# Compliance Automation Framework using AWS Config

**Objective:**

To develop an end-to-end compliance solution that

- Detects non-compliance using AWS Config.
- Automatically remediates using SSM Automation Documents or lambda
- Sends alerts via SNS and stores logs in S3/CloudWatch.

**AWS Services Used:**

- AWS Config
- SSM Automation Documents (SSM Docs)
- Amazon SNS
- AWS CloudTrail
- IAM
- Amazon S3
- Lambda
- Event bridge

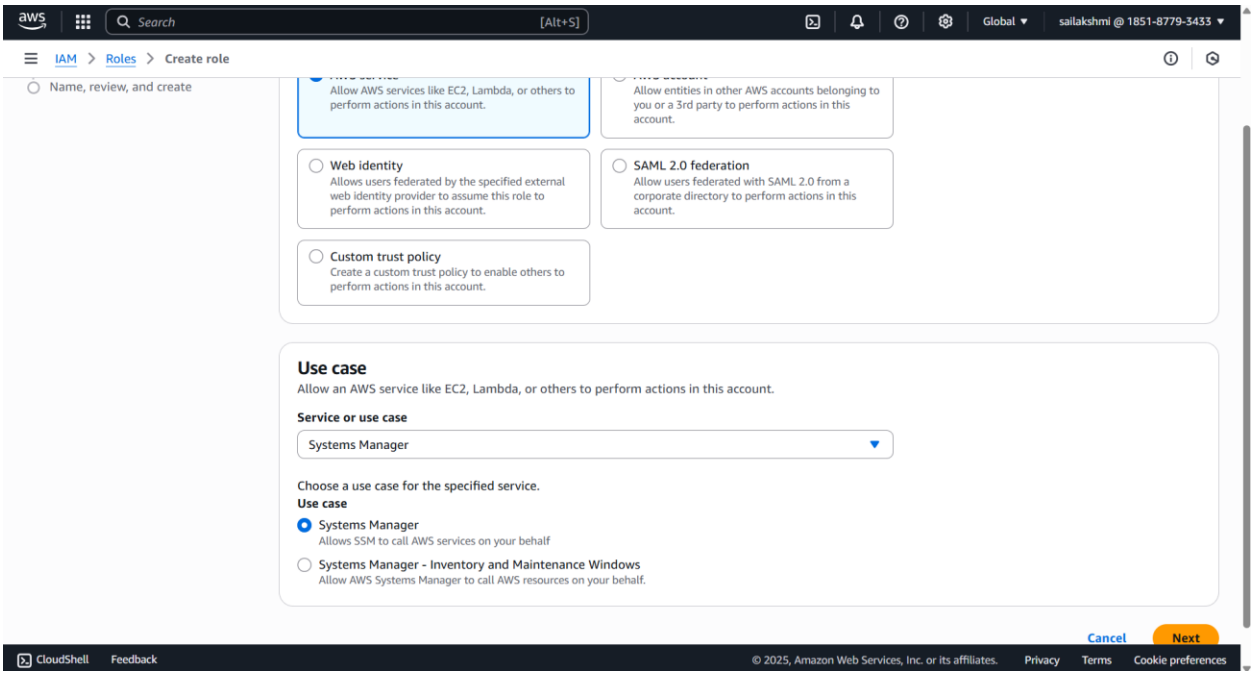
**Scenarios to Simulate**

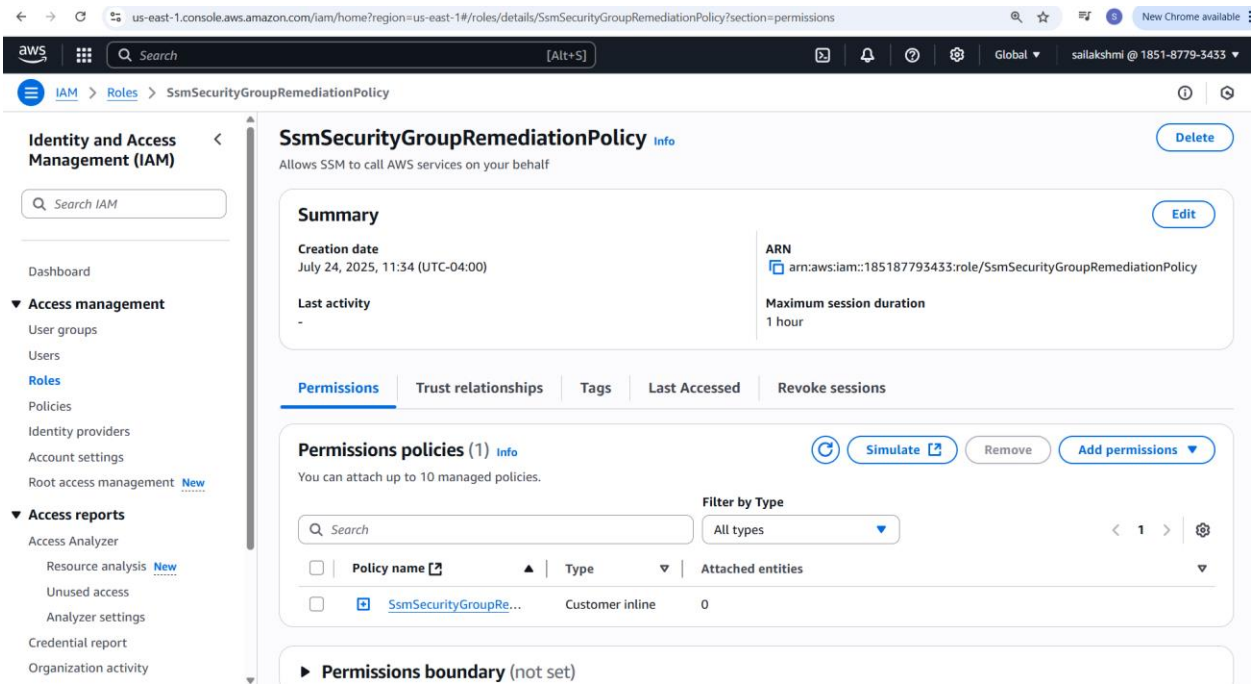
**Scenario 1: Open Security Group (Port 22 exposed to 0.0.0.0/0)**

**Step 1: Create the IAM Role for Remediation**

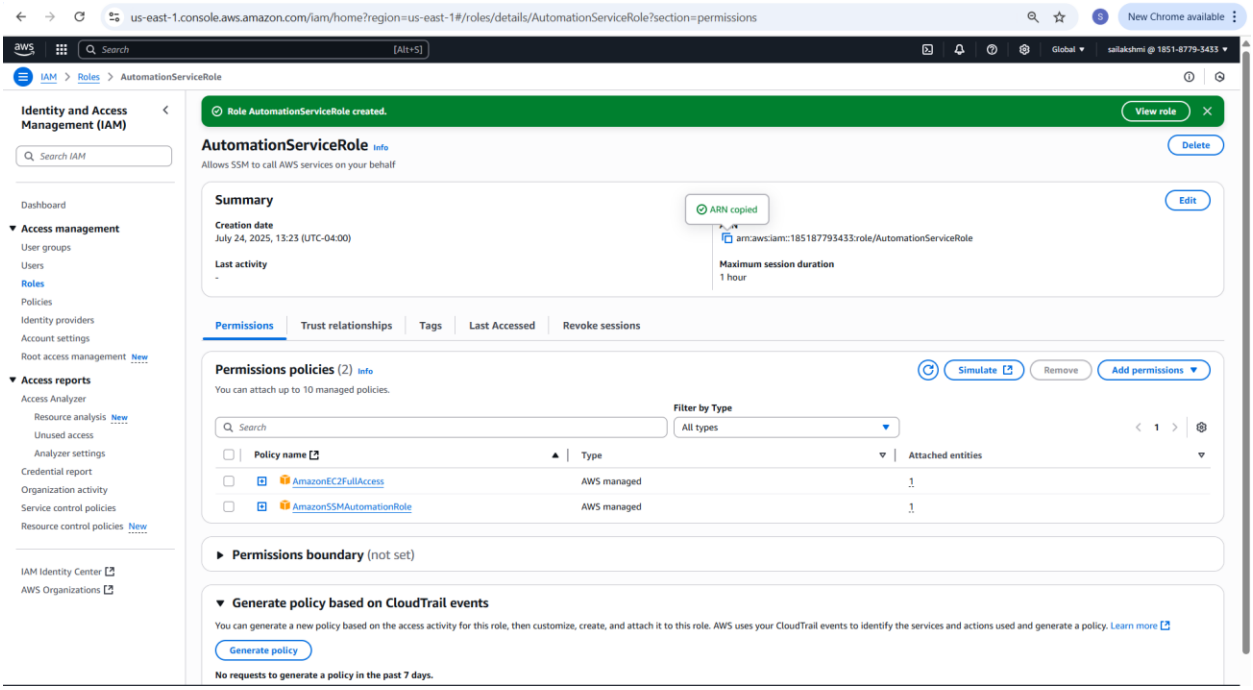
Our automation needs permission to perform actions (like changing a security group). We'll create a special role for this.

Create a IAM role for Remediation

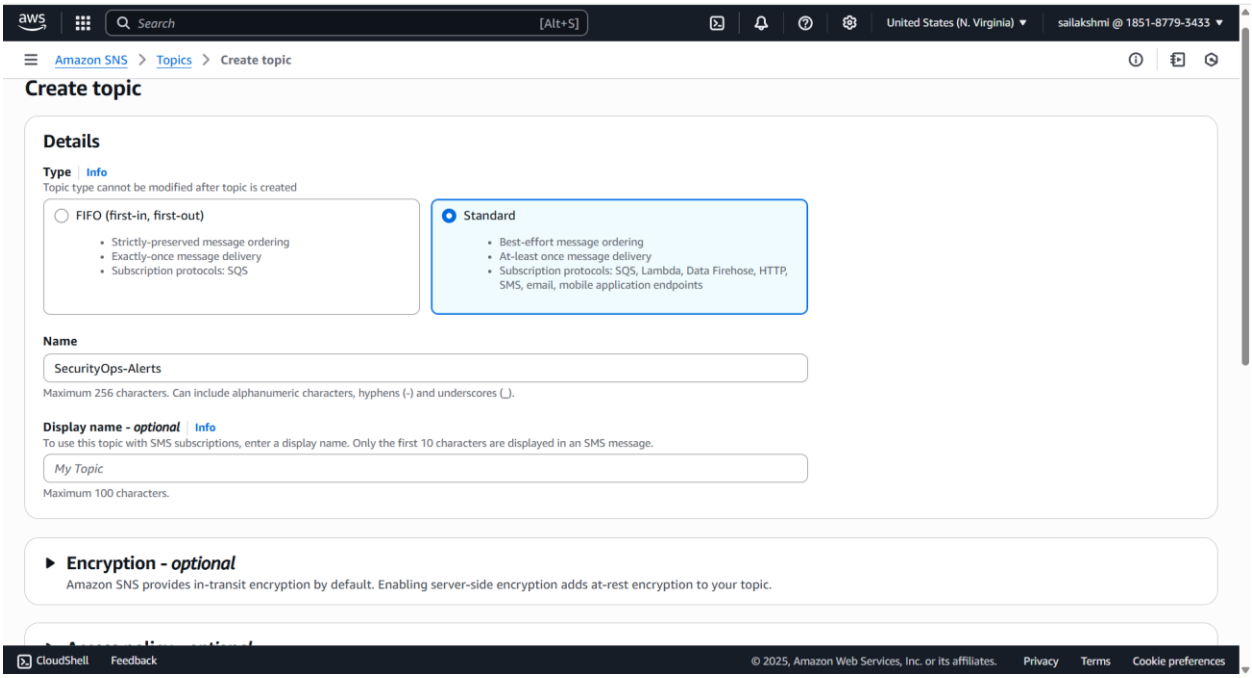


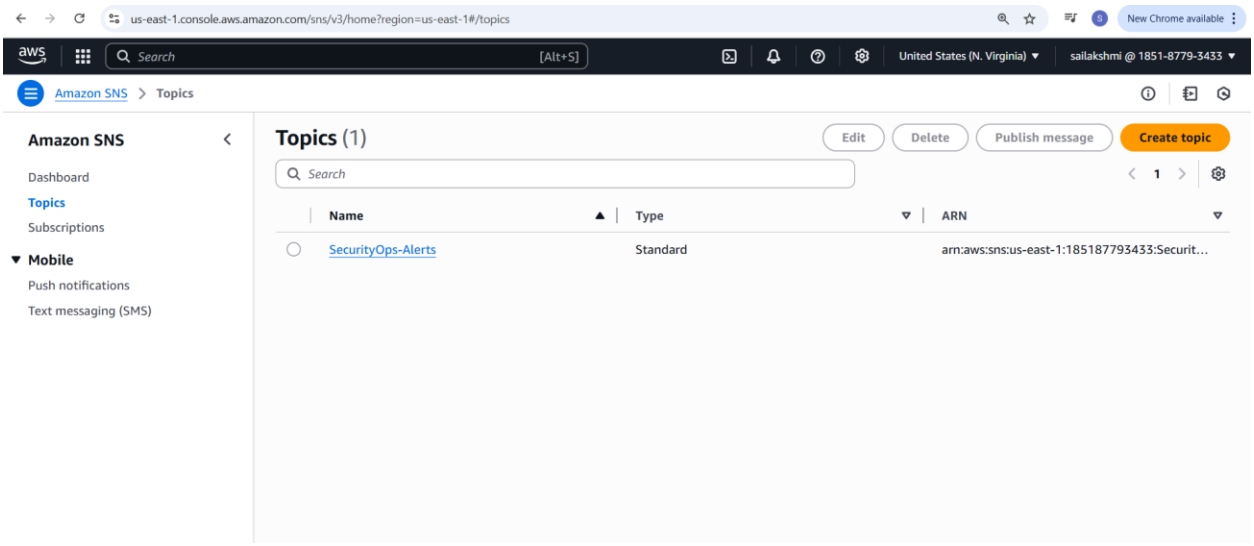




Create another role assume role

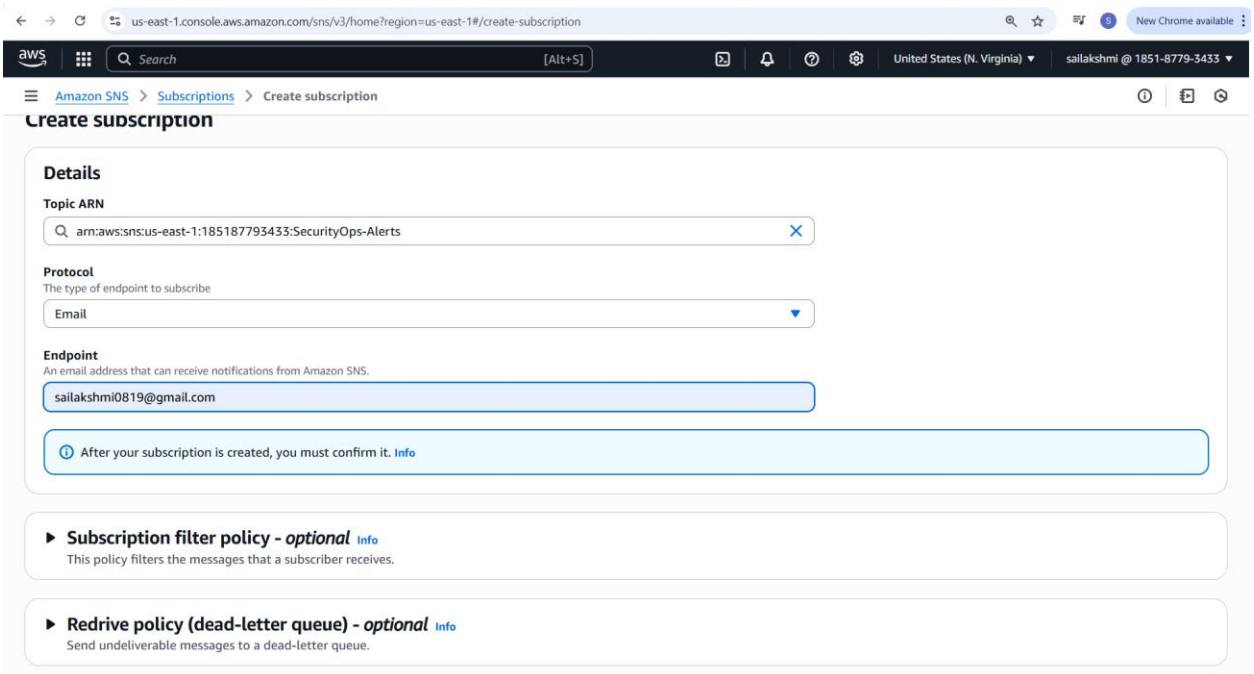


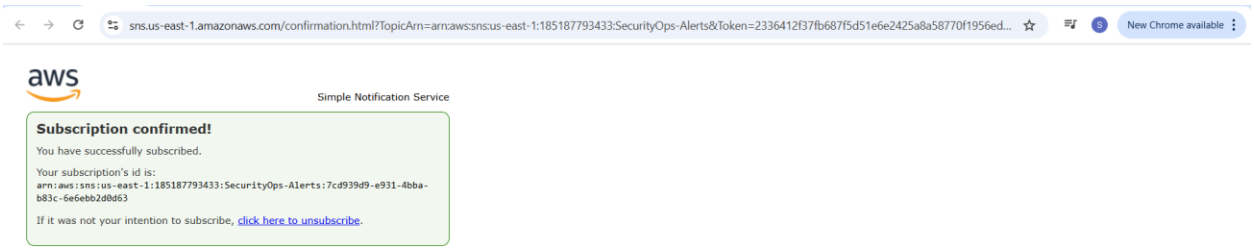

**Step 2: Create a SNS notification topic** This is how we'll get email alerts.

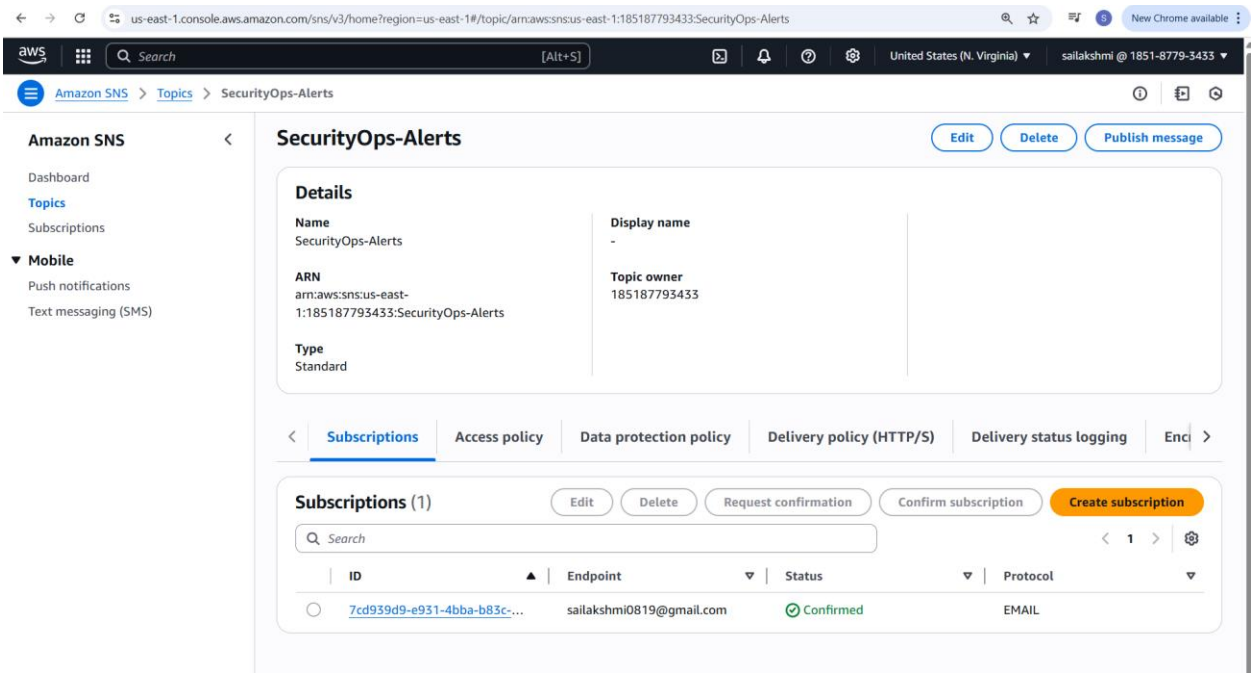





Create a subscription For Protocol, select Email

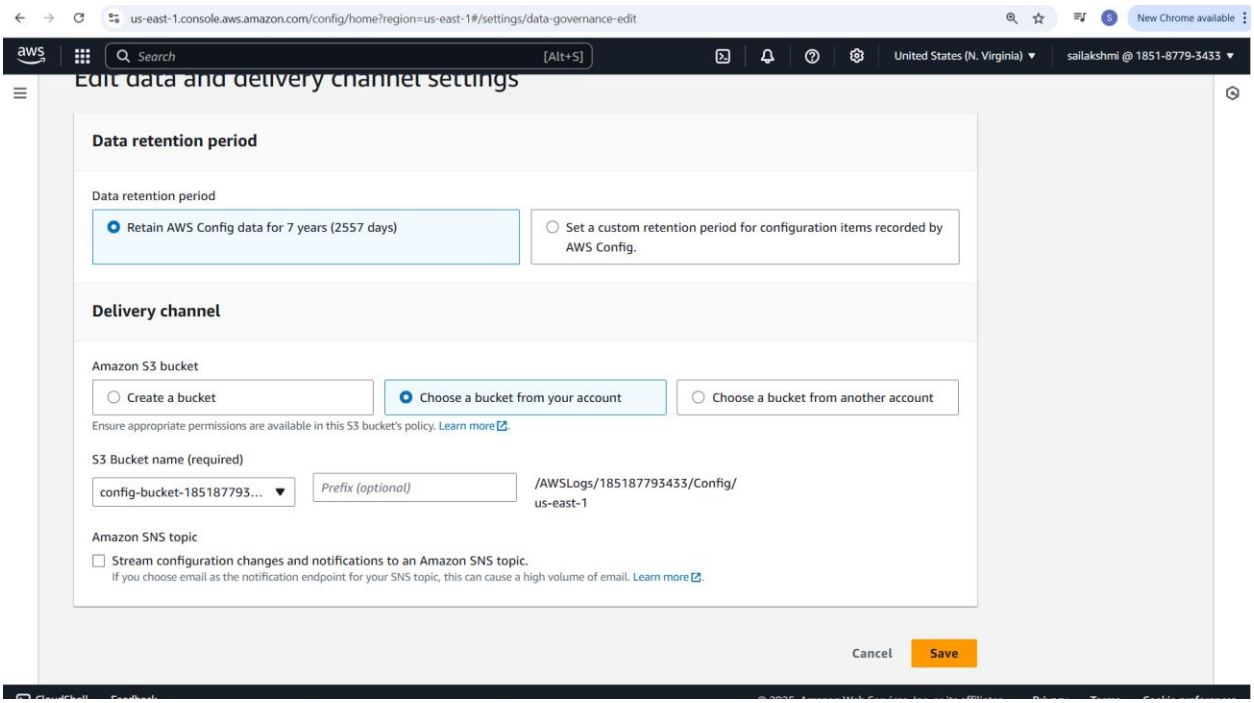


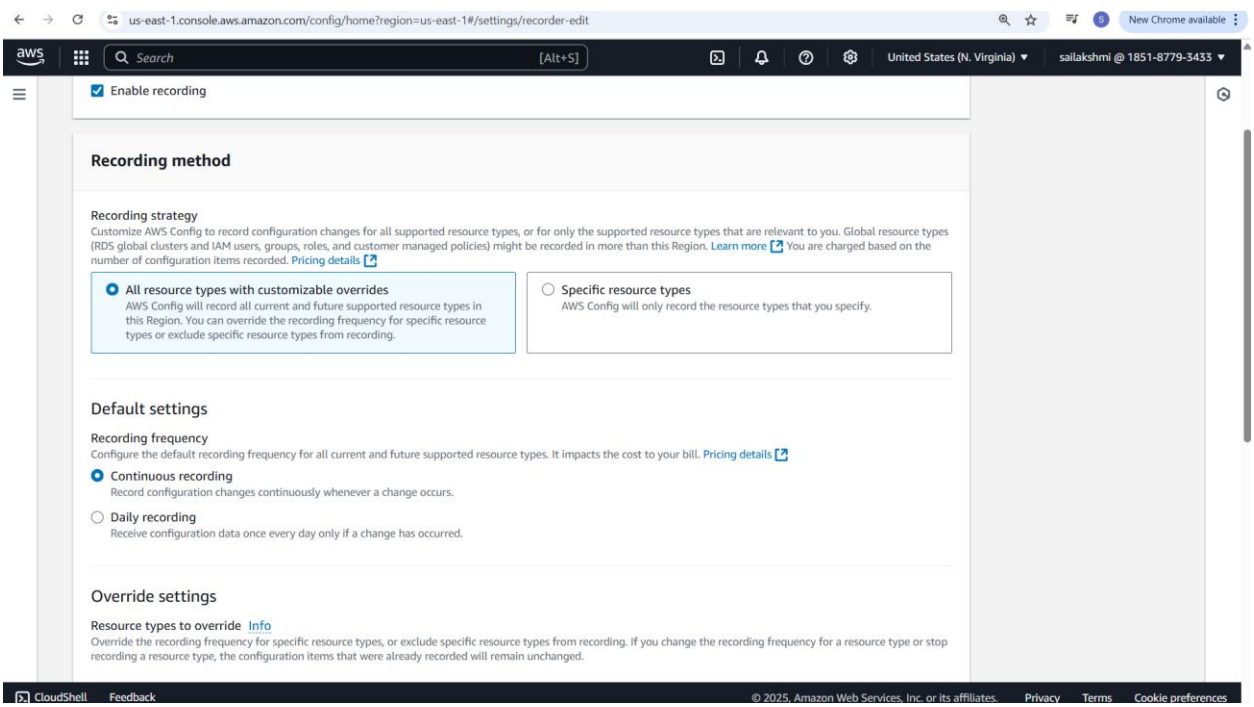


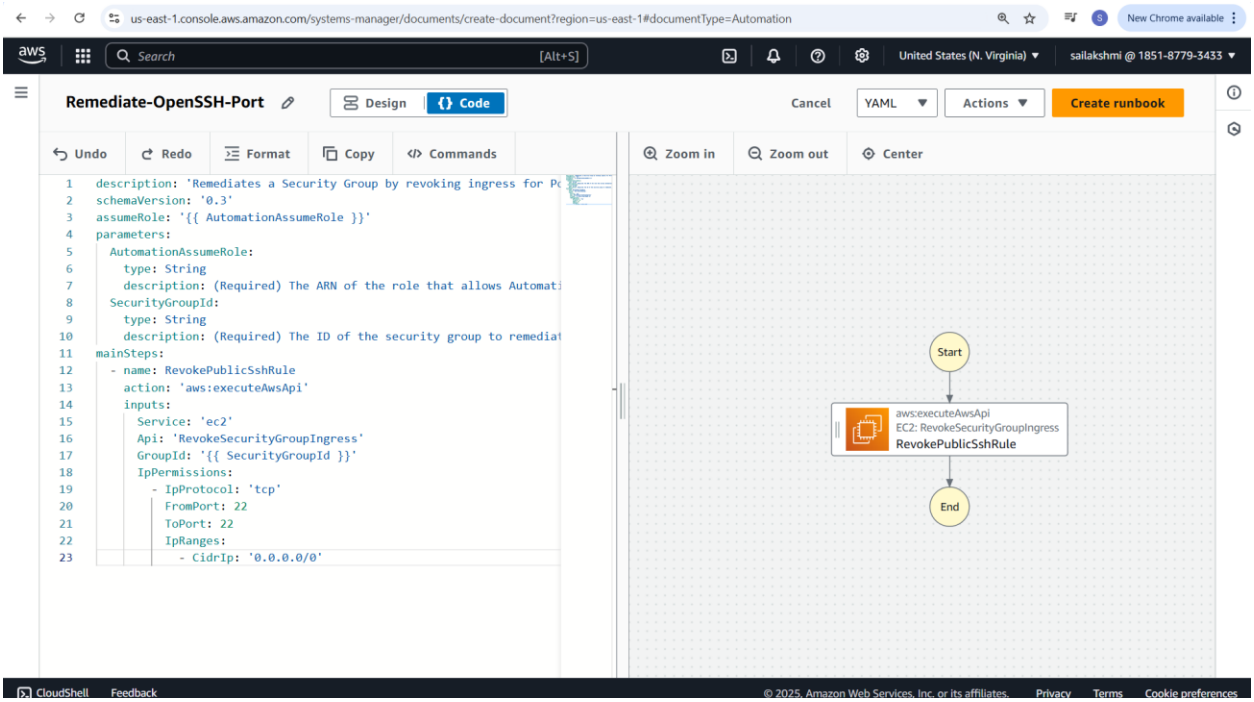

**Step 3: Enable AWS Config**

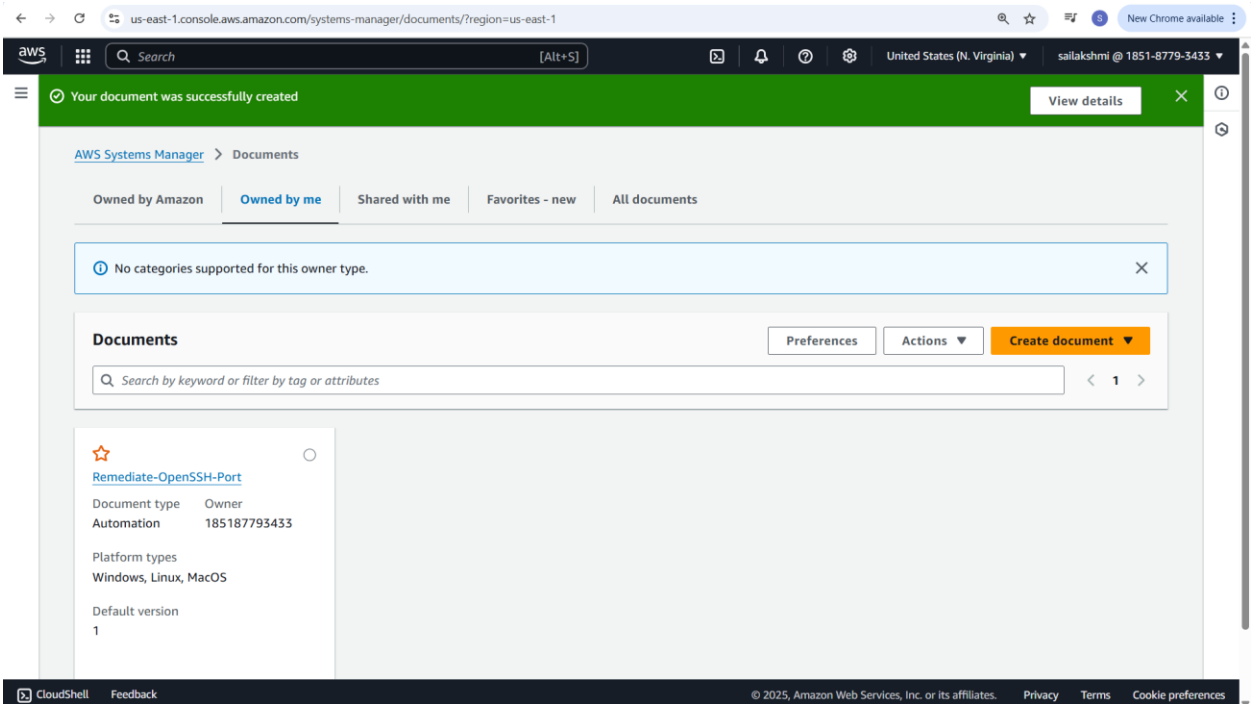
This rule will detect when a security group has Port 22 open to the world (0.0.0.0/0).




## Step 4: Create the SSM Automation Document

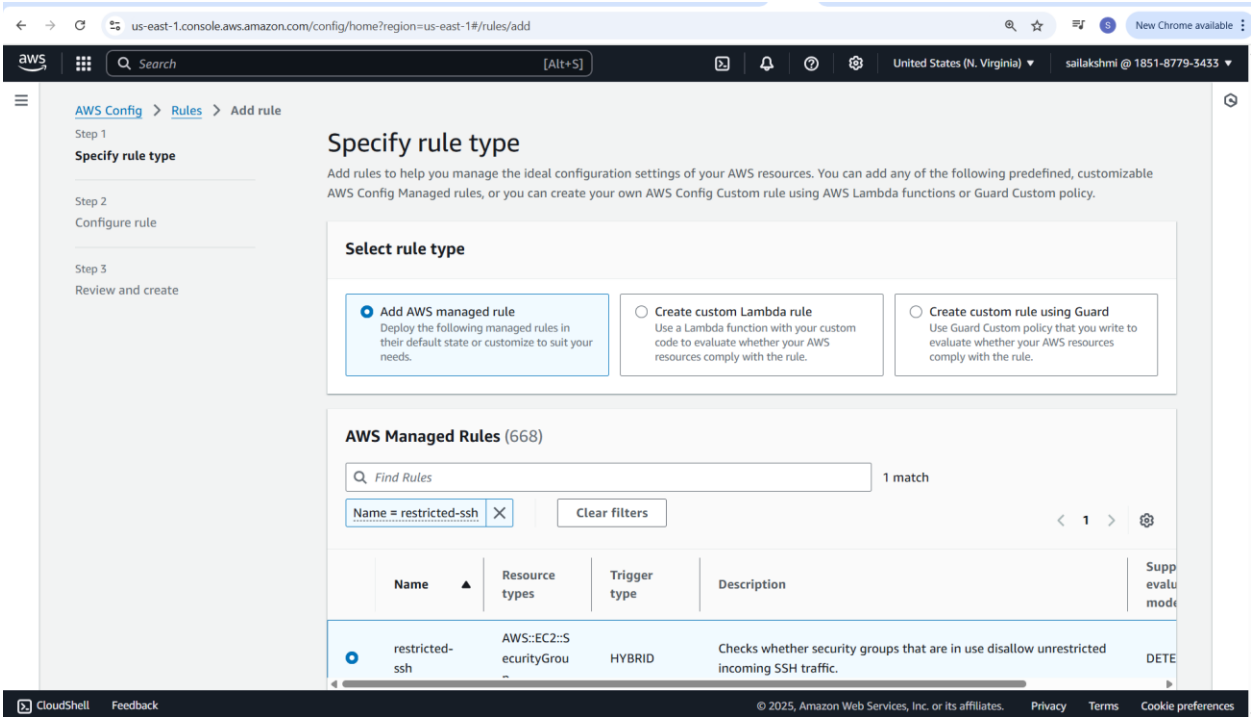


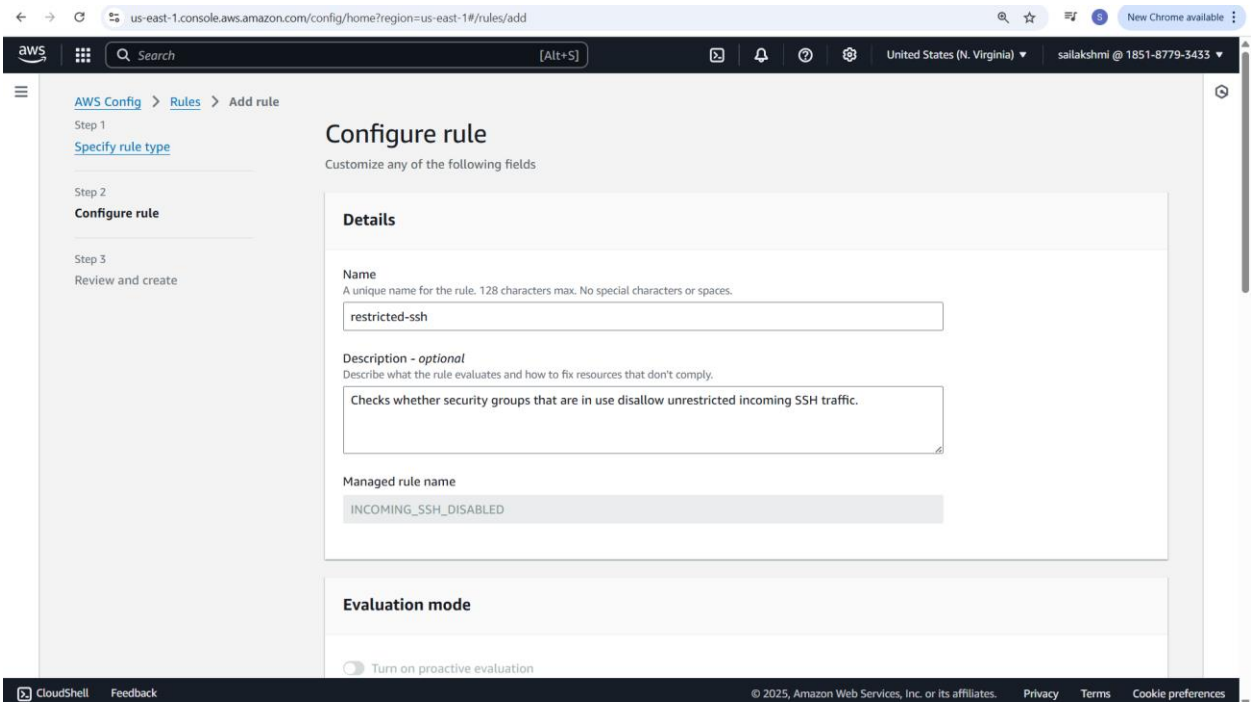




**Step 5: Create the AWS Config Rule (The "Detection Rule")**

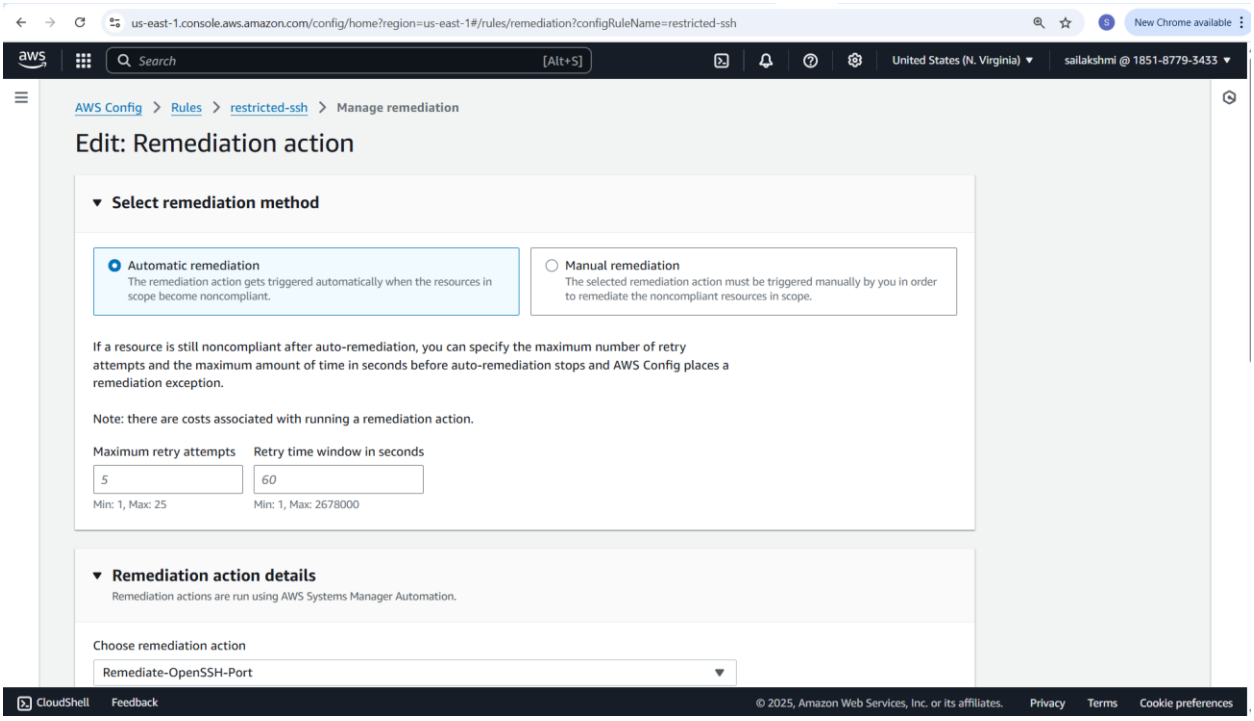
- Go to the AWS Config service.
- Ensure the recorder is ON.
- On the left menu, click Rules.
- Click Add rule.

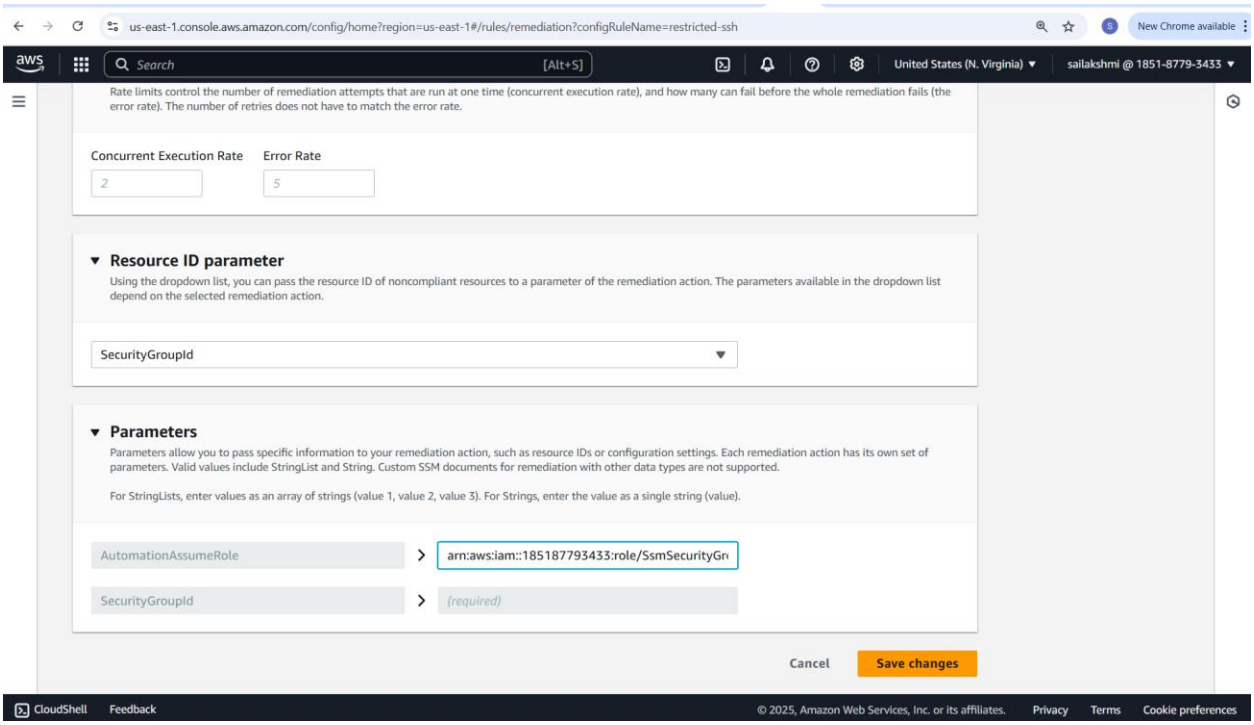
- Select Add AWS managed rule.
- In the search box, type restricted-ssh and select the rule named restricted-ssh.
- Click Next, then Add rule.



Remediation rule




**Step 6: Connect Everything with EventBridge**

This rule listens for the "Non-compliant" alert from Config and triggers our SSM document.

Create an event bridge

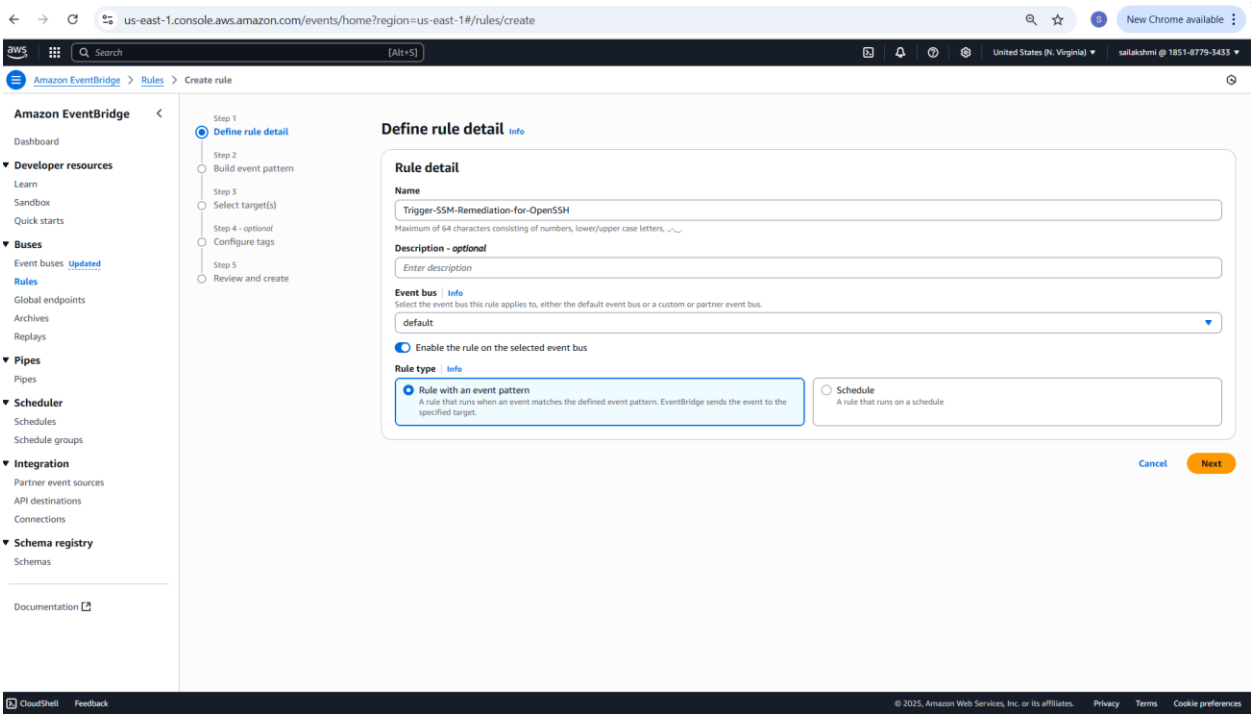
- Define rule detail: rule type give rule with an event pattern click on next
- Build event pattern:
- We want to detect whenever someone adds a security group inbound rule, specifically port 22.
- Select Event source: AWS events or AWS services
- AWS service: EC2
- Event type: AWS API Call via CloudTrail
- Any specific operation Yes
    - Type: AuthorizeSecurityGroupIngress
- This will catch events like adding an inbound SSH rule.
- Select target :
- target type –ssm automation
- Document –select your ssm document
- Configure Input Transformer Click “Create a new input transformer”
- Give input paths

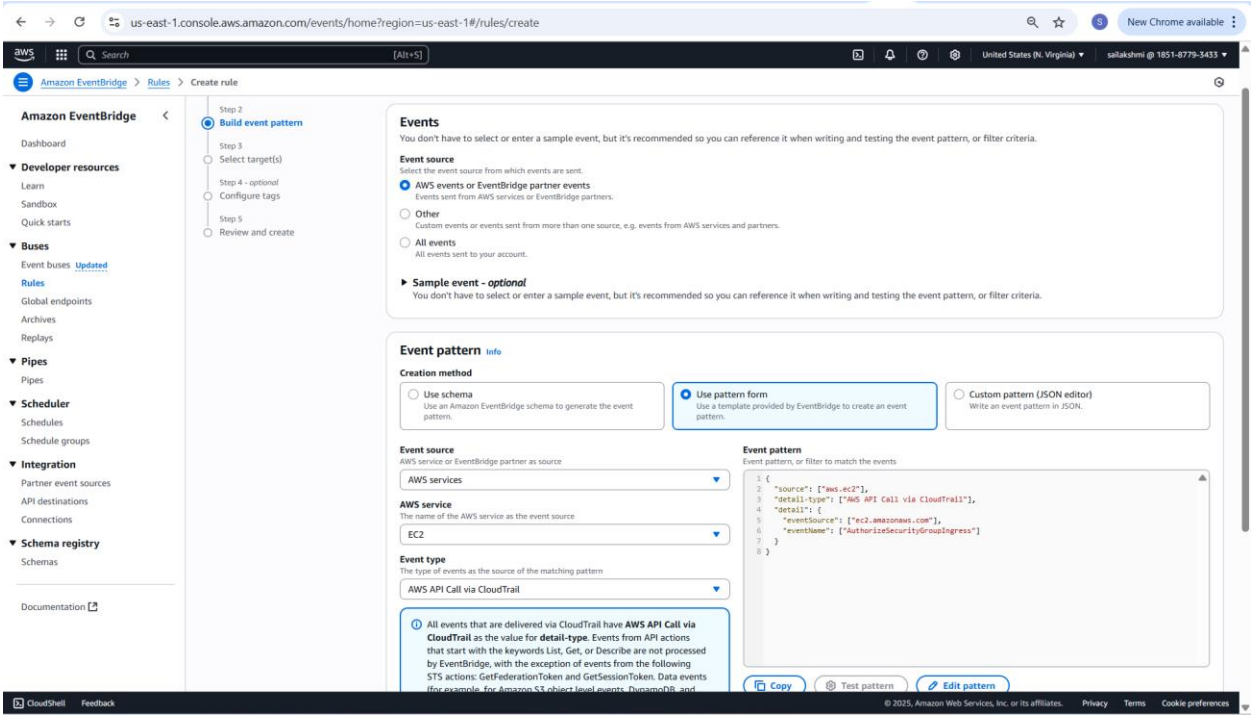
```
{
  "groupId": "$.detail.requestParameters.groupId"
}
```

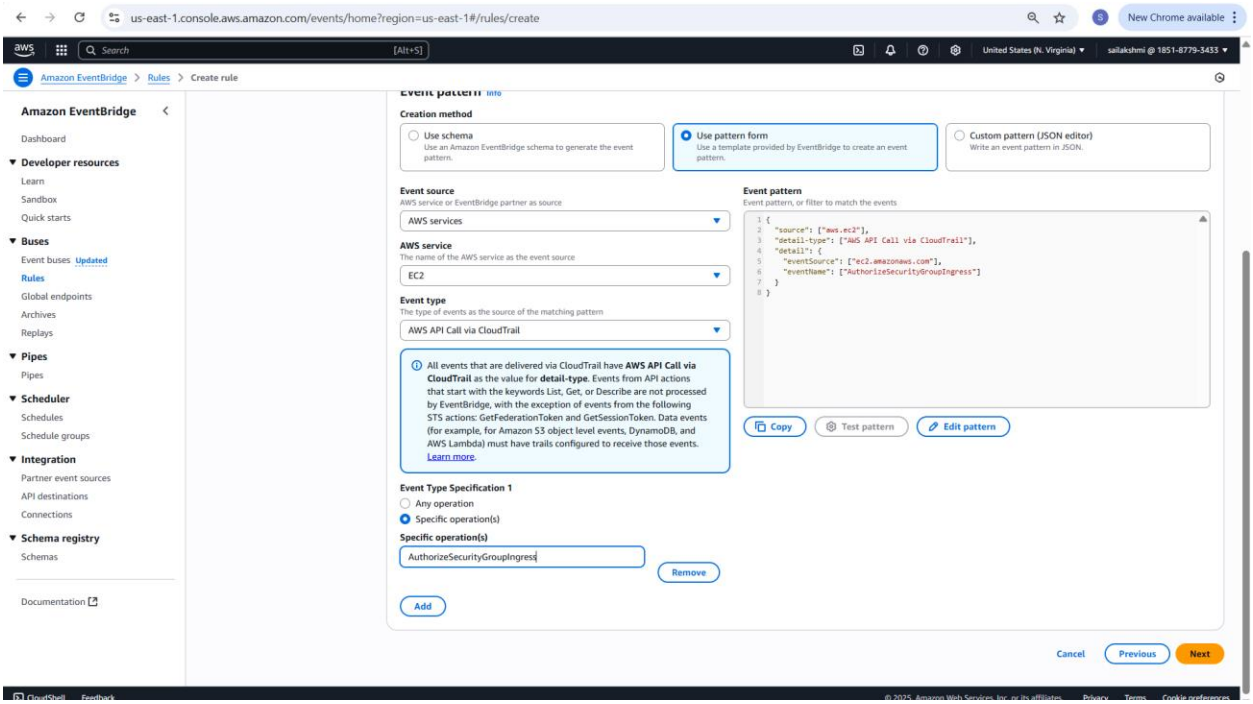
- Input template as

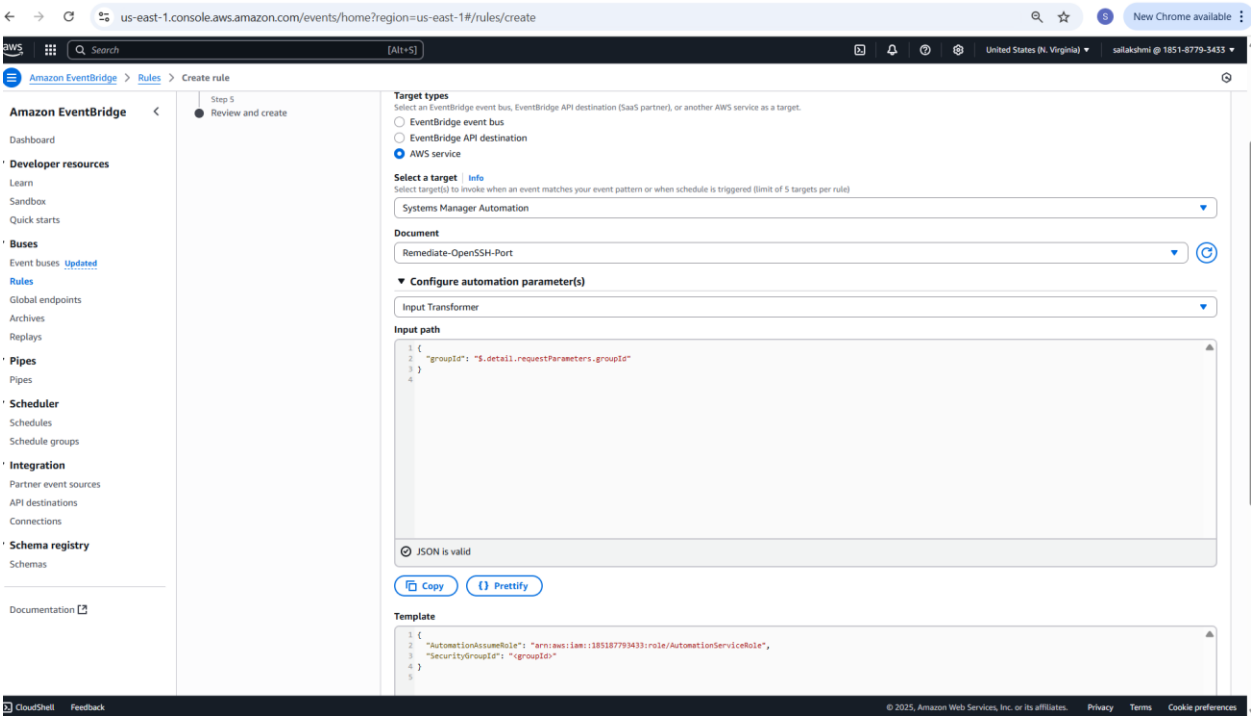
```
{
  "AutomationAssumeRole":
"arn:aws:iam::123456789012:role/SSMAutomationRemediationRole",
  "SecurityGroupId": "<groupId>"
}
```

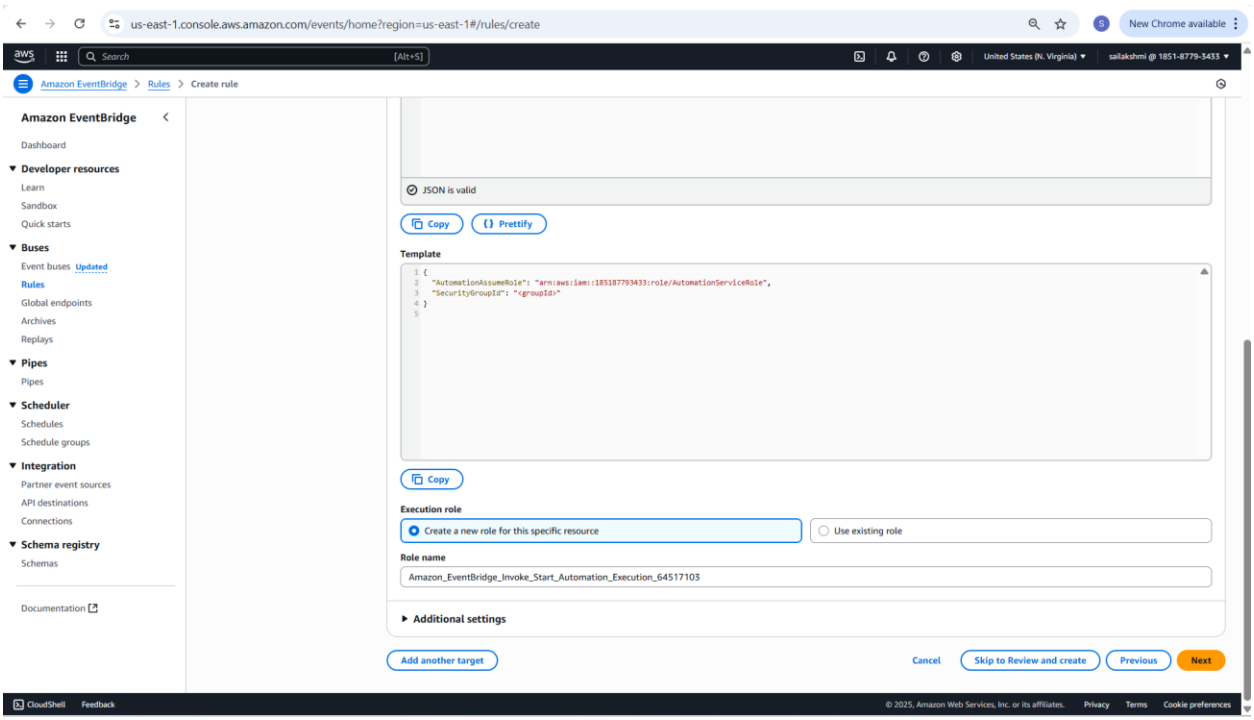
- Review and Create

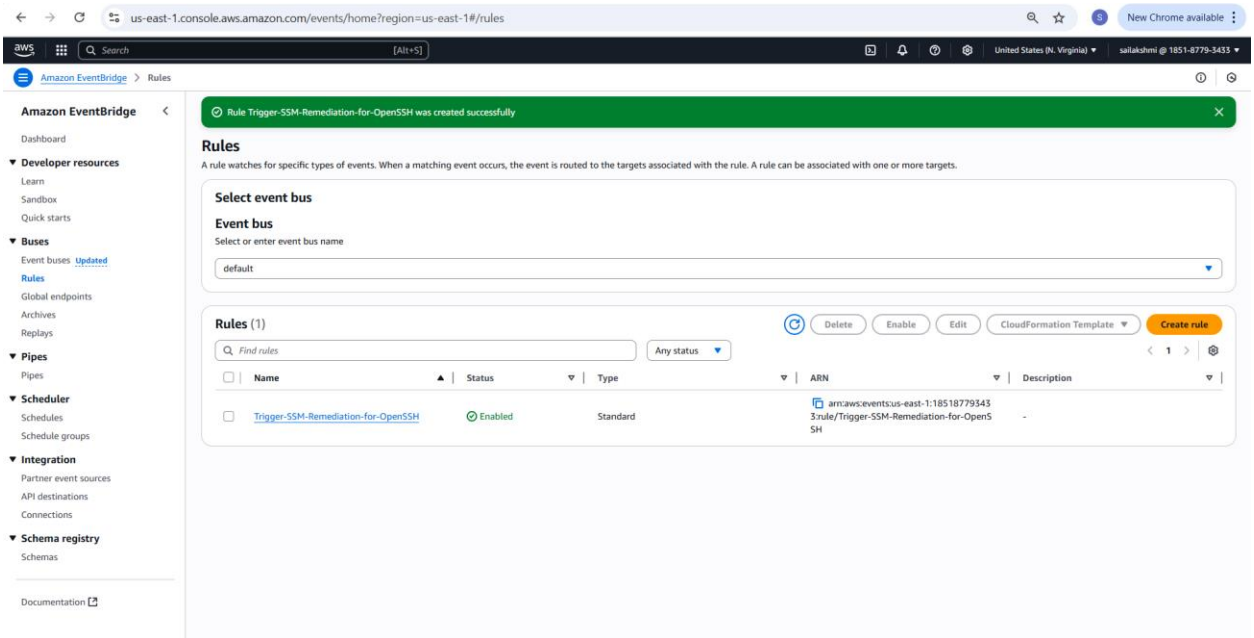

us-east-1.console.aws.amazon.com/events/home?region=us-east-1#/rules/create
New Chrome available
Search [Alt+S]
United States (N. Virginia)
sailakshmi @ 1851-8779-3433
Amazon EventBridge > Rules > Create rule
Amazon EventBridge
Dashboard
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses Updated
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
Integration
Partner event sources
API destinations
Connections
Schema registry
Schemas
Documentation
Step 1 Define rule detail
Step 2 Build event pattern
Step 3 Select target(s)
Step 4 - optional Configure tags
Step 5 Review and create
Define rule detail Info
Rule detail
Name
Trigger-SSM-Remediation-for-OpenSSH
Maximum of 64 characters consisting of numbers, lower/upper case letters, .-_.
Description - optional
Enter description
Event bus Info
Select the event bus this rule applies to, either the default event bus or a custom or partner event bus.
default
Enable the rule on the selected event bus
Rule type Info
Rule with an event pattern
A rule that runs when an event matches the defined event pattern. EventBridge sends the event to the specified target.
Schedule
A rule that runs on a schedule
Cancel
Next
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences


us-east-1.console.aws.amazon.com/events/home?region=us-east-1#/rules/create
New Chrome available
Search [Alt+S]
United States (N. Virginia)
sailakshmi @ 1851-8779-3433
Amazon EventBridge > Rules > Create rule
Amazon EventBridge
Dashboard
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses Updated
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
Integration
Partner event sources
API destinations
Connections
Schema registry
Schemas
Documentation
Step 2 Build event pattern
Step 3 Select target(s)
Step 4 - optional Configure tags
Step 5 Review and create
Events
You don't have to select or enter a sample event, but it's recommended so you can reference it when writing and testing the event pattern, or filter criteria.
Event source
Select the event source from which events are sent.
AWS events or EventBridge partner events
Events sent from AWS services or EventBridge partners.
Other
Custom events or events sent from more than one source, e.g. events from AWS services and partners.
All events
All events sent to your account.
Sample event - optional
You don't have to select or enter a sample event, but it's recommended so you can reference it when writing and testing the event pattern, or filter criteria.
Event pattern Info
Creation method
Use schema
Use an Amazon EventBridge schema to generate the event pattern.
Use pattern form
Use a template provided by EventBridge to create an event pattern.
Custom pattern (JSON editor)
Write an event pattern in JSON.
Event source
AWS service or EventBridge partner as source
AWS services
AWS service
The name of the AWS service as the event source
EC2
Event type
The type of events as the source of the matching pattern
AWS API Call via CloudTrail
All events that are delivered via CloudTrail have AWS API Call via CloudTrail as the value for detail-type. Events from API actions that start with the keywords List, Get, or Describe are not processed by EventBridge, with the exception of events from the following STS actions: GetFederationToken and GetSessionToken. Data events (for example, for Amazon S3 object level events, DynamoDB, and
Event pattern
Event pattern, or filter to match the events
{
"source": ["aws.ec2"],
"detail-type": ["AWS API Call via CloudTrail"],
"detail": {
"eventSource": ["ec2.amazonaws.com"],
"eventName": ["AuthorizeSecurityGroupIngress"]
}
}
Copy
Test pattern
Edit pattern
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences


us-east-1.console.aws.amazon.com/events/home?region=us-east-1#/rules/create
New Chrome available
Search [Alt+S]
United States (N. Virginia)
sailakshmi @ 1851-8779-3433
Amazon EventBridge > Rules > Create rule
Amazon EventBridge
Dashboard
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses Updated
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
Integration
Partner event sources
API destinations
Connections
Schema registry
Schemas
Documentation
Creation method
Use schema
Use an Amazon EventBridge schema to generate the event pattern.
Use pattern form
Use a template provided by EventBridge to create an event pattern.
Custom pattern (JSON editor)
Write an event pattern in JSON.
Event source
AWS service or EventBridge partner as source
AWS services
AWS service
The name of the AWS service as the event source
EC2
Event type
The type of events as the source of the matching pattern
AWS API Call via CloudTrail
All events that are delivered via CloudTrail have AWS API Call via CloudTrail as the value for detail-type. Events from API actions that start with the keywords List, Get, or Describe are not processed by EventBridge, with the exception of events from the following STS actions: GetFederationToken and GetSessionToken. Data events (for example, for Amazon S3 object level events, DynamoDB, and AWS Lambda) must have trails configured to receive those events. Learn more.
Event Type Specification 1
Any operation
Specific operation(s)
Specific operation(s)
AuthorizeSecurityGroupIngress
Remove
Add
Event pattern
Event pattern, or filter to match the events
{
"source": ["aws.ec2"],
"detail-type": ["AWS API Call via CloudTrail"],
"detail": {
"eventSource": ["ec2.amazonaws.com"],
"eventName": ["AuthorizeSecurityGroupIngress"]
}
}
Copy
Test pattern
Edit pattern
Cancel
Previous
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com/events/home?region=us-east-1#/rules/create
New Chrome available
Search [Alt+S]
United States (N. Virginia)
sailakshmi @ 1851-8779-3433
Amazon EventBridge > Rules > Create rule
Step 5
Review and create
Amazon EventBridge
Dashboard
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses Updated
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
Integration
Partner event sources
API destinations
Connections
Schema registry
Schemas
Documentation
Target types
Select an EventBridge event bus, EventBridge API destination (SaaS partner), or another AWS service as a target.
EventBridge event bus
EventBridge API destination
AWS service
Select a target Info
Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)
Systems Manager Automation
Document
Remediate-OpenSSH-Port
Configure automation parameter(s)
Input Transformer
Input path
{
"groupId": "$.detail.requestParameters.groupId"
}
JSON is valid
Copy
Prettify
Template
{
"AutomationAssumeRole": "arn:aws:iam::185187793433:role/AutomationServiceRole",
"SecurityGroupId": "<groupId>"
}
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

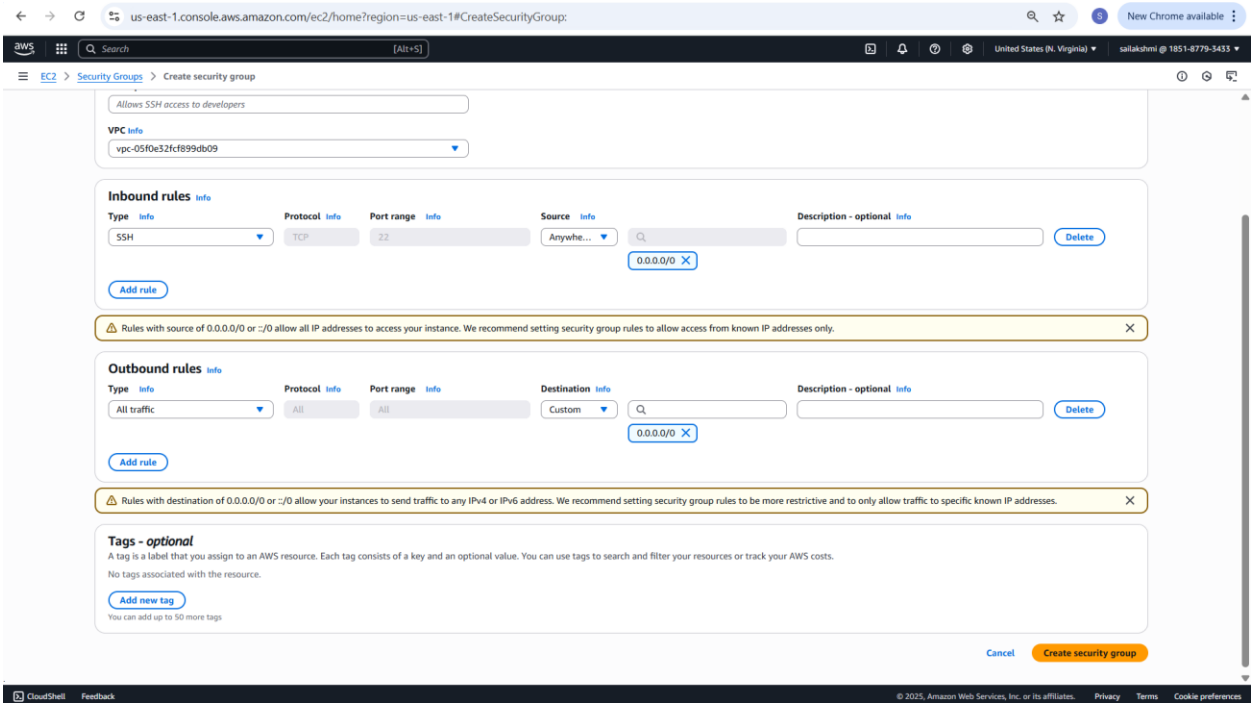



## Step 7: Testing the Automation setup

- Create a new security group Add an Inbound rule:

    - Type: SSH
    - Source: Anywhere-IPv4 (0.0.0.0/0)
- Save the rule.
- Now, wait. AWS Config can take a few minutes to evaluate the change.
- Check the result:
    - You should receive an email notification from SNS.
    - Go back to the Security Group in the EC2 console. Refresh the page. The rule you just added should be gone!
    - Go to AWS Config > Rules. The restricted-ssh rule might briefly show "Non-compliant" before changing back to "Compliant".
    - Go to Systems Manager > Automations. You will see an execution of your Remediate document with a "Success" status.




Got email form SNS

2 of 601

[AWS Config:us-east-1] AWS::EC2::SecurityGroup sg-0b62619d87fedf997 is NON_COMPLIANT with restric...

Inbox ×

**AWS Notifications** <no-reply@sns.amazonaws.com> 2:13 PM (3 minutes ago)

to me

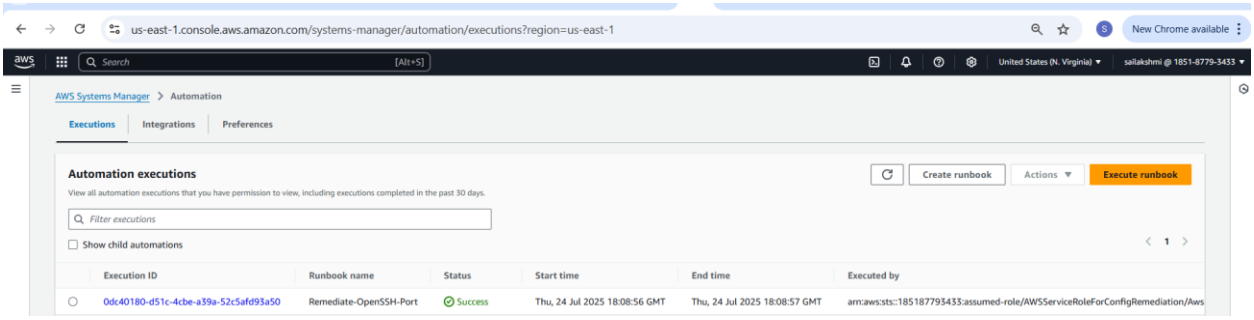
View the Timeline for this Resource in AWS Config Management Console:
https://console.aws.amazon.com/config/home?region=us-east-1#/timeline/AWS::EC2::SecurityGroup/sg-0b62619d87fedf997?time=2025-07-24T18:12:37.084Z

New Compliance Change Record:

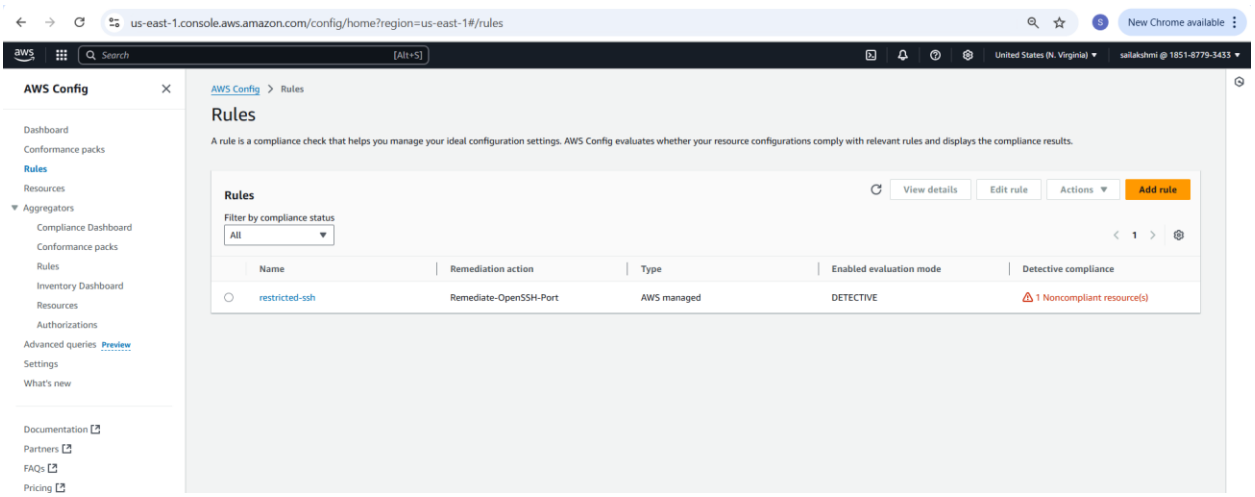
---


```
{
  "awsAccountId": "185187793433",
  "configRuleName": "restricted-ssh",
  "configRuleARN": "arn:aws:config:us-east-1:185187793433:config-rule/config-rule-bycacb",
  "resourceType": "AWS::EC2::SecurityGroup",
  "resourceId": "sg-0b62619d87fedf997",
  "awsRegion": "us-east-1",
  "newEvaluationResult": {
    "evaluationResultIdentifier": {
      "evaluationResultQualifier": {
        "configRuleName": "restricted-ssh",
        "resourceType": "AWS::EC2::SecurityGroup",
        "resourceId": "sg-0b62619d87fedf997",
        "evaluationMode": "DETECTIVE"
      },
      "resourceEvaluationId": null,
      "orderingTimestamp": "2025-07-24T18:12:37.084Z"
    },
    "complianceType": "NON_COMPLIANT"
```

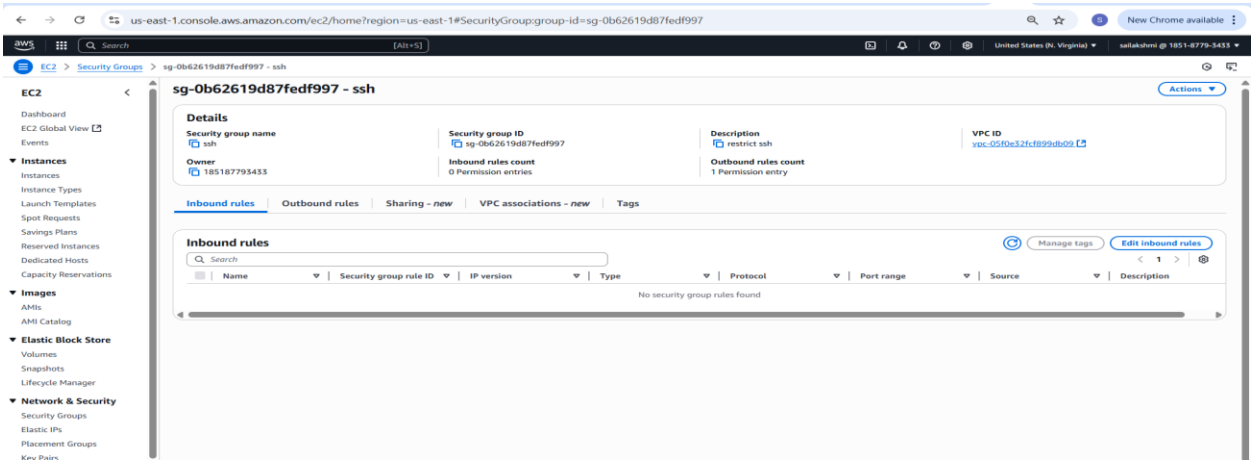

System manager with a "Success" status




AWS config show "Non-compliant"

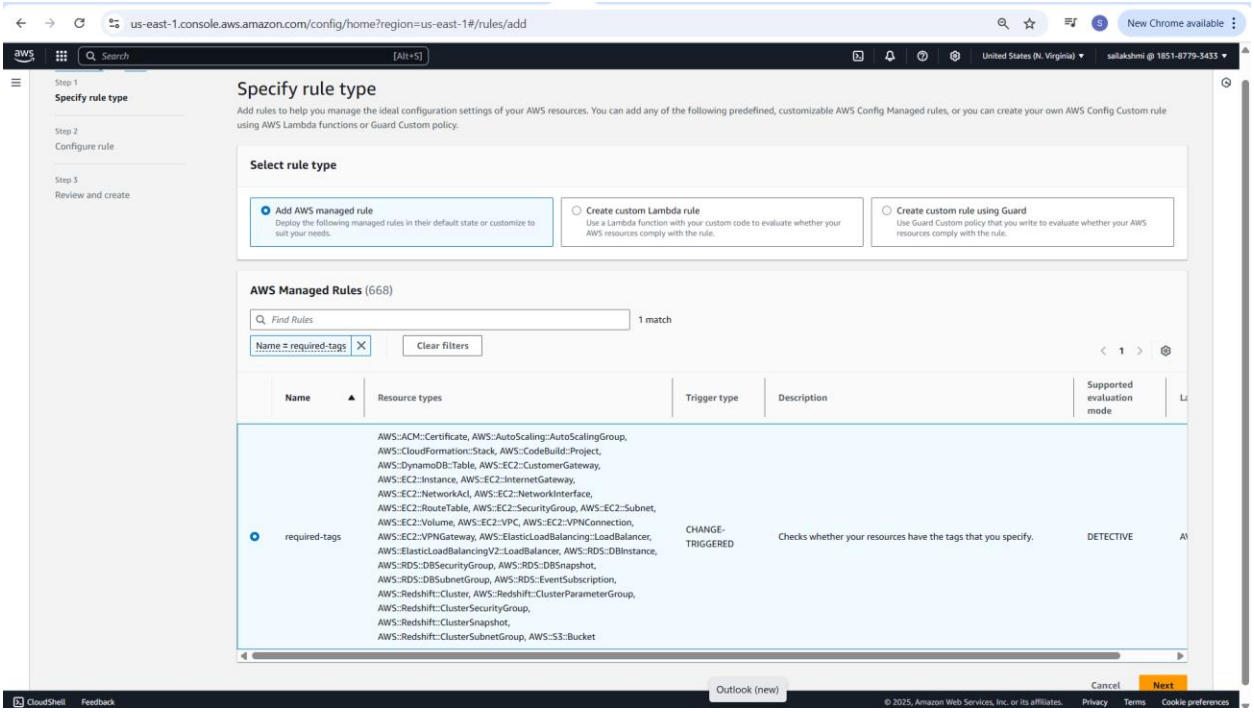


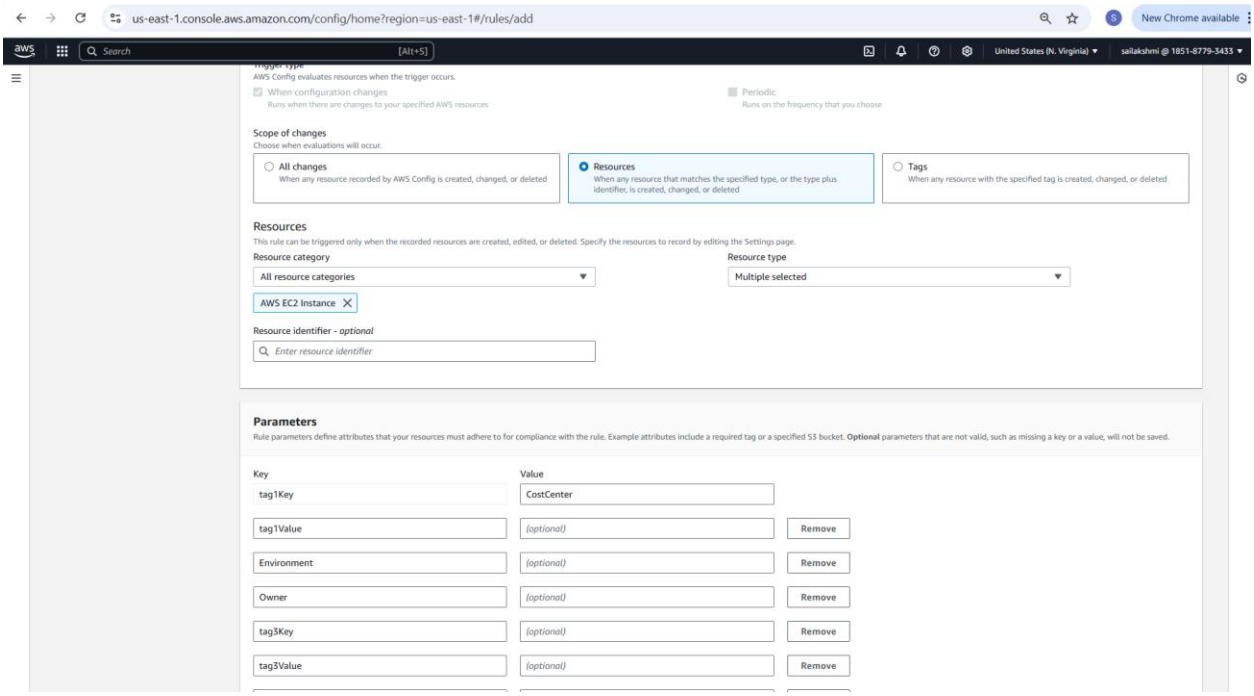

Security group rule deleted

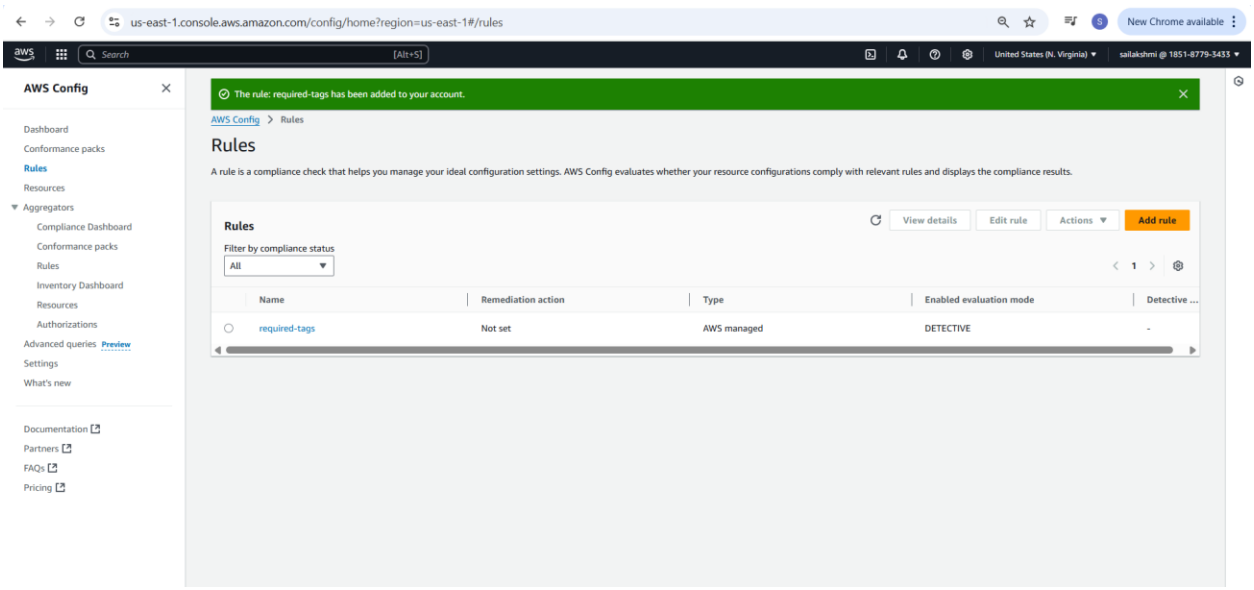



## Scenario 2: Missing Required Tags on EC2

## Step 1: Create AWS Config Rule to Detect Missing Tags

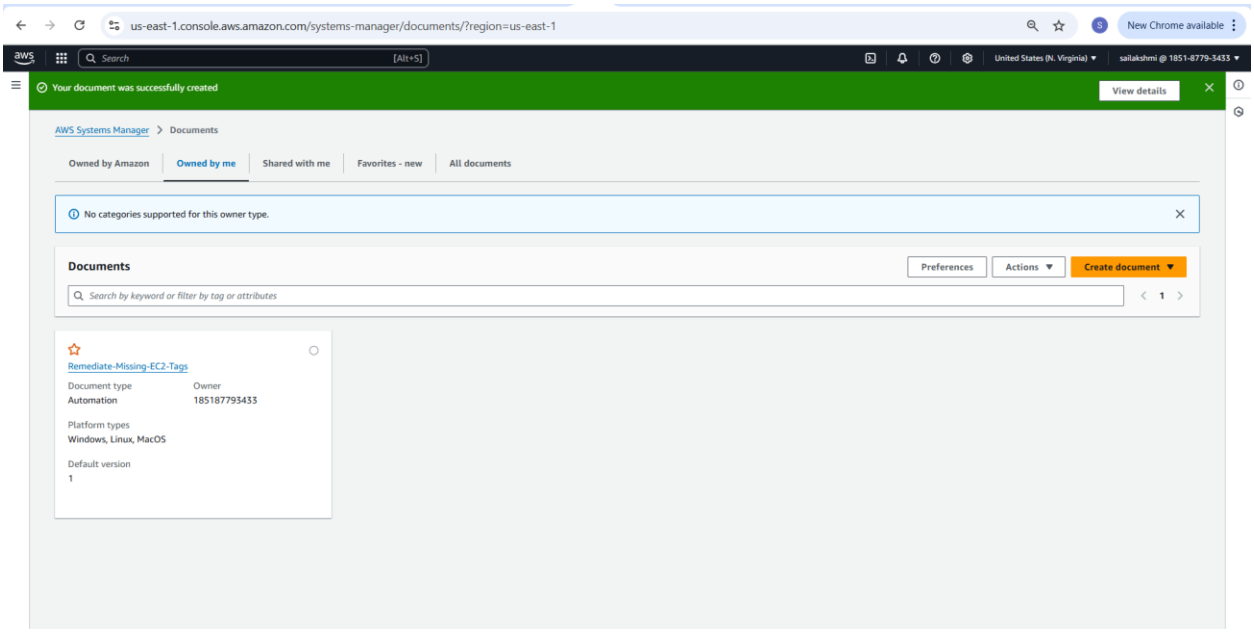

us-east-1.console.aws.amazon.com/config/home?region=us-east-1#/rules/add
New Chrome available
Search
[Alt+S]
United States (N. Virginia)
sailakshmi @ 1851-8779-3433
Step 1
Specify rule type
Step 2
Configure rule
Step 3
Review and create
Specify rule type
Add rules to help you manage the ideal configuration 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 (668)
Find Rules
1 match
Name = required-tags
Clear filters
Name
Resource types
Trigger type
Description
Supported evaluation mode
required-tags
AWS::ACM::Certificate, AWS::AutoScaling::AutoScalingGroup, AWS::CloudFormation::Stack, AWS::CodeBuild::Project, AWS::DynamoDB::Table, AWS::EC2::CustomerGateway, AWS::EC2::Instance, AWS::EC2::InternetGateway, AWS::EC2::NetworkAcl, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable, AWS::EC2::SecurityGroup, AWS::EC2::Subnet, AWS::EC2::Volume, AWS::EC2::VPC, AWS::EC2::VPNConnection, AWS::EC2::VPNGateway, AWS::ElasticLoadBalancing::LoadBalancer, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::RDS::DBInstance, AWS::RDS::DBSecurityGroup, AWS::RDS::DBSnapshot, AWS::RDS::DBSubnetGroup, AWS::RDS::EventSubscription, AWS::Redshift::Cluster, AWS::Redshift::ClusterParameterGroup, AWS::Redshift::ClusterSecurityGroup, AWS::Redshift::ClusterSnapshot, AWS::Redshift::ClusterSubnetGroup, AWS::S3::Bucket
CHANGE-TRIGGERED
Checks whether your resources have the tags that you specify.
DETECTIVE
Outlook (new)
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com/config/home?region=us-east-1#/rules/add
New Chrome available
Search
[Alt+S]
United States (N. Virginia)
sailakshmi @ 1851-8779-3433
AWS Config evaluates resources when the trigger occurs.
When configuration changes
Runs when there are changes to your specified AWS resources
Periodic
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 Instance
Resource identifier - optional
Enter resource identifier
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
CostCenter
tag1Value
(optional)
Remove
Environment
(optional)
Remove
Owner
(optional)
Remove
tag3Key
(optional)
Remove
tag3Value
(optional)
Remove




## Step 2: SSM Automation Document for EC2 Tag Remediation

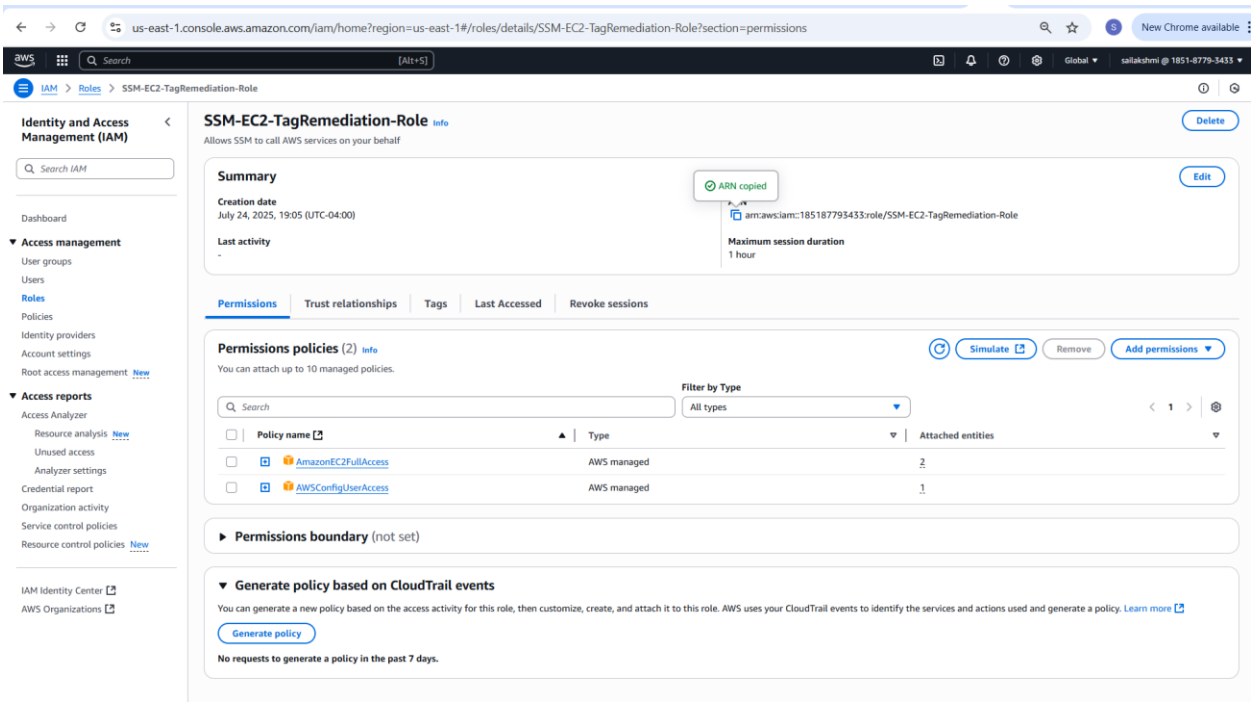
Create SSM Document: Remediate-Missing-EC2-Tags




## Step 3: IAM Role for EC2 Tag Remediation

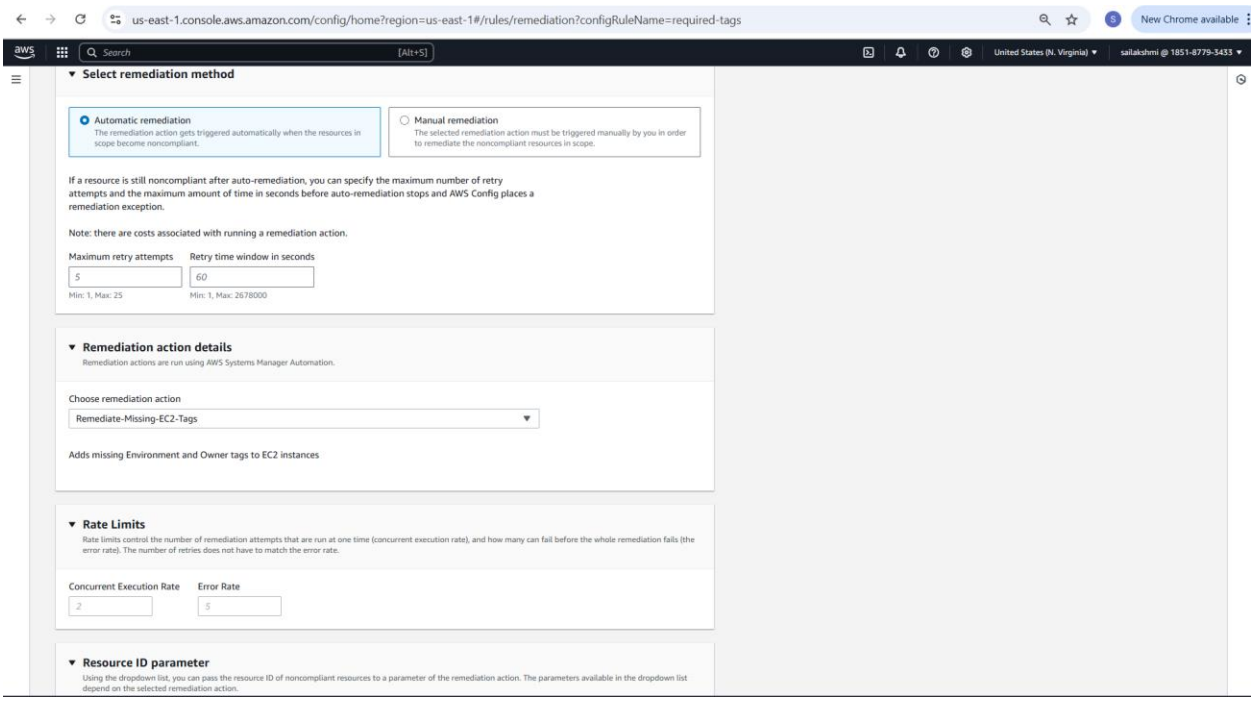
Policy: AmazonEC2FullAccess

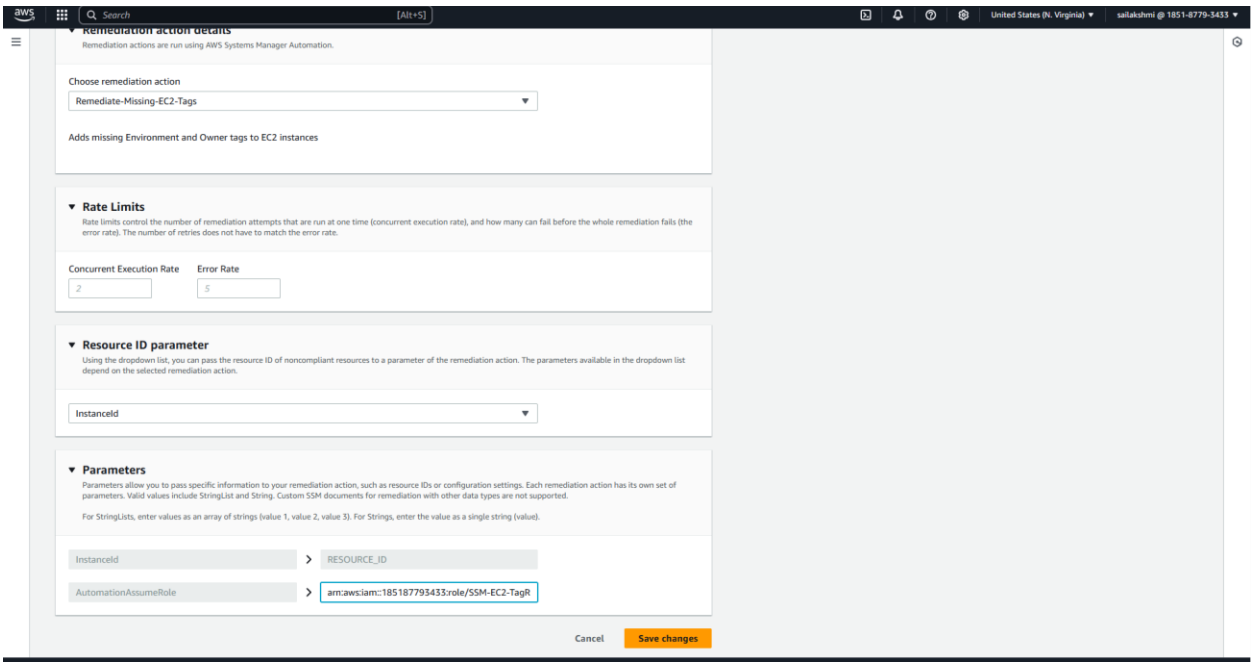
Attach to role: SSM-EC2-TagRemediation-Role




## Step 4: AWS Config Rule Remediation

- Rule: required-tags
- Remediation action: Remediate-Missing-EC2-Tags
- Parameter: InstanceId = resourceId
- IAM Role: SSM-EC2-TagRemediation-Role

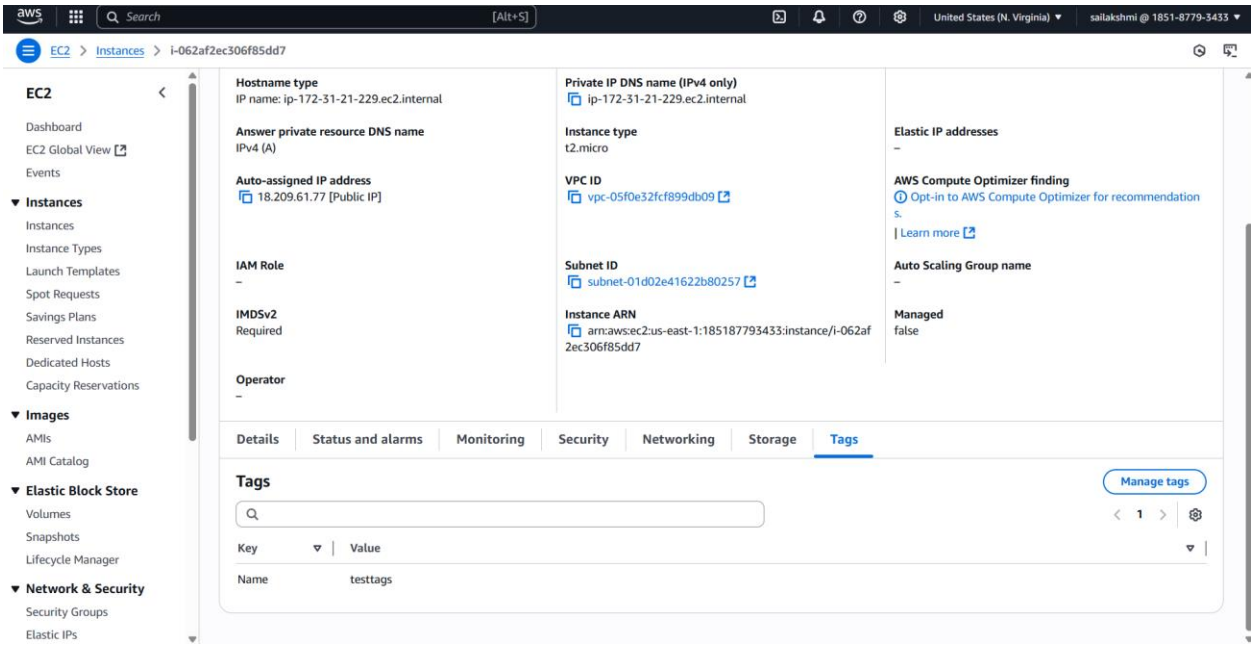


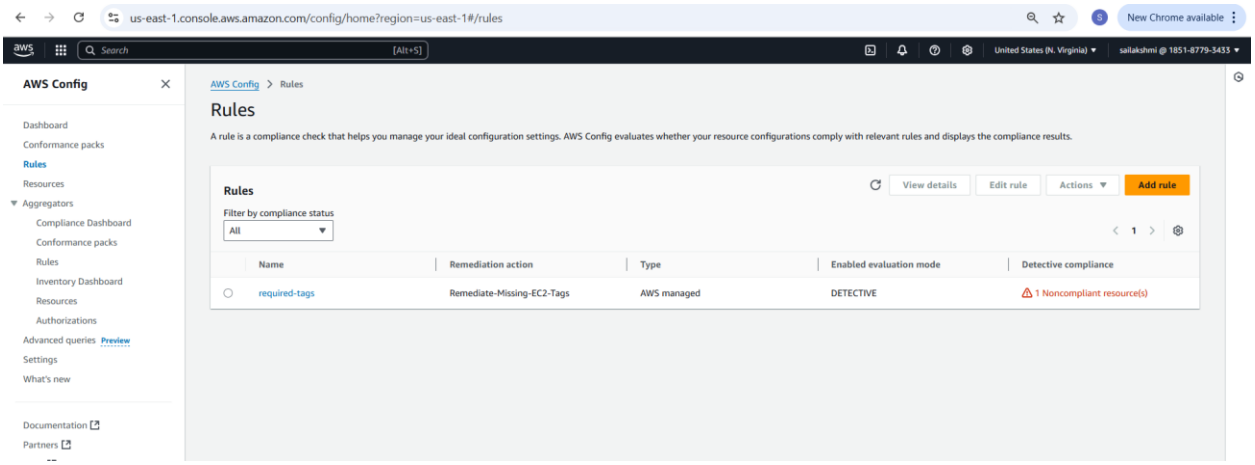

## Step 5: Testing the Automation setup

- launch a new EC2 instance with **no tags**.
- AWS Config detects it's **NON_COMPLIANT** with the `required-tags` rule.
- SSM automatically **adds the missing `Environment` and `Owner` tags** with default values.
- You should receive an email notification from SNS.

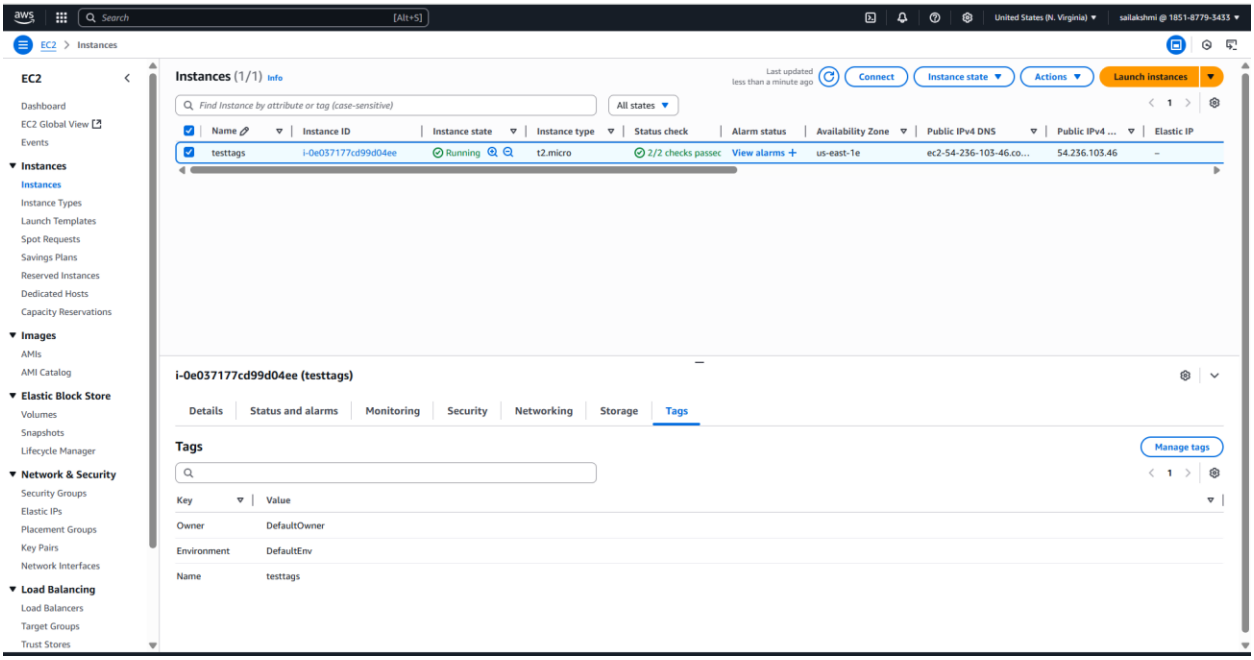
Ec2 instance with no tags



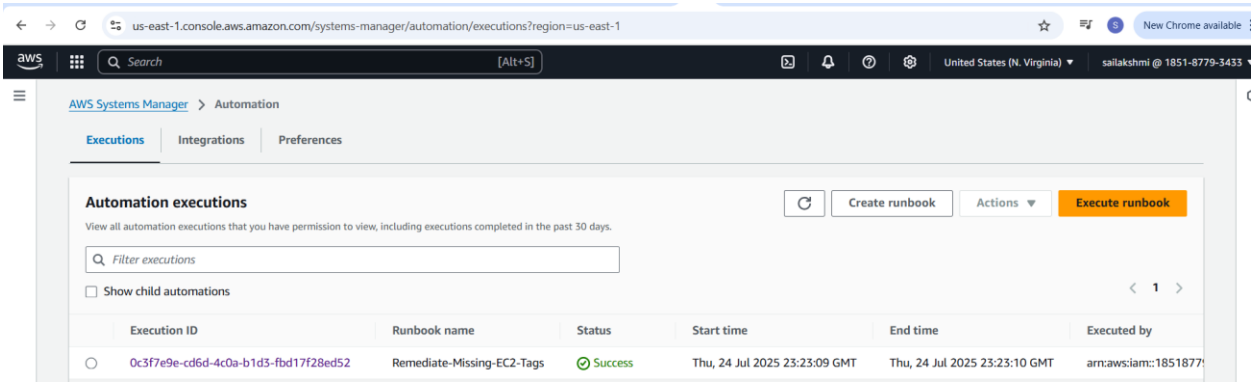

AWS Config detects it's **NON_COMPLIANT**



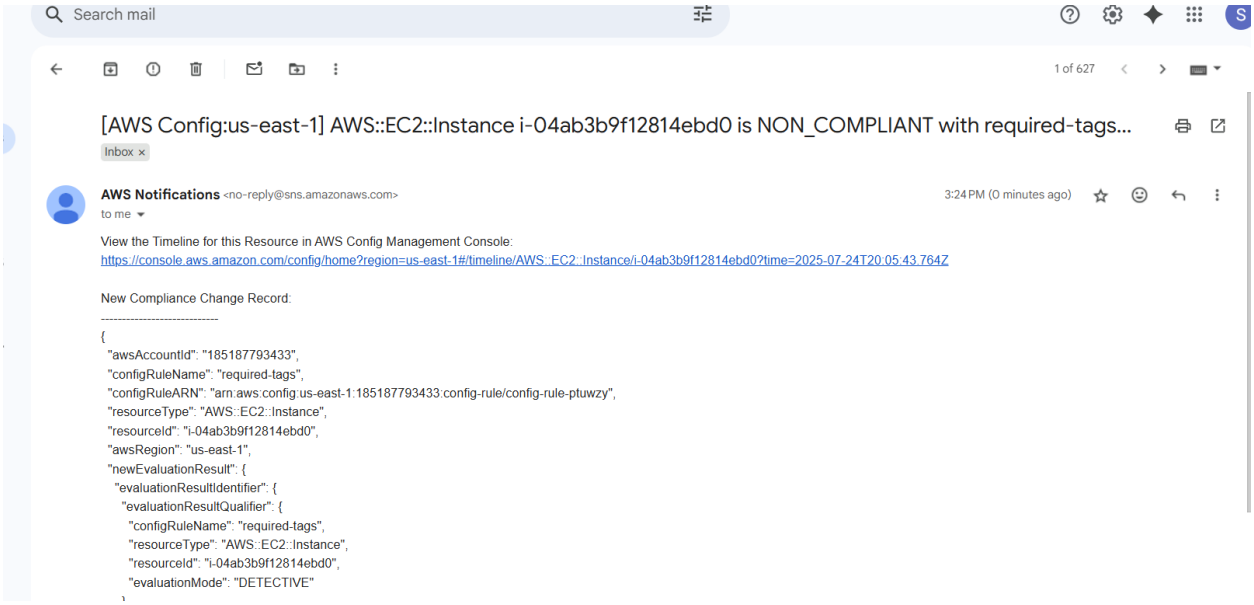

SSM automatically added the missing Tags




Remediate document with a "Success" status

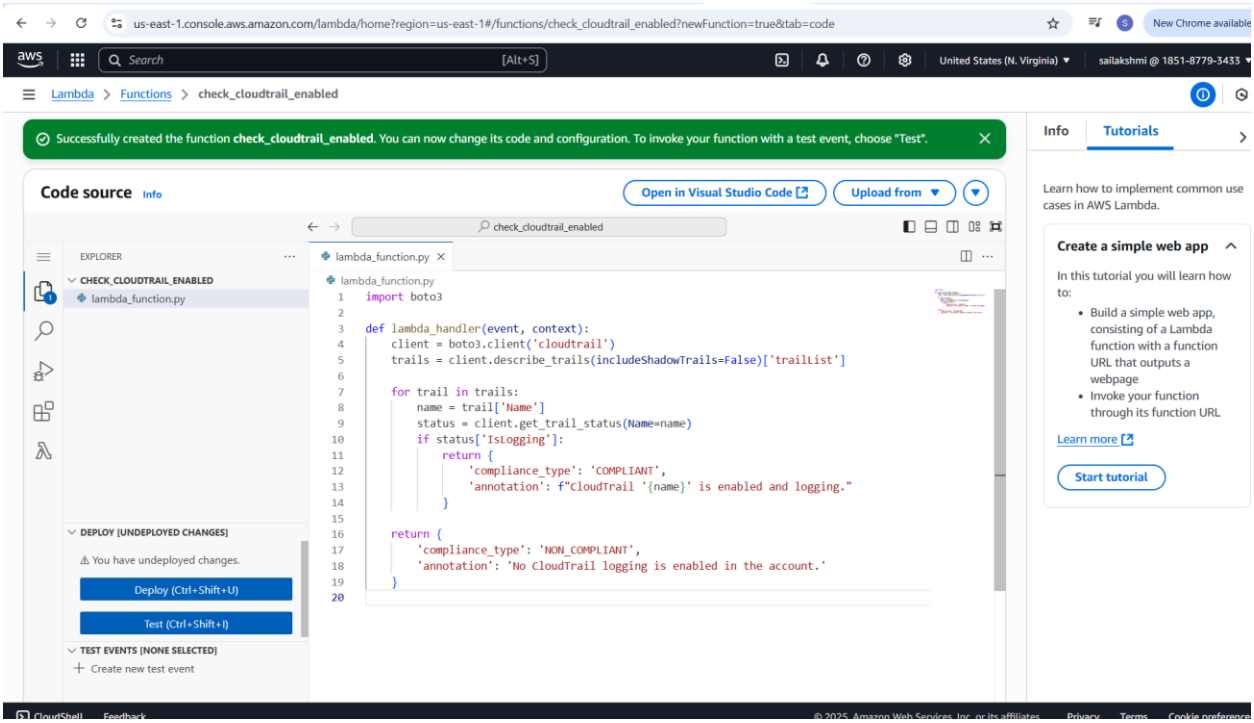



Received an email notification from SNS




## Scenario3: Disabled cloud trail

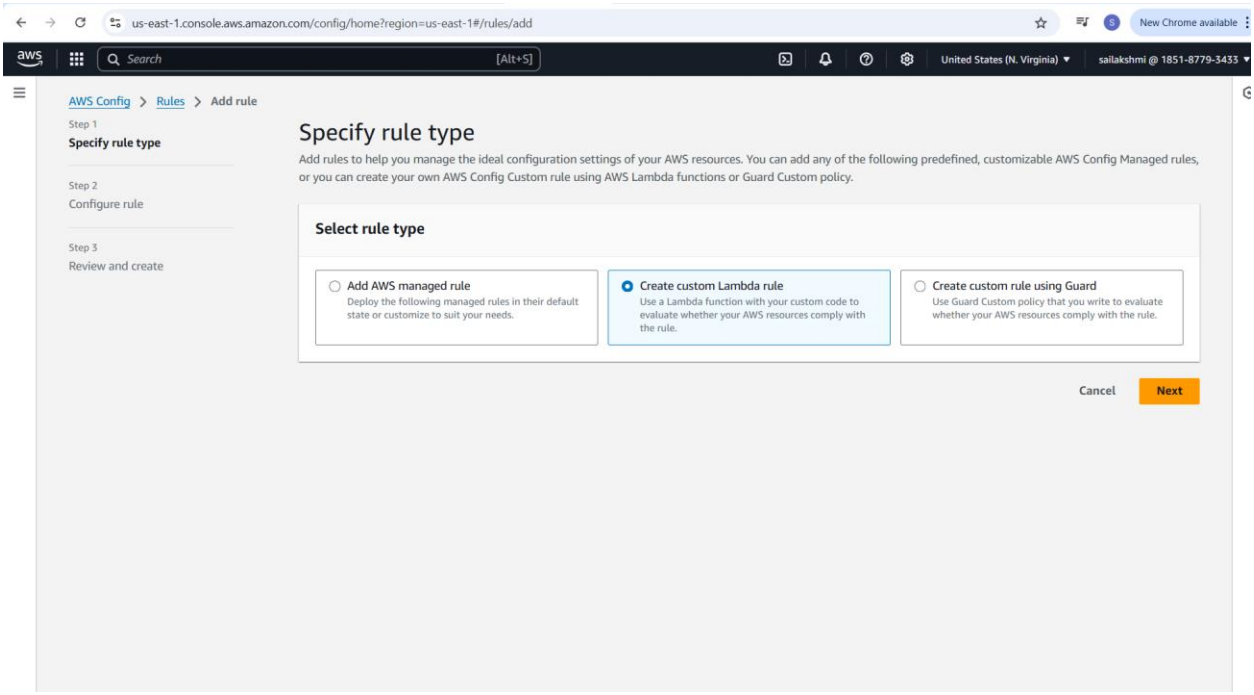
## Step1: Create a lambda function

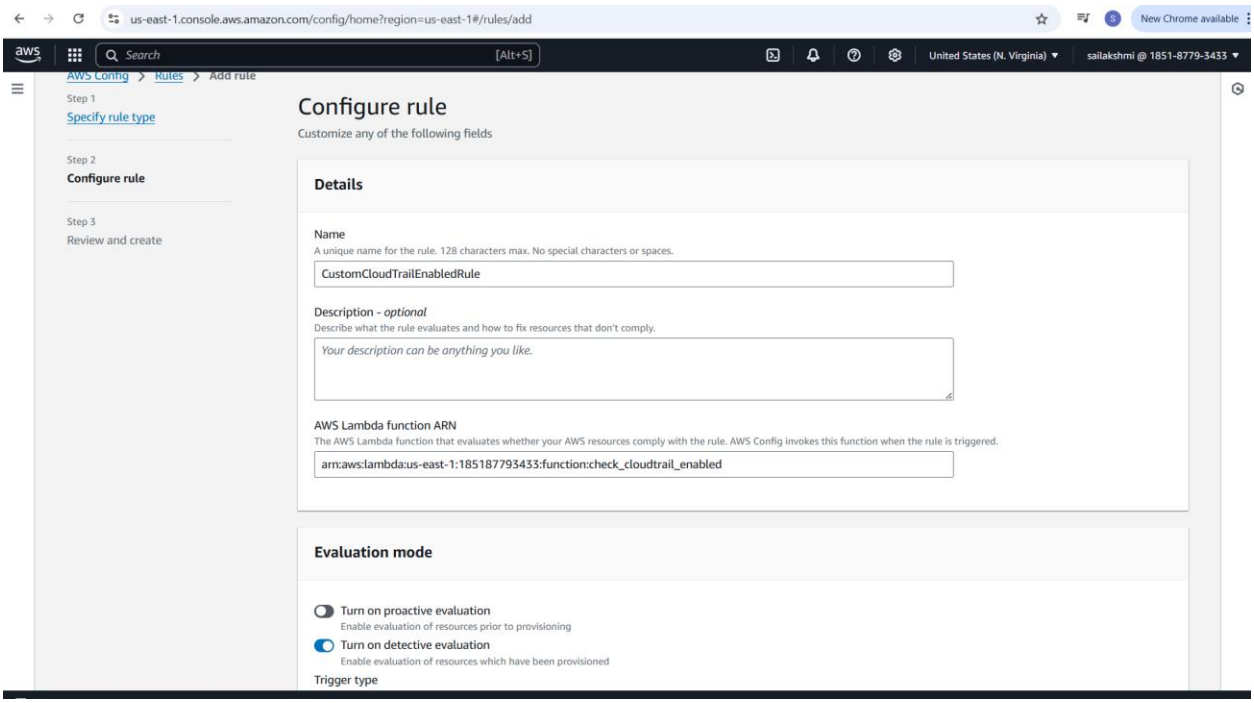


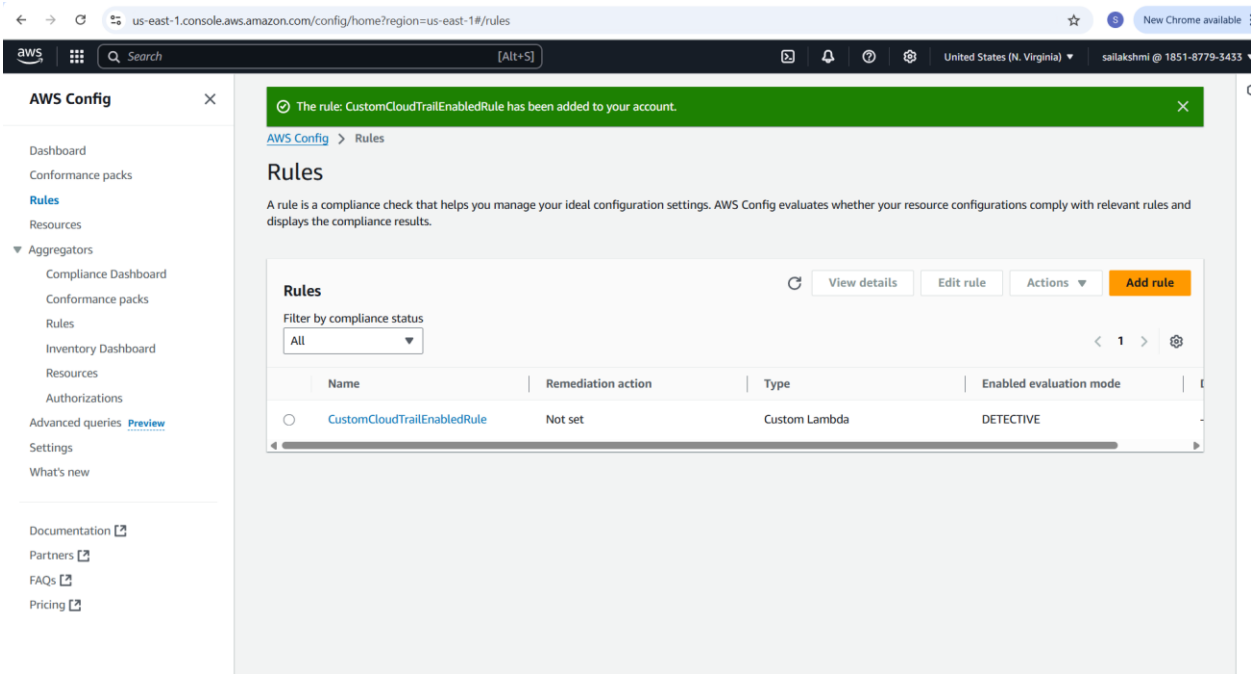

Step2: Create AWS Config Custom Rule with lambda

- Go to AWS Config → Rules → Add Rule
- Choose "Add custom rule"

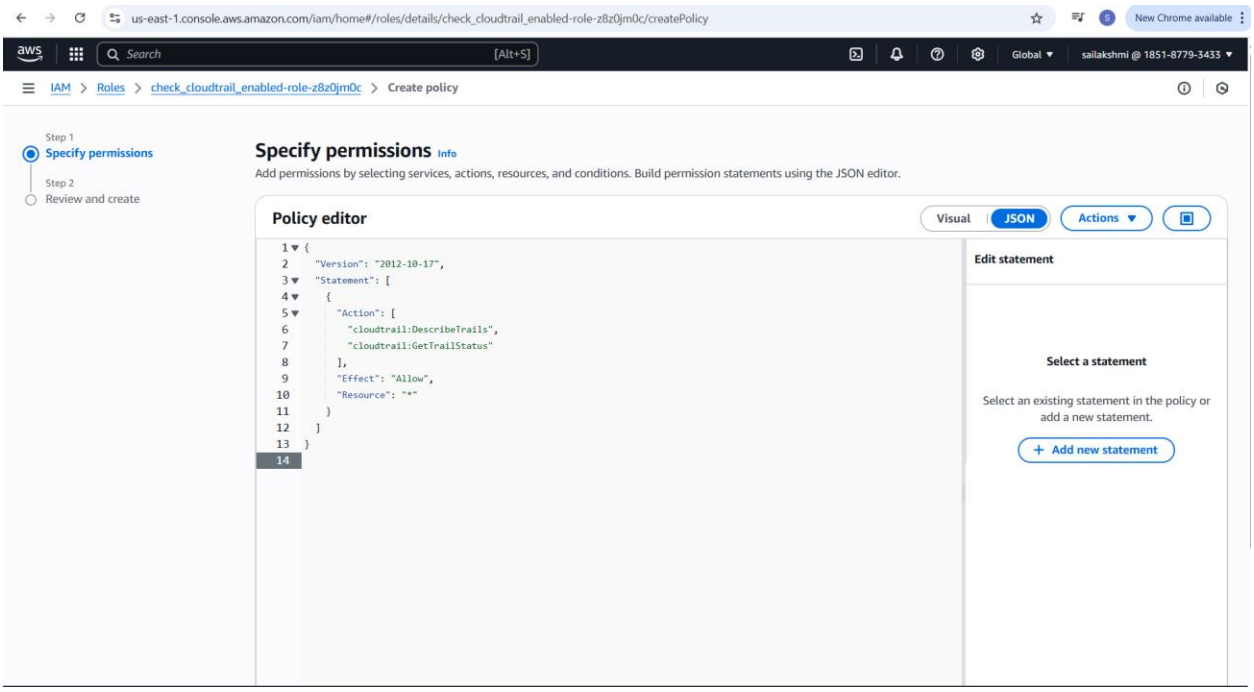
- Enter:
    - Name: CustomCloudTrailEnabledRule
    - Resource type: Choose AWS::CloudTrail::Trail or leave blank for all resources
    - Lambda Function: Choose the Lambda you created (check_cloudtrail_enabled)
    - Execution Role: Ensure Lambda has permissions to call cloudtrail:DescribeTrails, cloudtrail:GetTrailStatus

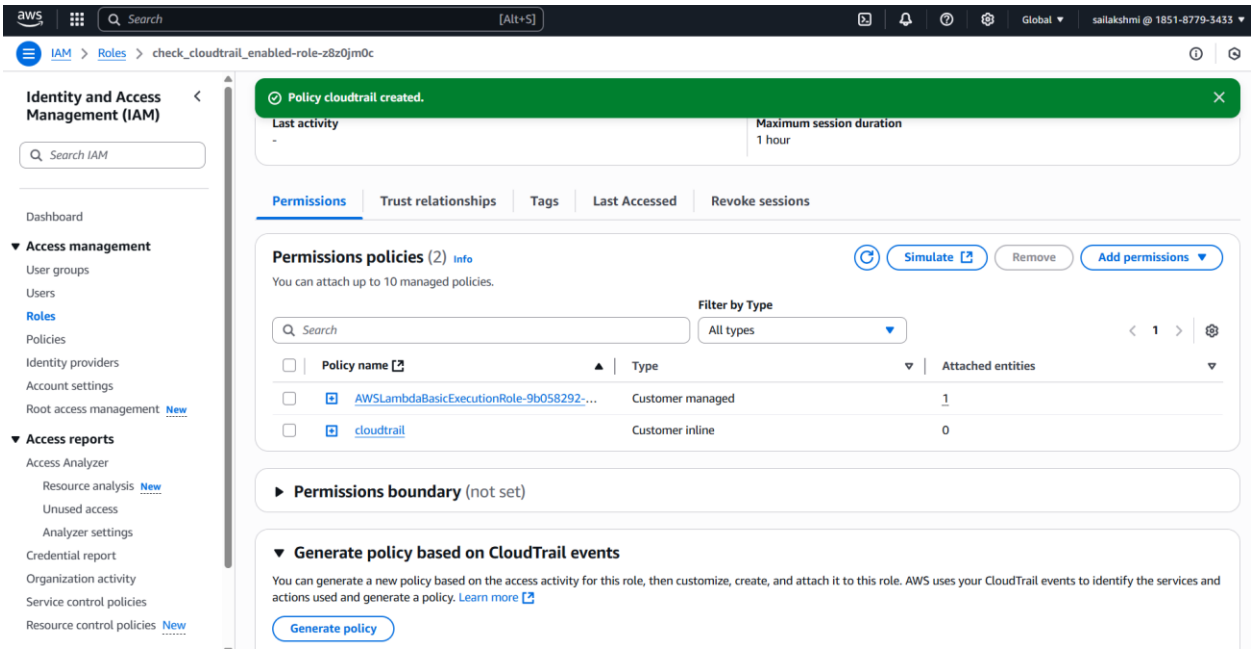





**Step 3: Check IAM role for lambda has permissions to call cloudtrail:DescribeTrails, cloudtrail:GetTrailStatus**



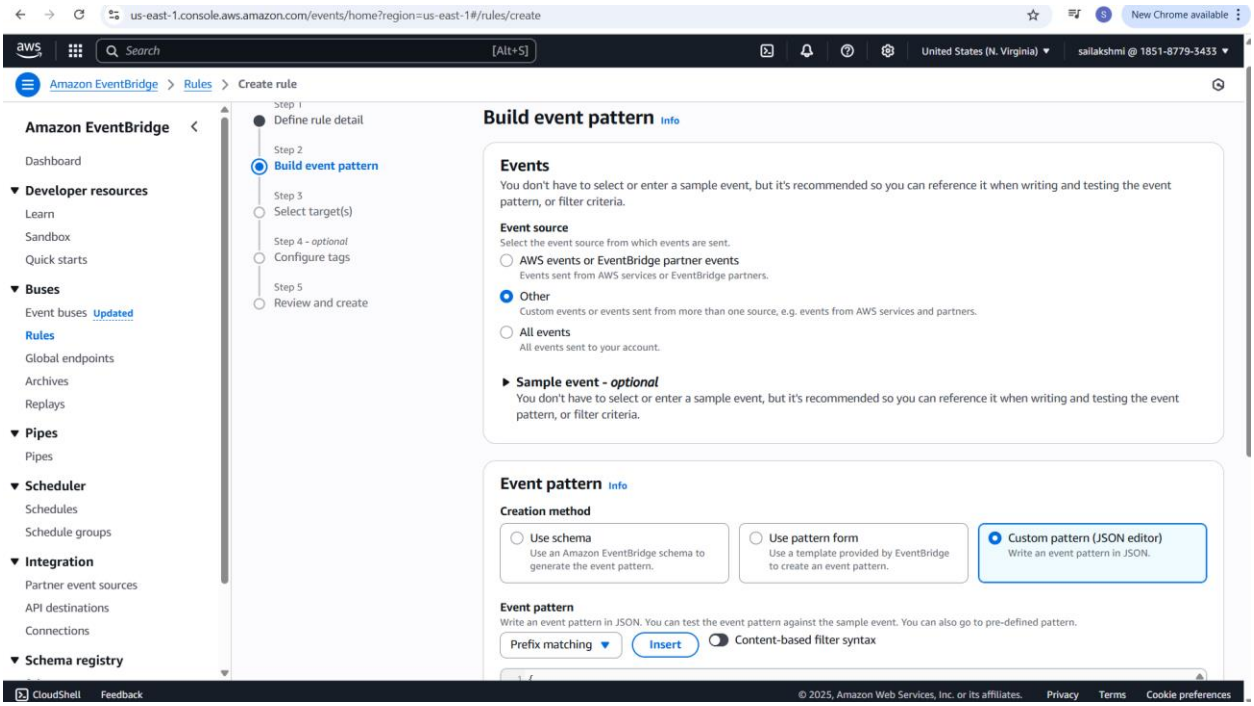

**Step 4: Create EventBridge Rule:**

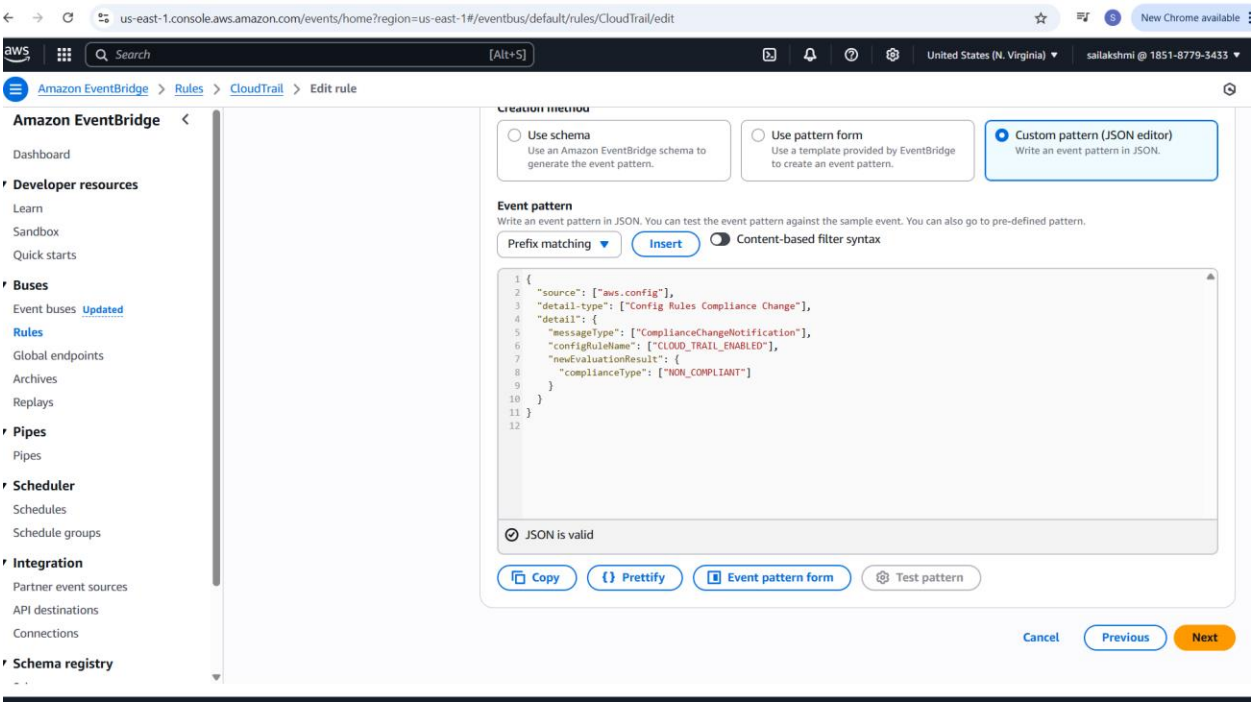
- Go to **EventBridge → Rules → Create rule**
- Event Source: AWS API Call via CloudTrail
- Event Pattern:

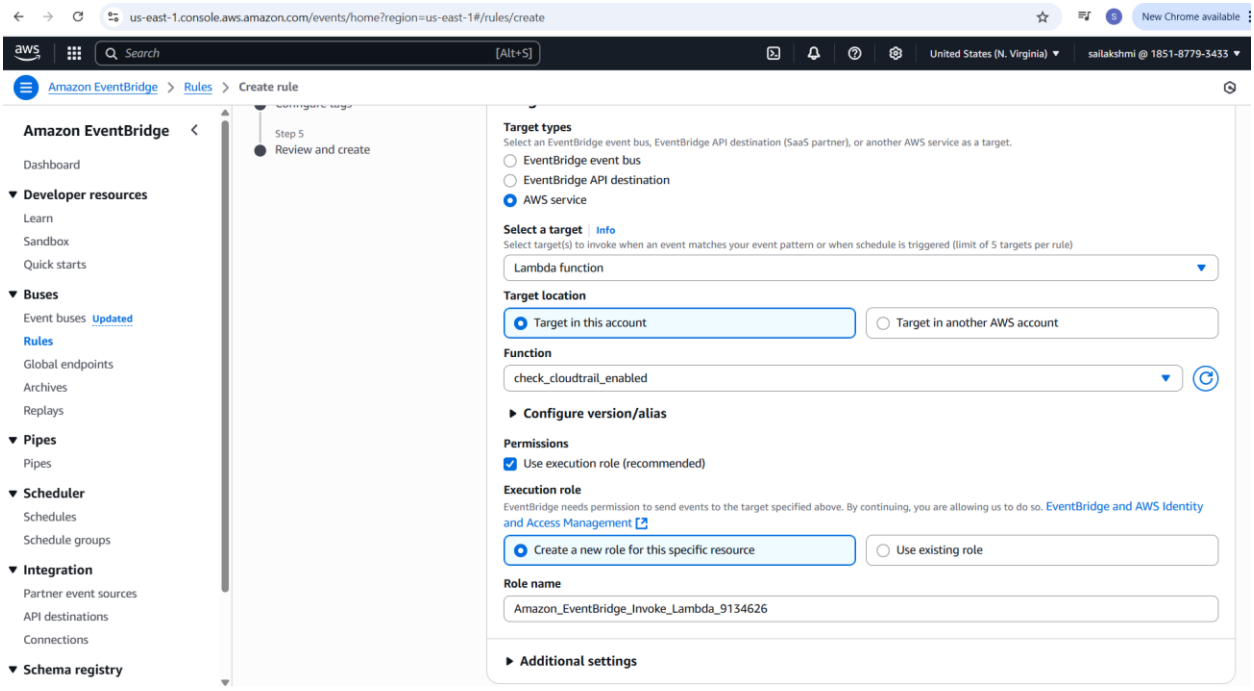
  {

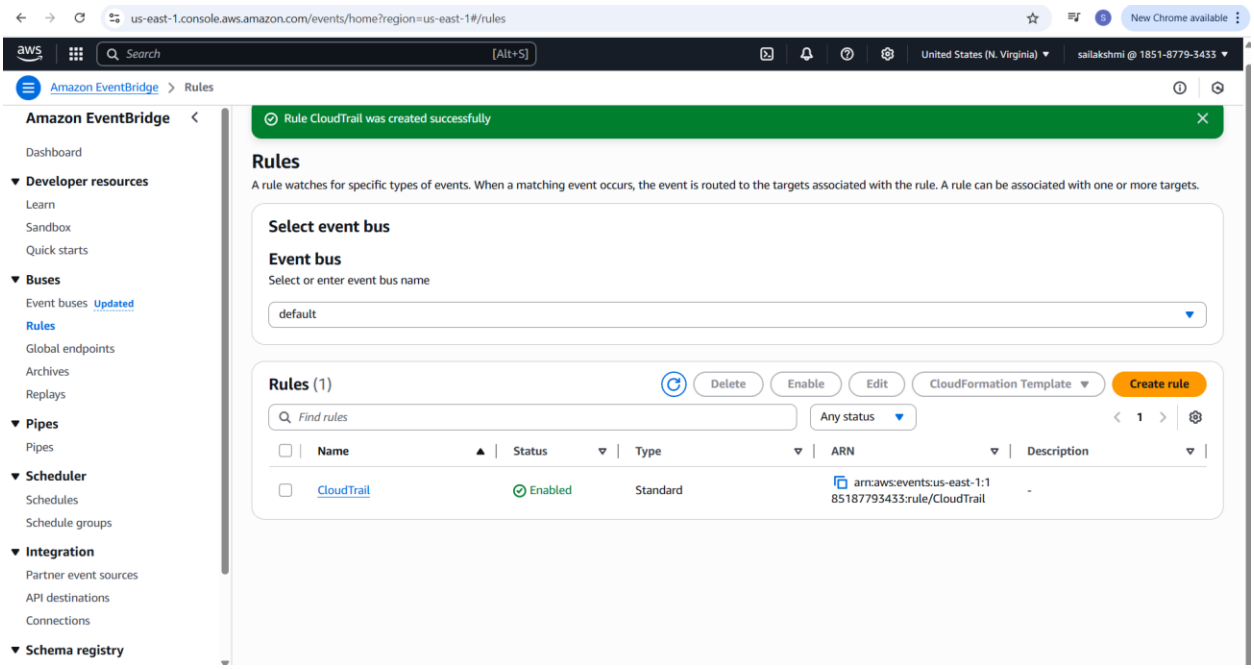
  "source": ["aws.config"],

```
  "detail-type": ["Config Rules Compliance Change"],
  "detail": {
    "messageType": ["ComplianceChangeNotification"],
    "configRuleName": ["CustomCloudTrailEnabledRule"],
    "newEvaluationResult": {
      "complianceType": ["NON_COMPLIANT"]
    }
  }
}
```

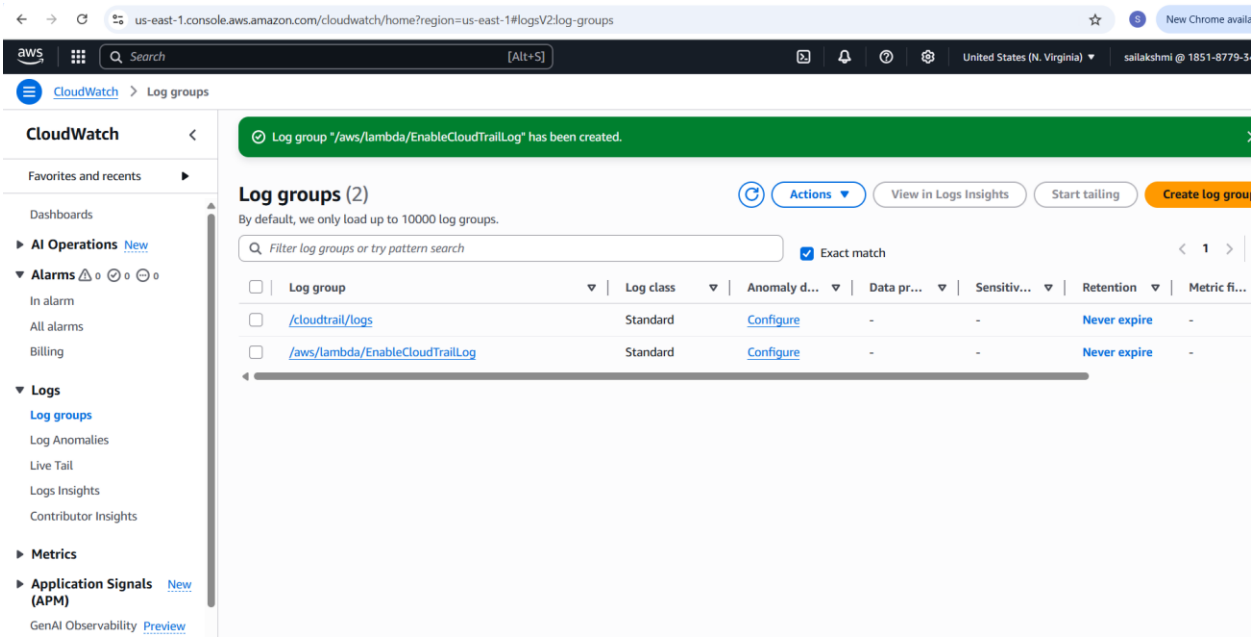



us-east-1.console.aws.amazon.com/events/home?region=us-east-1#/eventbus/default/rules/CloudTrail/edit
Search
[Alt+S]
United States (N. Virginia)
sailakshmi @ 1851-8779-3433
Amazon EventBridge > Rules > CloudTrail > Edit rule
Amazon EventBridge
Dashboard
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses Updated
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
Integration
Partner event sources
API destinations
Connections
Schema registry
Use schema
Use an Amazon EventBridge schema to generate the event pattern.
Use pattern form
Use a template provided by EventBridge to create an event pattern.
Custom pattern (JSON editor)
Write an event pattern in JSON.
Event pattern
Write an event pattern in JSON. You can test the event pattern against the sample event. You can also go to pre-defined pattern.
Prefix matching
Insert
Content-based filter syntax
{
"source": ["aws.config"],
"detail-type": ["Config Rules Compliance Change"],
"detail": {
"messageType": ["ComplianceChangeNotification"],
"configRuleName": ["CLOUD_TRAIL_ENABLED"],
"newEvaluationResult": {
"complianceType": ["NON_COMPLIANT"]
}
}
}
JSON is valid
Copy
Prettify
Event pattern form
Test pattern
Cancel
Previous
Next

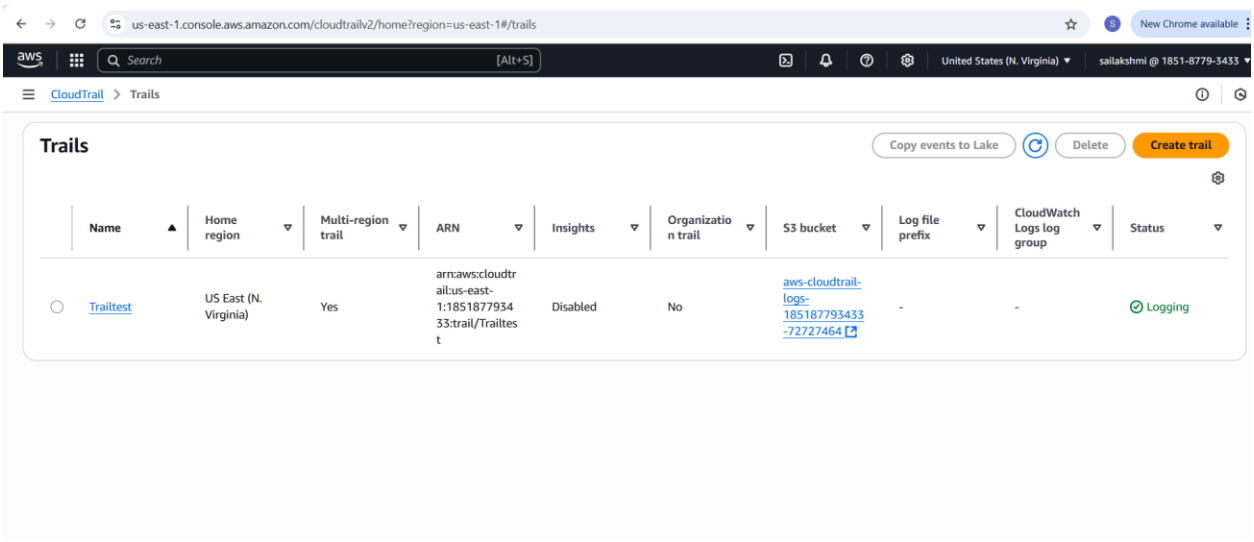

us-east-1.console.aws.amazon.com/events/home?region=us-east-1#/rules/create
Search
[Alt+S]
United States (N. Virginia)
sailakshmi @ 1851-8779-3433
Amazon EventBridge > Rules > Create rule
Amazon EventBridge
Dashboard
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses Updated
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
Integration
Partner event sources
API destinations
Connections
Schema registry
Step 5
Review and create
Target types
Select an EventBridge event bus, EventBridge API destination (SaaS partner), or another AWS service as a target.
EventBridge event bus
EventBridge API destination
AWS service
Select a target Info
Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)
Lambda function
Target location
Target in this account
Target in another AWS account
Function
check_cloudtrail_enabled
Configure version/alias
Permissions
Use execution role (recommended)
Execution role
EventBridge needs permission to send events to the target specified above. By continuing, you are allowing us to do so. EventBridge and AWS Identity and Access Management
Create a new role for this specific resource
Use existing role
Role name
Amazon_EventBridge_Invoke_Lambda_9134626
Additional settings




## Step 5: Create CloudWatch Log Group

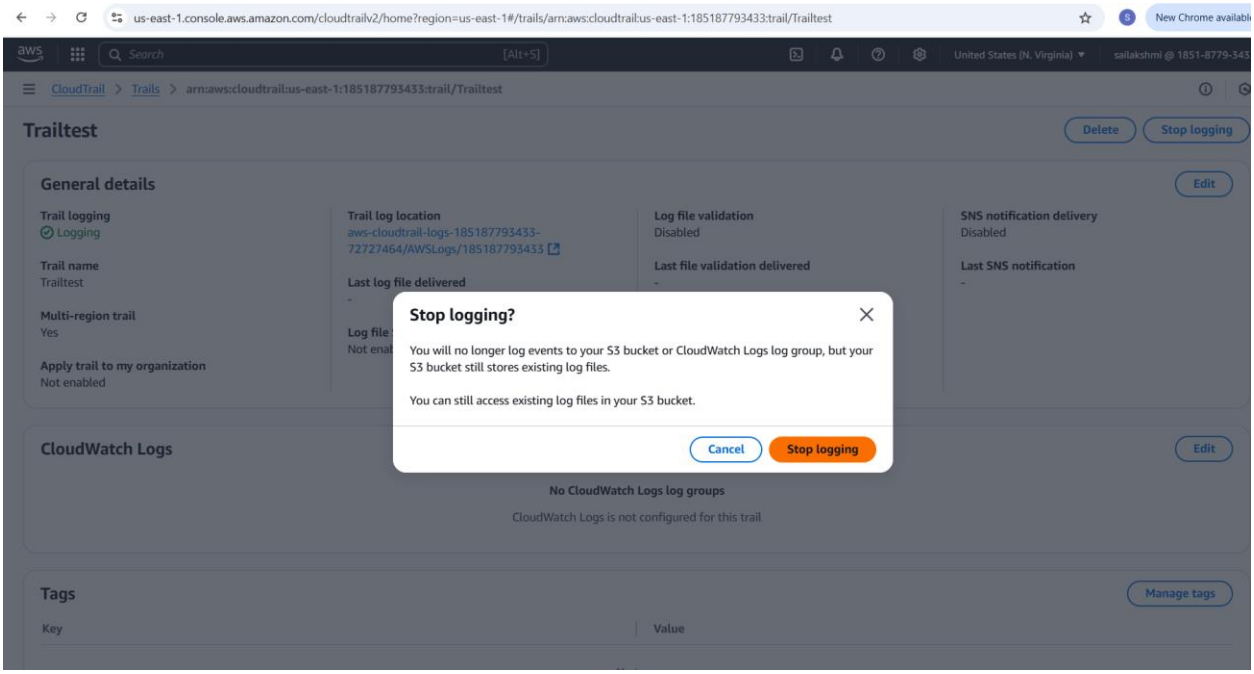



## Step 6: Create a cloud trail

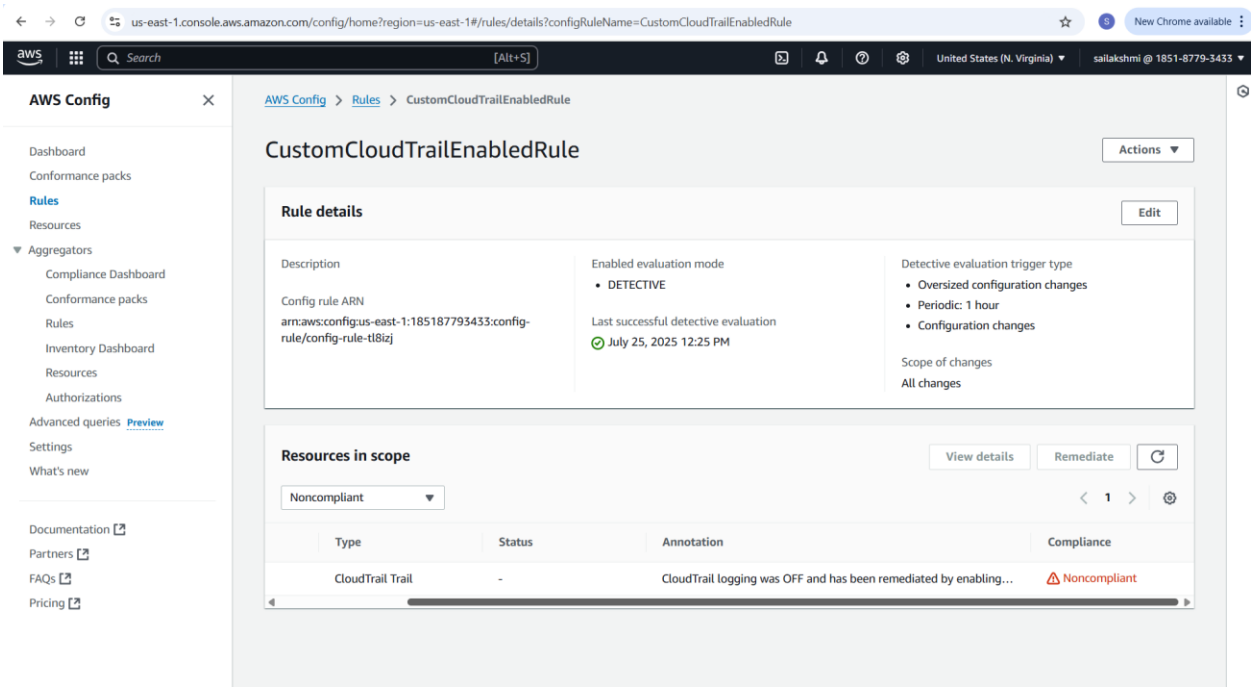



## Test the setup

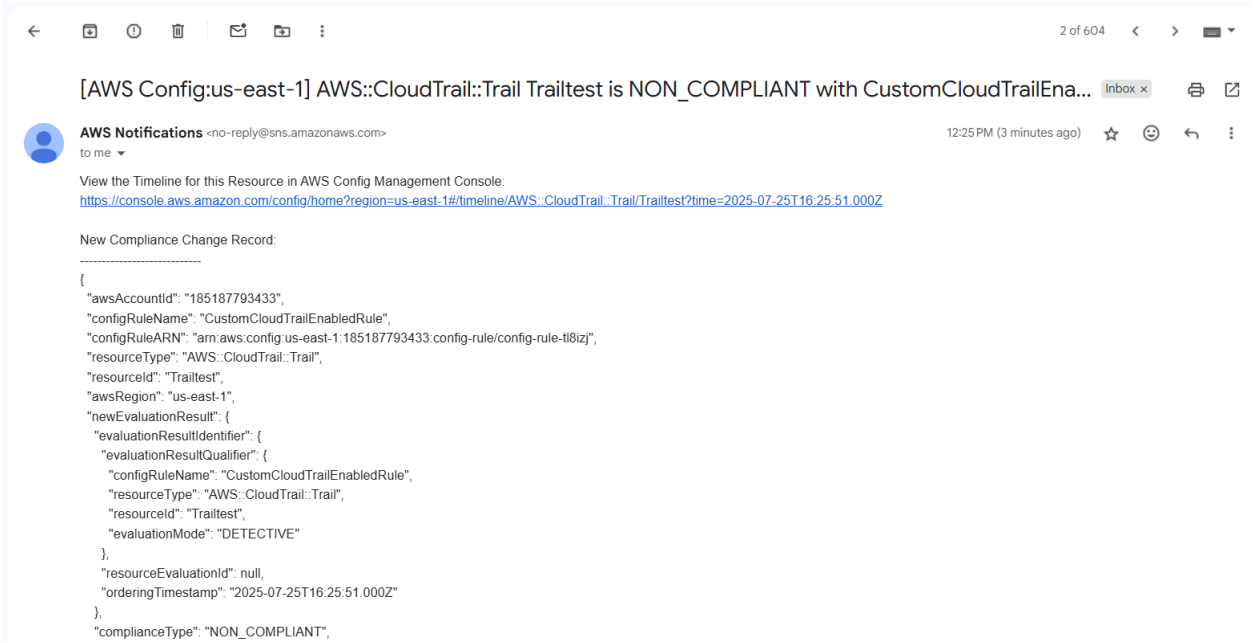
- Stop Logging: Select your trail → click Actions → Stop logging
- AWS Config detects it's **NON_COMPLIANT**
- EventBridge detects `NON_COMPLIANT` and triggers Lambda
- Lambda automatically calls `StartLogging`
- Go back to CloudTrail → Check Logging = ON
- You should receive an email notification from SNS.



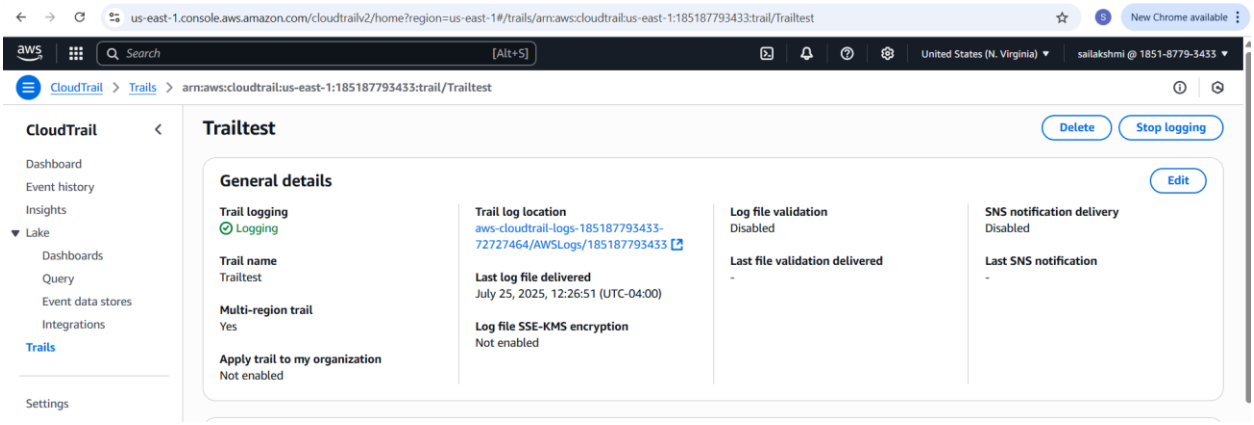
AWS Config detects it's **NON_COMPLIANT**



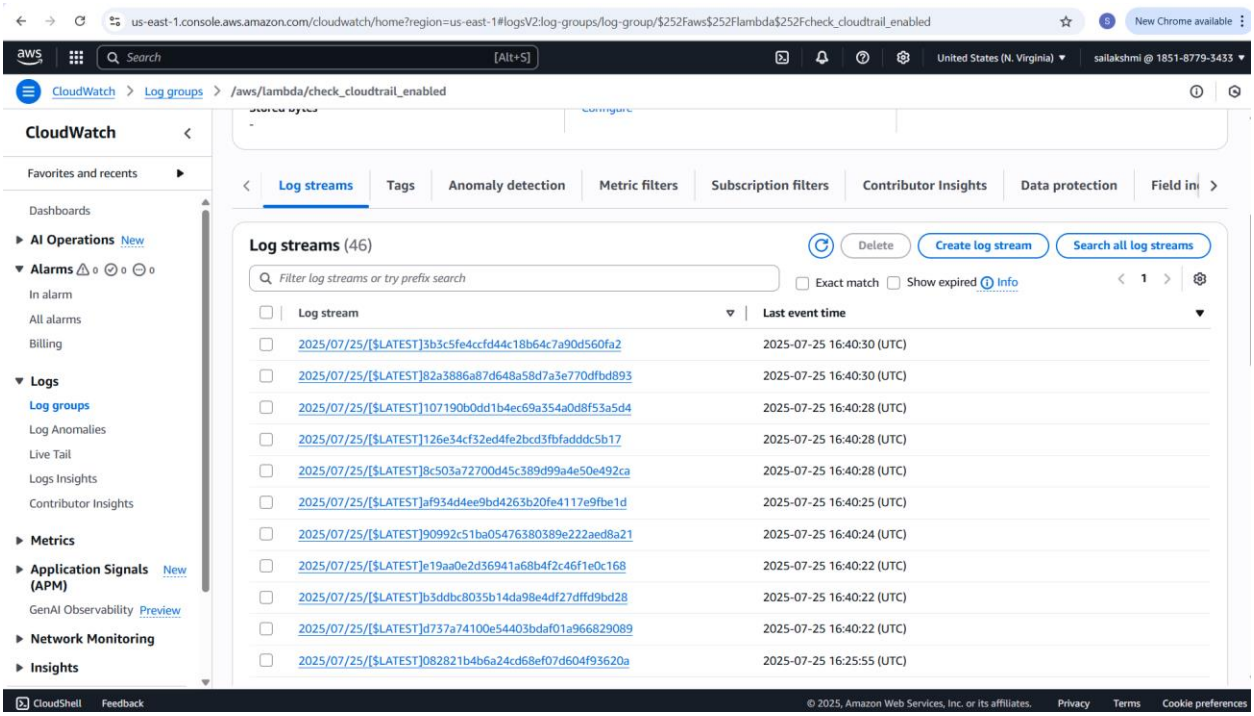

Received an email notification from SNS.

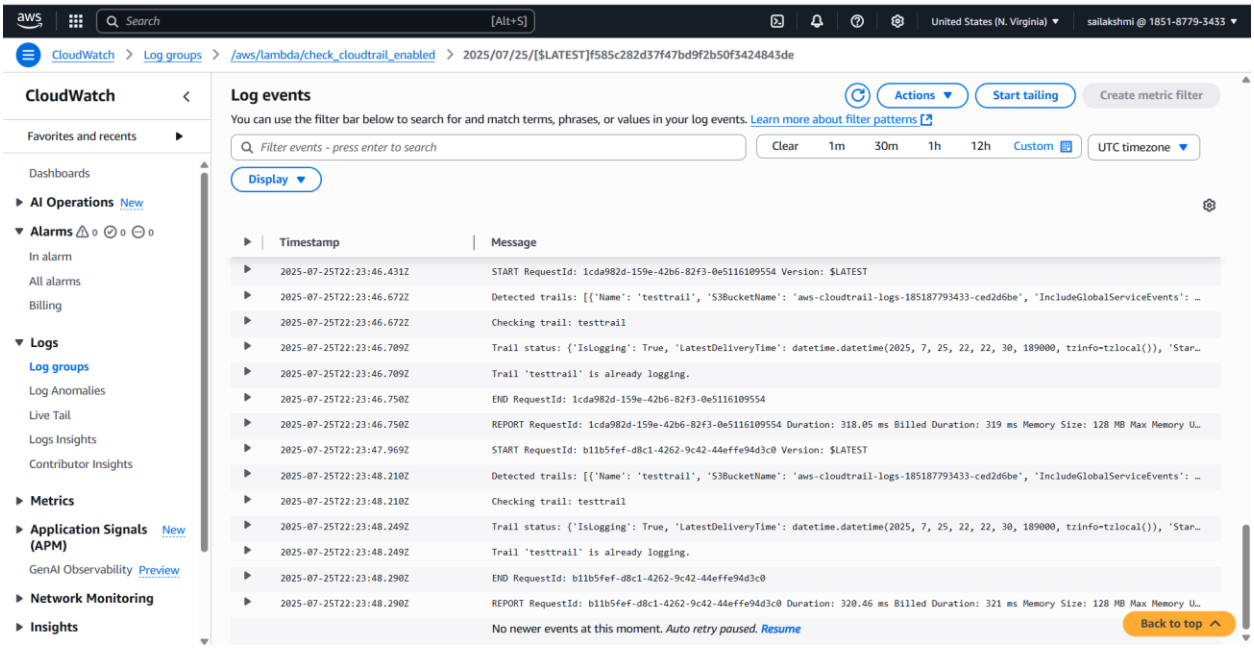


Check Logging = ON




Cloud watch logs

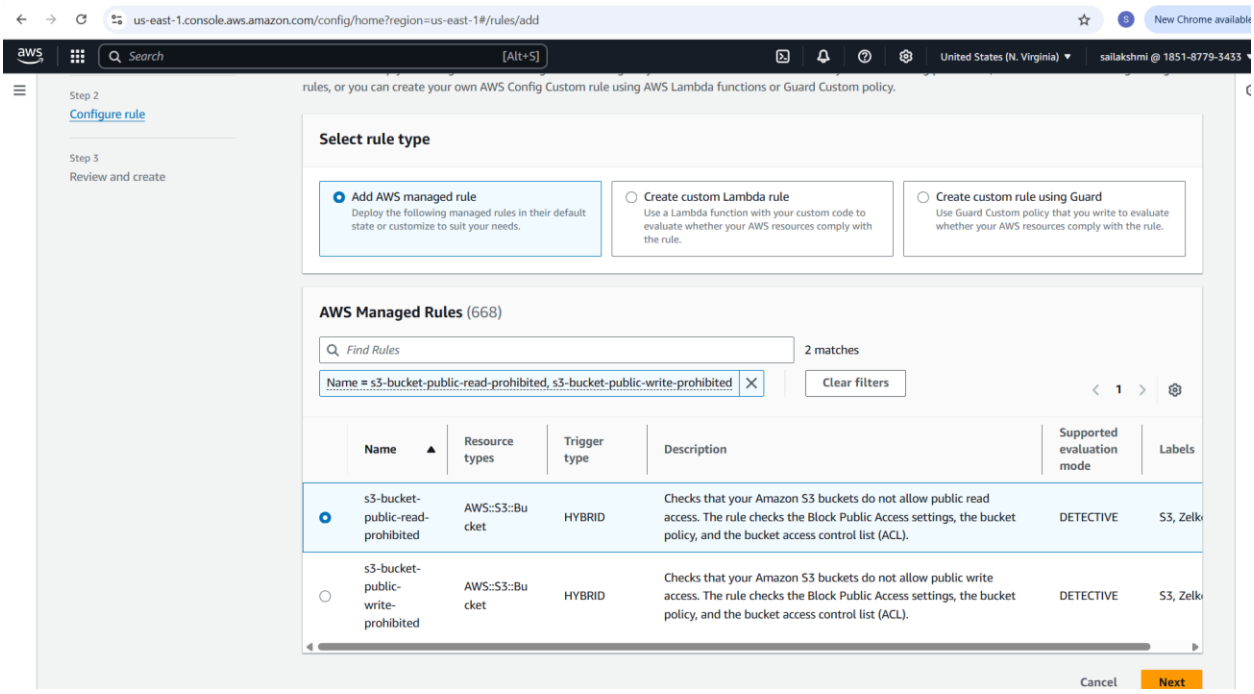


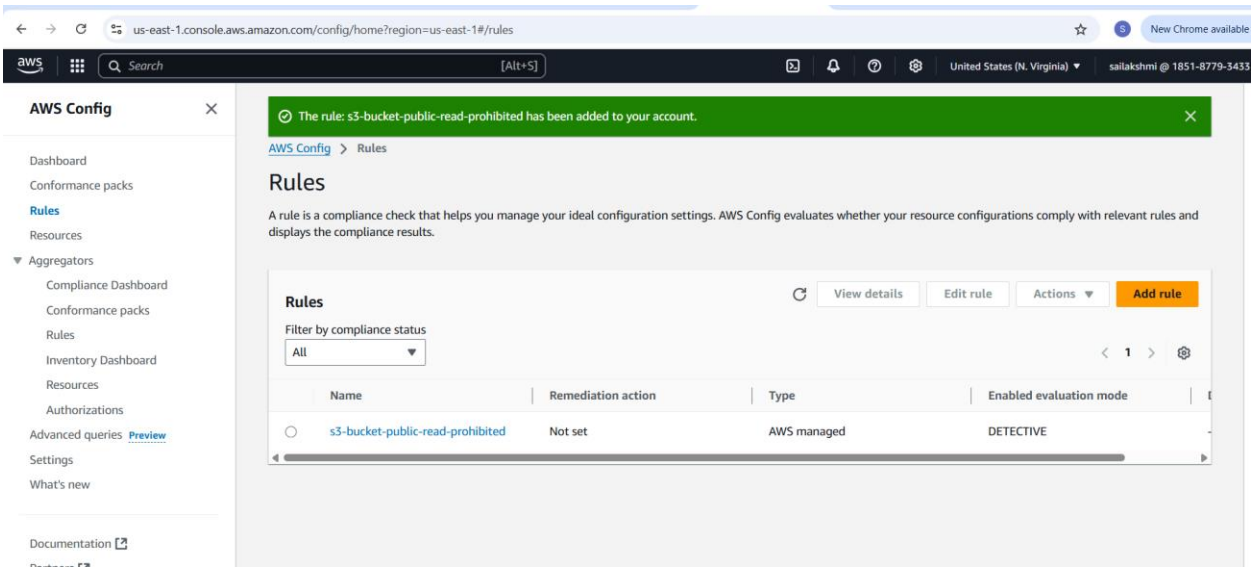


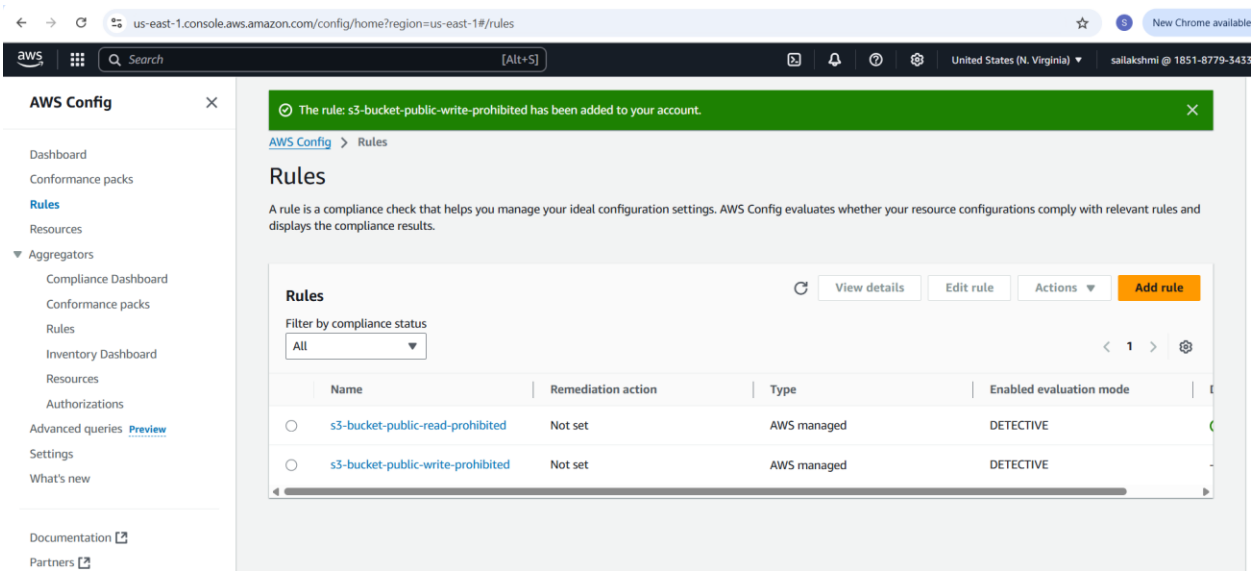

## Scenario 4 : S3 Bucket Public Access Block Enforcement

### Step 1: Enable AWS Config and Create Compliance Rule

- Go to **AWS Config** Console.
- Click **Rules** > **Add rule**.
- Search for and select these **managed rules**:
    - s3-bucket-public-read-prohibited
    - s3-bucket-public-write-prohibited
- Configure the rules to evaluate all S3 buckets.
- Save and enable the rules.

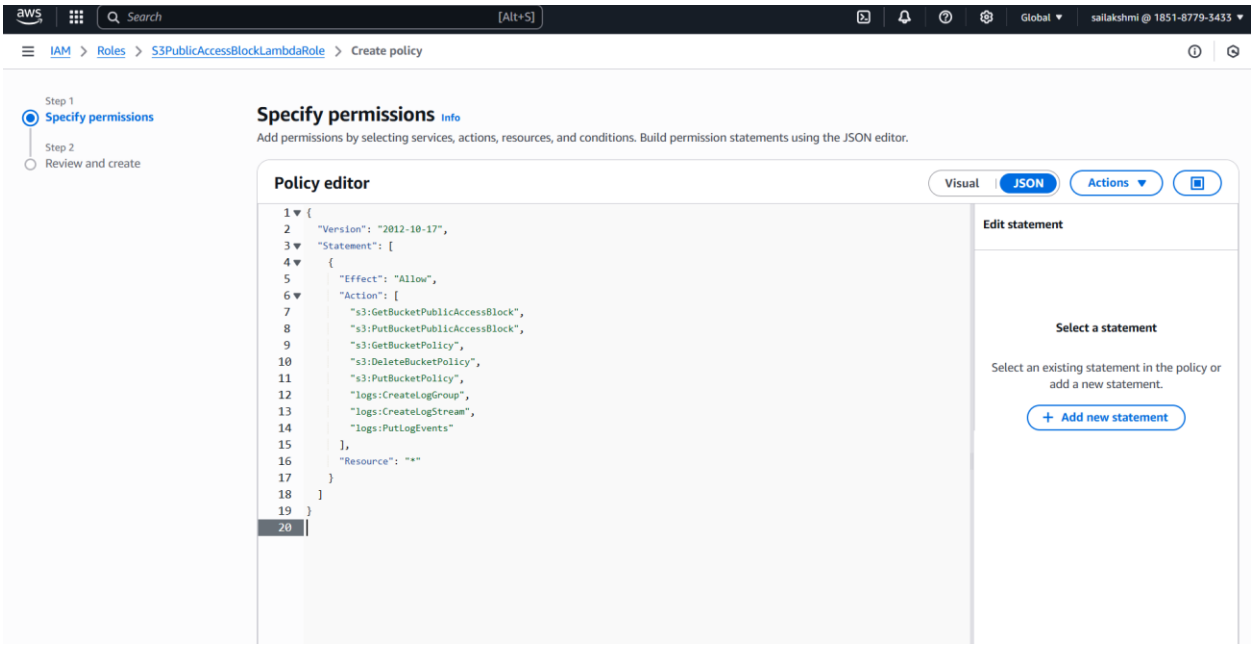

us-east-1.console.aws.amazon.com/config/home?region=us-east-1#/rules/add
Search
[Alt+S]
United States (N. Virginia)
Step 2
Configure rule
Step 3
Review and create
rules, or you can create your own AWS Config Custom rule using AWS Lambda functions or Guard Custom policy.
Select rule type
Add AWS managed 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 (668)
Find Rules
2 matches
Name = s3-bucket-public-read-prohibited, s3-bucket-public-write-prohibited
Clear filters
Name
Resource types
Trigger type
Description
Supported evaluation mode
Labels
s3-bucket-public-read-prohibited
AWS::S3::Bucket
HYBRID
Checks that your Amazon S3 buckets do not allow public read access. The rule checks the Block Public Access settings, the bucket policy, and the bucket access control list (ACL).
DETECTIVE
S3, Zelk
s3-bucket-public-write-prohibited
AWS::S3::Bucket
HYBRID
Checks that your Amazon S3 buckets do not allow public write access. The rule checks the Block Public Access settings, the bucket policy, and the bucket access control list (ACL).
DETECTIVE
S3, Zelk
Cancel
Next

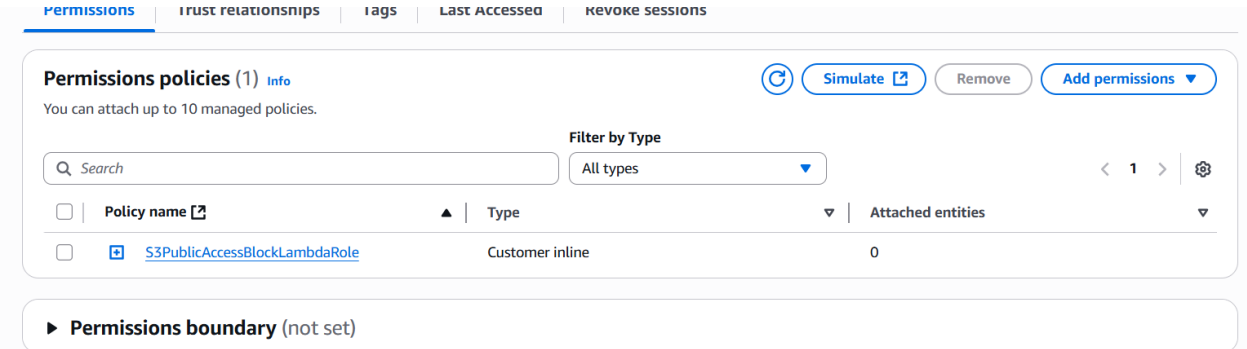

us-east-1.console.aws.amazon.com/config/home?region=us-east-1#/rules
Search
[Alt+S]
United States (N. Virginia)
AWS Config
Dashboard
Conformance packs
Rules
Resources
Aggregators
Compliance Dashboard
Conformance packs
Rules
Inventory Dashboard
Resources
Authorizations
Advanced queries Preview
Settings
What's new
Documentation
The rule: s3-bucket-public-read-prohibited has been added to your account.
AWS Config > Rules
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
View details
Edit rule
Actions
Add rule
Filter by compliance status
All
Name
Remediation action
Type
Enabled evaluation mode
s3-bucket-public-read-prohibited
Not set
AWS managed
DETECTIVE




## Step 2: Create an IAM Role for Lambda

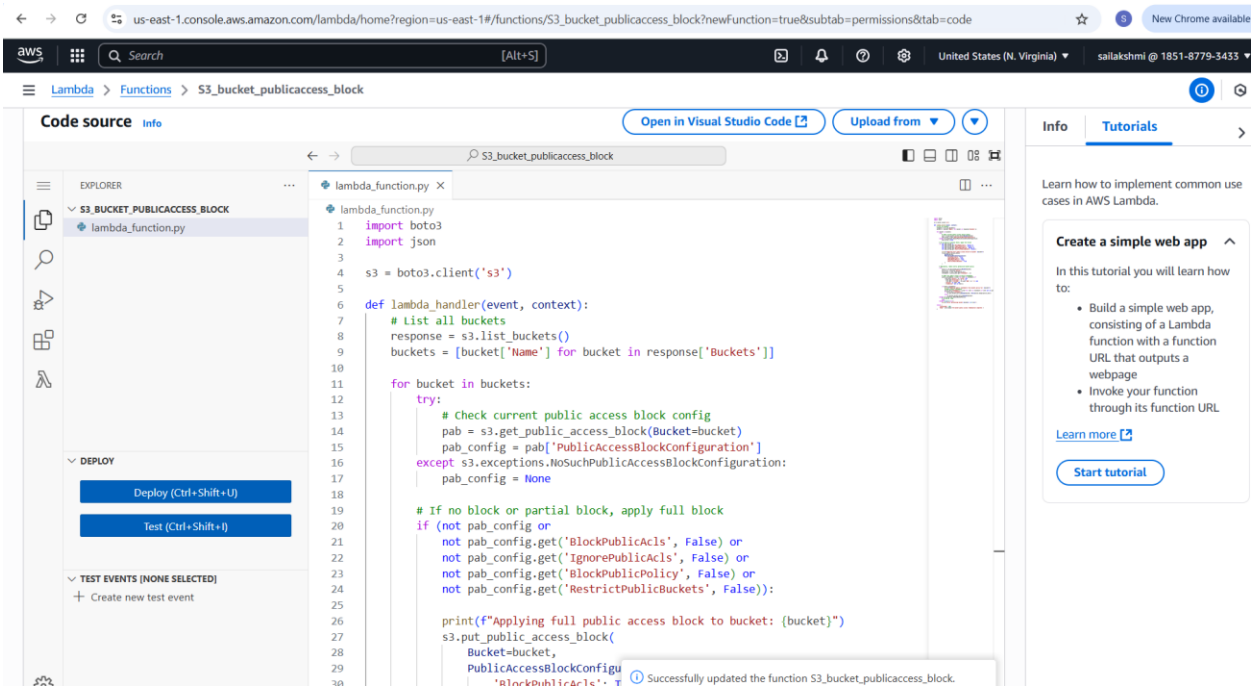
Create a role named S3PublicAccessBlockLambdaRole






## Step 3: Create the Lambda Function for Remediation

Attach a role to lambda which we created before



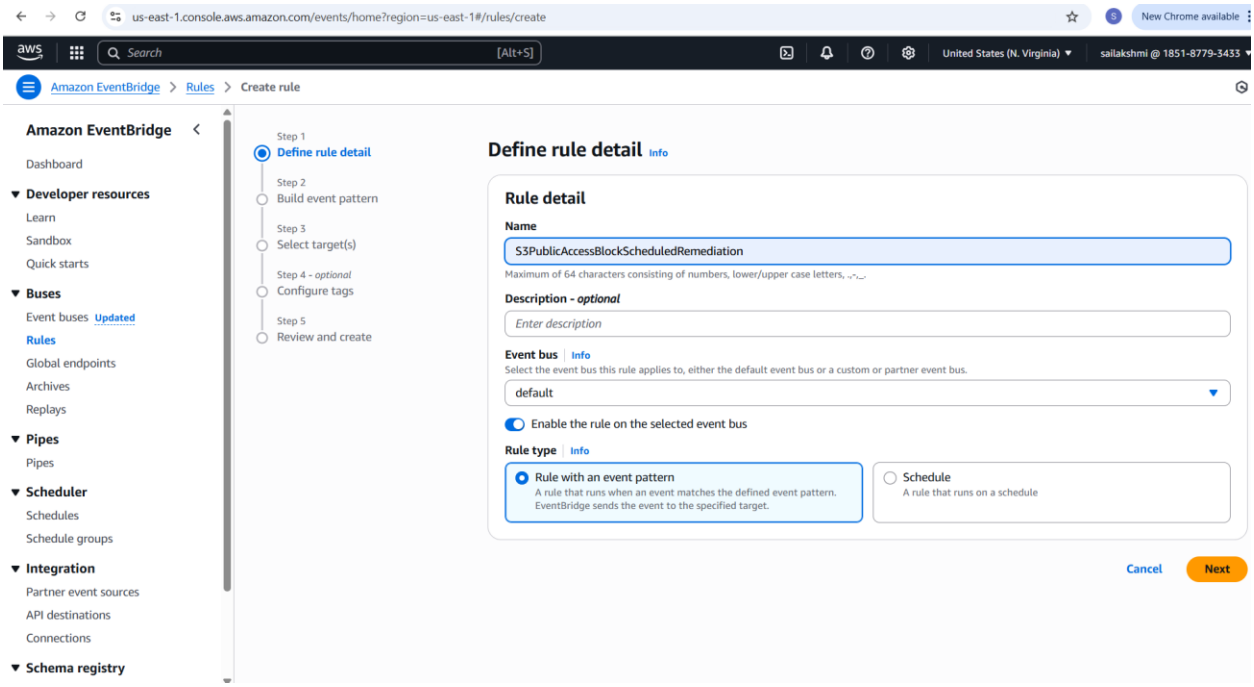

## Step 4: Create an EventBridge Rule

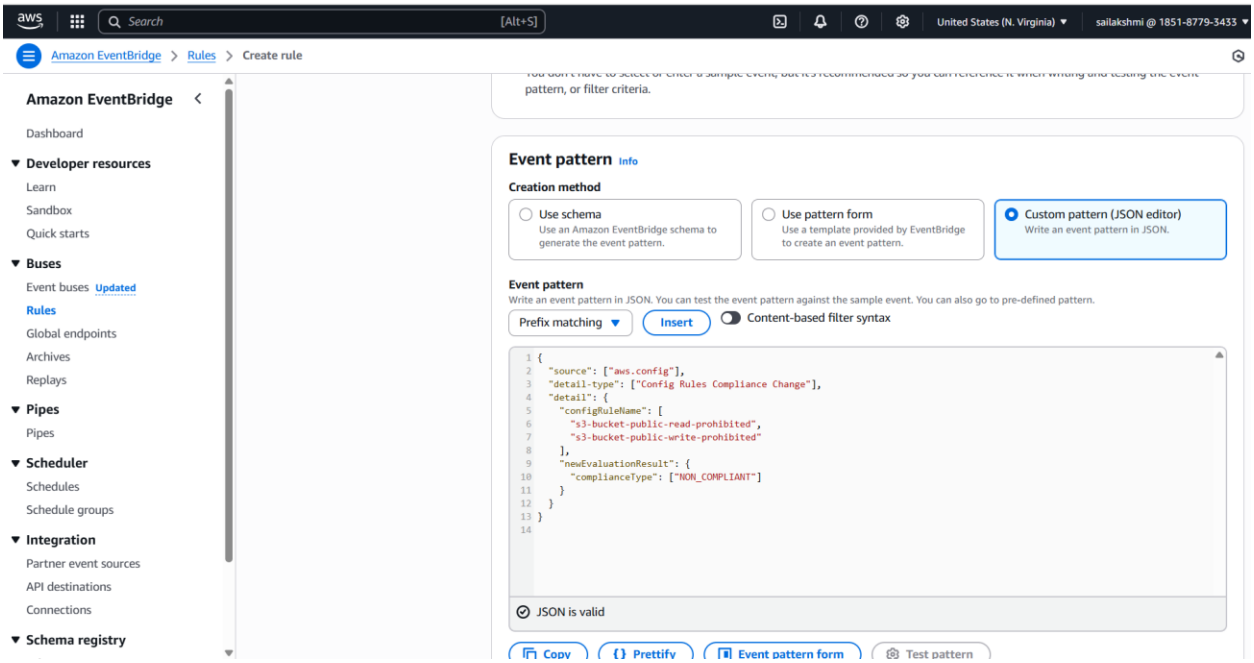
- Go to **Amazon EventBridge** Console.
- Click **Rules** > **Create rule**.
- Name: S3PublicAccessBlockScheduledRemediation
- Select **Target**: Lambda function
- Define event pattern
- Create rule.

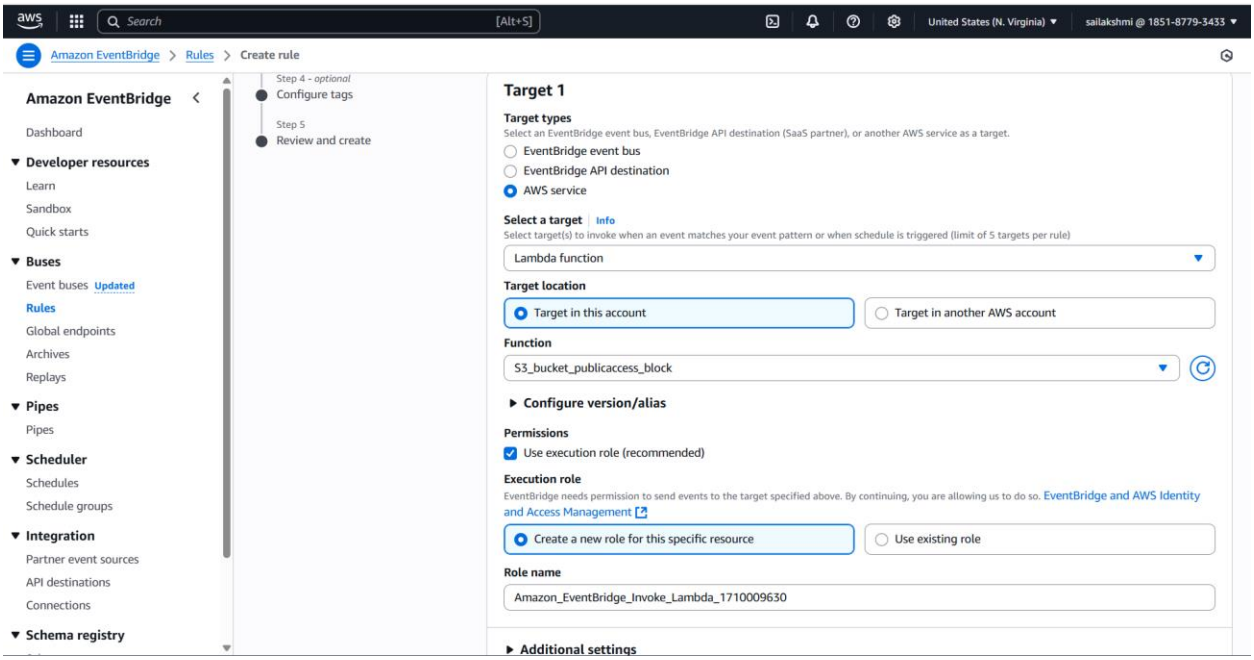
{

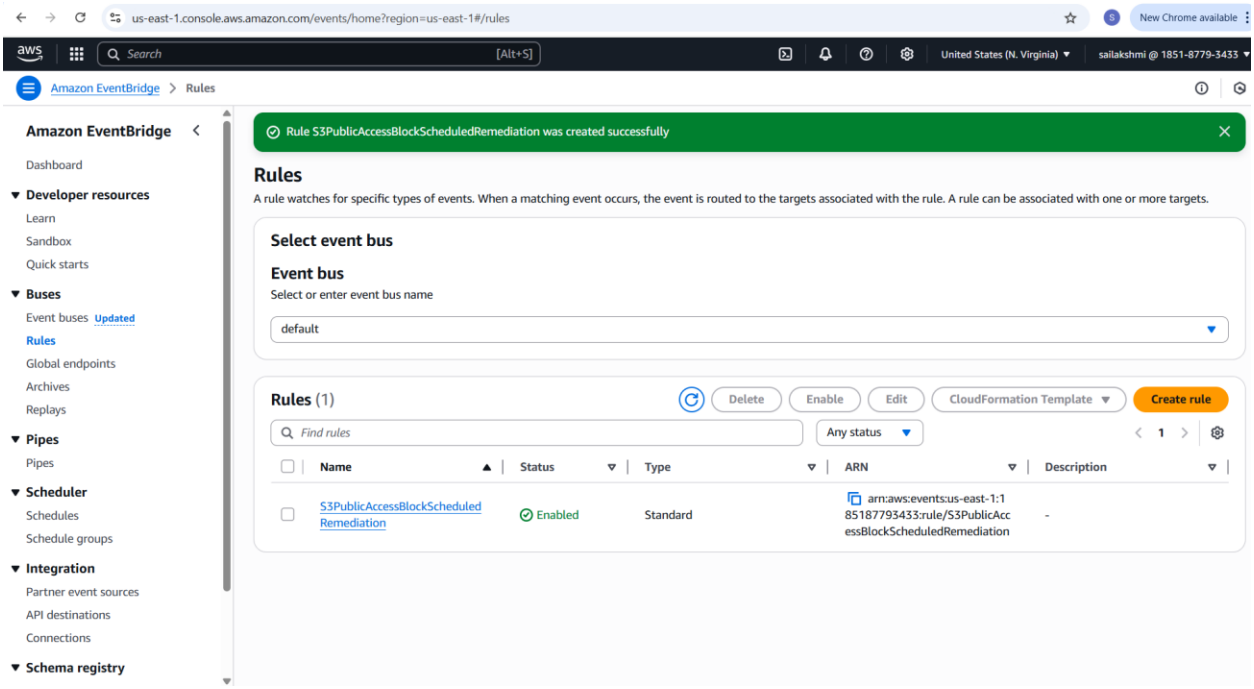
"source": ["aws.config"],

```
"detail-type": ["Config Rules Compliance Change"],
"detail": {
 "configRuleName": [
  "s3-bucket-public-read-prohibited",
  "s3-bucket-public-write-prohibited"
 ],
 "newEvaluationResult": {
  "complianceType": ["NON_COMPLIANT"]
 }
}
}
```




aws
Search
[Alt+S]
United States (N. Virginia)
sailakshmi @ 1851-8779-3433
Amazon EventBridge > Rules > Create rule
Amazon EventBridge
Dashboard
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses Updated
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
Integration
Partner event sources
API destinations
Connections
Schema registry
pattern, or filter criteria.
Event pattern Info
Creation method
Use schema
Use an Amazon EventBridge schema to generate the event pattern.
Use pattern form
Use a template provided by EventBridge to create an event pattern.
Custom pattern (JSON editor)
Write an event pattern in JSON.
Event pattern
Write an event pattern in JSON. You can test the event pattern against the sample event. You can also go to pre-defined pattern.
Prefix matching
Insert
Content-based filter syntax
{
"source": ["aws.config"],
"detail-type": ["Config Rules Compliance Change"],
"detail": {
"configRuleName": [
"s3-bucket-public-read-prohibited",
"s3-bucket-public-write-prohibited"
],
"newEvaluationResult": {
"complianceType": ["NON_COMPLIANT"]
}
}
}
JSON is valid
Copy
Prettify
Event pattern form
Test pattern

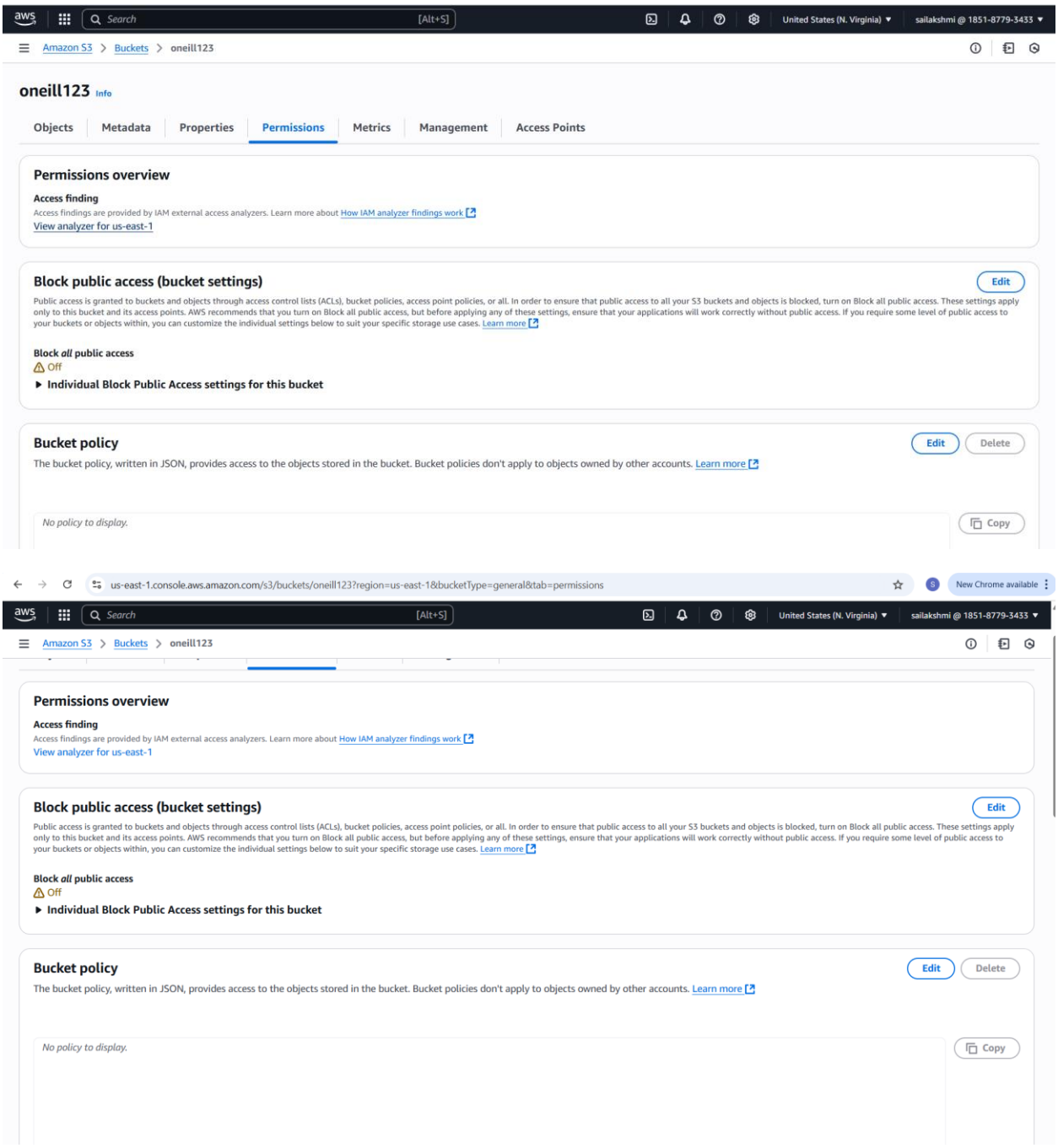

aws
Search
[Alt+S]
United States (N. Virginia)
sailakshmi @ 1851-8779-3433
Amazon EventBridge > Rules > Create rule
Amazon EventBridge
Dashboard
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses Updated
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
Integration
Partner event sources
API destinations
Connections
Schema registry
Step 4 - optional
Configure tags
Step 5
Review and create
Target 1
Target types
Select an EventBridge event bus, EventBridge API destination (SaaS partner), or another AWS service as a target.
EventBridge event bus
EventBridge API destination
AWS service
Select a target Info
Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)
Lambda function
Target location
Target in this account
Target in another AWS account
Function
S3_bucket_publicaccess_block
Configure version/alias
Permissions
Use execution role (recommended)
Execution role
EventBridge needs permission to send events to the target specified above. By continuing, you are allowing us to do so. EventBridge and AWS Identity and Access Management
Create a new role for this specific resource
Use existing role
Role name
Amazon_EventBridge_Invoke_Lambda_1710009630
Additional settings




## Step 5 : Test the set up

- Create a Test S3 Bucket
- Make the Bucket Public
- Wait for AWS Config to Evaluate and Check the Rule It should show Noncompliant
- You should receive an email notification from SNS

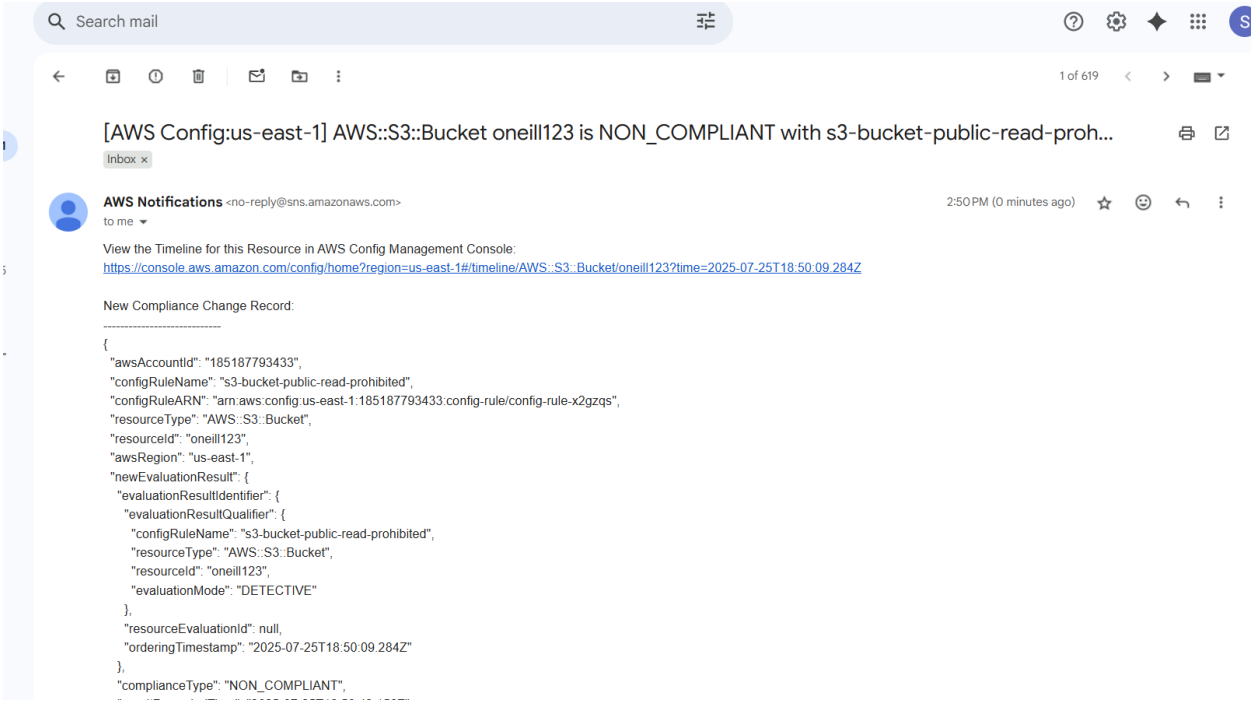
Created a bucket with public access



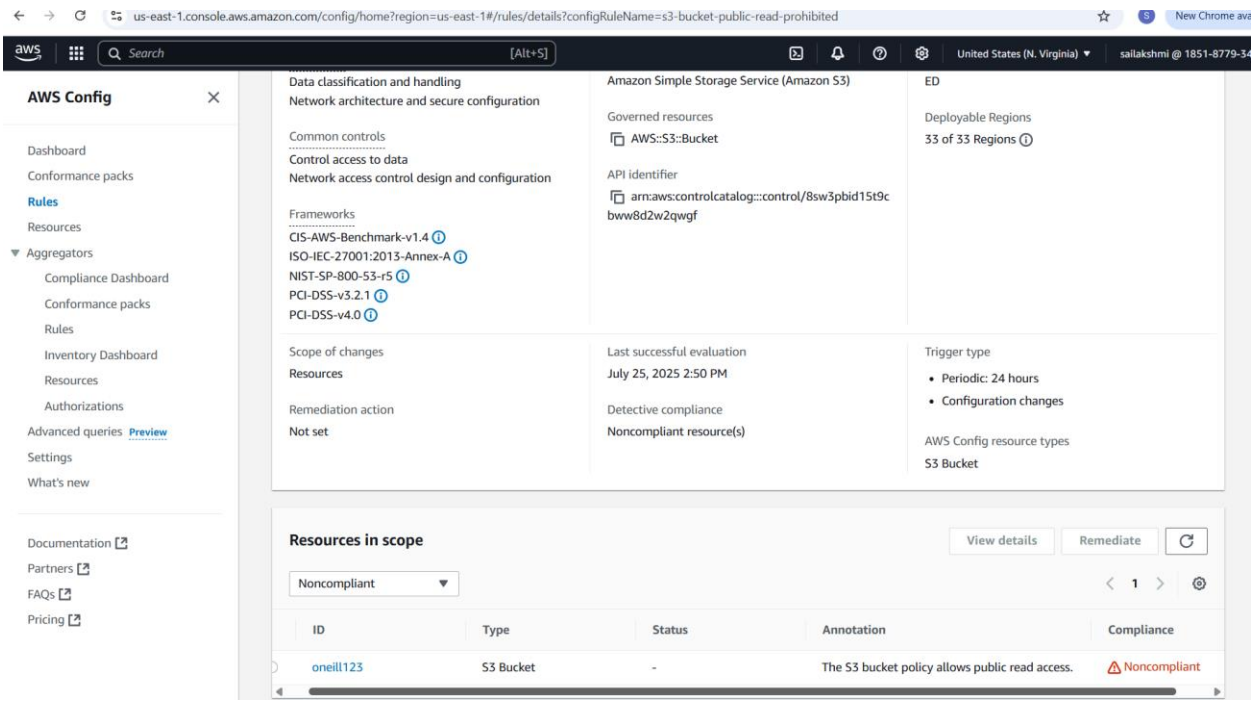


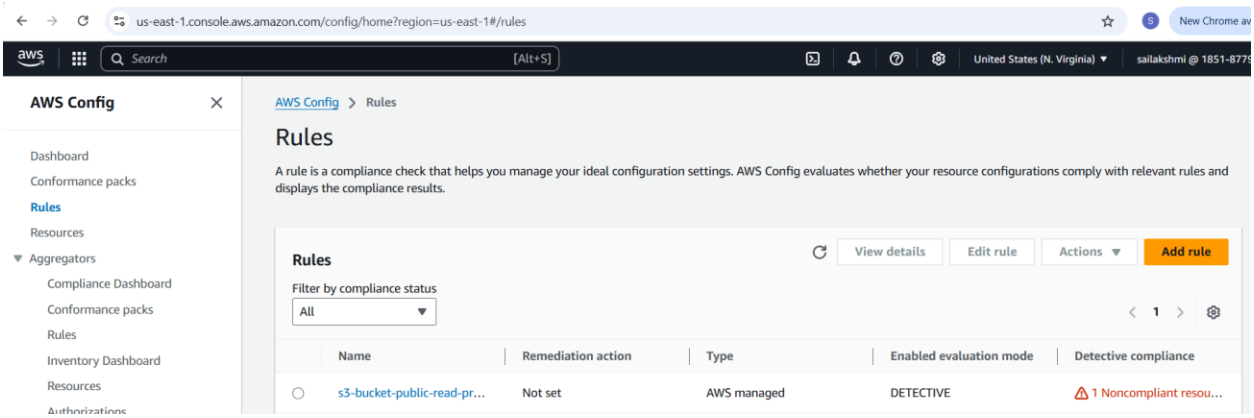


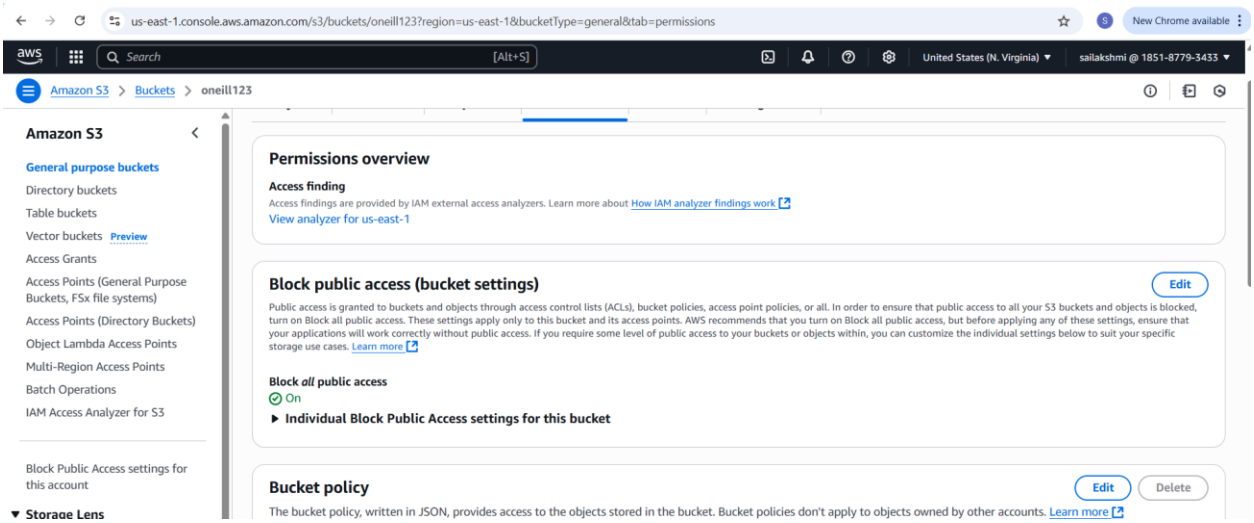
Received an email notification from SNS



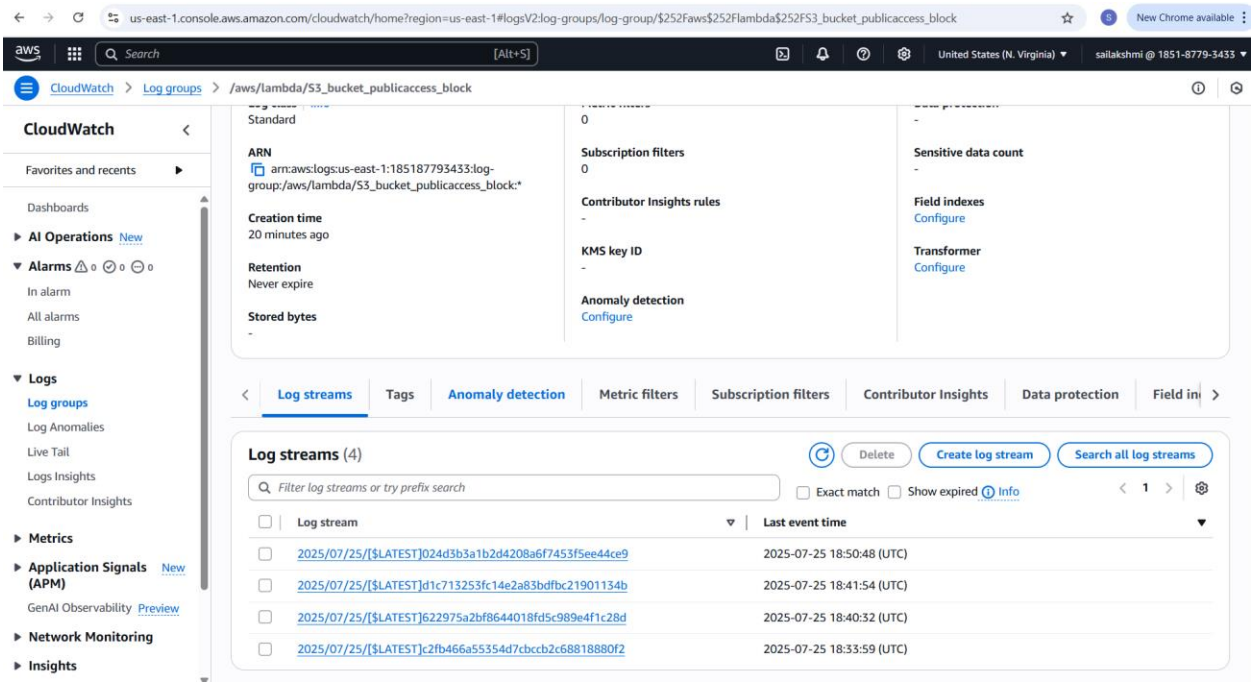

AWS Config detects it's **NON_COMPLIANT**

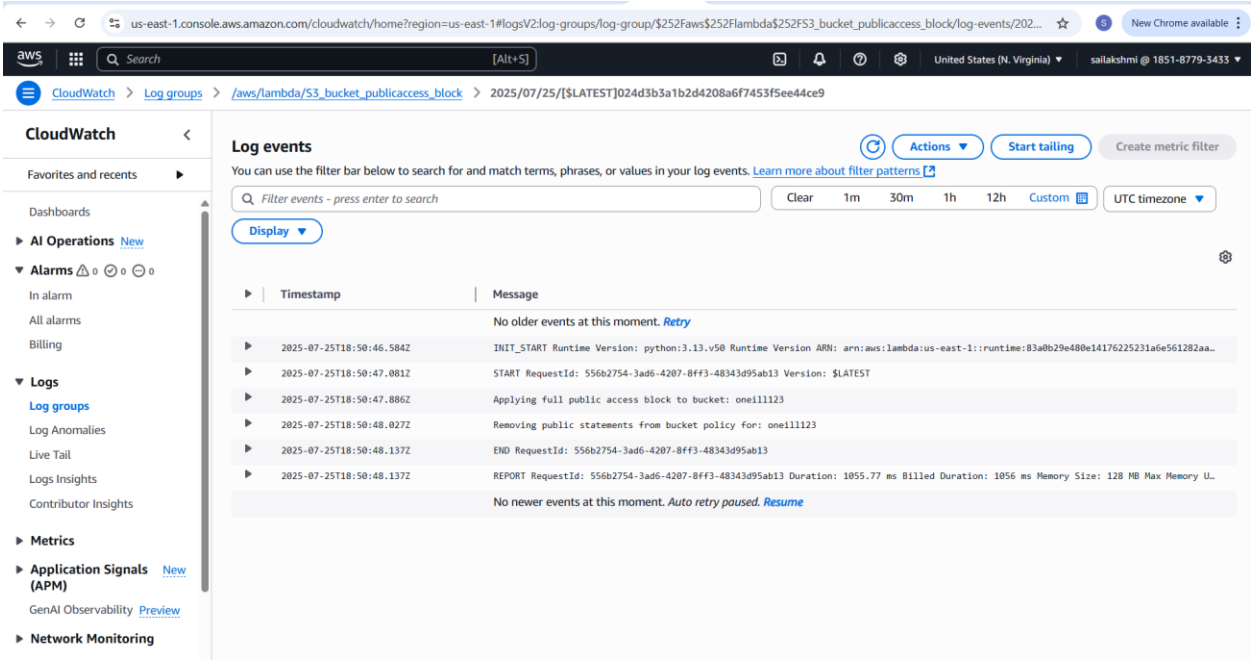


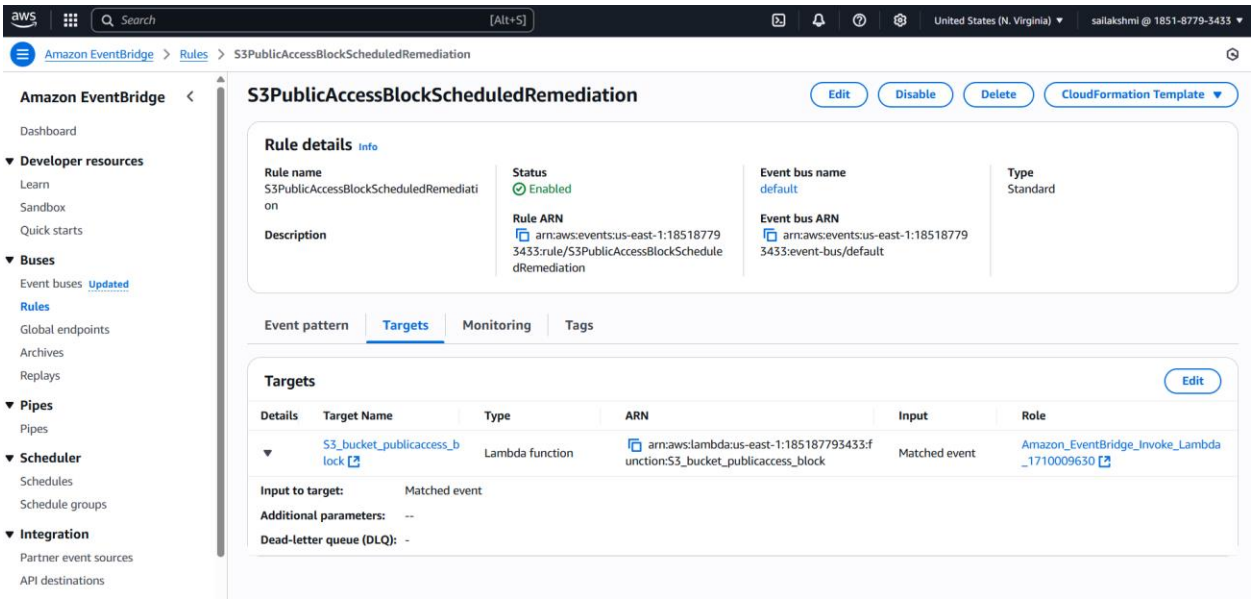



Cloud watch logs


us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2:log-groups/log-group/$252Faws$252Flambda$252FS3_bucket_publicaccess_block
New Chrome available
Search
[Alt+S]
United States (N. Virginia)
sailakshmi @ 1851-8779-3433
CloudWatch > Log groups > /aws/lambda/S3_bucket_publicaccess_block
CloudWatch
Favorites and recents
Dashboards
AI Operations New
Alarms 0 0 0
In alarm
All alarms
Billing
Logs
Log groups
Log Anomalies
Live Tail
Logs Insights
Contributor Insights
Metrics
Application Signals (APM) New
GenAI Observability Preview
Network Monitoring
Insights
Standard
ARN
arn:aws:logs:us-east-1:185187793433:log-group:/aws/lambda/S3_bucket_publicaccess_block:*
Creation time
20 minutes ago
Retention
Never expire
Stored bytes
-
0
Subscription filters
0
Contributor Insights rules
-
KMS key ID
-
Anomaly detection
Configure
-
Sensitive data count
-
Field indexes
Configure
Transformer
Configure
Log streams
Tags
Anomaly detection
Metric filters
Subscription filters
Contributor Insights
Data protection
Field in
Log streams (4)
Delete
Create log stream
Search all log streams
Filter log streams or try prefix search
Exact match
Show expired
Info
1
Log stream
Last event time
2025/07/25/[$LATEST]024d3b3a1b2d4208a6f7453f5ee44ce9
2025-07-25 18:50:48 (UTC)
2025/07/25/[$LATEST]d1c713253fc14e2a83bdfbc21901134b
2025-07-25 18:41:54 (UTC)
2025/07/25/[$LATEST]622975a2bf8644018fd5c989e4f1c28d
2025-07-25 18:40:32 (UTC)
2025/07/25/[$LATEST]c2fb466a55354d7cbccb2c68818880f2
2025-07-25 18:33:59 (UTC)


us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2:log-groups/log-group/$252Faws$252Flambda$252FS3_bucket_publicaccess_block/log-events/202...
New Chrome available
Search
[Alt+S]
United States (N. Virginia)
sailakshmi @ 1851-8779-3433
CloudWatch > Log groups > /aws/lambda/S3_bucket_publicaccess_block > 2025/07/25/[$LATEST]024d3b3a1b2d4208a6f7453f5ee44ce9
CloudWatch
Favorites and recents
Dashboards
AI Operations New
Alarms 0 0 0
In alarm
All alarms
Billing
Logs
Log groups
Log Anomalies
Live Tail
Logs Insights
Contributor Insights
Metrics
Application Signals (APM) New
GenAI Observability Preview
Network Monitoring
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
Clear
1m
30m
1h
12h
Custom
UTC timezone
Display
Timestamp
Message
No older events at this moment. Retry
2025-07-25T18:50:46.584Z
INIT_START Runtime Version: python:3.13.v50 Runtime Version ARN: arn:aws:lambda:us-east-1::runtime:83a0b29e480e14176225231a6e561282aa...
2025-07-25T18:50:47.081Z
START RequestId: 556b2754-3ad6-4207-8ff3-48343d95ab13 Version: $LATEST
2025-07-25T18:50:47.886Z
Applying full public access block to bucket: onei11123
2025-07-25T18:50:48.027Z
Removing public statements from bucket policy for: onei11123
2025-07-25T18:50:48.137Z
END RequestId: 556b2754-3ad6-4207-8ff3-48343d95ab13
2025-07-25T18:50:48.137Z
REPORT RequestId: 556b2754-3ad6-4207-8ff3-48343d95ab13 Duration: 1055.77 ms Billed Duration: 1056 ms Memory Size: 128 MB Max Memory U...
No newer events at this moment. Auto retry paused. Resume


Search
[Alt+S]
United States (N. Virginia)
sailakshmi @ 1851-8779-3433
Amazon EventBridge > Rules > S3PublicAccessBlockScheduledRemediation
Amazon EventBridge
Dashboard
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses Updated
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
Integration
Partner event sources
API destinations
S3PublicAccessBlockScheduledRemediation
Edit
Disable
Delete
CloudFormation Template
Rule details Info
Rule name
S3PublicAccessBlockScheduledRemediation
Description
Status
Enabled
Rule ARN
arn:aws:events:us-east-1:185187793433:rule/S3PublicAccessBlockScheduledRemediation
Event bus name
default
Event bus ARN
arn:aws:events:us-east-1:185187793433:event-bus/default
Type
Standard
Event pattern
Targets
Monitoring
Tags
Targets
Edit
Details
Target Name
Type
ARN
Input
Role
S3_bucket_publicaccess_block
Lambda function
arn:aws:lambda:us-east-1:185187793433:function:S3_bucket_publicaccess_block
Matched event
Amazon_EventBridge_Invoke_Lambda_1710009630
Input to target: Matched event
Additional parameters: --
Dead-letter queue (DLQ): -