unsubscribe.

Step 3: create AWS config rules for EC2 tags

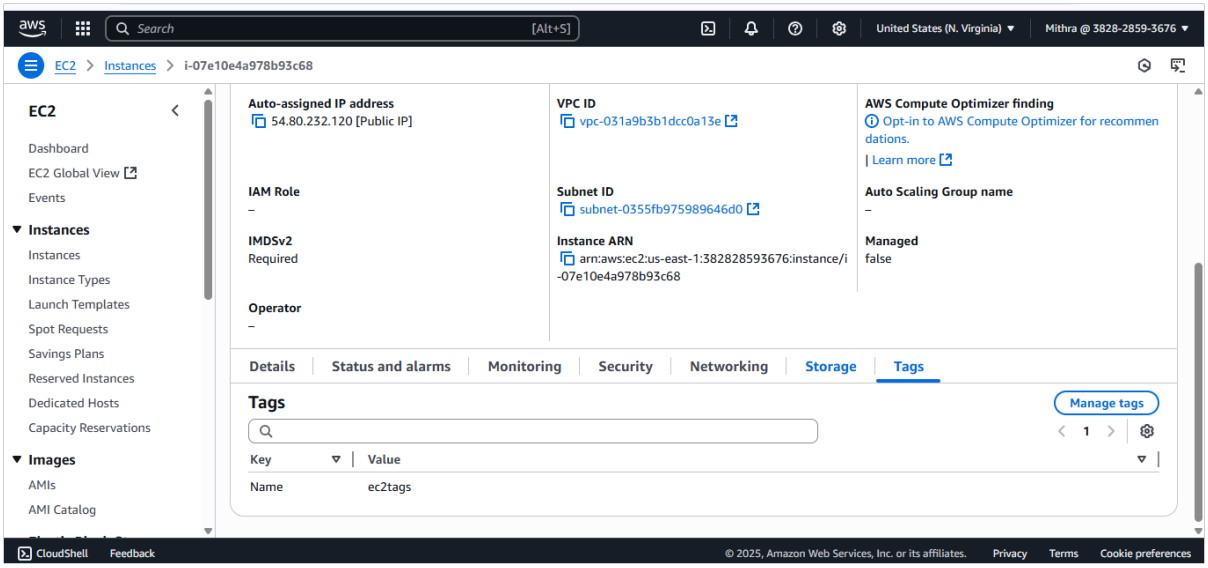


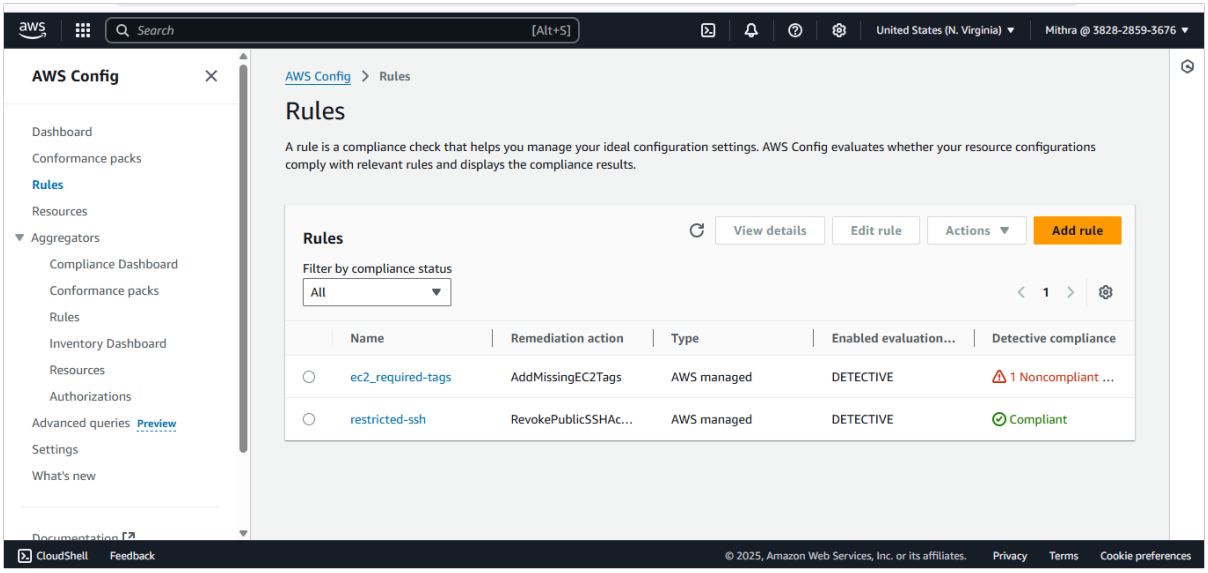


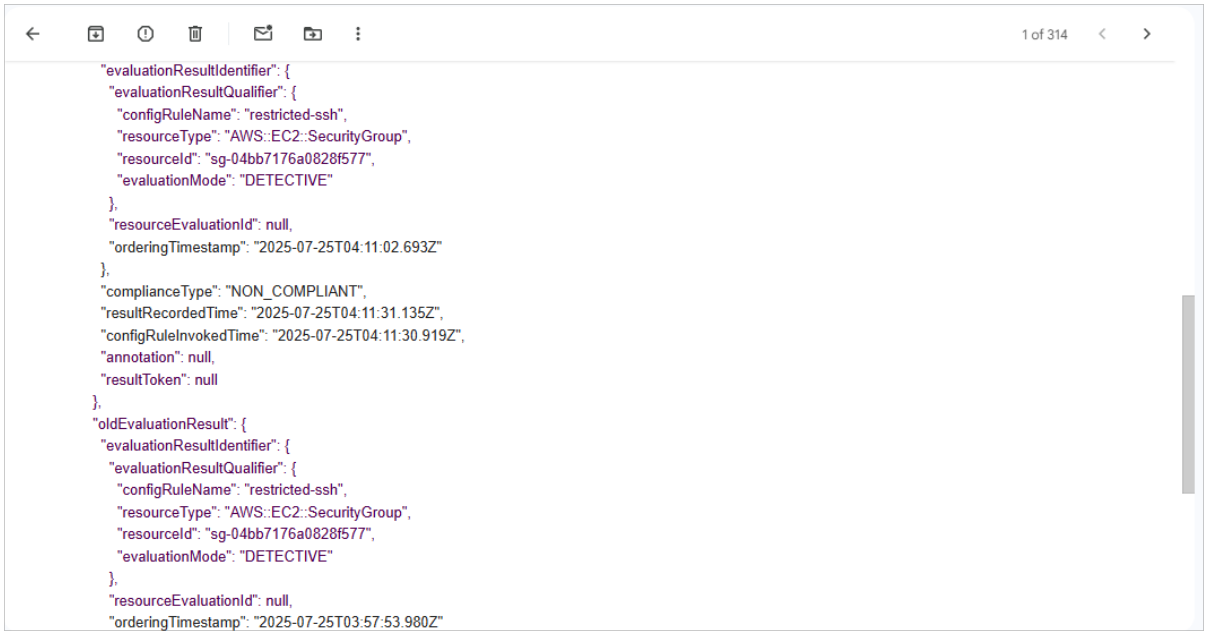

Search
[Alt+S]
United States (N. Virginia)
Mithra @ 3828-2859-3676
Parameters
Rule parameters define attributes that your resources must adhere to for compliance with the rule. Example attributes include a required tag or a specified S3 bucket. Optional parameters that are not valid, such as missing a key or a value, will not be saved.
Key
Value
tag1Key
Environment
Key
Value
tag2Key
Owner
Remove
Add another row
Rule tags - optional


Search
[Alt+S]
United States (N. Virginia)
Mithra @ 3828-2859-3676
AWS Config
Rules
Add rule
Step 1
Specify rule type
Step 2
Configure rule
Step 3
Review and create
Review and create
Review this rule before adding it to your account
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

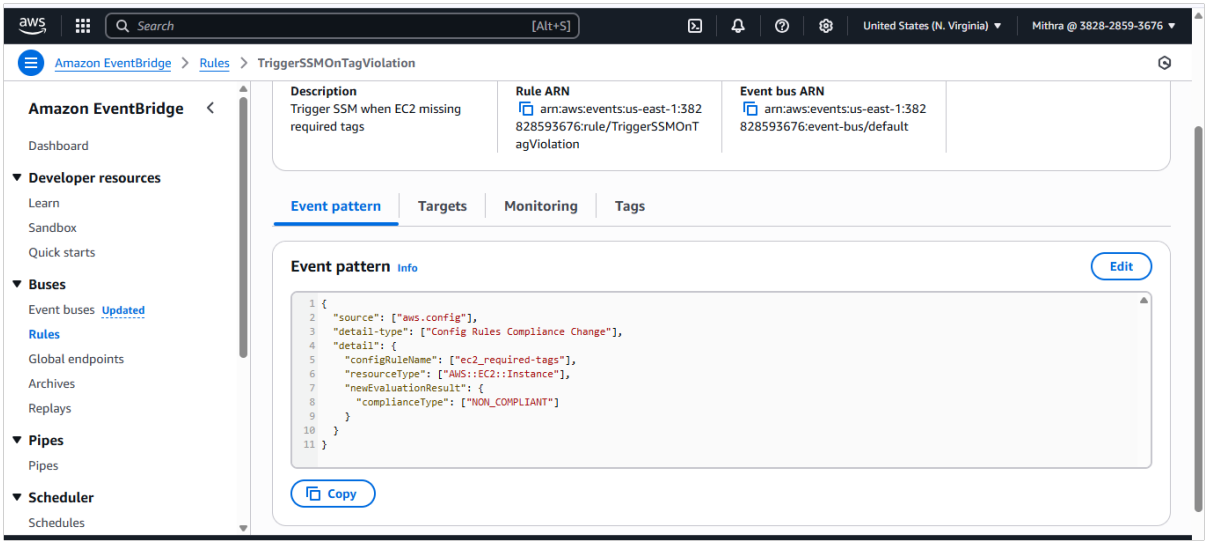
Step 4: by default the EC2 instance don’t have tags(Environment and Owner) so the AWS config rule become NON-COMPLIANT

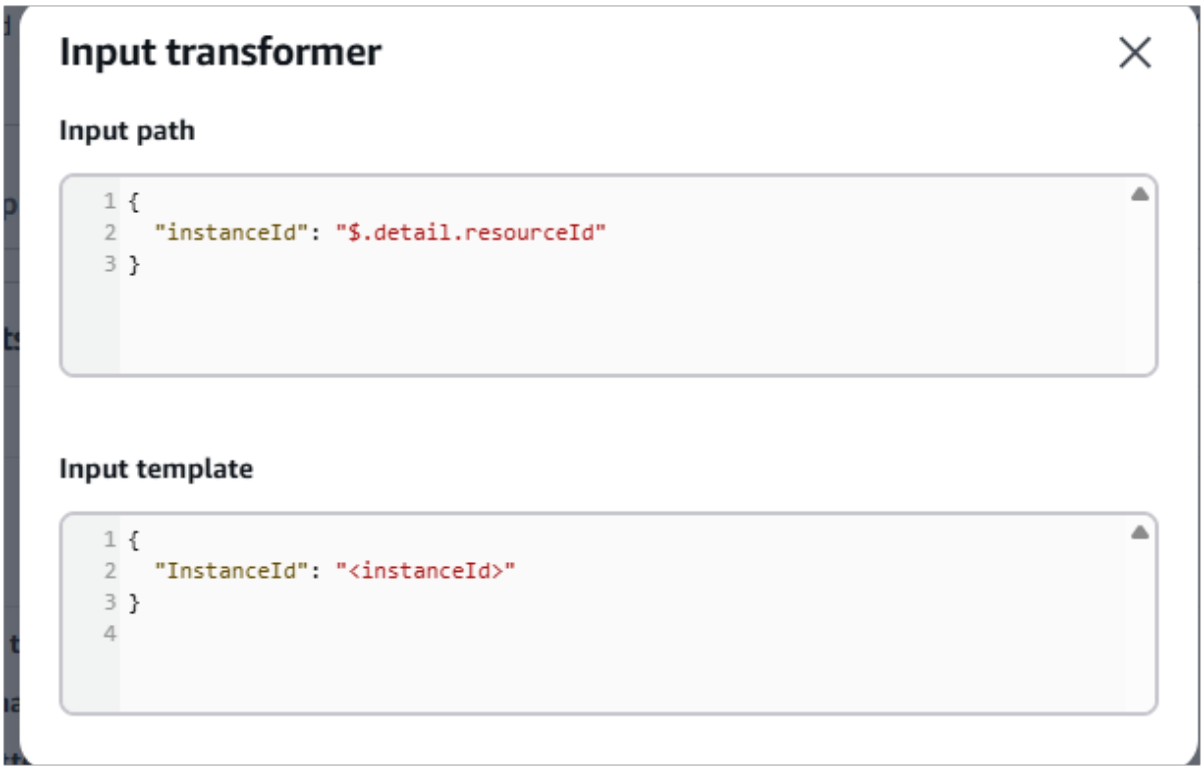




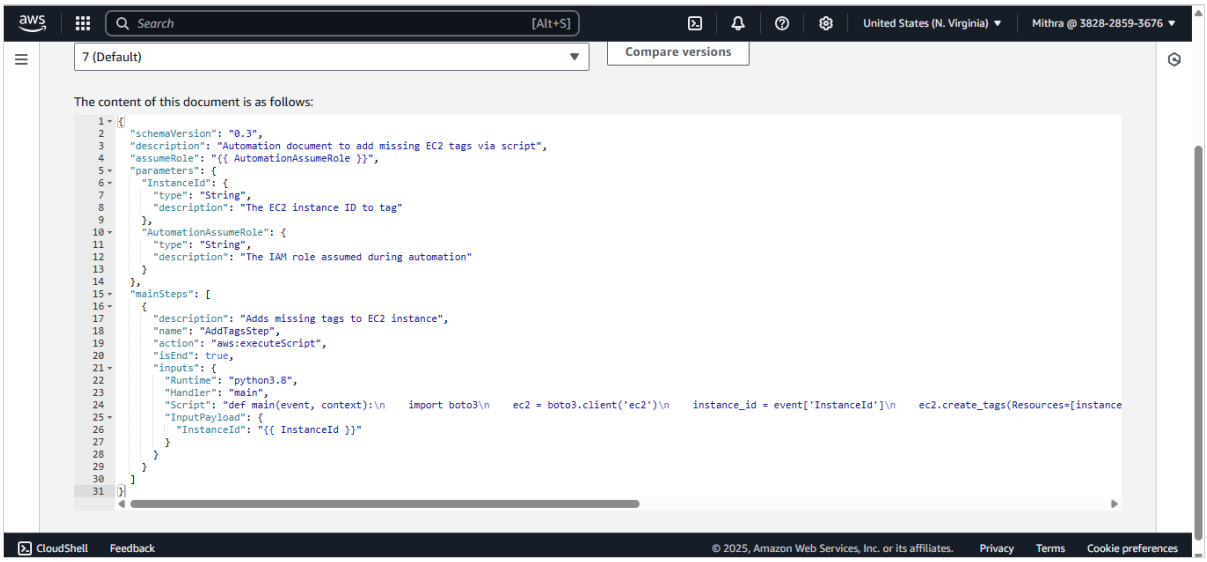


Step 5: Now add the Eventbridge rule to trigger Auto-remediation , so it will trigger when there is change in status to NON-COMPLIANT

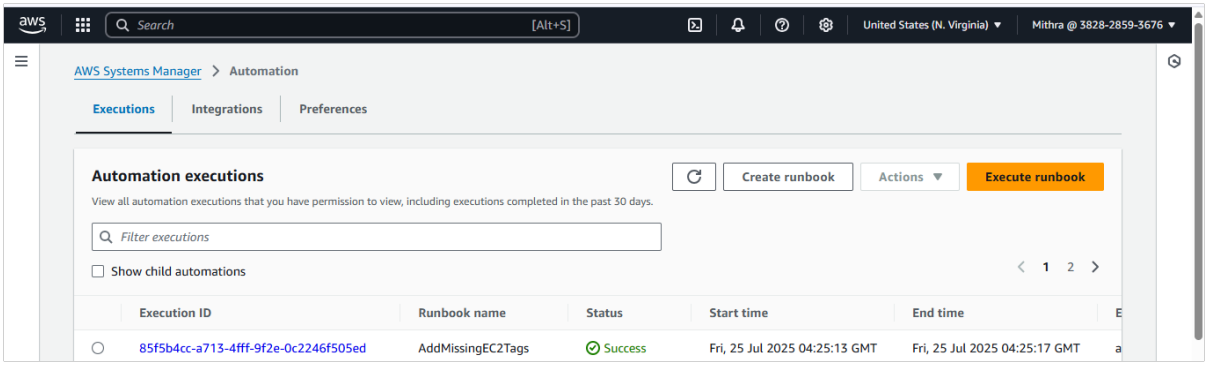




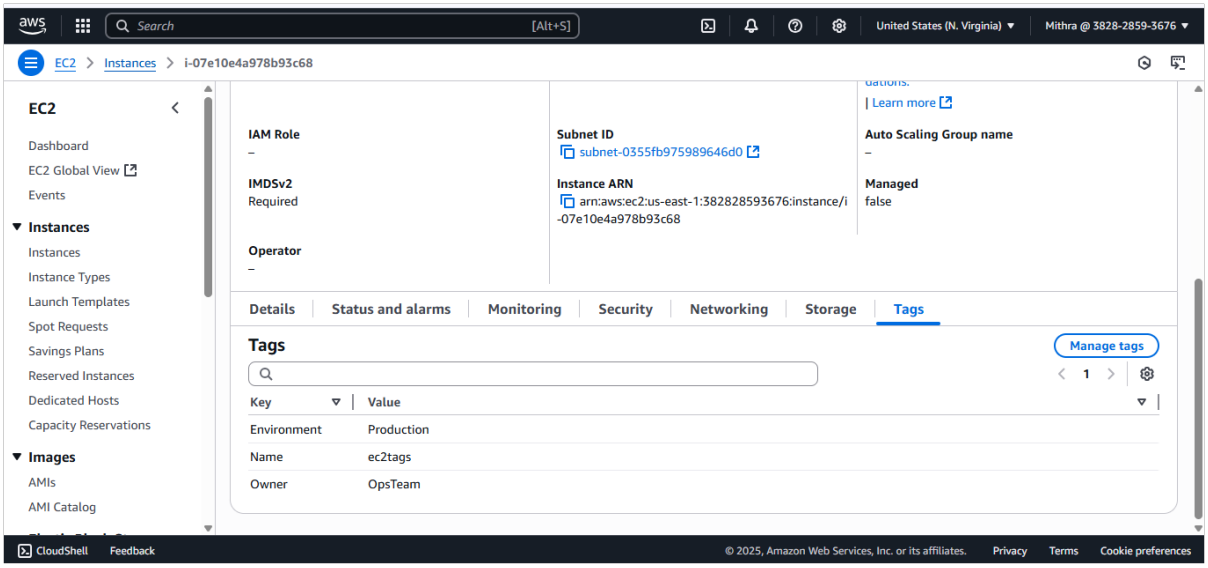
Step 6: Now create the custom runbook for Auto remediation



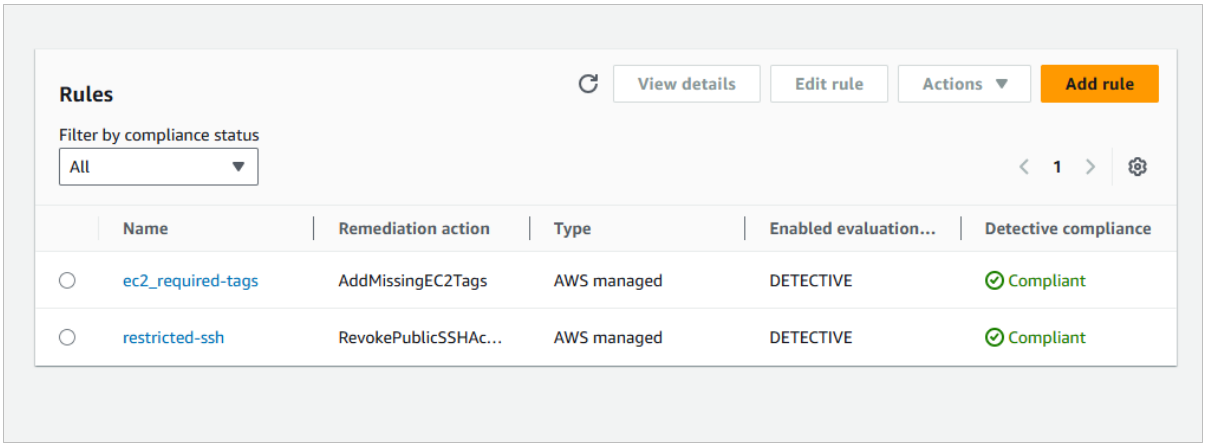
Step 7: once the auto remediation starts we can see the progress in Automation history



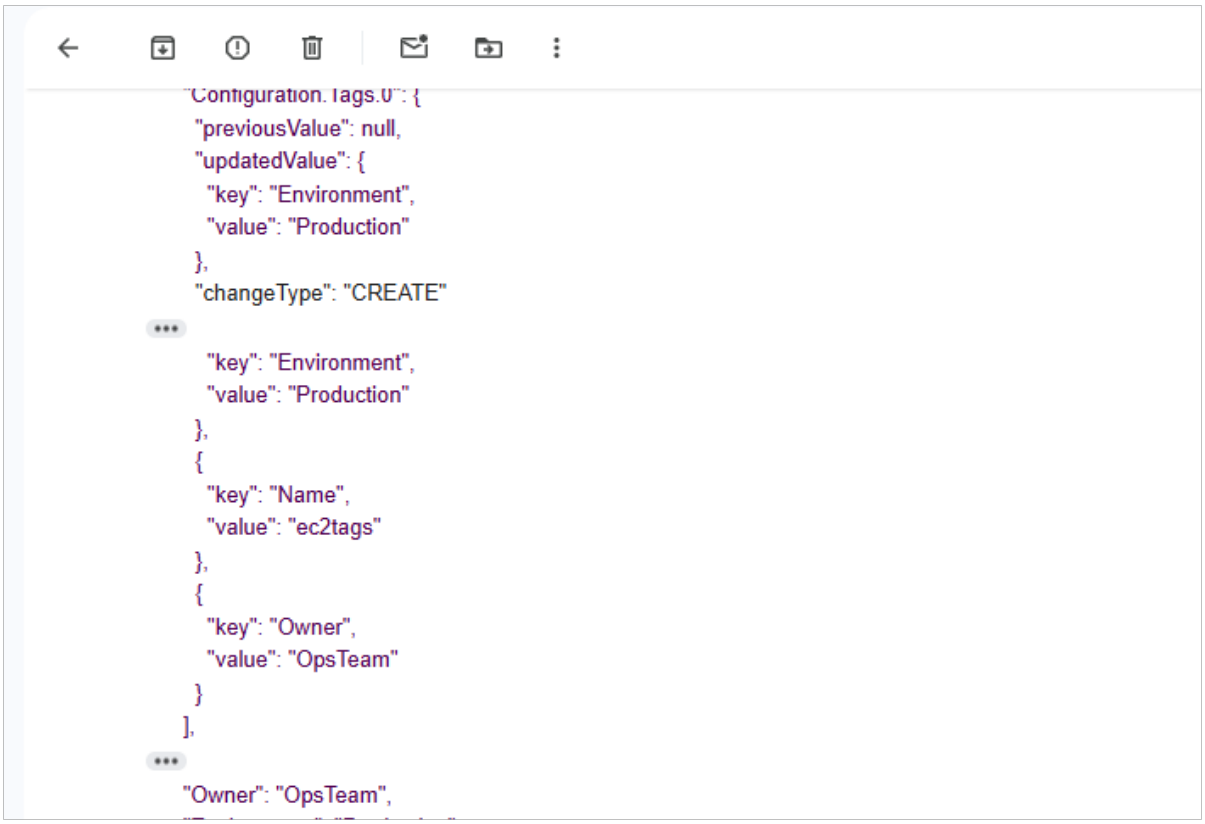
Step 8: And now we can see the tags added to EC2 instance

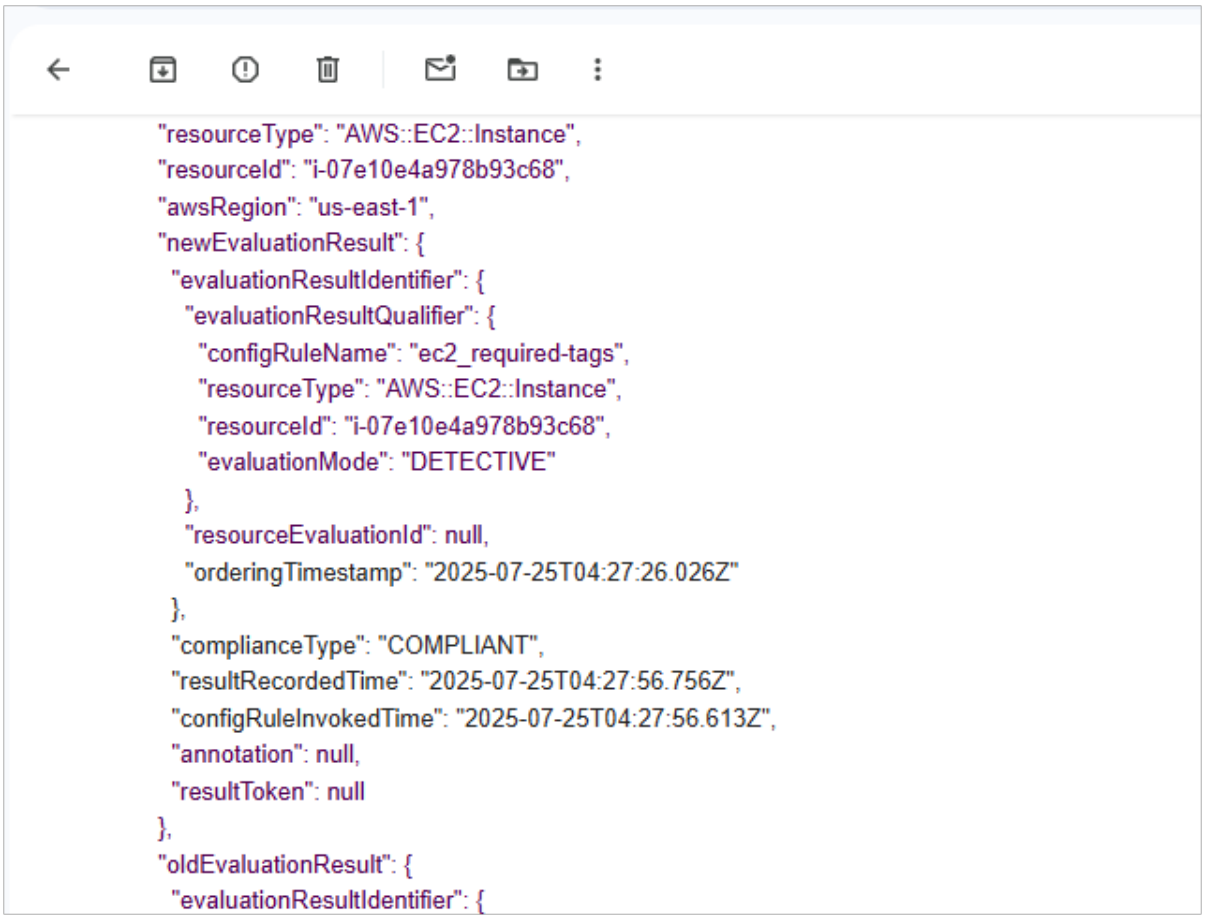


Step 9: And now the NON- COMPLIANT will move to COMPLIANT



Step 10 : Got an SNS notification also for COMPLIANT status

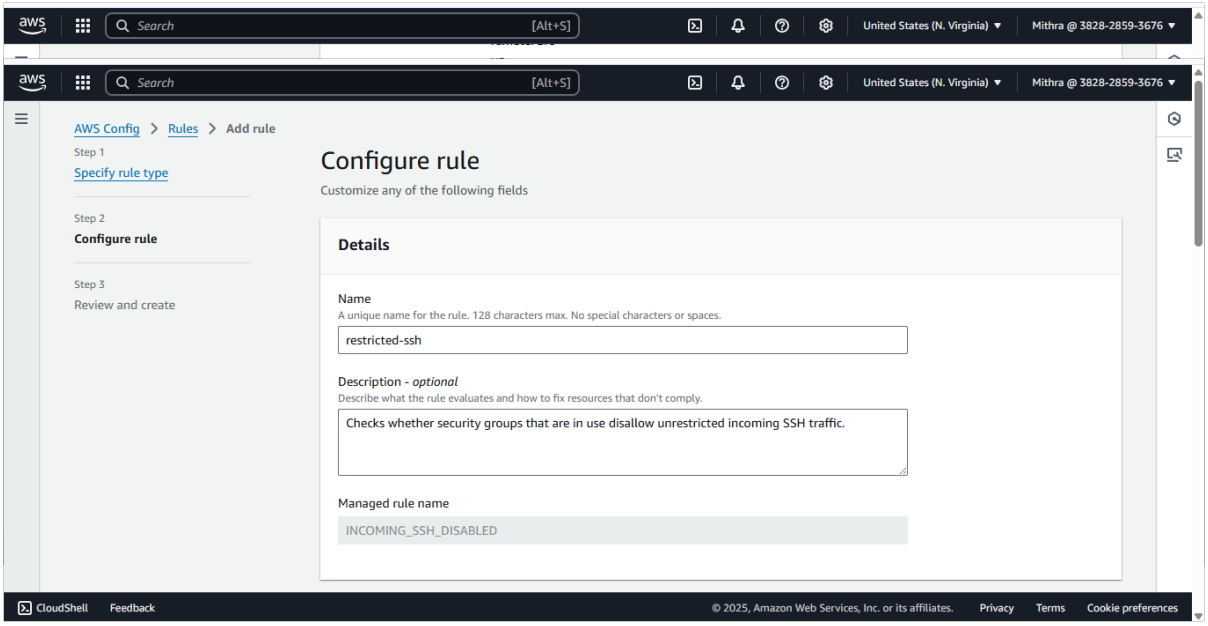

"Configuration.Tags.0": {
"previousValue": null,
"updatedValue": {
"key": "Environment",
"value": "Production"
},
"changeType": "CREATE"
"key": "Environment",
"value": "Production"
},
{
"key": "Name",
"value": "ec2tags"
},
{
"key": "Owner",
"value": "OpsTeam"
}
],
"Owner": "OpsTeam",

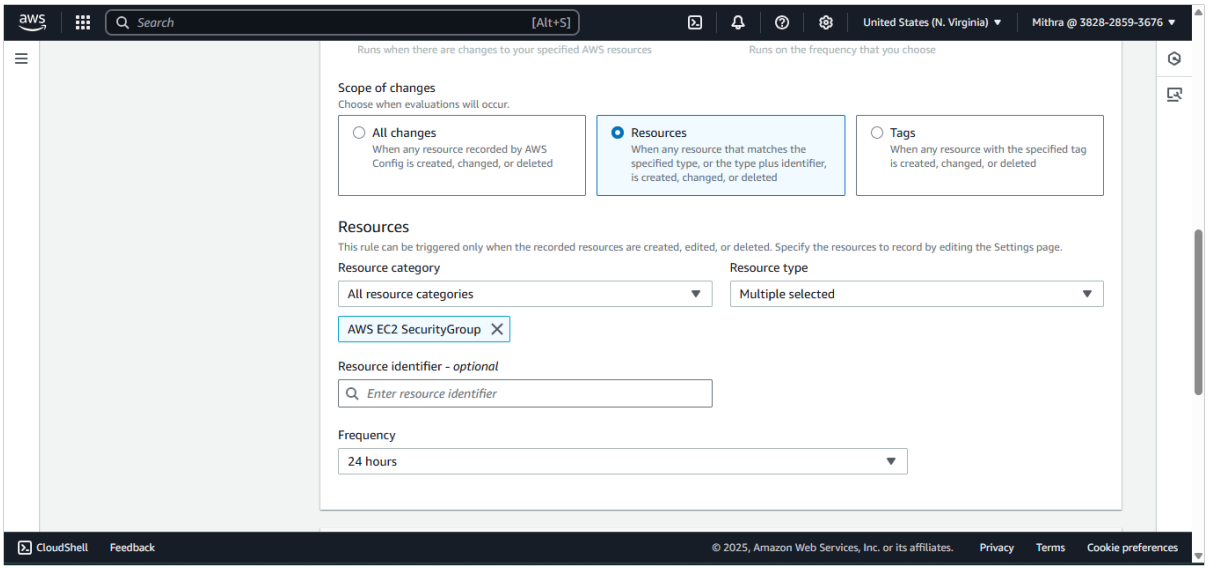


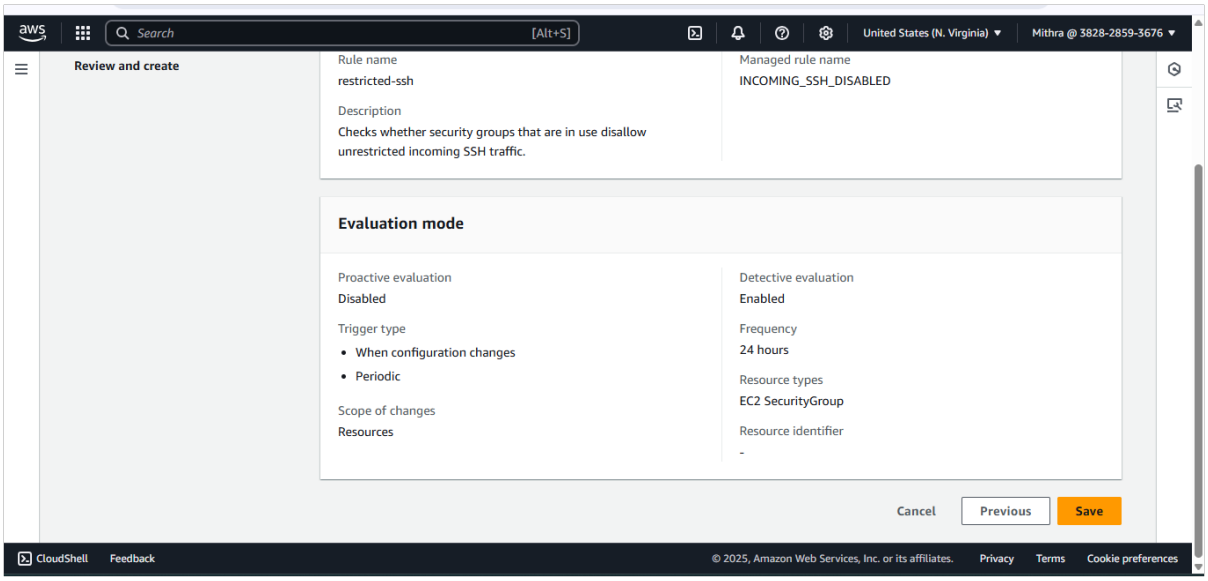
Security Group SSH Open Access

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

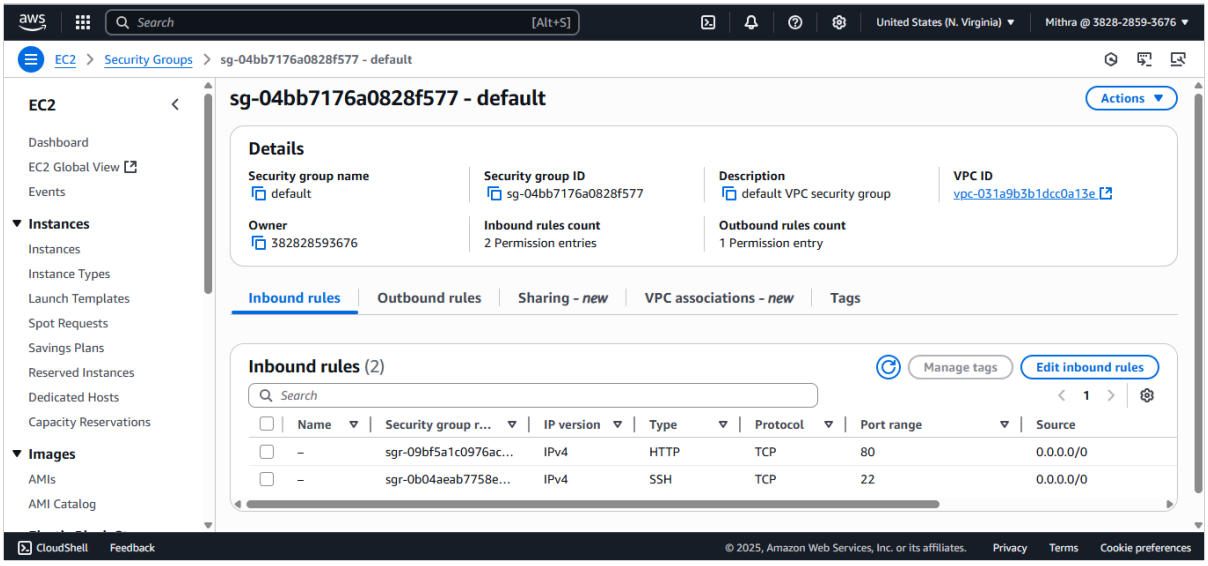
Step 1: create AWS config rule for EC2 security group

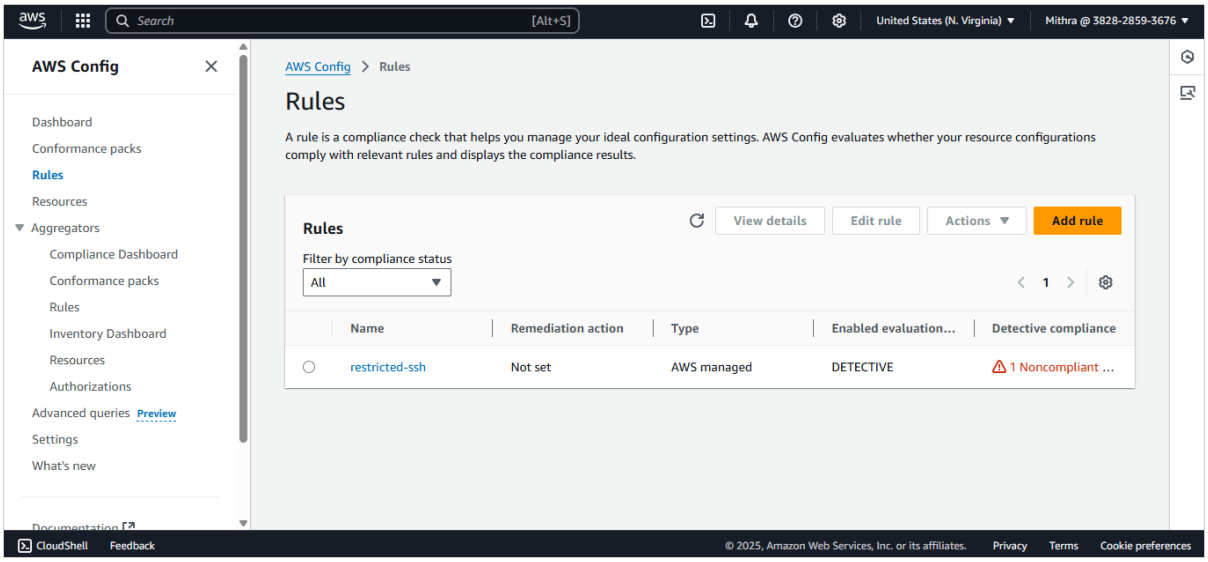

Search [Alt+S]
United States (N. Virginia)
Mithra @ 3828-2859-3676
AWS Config > Rules > Add rule
Step 1
Specify rule type
Step 2
Configure rule
Step 3
Review and create
Configure rule
Customize any of the following fields
Details
Name
A unique name for the rule. 128 characters max. No special characters or spaces.
restricted-ssh
Description - optional
Describe what the rule evaluates and how to fix resources that don't comply.
Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.
Managed rule name
INCOMING_SSH_DISABLED
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
United States (N. Virginia)
Mithra @ 3828-2859-3676
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
Enter resource identifier
Frequency
24 hours
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

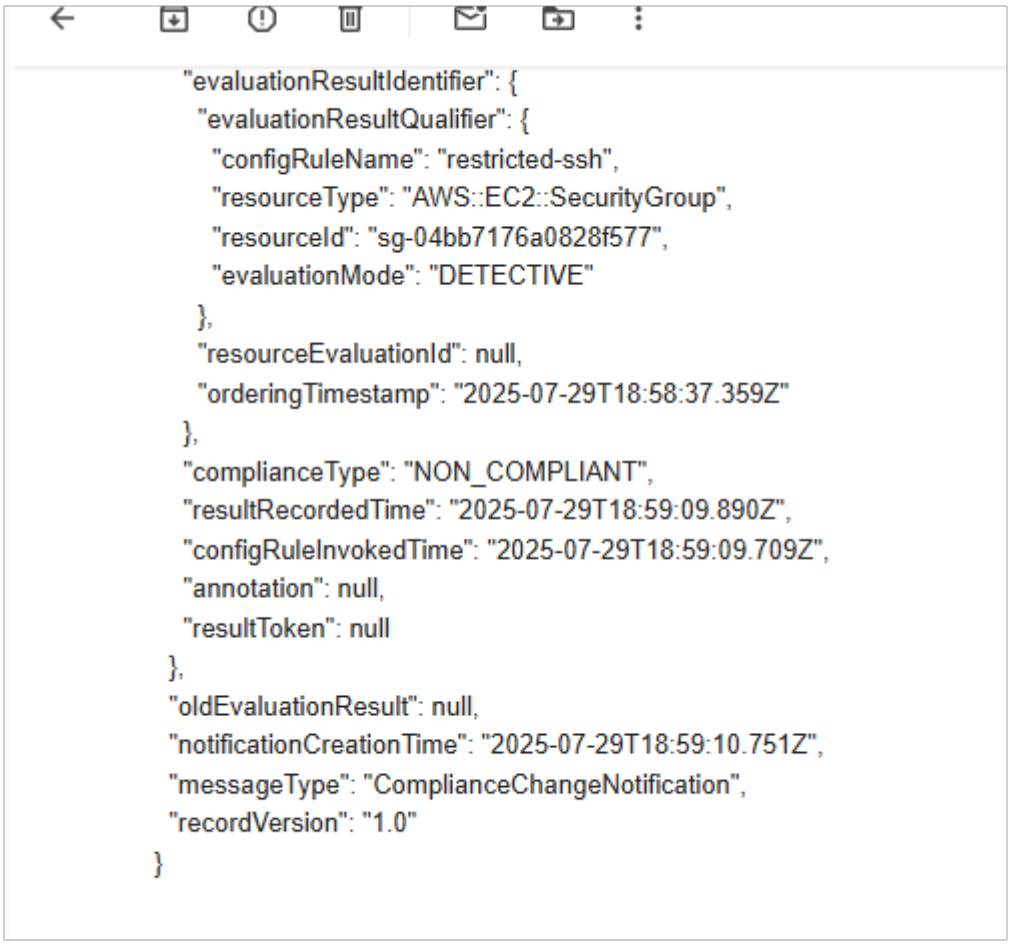


Step 2: Get the security group with 0.0.0.0/0 and it should move with NON-COMPLIANT



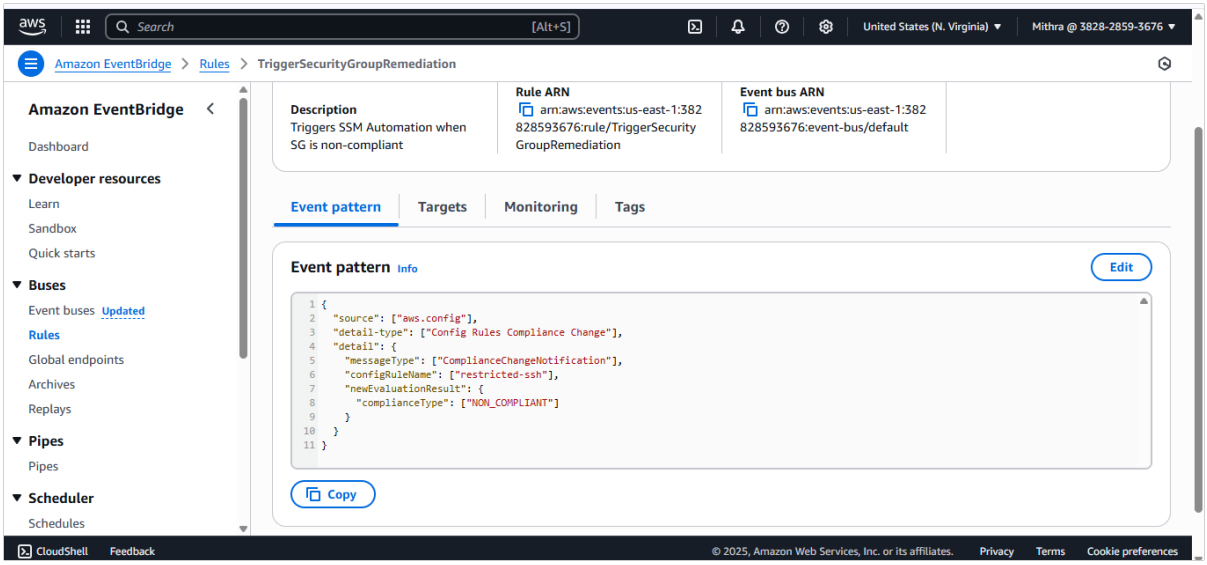


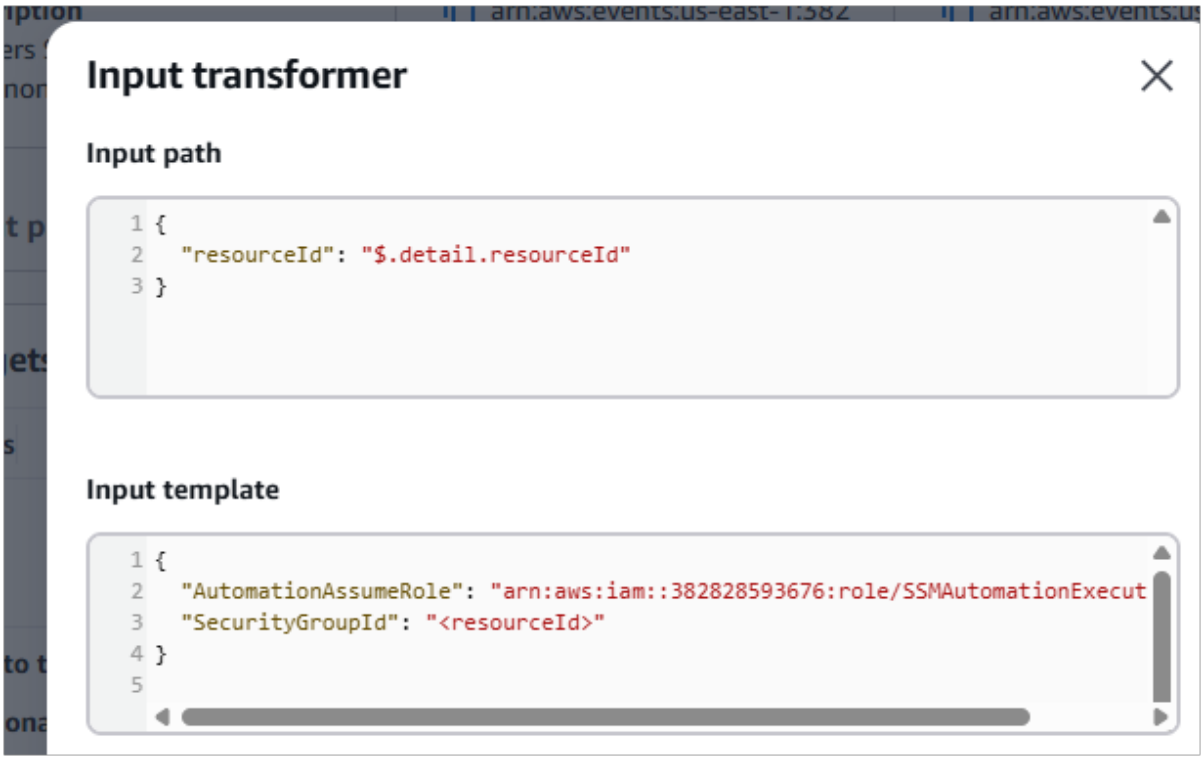
Step 3: Got an email for NON-COMPLIANT



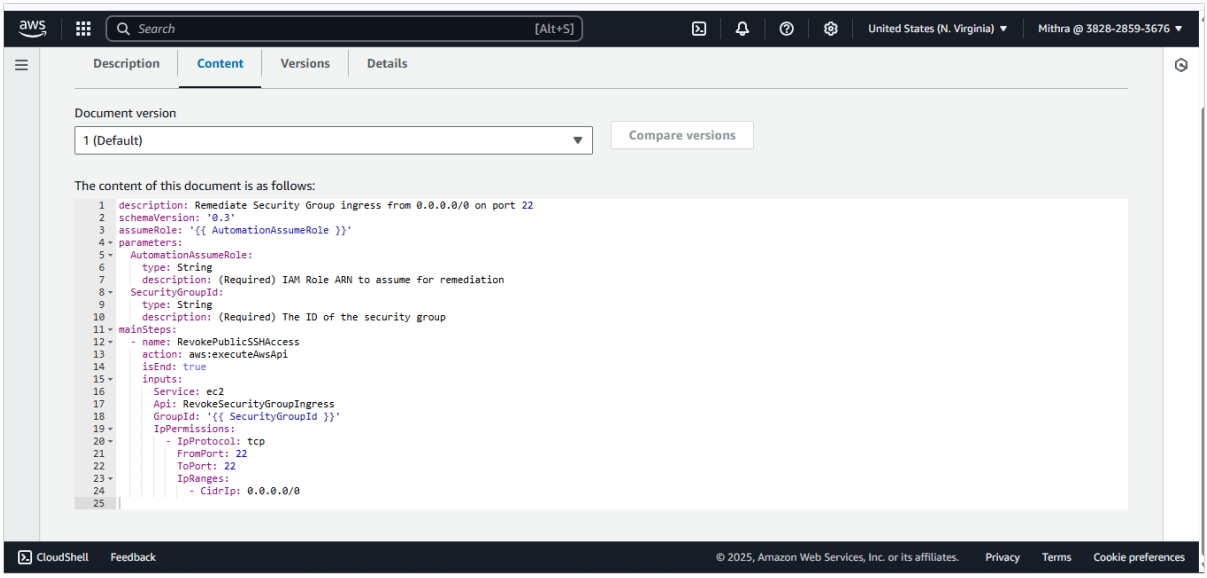

```
"evaluationResultIdentifier": {
 "evaluationResultQualifier": {
  "configRuleName": "restricted-ssh",
  "resourceType": "AWS::EC2::SecurityGroup",
  "resourceId": "sg-04bb7176a0828f577",
  "evaluationMode": "DETECTIVE"
 },
 "resourceEvaluationId": null,
 "orderingTimestamp": "2025-07-29T18:58:37.359Z"
},
"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"
}
```

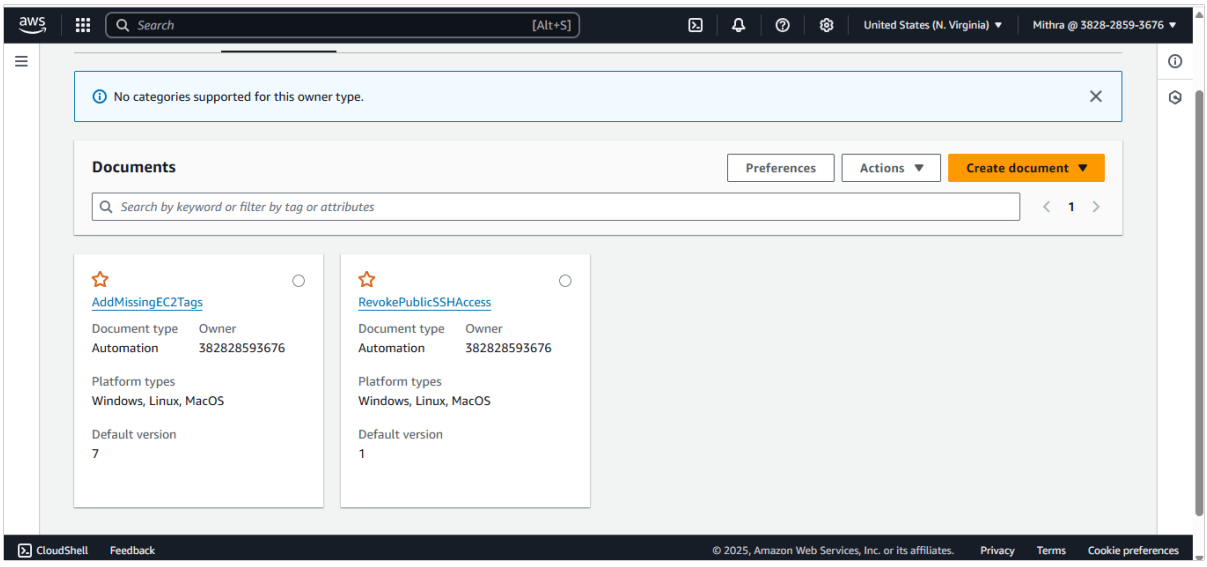
Step 4: Now create the Eventbridge rule to trigger NON-COMPLAINT



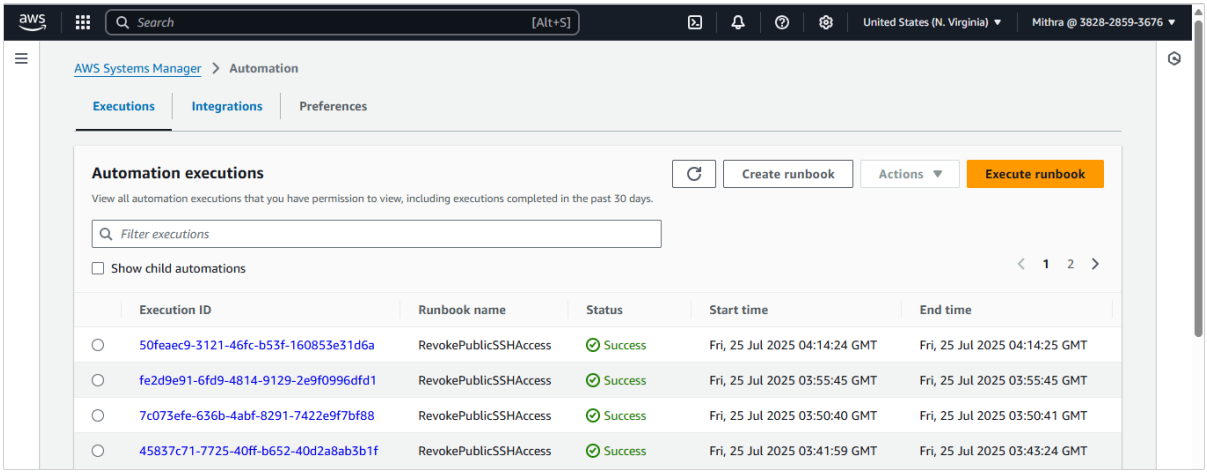


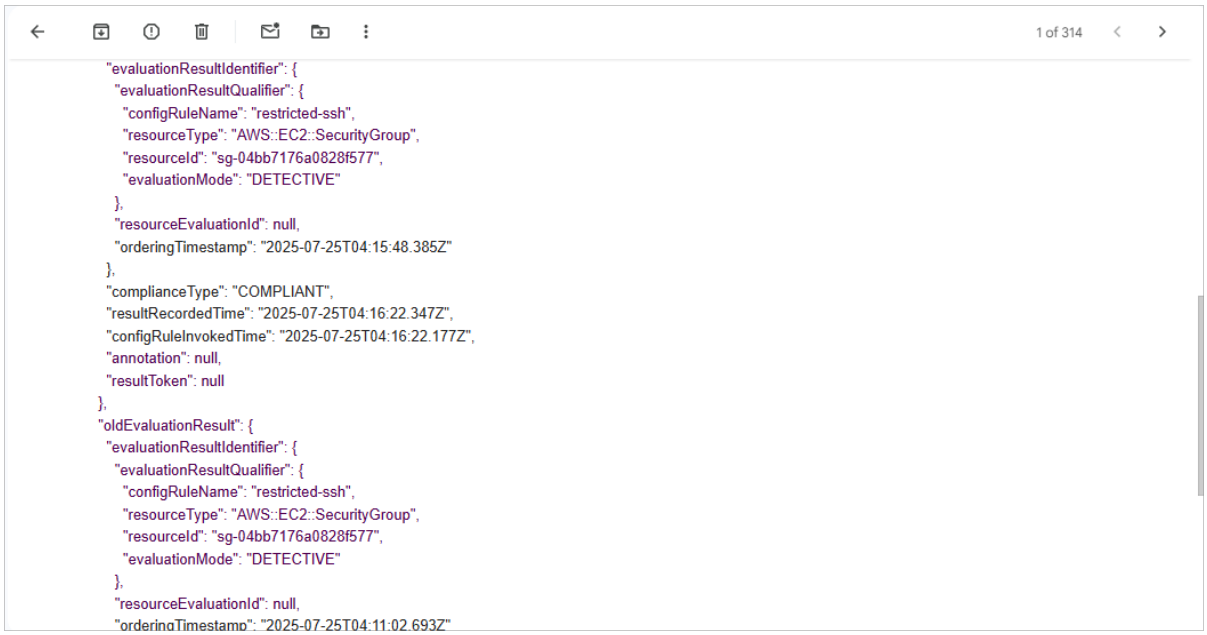
Step 5: Create the Custom SSM document for auto remediation

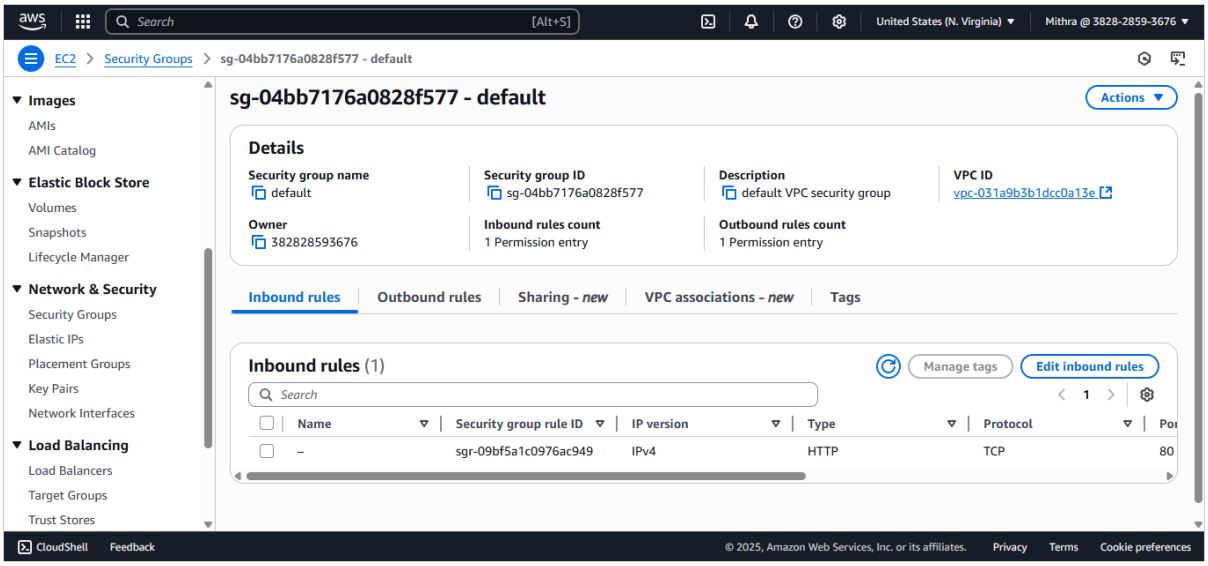


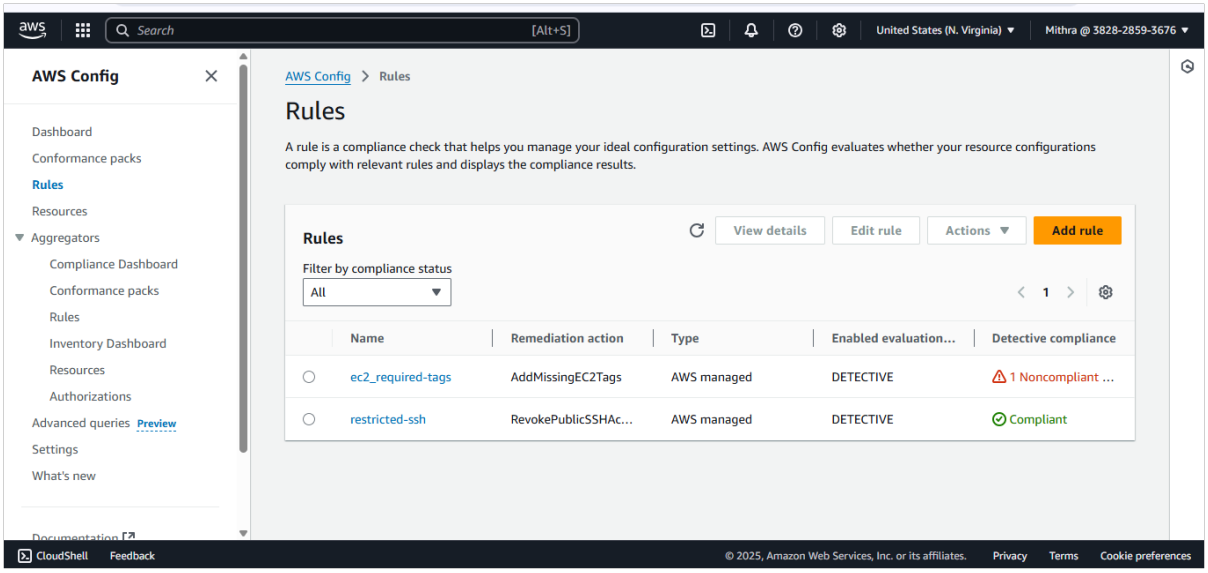


Step 6: Now the SSH public access will get removed and the config rule will move it to COMPLIANT


aws
Search
[Alt+S]
United States (N. Virginia)
Mithra @ 3828-2859-3676
AWS Systems Manager
Automation
Executions
Integrations
Preferences
Automation executions
View all automation executions that you have permission to view, including executions completed in the past 30 days.
Create runbook
Actions
Execute runbook
Filter executions
Show child automations
1
2
Execution ID
Runbook name
Status
Start time
End time
50feaec9-3121-46fc-b53f-160853e31d6a
RevokePublicSSHAccess
Success
Fri, 25 Jul 2025 04:14:24 GMT
Fri, 25 Jul 2025 04:14:25 GMT
fe2d9e91-6fd9-4814-9129-2e9f0996dfd1
RevokePublicSSHAccess
Success
Fri, 25 Jul 2025 03:55:45 GMT
Fri, 25 Jul 2025 03:55:45 GMT
7c073efe-636b-4abf-8291-7422e9f7bf88
RevokePublicSSHAccess
Success
Fri, 25 Jul 2025 03:50:40 GMT
Fri, 25 Jul 2025 03:50:41 GMT
45837c71-7725-40ff-b652-40d2a8ab3b1f
RevokePublicSSHAccess
Success
Fri, 25 Jul 2025 03:41:59 GMT
Fri, 25 Jul 2025 03:43:24 GMT


1 of 314
"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"



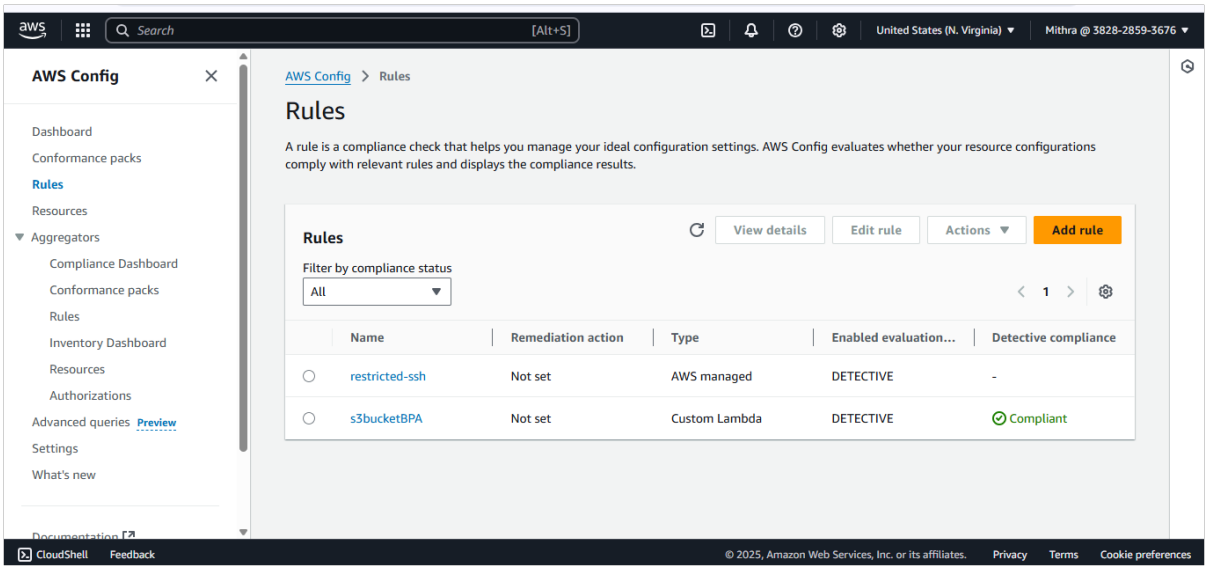


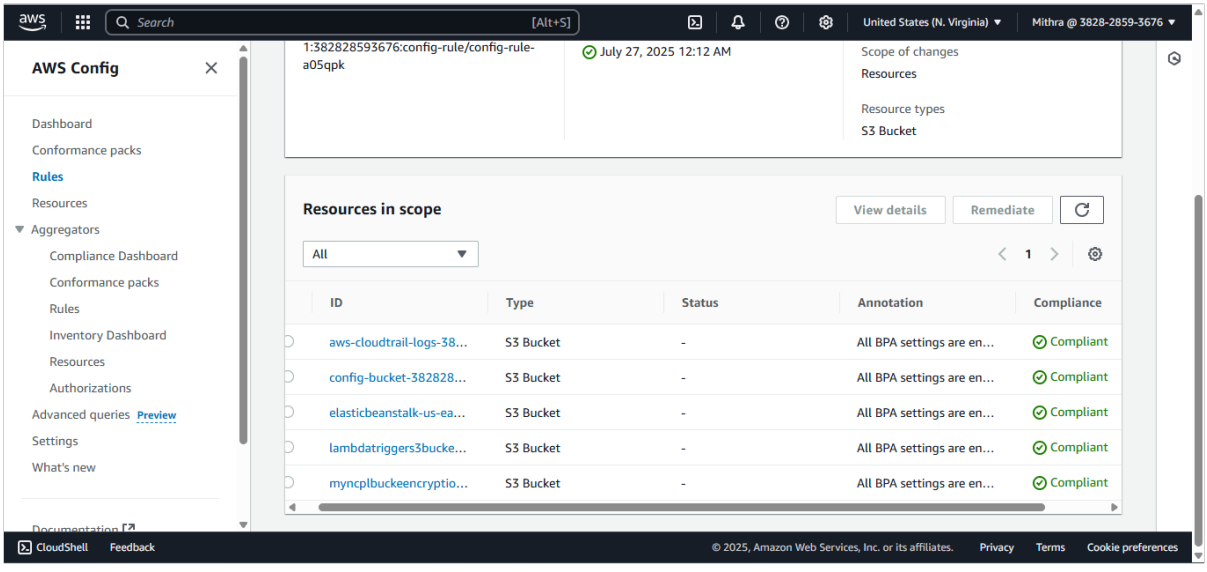
S3 Bucket Public Access Blocked

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

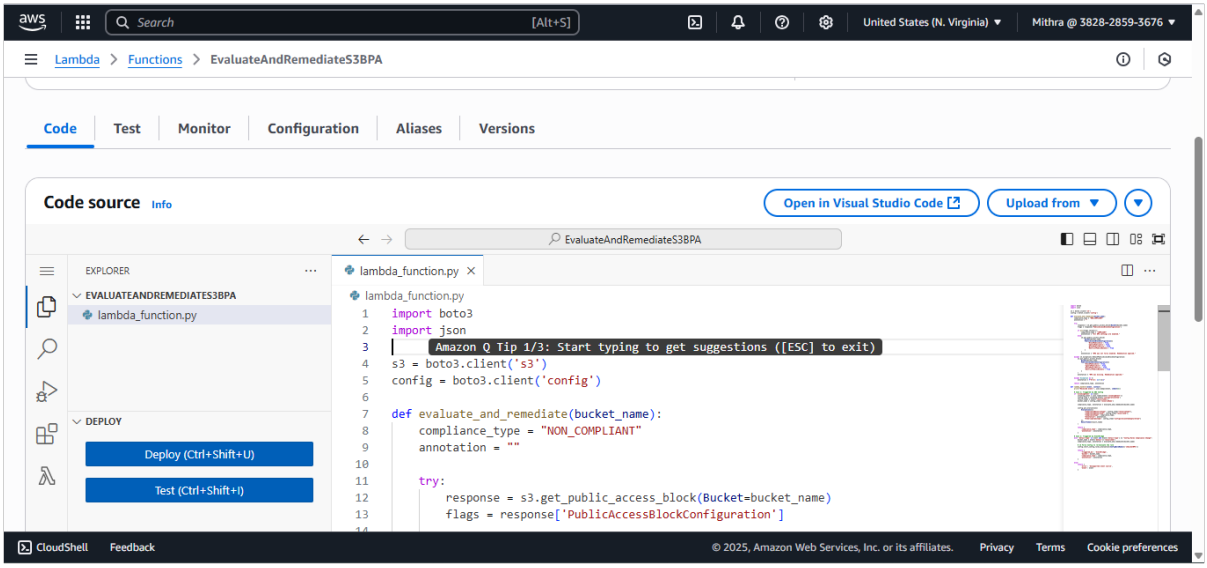
- Lambda writes to CloudWatch Logs

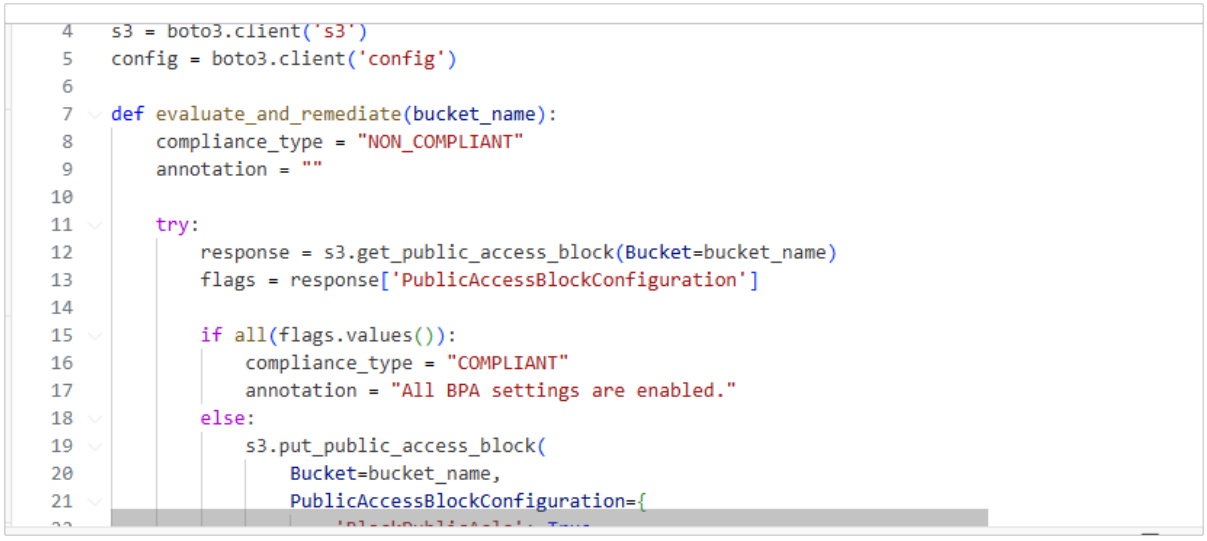
Step 1: Create AWS config rule with custom lambda function and default all the buckets will have public access enabled , so the config rule is COMPLIANT





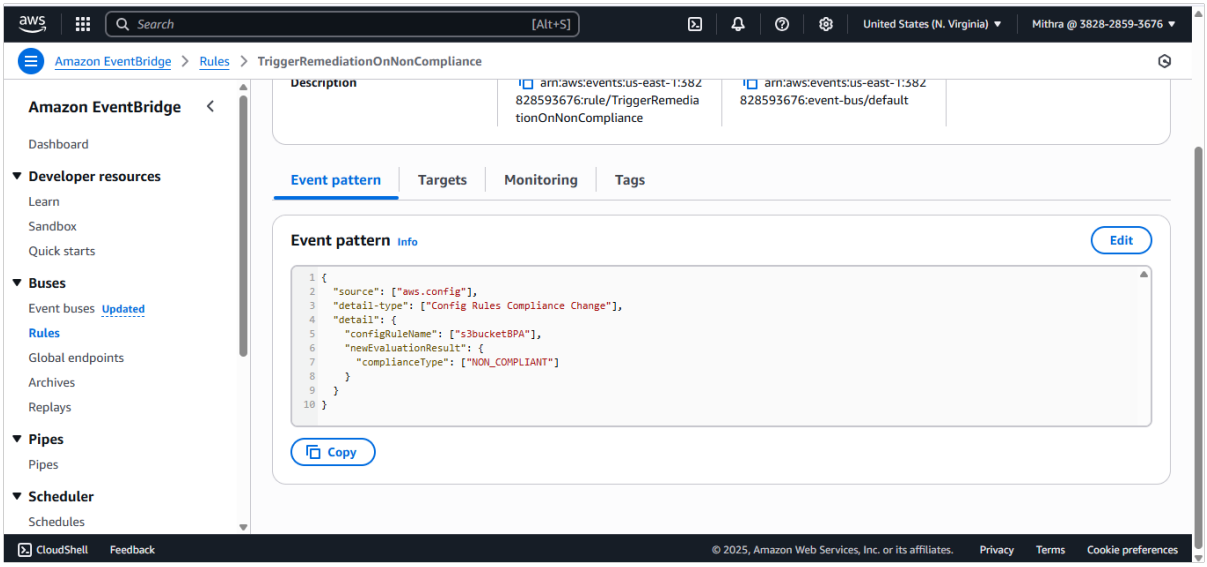
Step 2: Create the Lambda function for Evaluating AWS config rule

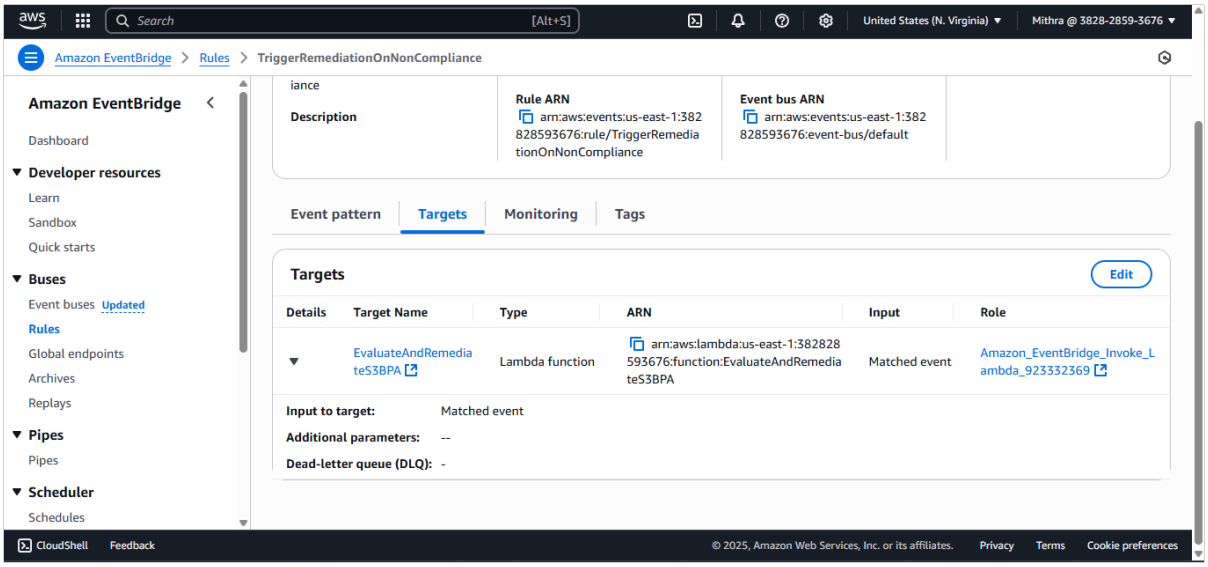




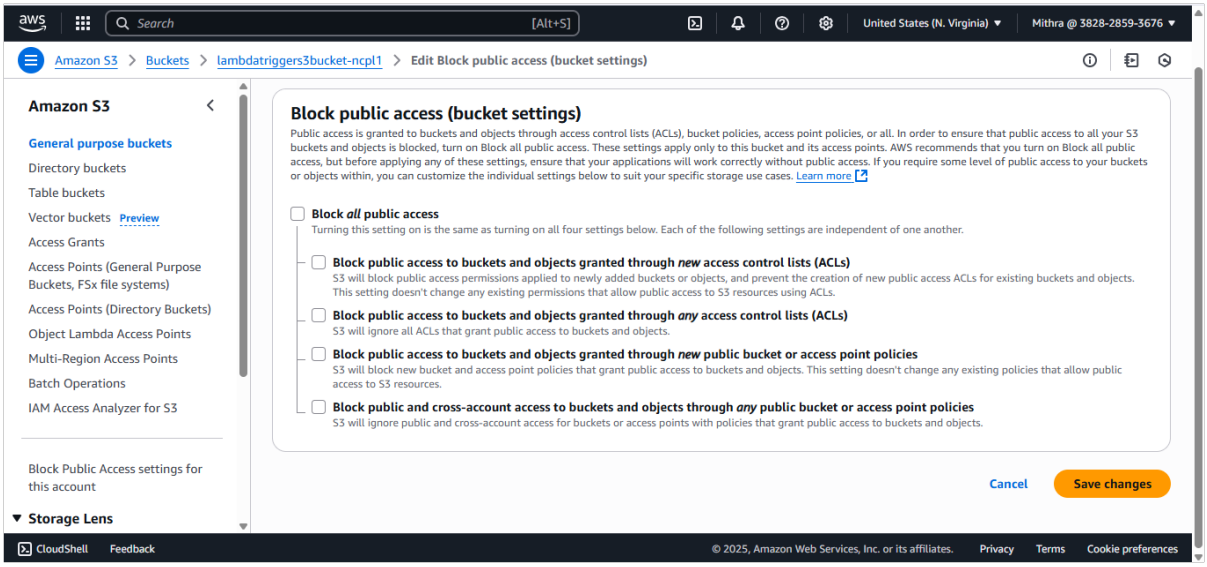
```
s3 = boto3.client('s3')
config = boto3.client('config')

def evaluate_and_remediate(bucket_name):
    compliance_type = "NON_COMPLIANT"
    annotation = ""

    try:
        response = s3.get_public_access_block(Bucket=bucket_name)
        flags = response['PublicAccessBlockConfiguration']

        if all(flags.values()):
            compliance_type = "COMPLIANT"
            annotation = "All BPA settings are enabled."
        else:
            s3.put_public_access_block(
                Bucket=bucket_name,
                PublicAccessBlockConfiguration={
```

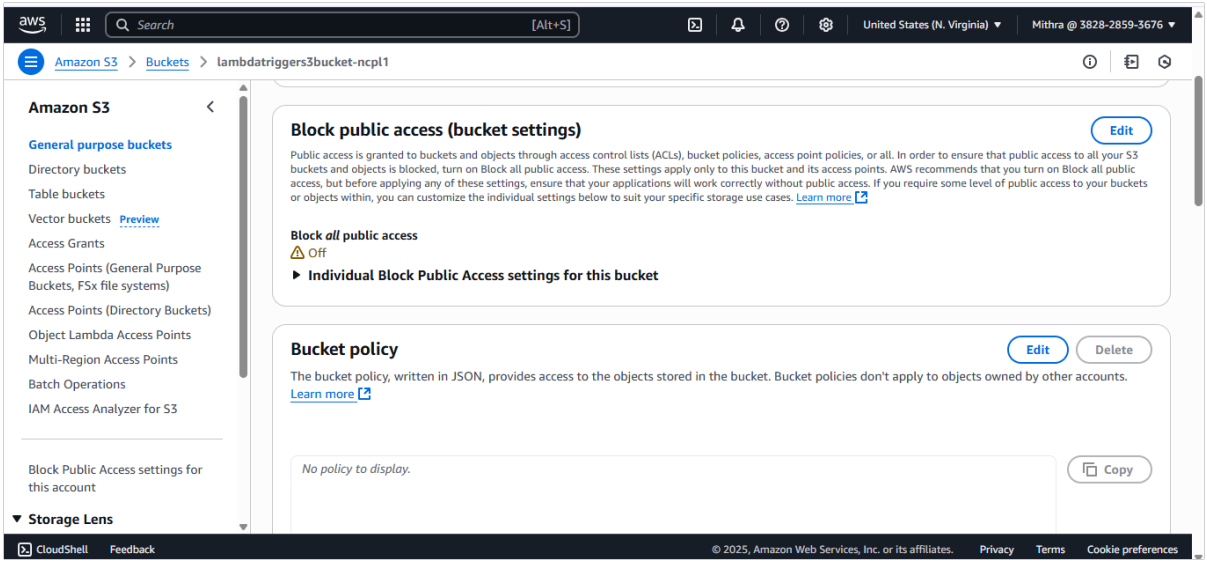
Step 3: create Eventbridge rue will trigger when AWS config rule become NON-Compliant and choose the target as lambda function



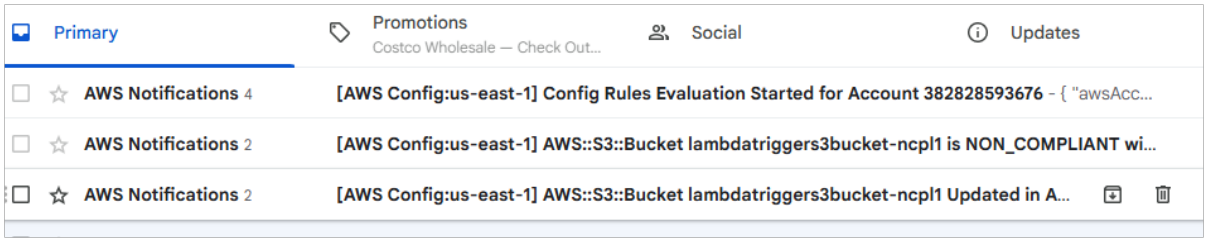


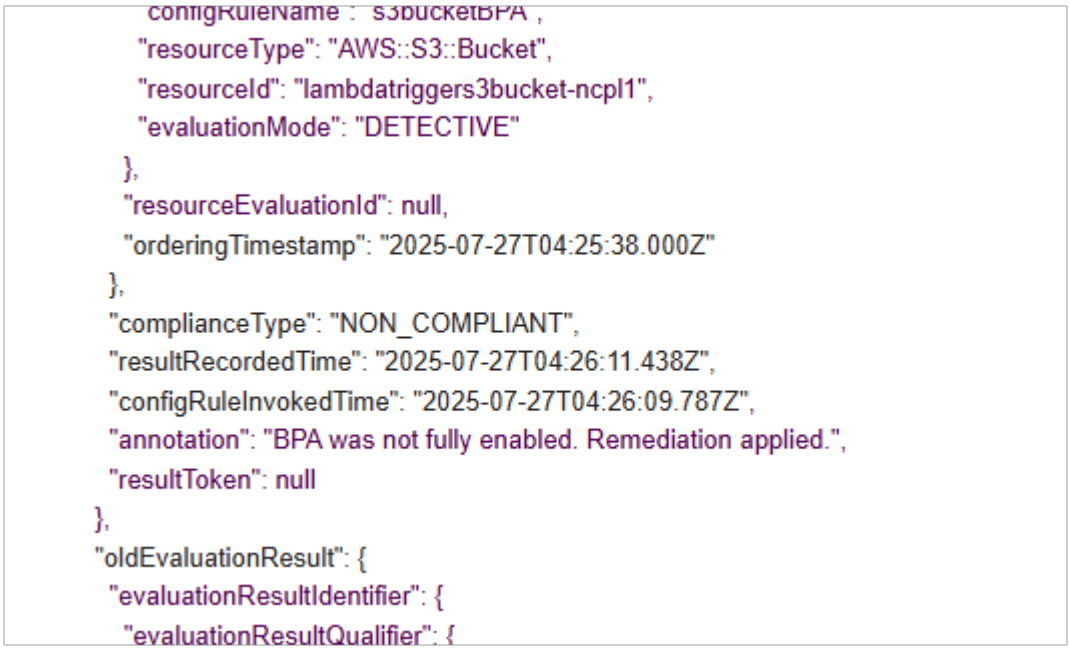
Step 4: Now test the full flow by disabling the S3 public access



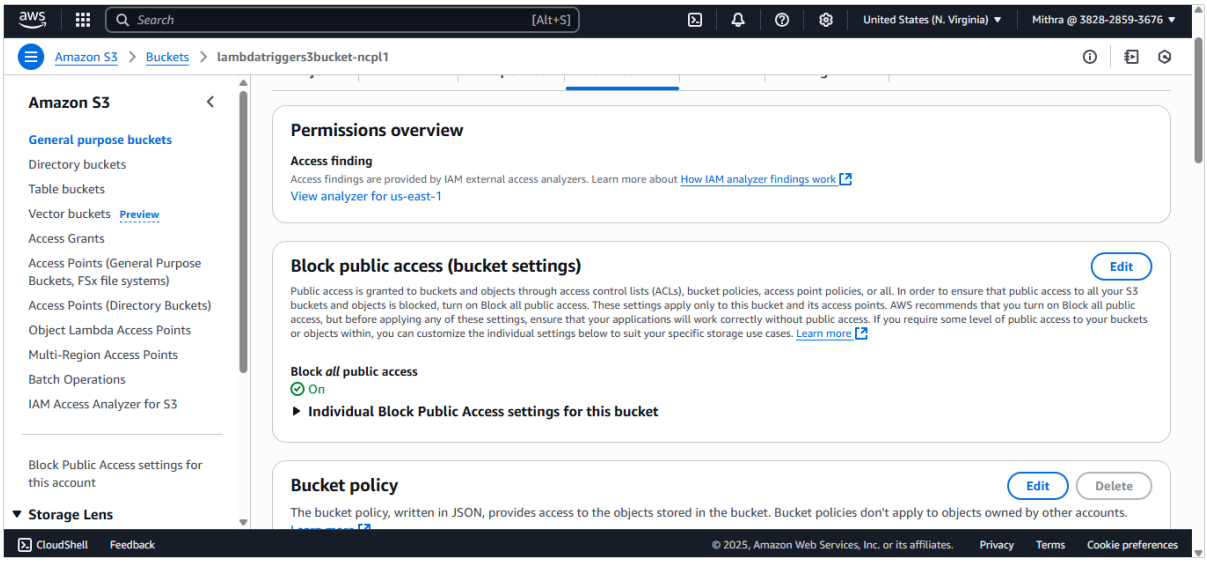


Step 5: Now the config rule become NON-COMPLIANT

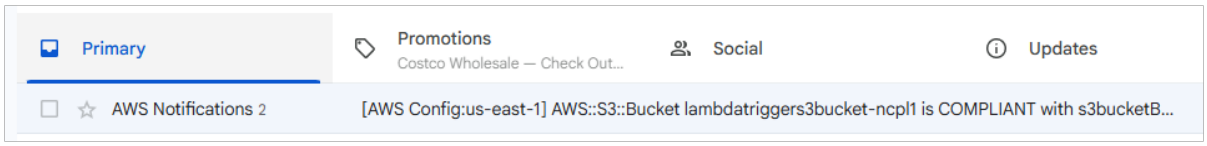


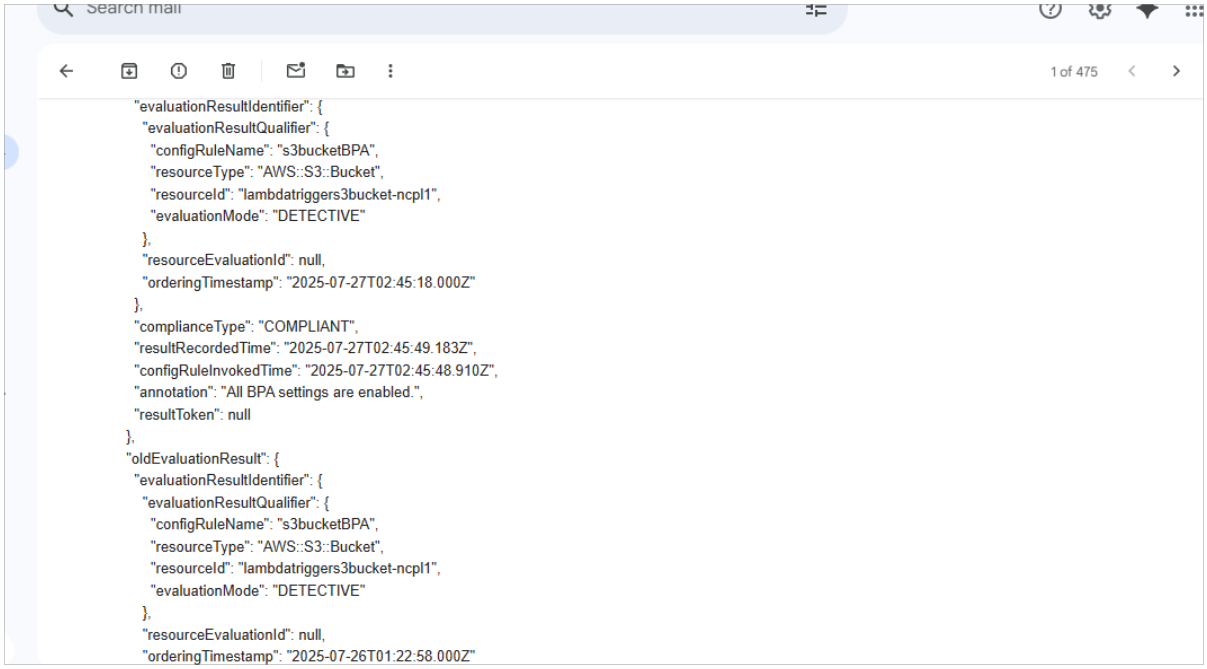


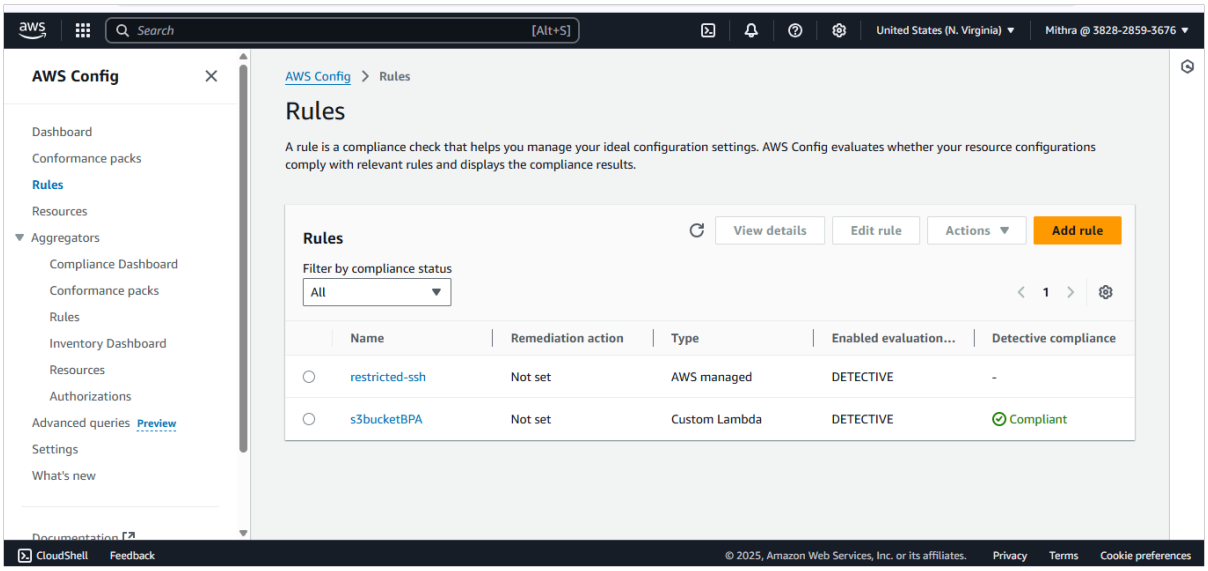
Step 6: Now we can see the public access got enabled after auto remediation



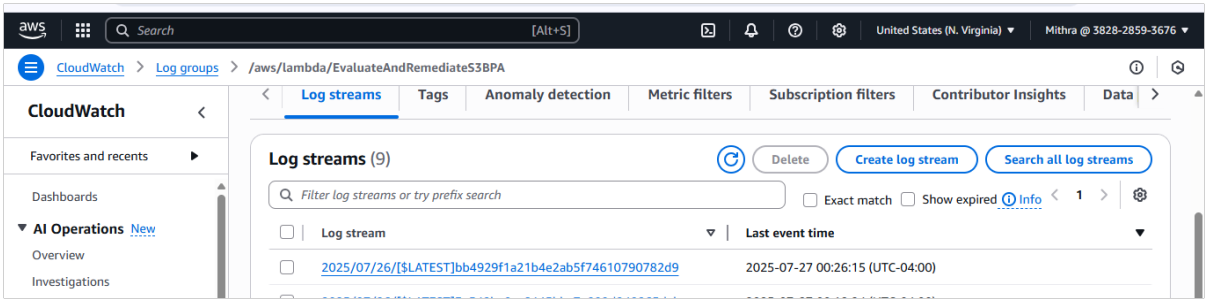
Step 7: Now we can see the config rule become COMPLIANT

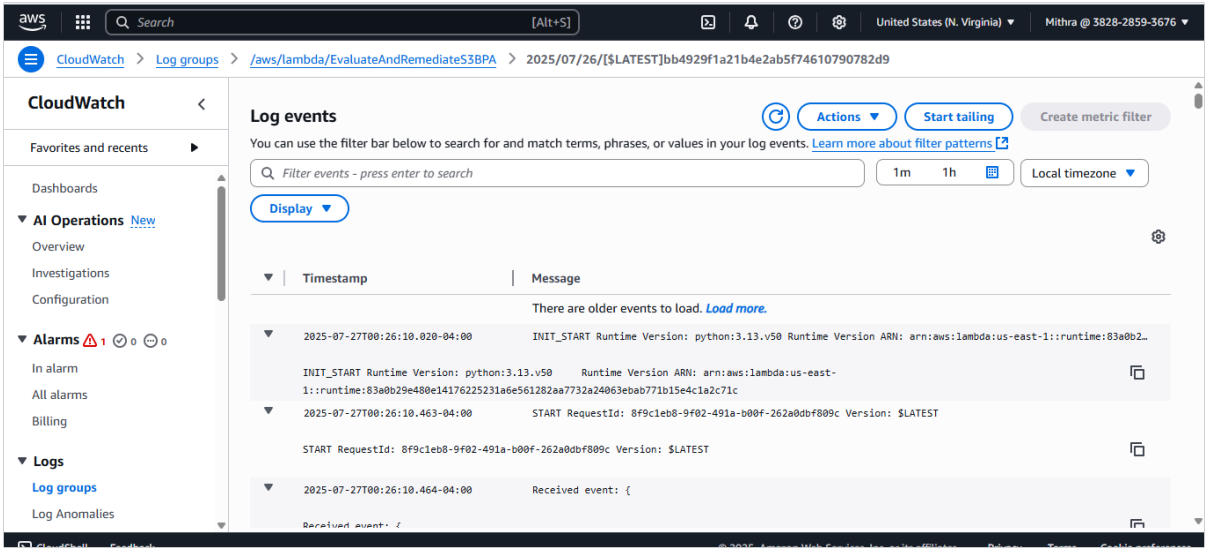


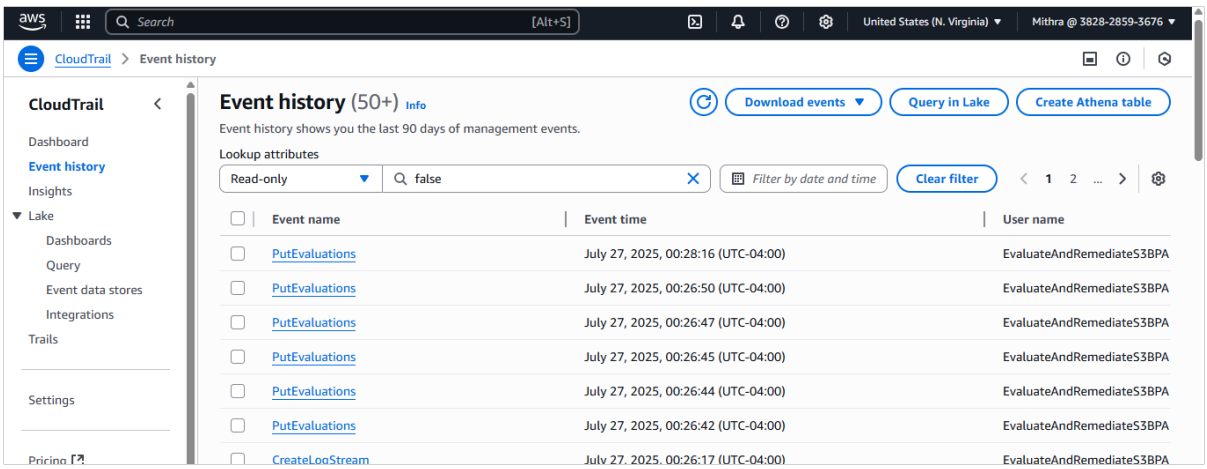




Step 8: CloudWatch logs also captured with lambda function


Search [Alt+S]
United States (N. Virginia)
Mithra @ 3828-2859-3676
CloudWatch > Log groups > /aws/lambda/EvaluateAndRemediateS3BPA
CloudWatch
Favorites and recents
Dashboards
AI Operations New
Overview
Investigations
Log streams
Tags
Anomaly detection
Metric filters
Subscription filters
Contributor Insights
Data
Log streams (9)
Delete
Create log stream
Search all log streams
Filter log streams or try prefix search
Exact match
Show expired
Info
Log stream
Last event time
2025/07/26/[$LATEST]bb4929f1a21b4e2ab5f74610790782d9
2025-07-27 00:26:15 (UTC-04:00)

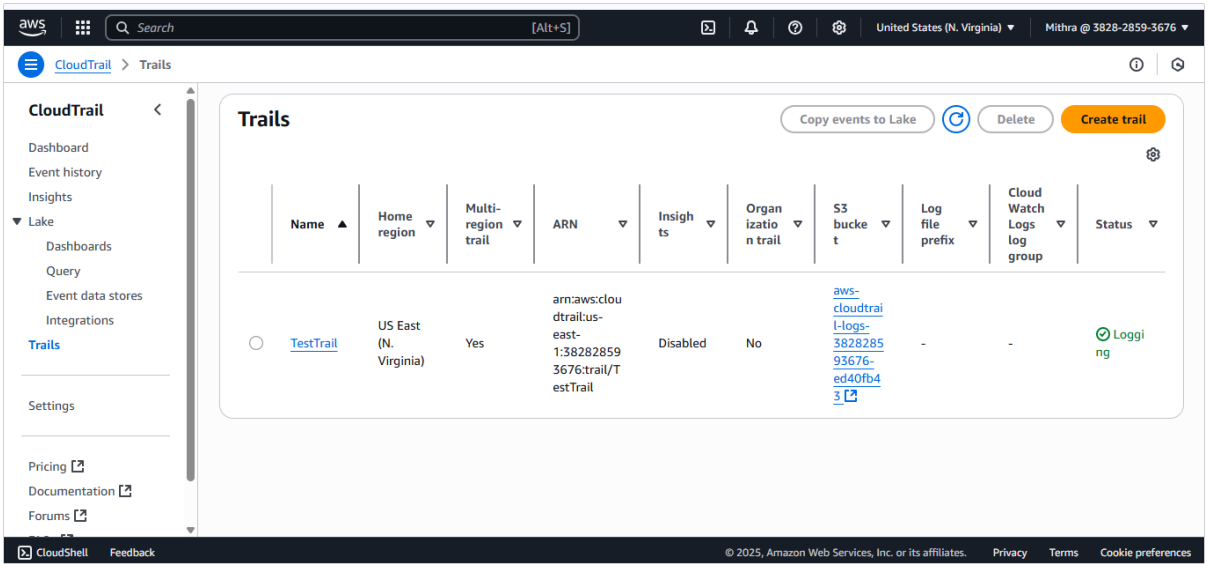

Search [Alt+S]
United States (N. Virginia)
Mithra @ 3828-2859-3676
CloudWatch > Log groups > /aws/lambda/EvaluateAndRemediateS3BPA > 2025/07/26/[$LATEST]bb4929f1a21b4e2ab5f74610790782d9
CloudWatch
Favorites and recents
Dashboards
AI Operations New
Overview
Investigations
Configuration
Alarms
In alarm
All alarms
Billing
Logs
Log groups
Log Anomalies
Log events
Actions
Start tailing
Create metric filter
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns
Filter events - press enter to search
1m
1h
Local timezone
Display
Timestamp
Message
There are older events to load. Load more.
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…
INIT_START Runtime Version: python:3.13.v50 Runtime Version ARN: arn:aws:lambda:us-east-1::runtime:83a0b29e480e14176225231a6e561282aa7732a24063ebab771b15e4c1a2c71c
2025-07-27T00:26:10.463-04:00
START RequestId: 8f9c1eb8-9f02-491a-b00f-262a0dbf809c Version: $LATEST
START RequestId: 8f9c1eb8-9f02-491a-b00f-262a0dbf809c Version: $LATEST
2025-07-27T00:26:10.464-04:00
Received event: {


Search [Alt+S]
United States (N. Virginia)
Mithra @ 3828-2859-3676
CloudTrail > Event history
CloudTrail
Dashboard
Event history
Insights
Lake
Dashboards
Query
Event data stores
Integrations
Trails
Settings
Pricing
Event history (50+) Info
Download events
Query in Lake
Create Athena table
Event history shows you the last 90 days of management events.
Lookup attributes
Read-only
false
Filter by date and time
Clear filter
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

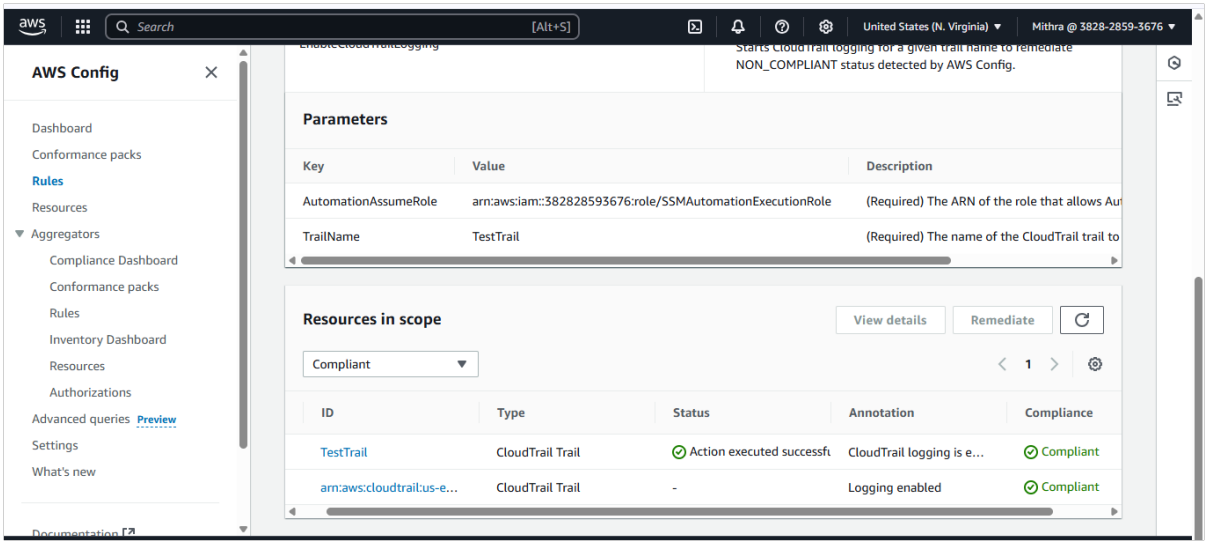
CloudTrail Logging Compliance

- 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

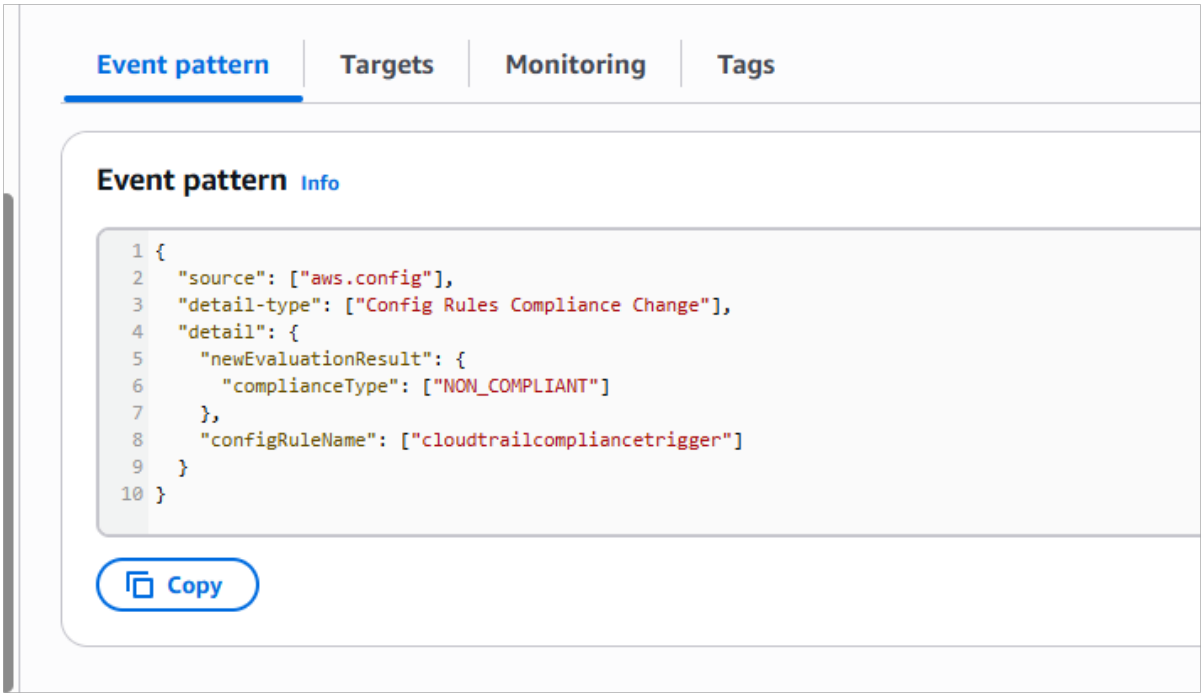
Step 1: Create Cloud trail and provide name as “TestTrail”

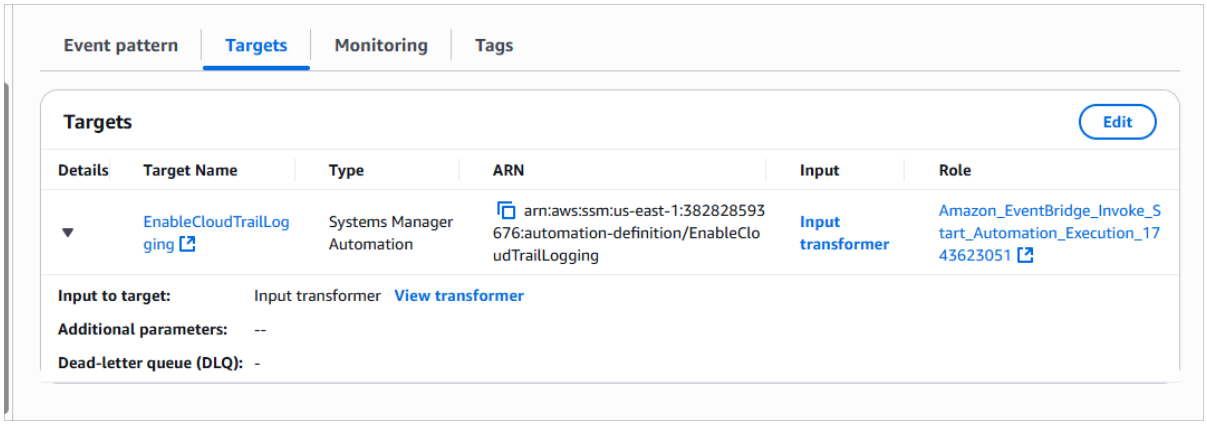


Step 3: Create AWS config rule with custom lambda function and it will become COMPLIANT

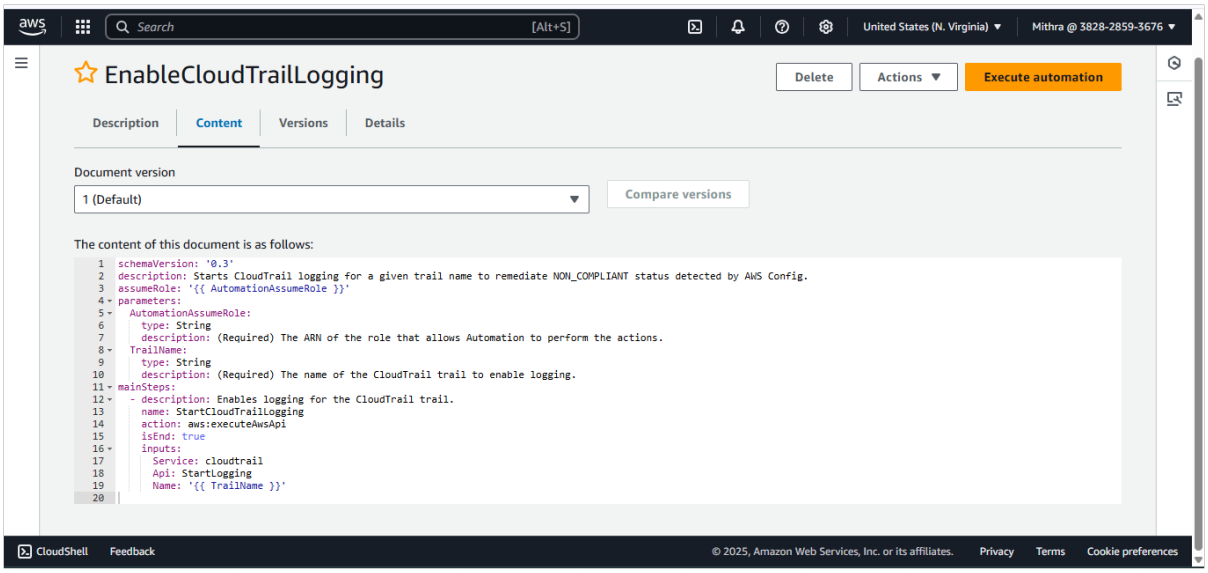


Step 4: Now create Eventbridge rule and choose target as SSM for Automatic remediation

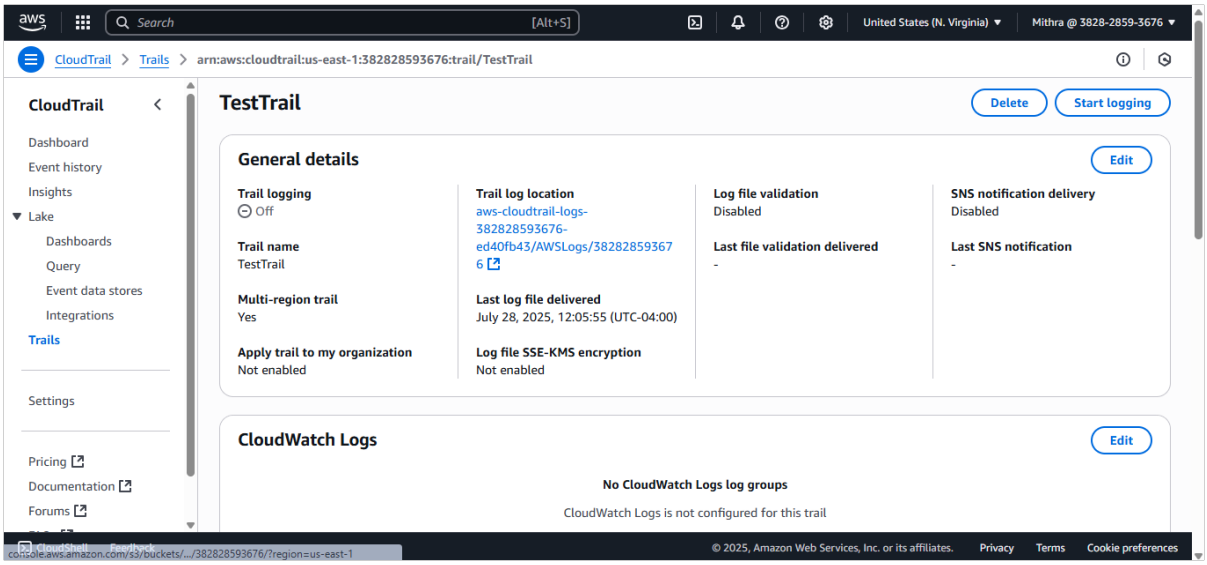


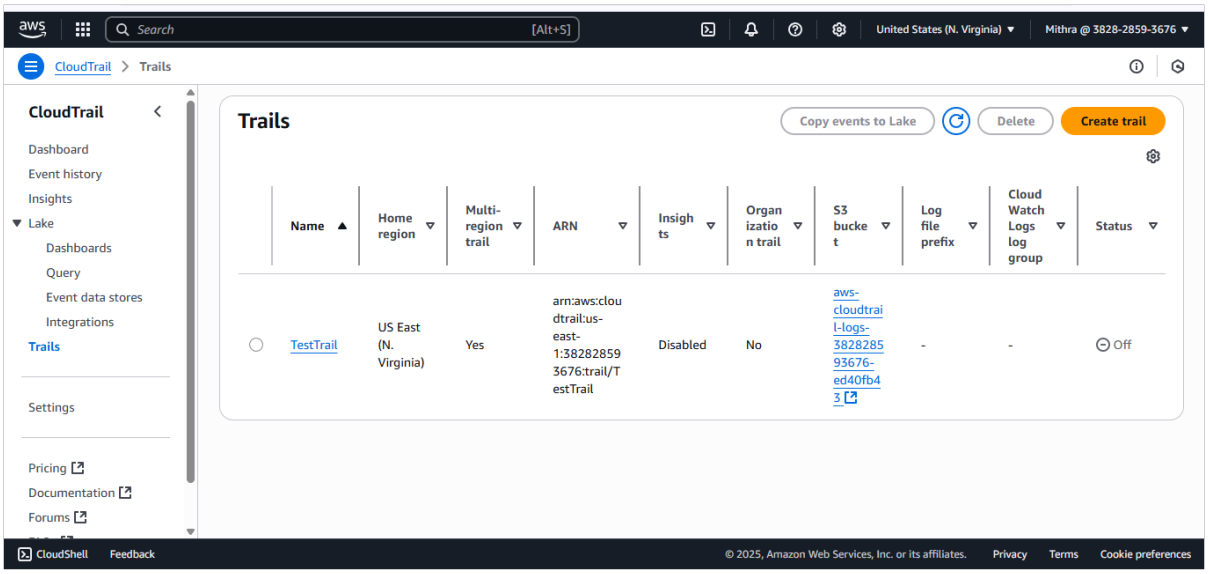


Step 5: Create SSM runbook for automatic remediation

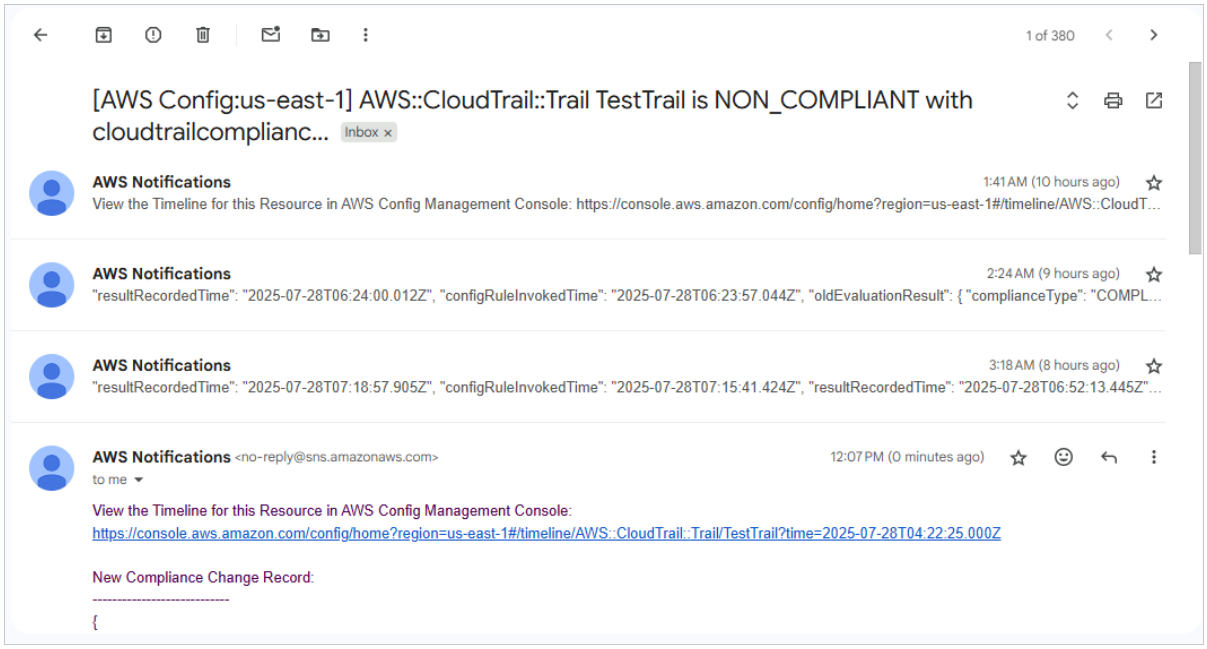


Step 6: Now manually test the CloudTrail by disabling the logging

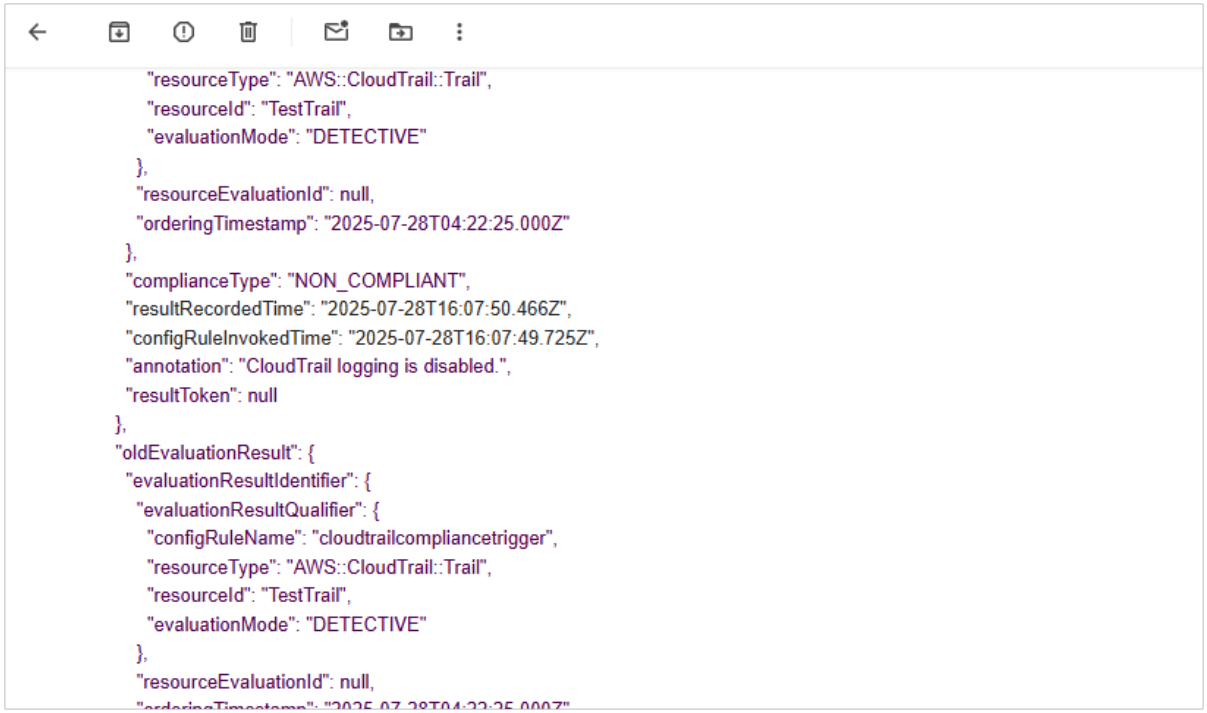


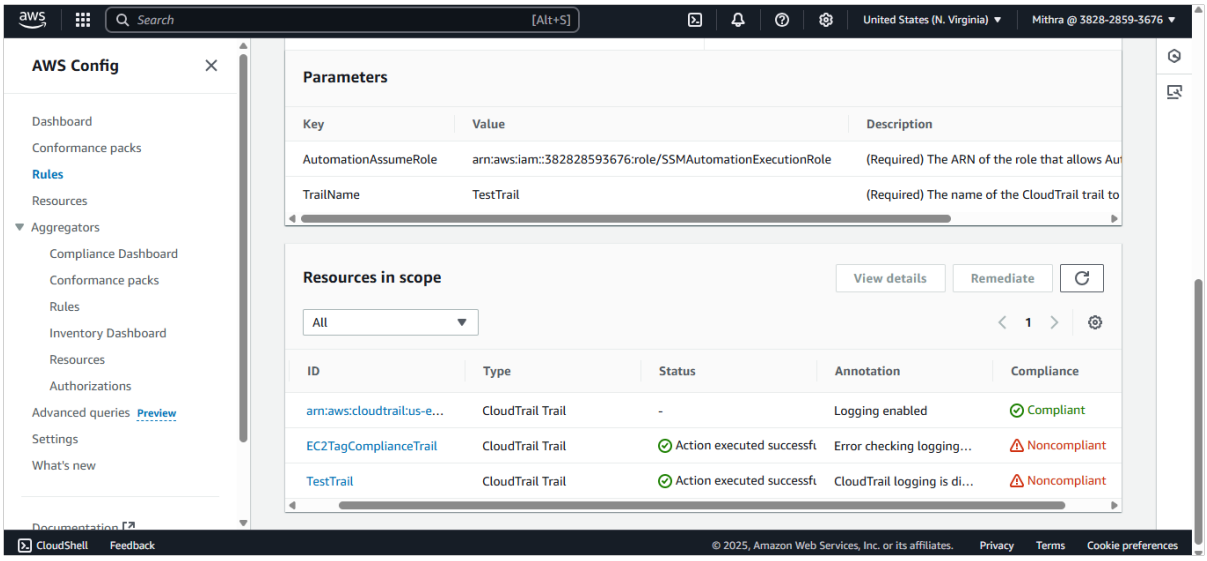


Step 8: Now config rule changed to NON-COMPLIANT

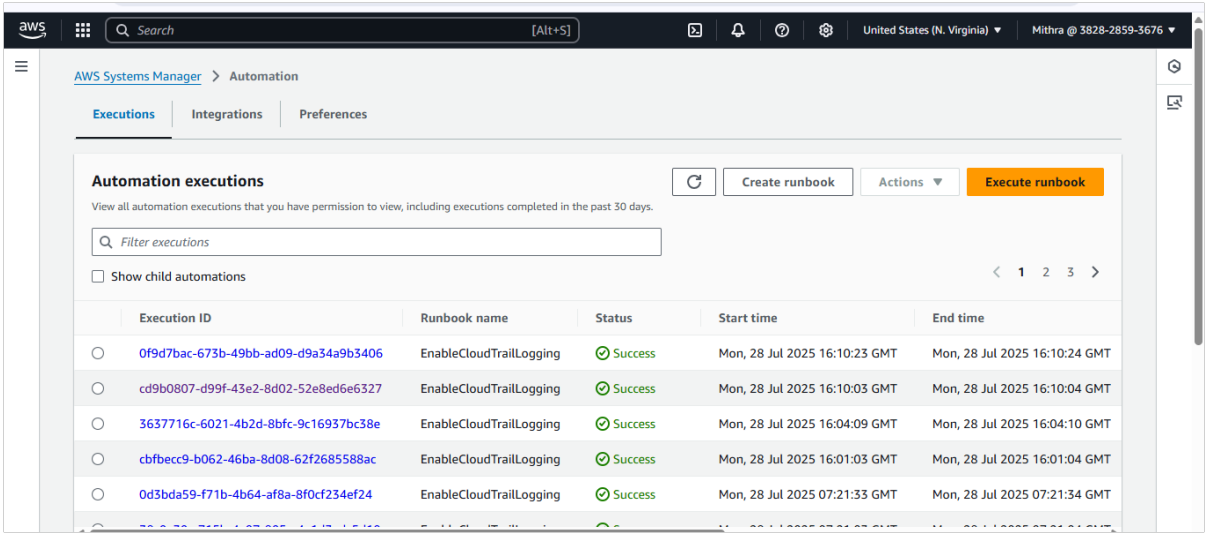

1 of 380
[AWS Config:us-east-1] AWS::CloudTrail::Trail TestTrail is NON_COMPLIANT with cloudtrailcomplianc...
Inbox ×
AWS Notifications
1:41 AM (10 hours ago)
View the Timeline for this Resource in AWS Config Management Console: https://console.aws.amazon.com/config/home?region=us-east-1#/timeline/AWS::CloudT...
AWS Notifications
2:24 AM (9 hours ago)
"resultRecordedTime": "2025-07-28T06:24:00.012Z", "configRuleInvokedTime": "2025-07-28T06:23:57.044Z", "oldEvaluationResult": { "complianceType": "COMPL...
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"...
AWS Notifications <no-reply@sns.amazonaws.com>
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:

{

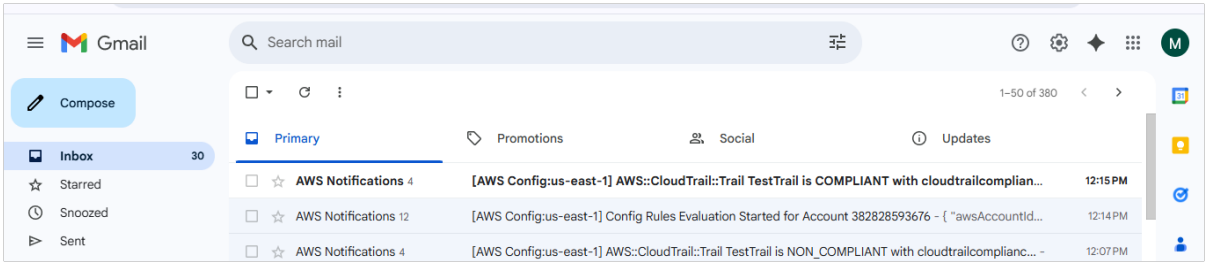

"resourceType": "AWS::CloudTrail::Trail",
"resourceId": "TestTrail",
"evaluationMode": "DETECTIVE"
},
"resourceEvaluationId": null,
"orderingTimestamp": "2025-07-28T04:22:25.000Z"
},
"complianceType": "NON_COMPLIANT",
"resultRecordedTime": "2025-07-28T16:07:50.466Z",
"configRuleInvokedTime": "2025-07-28T16:07:49.725Z",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

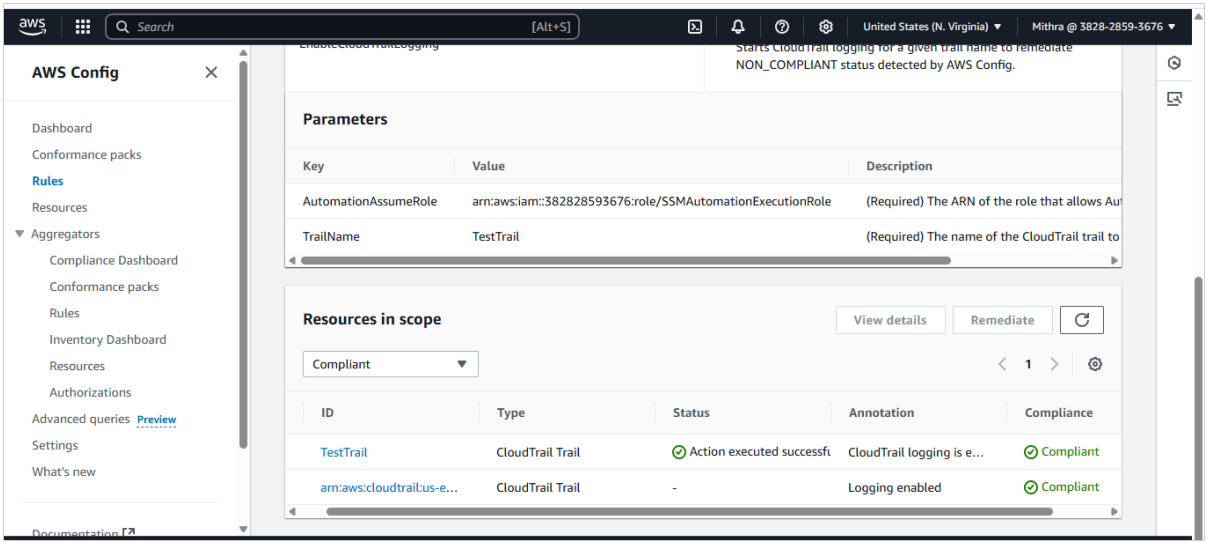


Step 9: Now the eventbridge rule will trigger and execute the SSM document



Step 10: Now we the config rule changed to COMPLIANT


Gmail
Search mail
Compose
Inbox 30
Starred
Snoozed
Sent
1–50 of 380
Primary
Promotions
Social
Updates
AWS Notifications 4 [AWS Config:us-east-1] AWS::CloudTrail::Trail TestTrail is COMPLIANT with cloudtrailcompliant... 12:15 PM
AWS Notifications 12 [AWS Config:us-east-1] Config Rules Evaluation Started for Account 382828593676 - { "awsAccountId... 12:14 PM
AWS Notifications 4 [AWS Config:us-east-1] AWS::CloudTrail::Trail TestTrail is NON_COMPLIANT with cloudtrailcomplianc... 12:07 PM


aws
Search
[Alt+S]
United States (N. Virginia)
Mithra @ 3828-2859-3676
AWS Config
Dashboard
Conformance packs
Rules
Resources
Aggregators
Compliance Dashboard
Conformance packs
Rules
Inventory Dashboard
Resources
Authorizations
Advanced queries Preview
Settings
What's new
NON_COMPLIANT status detected by AWS Config.
Parameters
Key
Value
Description
AutomationAssumeRole
arn:aws:iam::382828593676:role/SSMAutomationExecutionRole
(Required) The ARN of the role that allows Au
TrailName
TestTrail
(Required) The name of the CloudTrail trail to
Resources in scope
View details
Remediate
Compliant
1
ID
Type
Status
Annotation
Compliance
TestTrail
CloudTrail Trail
Action executed successfu
CloudTrail logging is e...
Compliant
arn:aws:cloudtrail:us-e...
CloudTrail Trail
-
Logging enabled
Compliant