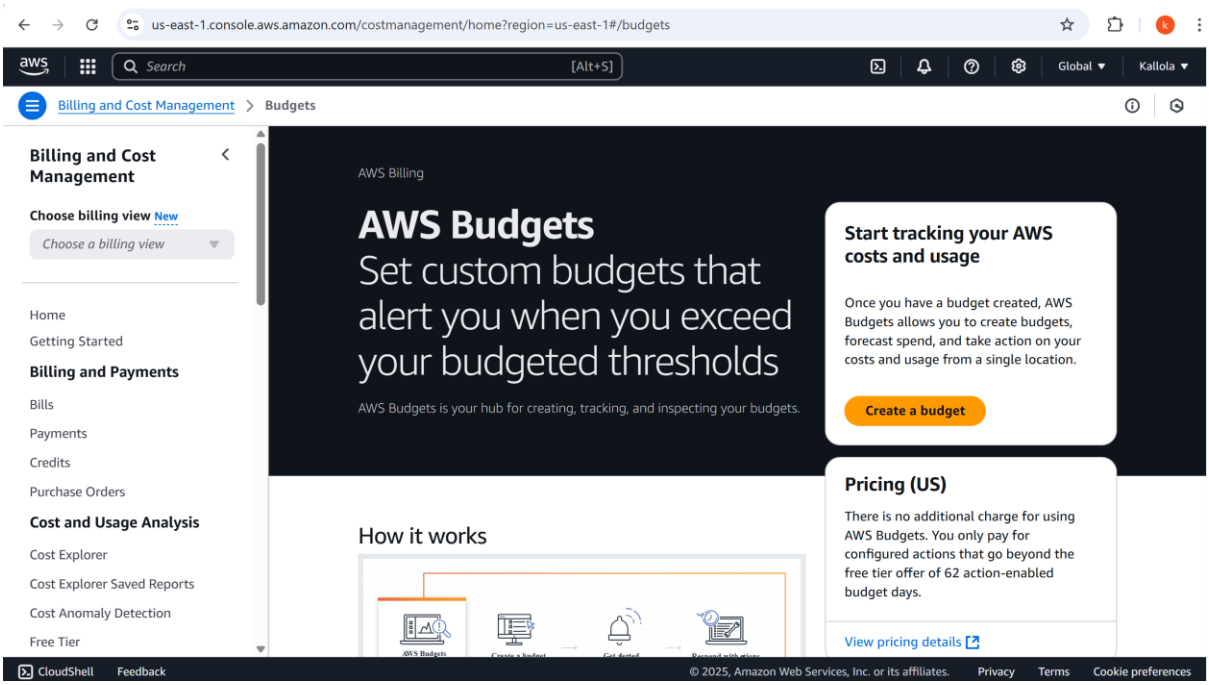
AWS Security Monitoring & Alerting Project

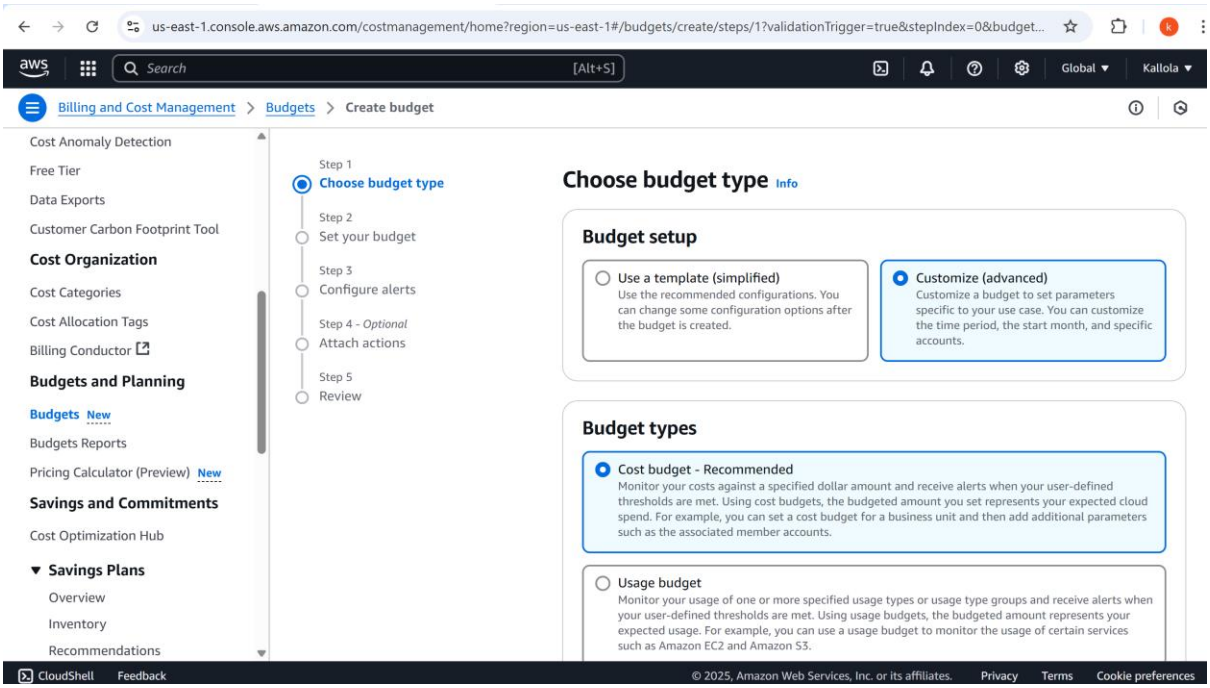
Phase-1. Enable Core AWS Security Services

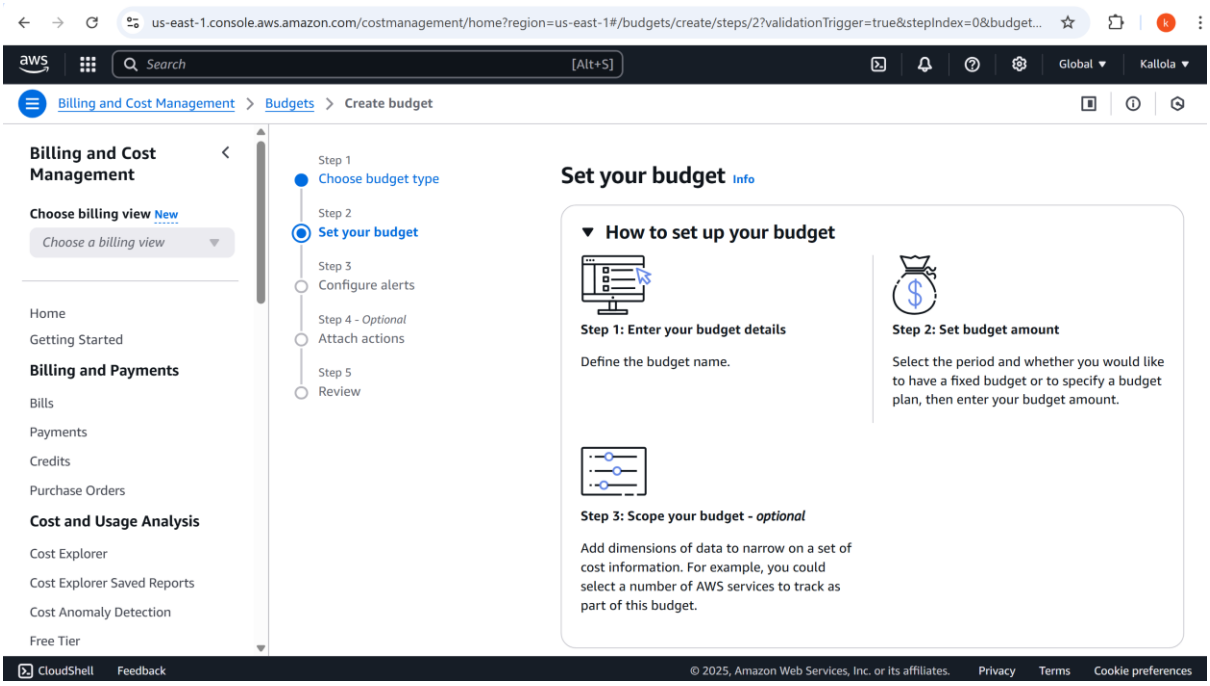
- **AWS CloudTrail (management and data events)**
- **GuardDuty (threat detection)**
- **AWS Config (change tracking)**
- **CloudWatch Logs and SNS (for alerting)**

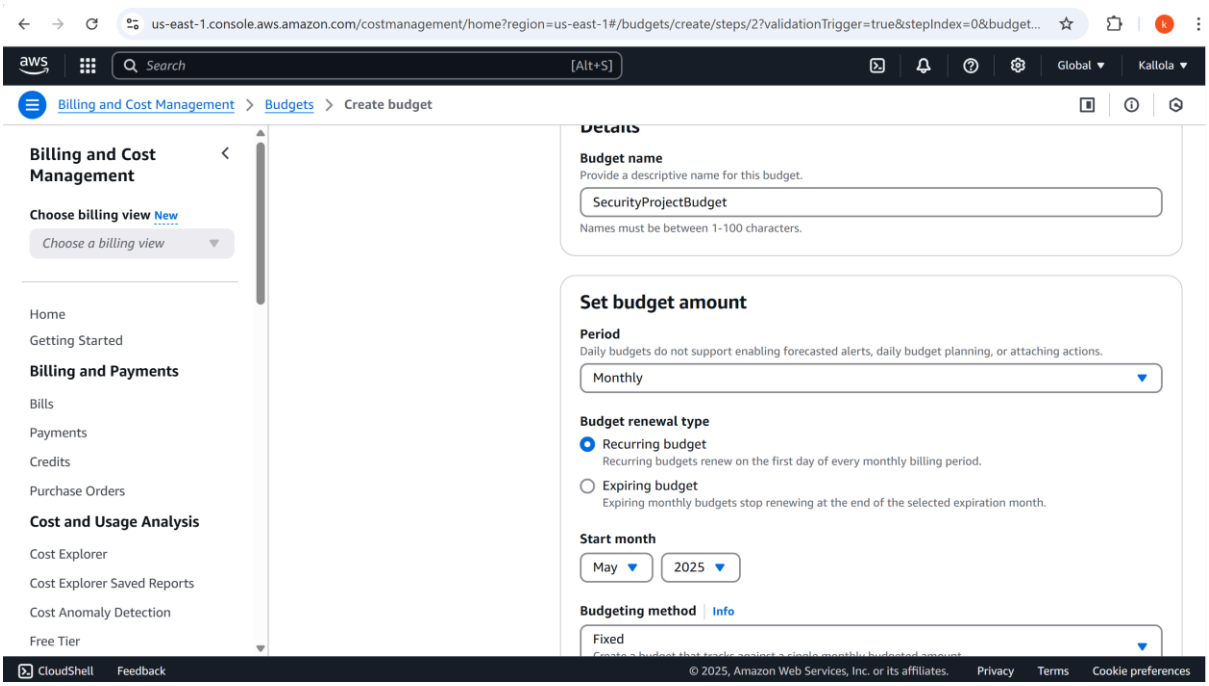
1. AWS budget Alarm setup:-

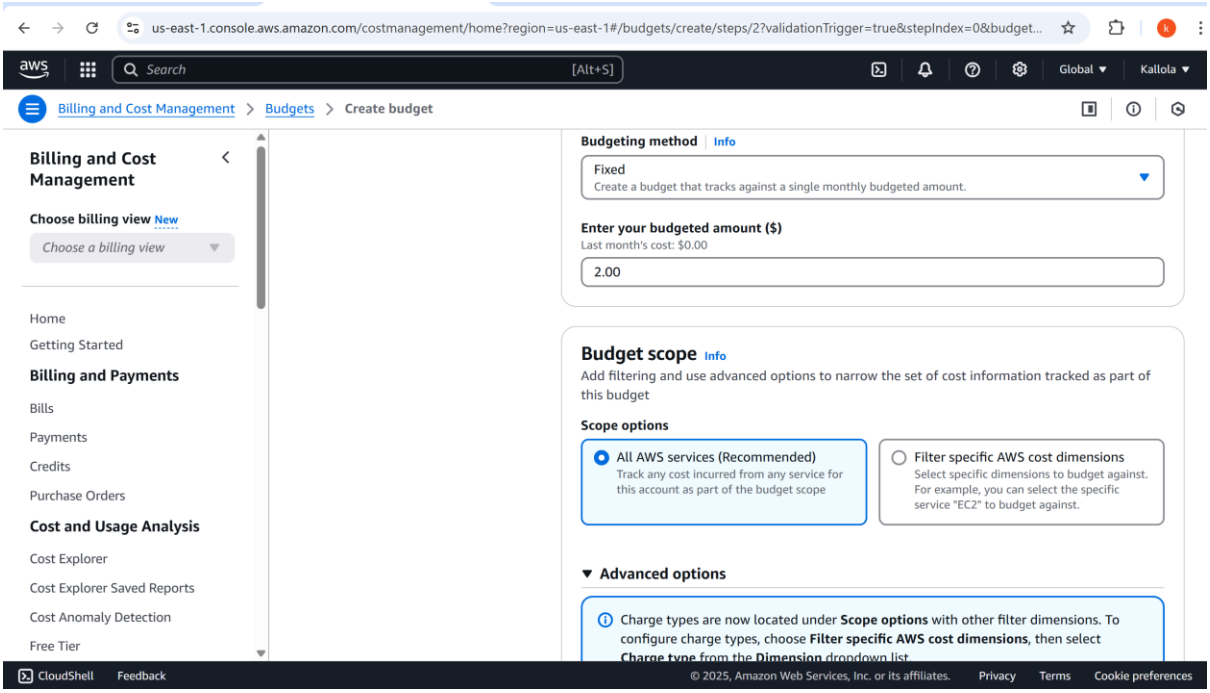


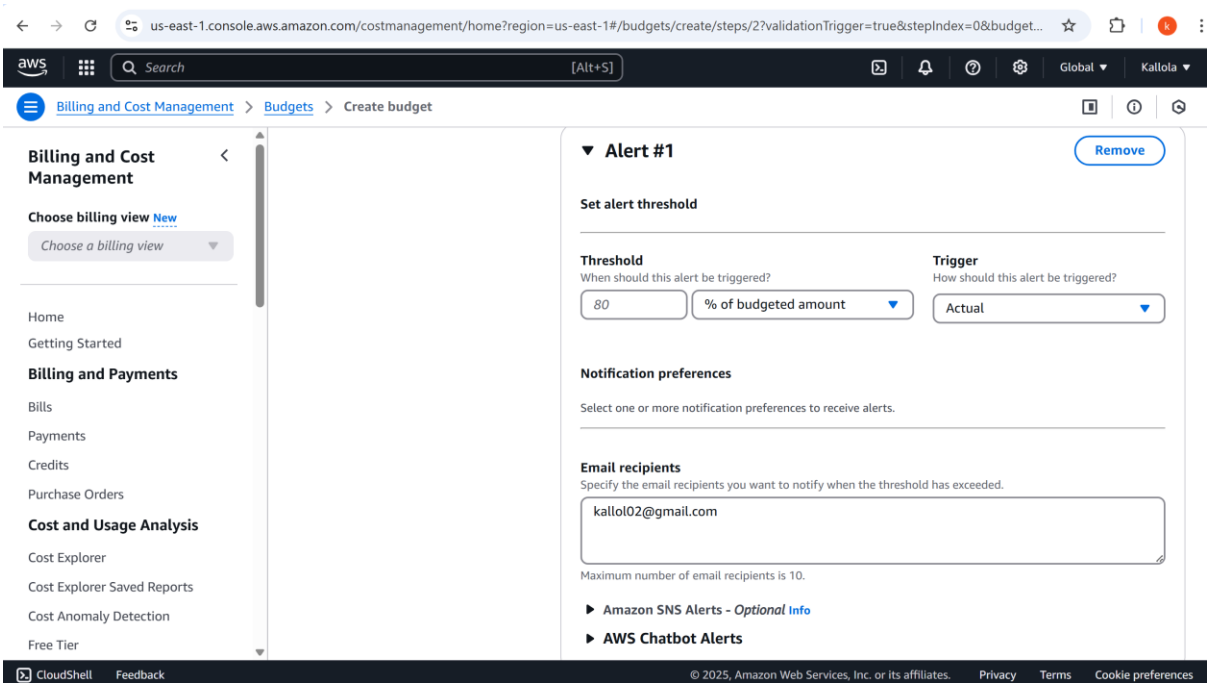
2. Create a new budget:-

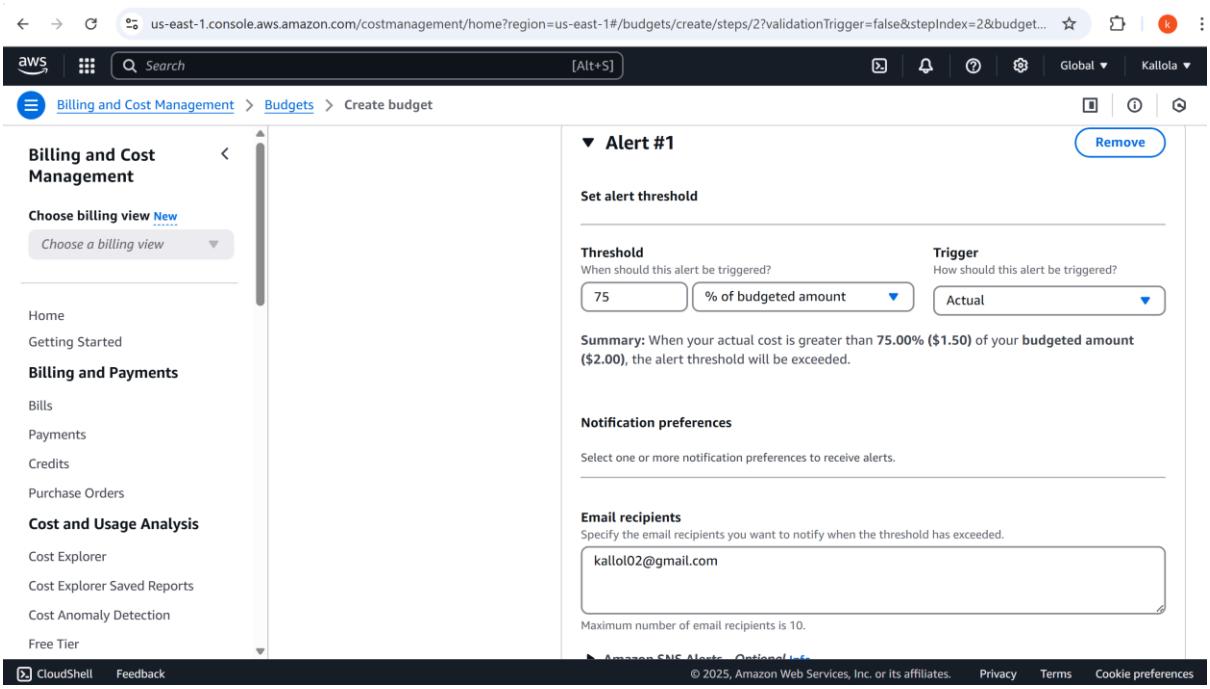

us-east-1.console.aws.amazon.com/costmanagement/home?region=us-east-1#/budgets/create/steps/1?validationTrigger=true&stepIndex=0&budget...
aws
Search
[Alt+S]
Global
Kallola
Billing and Cost Management
Budgets
Create budget
Cost Anomaly Detection
Free Tier
Data Exports
Customer Carbon Footprint Tool
Cost Organization
Cost Categories
Cost Allocation Tags
Billing Conductor
Budgets and Planning
Budgets New
Budgets Reports
Pricing Calculator (Preview) New
Savings and Commitments
Cost Optimization Hub
Savings Plans
Overview
Inventory
Recommendations
Step 1
Choose budget type
Step 2
Set your budget
Step 3
Configure alerts
Step 4 - Optional
Attach actions
Step 5
Review
Choose budget type Info
Budget setup
Use a template (simplified)
Use the recommended configurations. You can change some configuration options after the budget is created.
Customize (advanced)
Customize a budget to set parameters specific to your use case. You can customize the time period, the start month, and specific accounts.
Budget types
Cost budget - Recommended
Monitor your costs against a specified dollar amount and receive alerts when your user-defined thresholds are met. Using cost budgets, the budgeted amount you set represents your expected cloud spend. For example, you can set a cost budget for a business unit and then add additional parameters such as the associated member accounts.
Usage budget
Monitor your usage of one or more specified usage types or usage type groups and receive alerts when your user-defined thresholds are met. Using usage budgets, the budgeted amount represents your expected usage. For example, you can use a usage budget to monitor the usage of certain services such as Amazon EC2 and Amazon S3.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

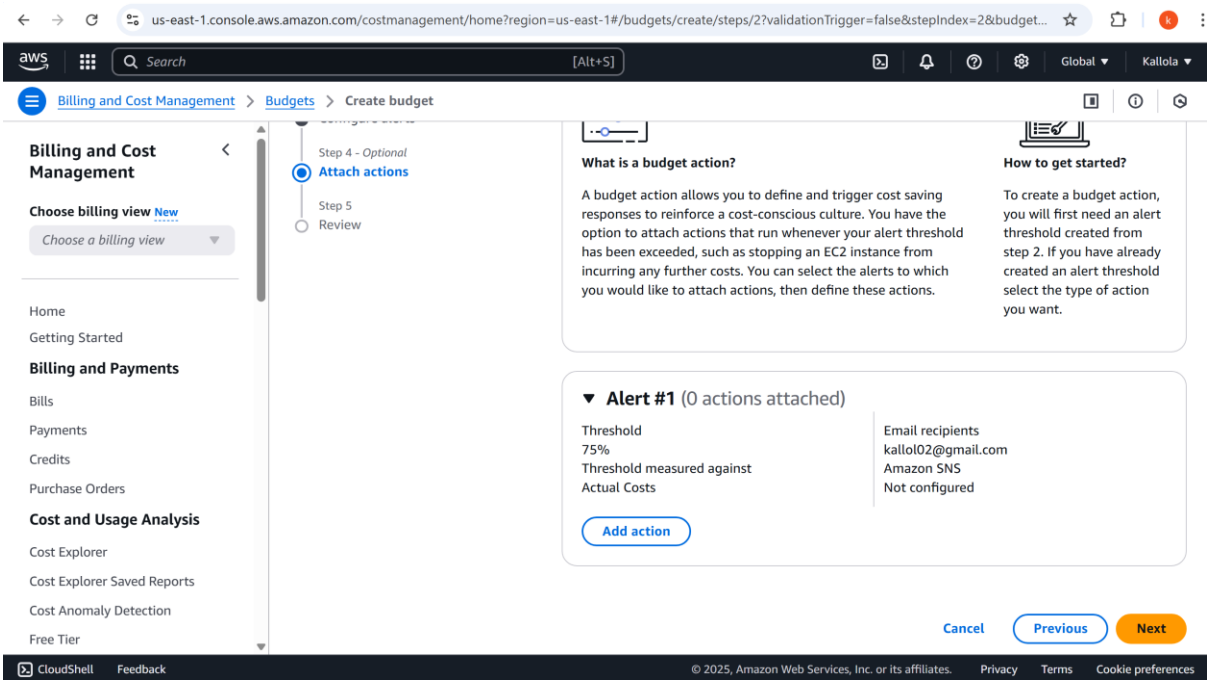

us-east-1.console.aws.amazon.com/costmanagement/home?region=us-east-1#/budgets/create/steps/2?validationTrigger=true&stepIndex=0&budget...
aws
Search
[Alt+S]
Global
Kallola
Billing and Cost Management
Budgets
Create budget
Billing and Cost Management
Choose billing view New
Choose a billing view
Home
Getting Started
Billing and Payments
Bills
Payments
Credits
Purchase Orders
Cost and Usage Analysis
Cost Explorer
Cost Explorer Saved Reports
Cost Anomaly Detection
Free Tier
Step 1
Choose budget type
Step 2
Set your budget
Step 3
Configure alerts
Step 4 - Optional
Attach actions
Step 5
Review
Set your budget Info
How to set up your budget
Step 1: Enter your budget details
Define the budget name.
Step 2: Set budget amount
Select the period and whether you would like to have a fixed budget or to specify a budget plan, then enter your budget amount.
Step 3: Scope your budget - optional
Add dimensions of data to narrow on a set of cost information. For example, you could select a number of AWS services to track as part of this budget.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

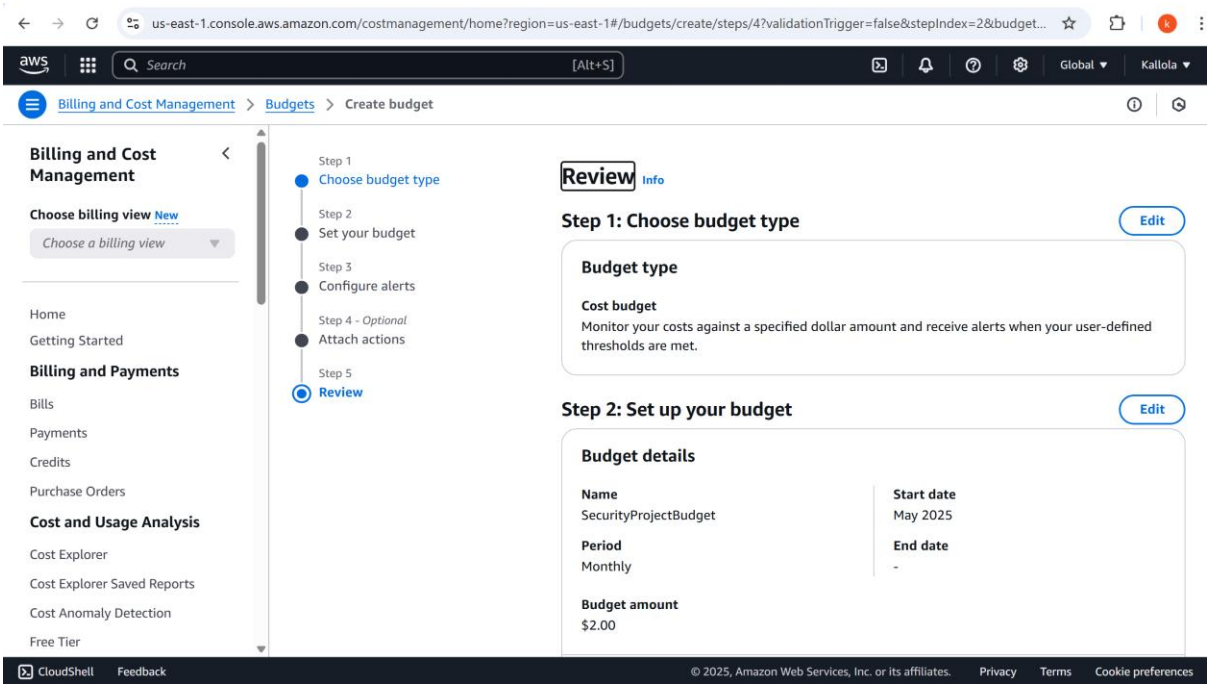

us-east-1.console.aws.amazon.com/costmanagement/home?region=us-east-1#/budgets/create/steps/2?validationTrigger=true&stepIndex=0&budget...
Search
[Alt+S]
Global
Kallola
Billing and Cost Management > Budgets > Create budget
Billing and Cost Management
Choose billing view New
Choose a billing view
Home
Getting Started
Billing and Payments
Bills
Payments
Credits
Purchase Orders
Cost and Usage Analysis
Cost Explorer
Cost Explorer Saved Reports
Cost Anomaly Detection
Free Tier
Budget name
Provide a descriptive name for this budget.
SecurityProjectBudget
Names must be between 1-100 characters.
Set budget amount
Period
Daily budgets do not support enabling forecasted alerts, daily budget planning, or attaching actions.
Monthly
Budget renewal type
Recurring budget
Recurring budgets renew on the first day of every monthly billing period.
Expiring budget
Expiring monthly budgets stop renewing at the end of the selected expiration month.
Start month
May
2025
Budgeting method Info
Fixed
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

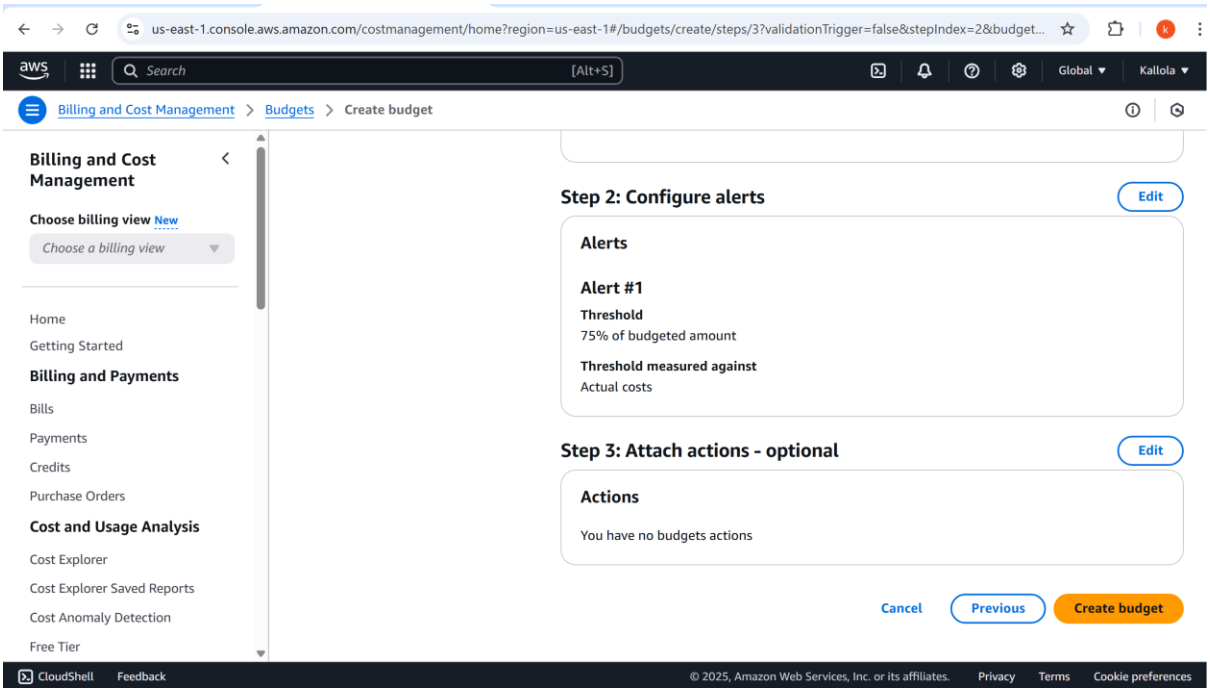

us-east-1.console.aws.amazon.com/costmanagement/home?region=us-east-1#/budgets/create/steps/2?validationTrigger=true&stepIndex=0&budget...
Search
[Alt+S]
Global
Kallola
Billing and Cost Management > Budgets > Create budget
Billing and Cost Management
Choose billing view New
Choose a billing view
Home
Getting Started
Billing and Payments
Bills
Payments
Credits
Purchase Orders
Cost and Usage Analysis
Cost Explorer
Cost Explorer Saved Reports
Cost Anomaly Detection
Free Tier
Budgeting method Info
Fixed
Create a budget that tracks against a single monthly budgeted amount.
Enter your budgeted amount ($)
Last month's cost: $0.00
2.00
Budget scope Info
Add filtering and use advanced options to narrow the set of cost information tracked as part of this budget
Scope options
All AWS services (Recommended)
Track any cost incurred from any service for this account as part of the budget scope
Filter specific AWS cost dimensions
Select specific dimensions to budget against. For example, you can select the specific service "EC2" to budget against.
Advanced options
Charge types are now located under Scope options with other filter dimensions. To configure charge types, choose Filter specific AWS cost dimensions, then select Charge type from the Dimension dropdown list.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

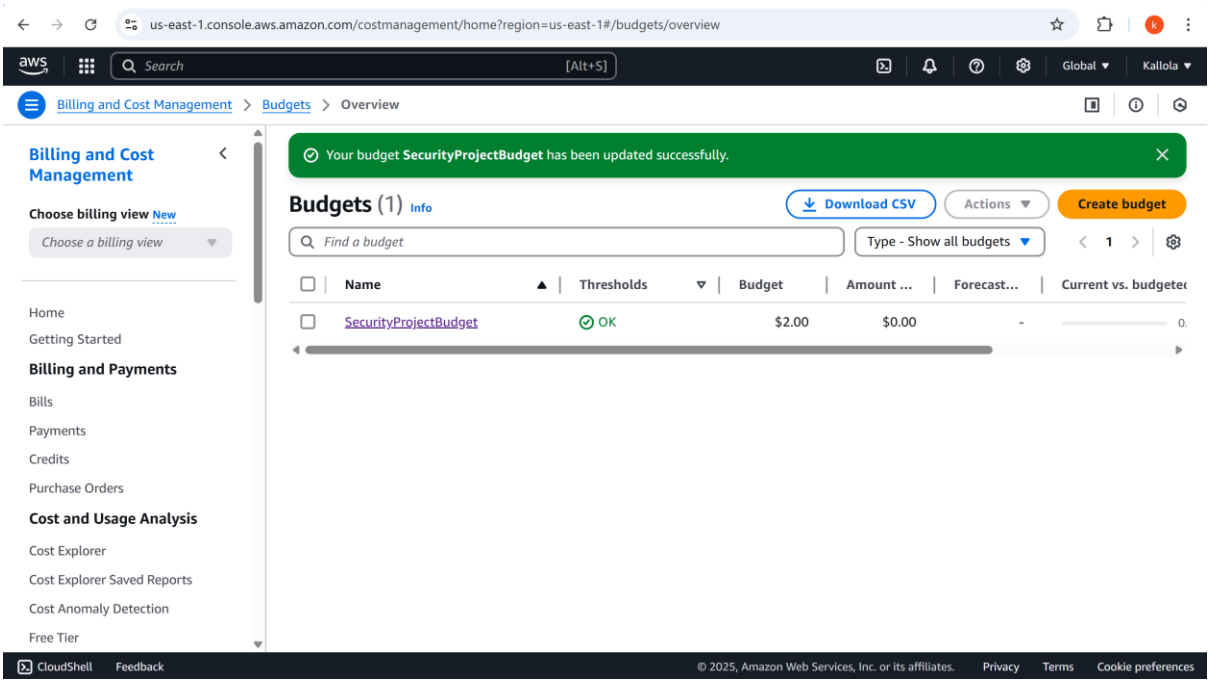

us-east-1.console.aws.amazon.com/costmanagement/home?region=us-east-1#/budgets/create/steps/2?validationTrigger=true&stepIndex=0&budget...
Search
[Alt+S]
Global
Kallola
Billing and Cost Management > Budgets > Create budget
Billing and Cost Management
Choose billing view New
Choose a billing view
Home
Getting Started
Billing and Payments
Bills
Payments
Credits
Purchase Orders
Cost and Usage Analysis
Cost Explorer
Cost Explorer Saved Reports
Cost Anomaly Detection
Free Tier
Alert #1
Remove
Set alert threshold
Threshold
When should this alert be triggered?
80
% of budgeted amount
Trigger
How should this alert be triggered?
Actual
Notification preferences
Select one or more notification preferences to receive alerts.
Email recipients
Specify the email recipients you want to notify when the threshold has exceeded.
kallol02@gmail.com
Maximum number of email recipients is 10.
Amazon SNS Alerts - Optional Info
AWS Chatbot Alerts
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

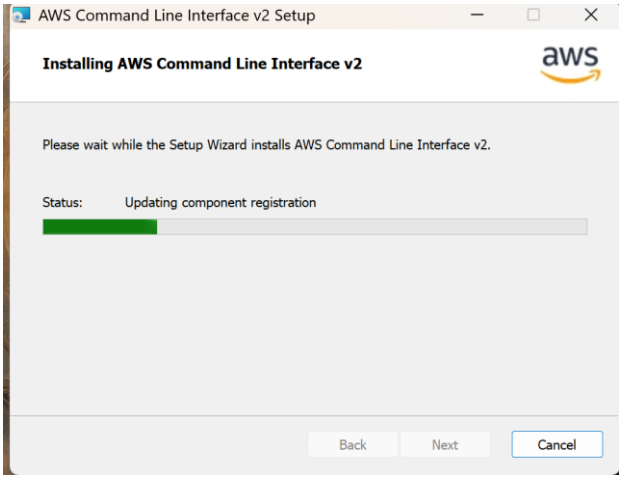

us-east-1.console.aws.amazon.com/costmanagement/home?region=us-east-1#/budgets/create/steps/2?validationTrigger=false&stepIndex=2&budget...
Search
[Alt+S]
Global
Kallola
Billing and Cost Management > Budgets > Create budget
Billing and Cost Management
Choose billing view New
Choose a billing view
Home
Getting Started
Billing and Payments
Bills
Payments
Credits
Purchase Orders
Cost and Usage Analysis
Cost Explorer
Cost Explorer Saved Reports
Cost Anomaly Detection
Free Tier
Alert #1
Remove
Set alert threshold
Threshold
When should this alert be triggered?
75
% of budgeted amount
Trigger
How should this alert be triggered?
Actual
Summary: When your actual cost is greater than 75.00% ($1.50) of your budgeted amount ($2.00), the alert threshold will be exceeded.
Notification preferences
Select one or more notification preferences to receive alerts.
Email recipients
Specify the email recipients you want to notify when the threshold has exceeded.
kallol02@gmail.com
Maximum number of email recipients is 10.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

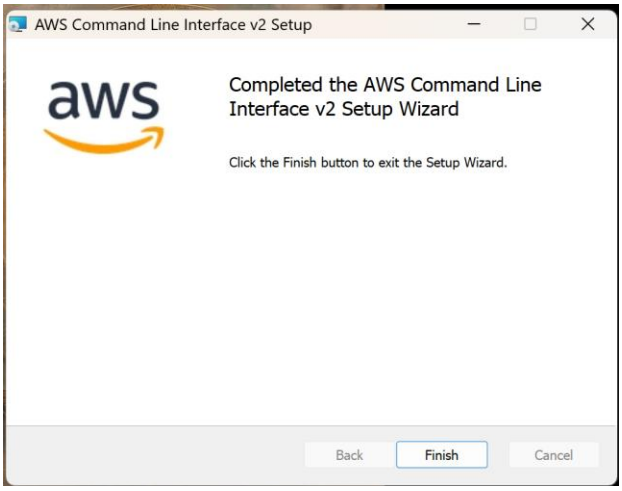

us-east-1.console.aws.amazon.com/costmanagement/home?region=us-east-1#/budgets/create/steps/2?validationTrigger=false&stepIndex=2&budget...
Search
[Alt+S]
Global
Kallola
Billing and Cost Management
Budgets
Create budget
Billing and Cost Management
Choose billing view New
Choose a billing view
Home
Getting Started
Billing and Payments
Bills
Payments
Credits
Purchase Orders
Cost and Usage Analysis
Cost Explorer
Cost Explorer Saved Reports
Cost Anomaly Detection
Free Tier
Step 4 - Optional
Attach actions
Step 5
Review
What is a budget action?
A budget action allows you to define and trigger cost saving responses to reinforce a cost-conscious culture. You have the option to attach actions that run whenever your alert threshold has been exceeded, such as stopping an EC2 instance from incurring any further costs. You can select the alerts to which you would like to attach actions, then define these actions.
How to get started?
To create a budget action, you will first need an alert threshold created from step 2. If you have already created an alert threshold select the type of action you want.
Alert #1 (0 actions attached)
Threshold
75%
Threshold measured against
Actual Costs
Email recipients
kallol02@gmail.com
Amazon SNS
Not configured
Add action
Cancel
Previous
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

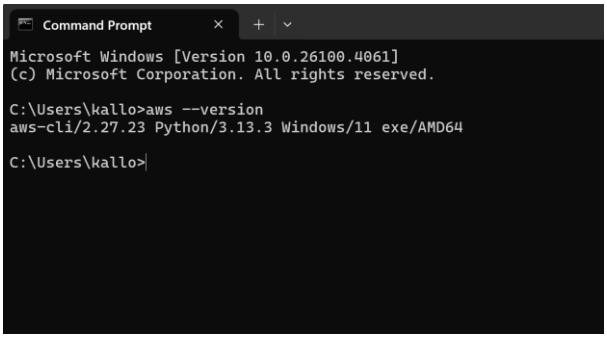

us-east-1.console.aws.amazon.com/costmanagement/home?region=us-east-1#/budgets/create/steps/4?validationTrigger=false&stepIndex=2&budget...
Search
[Alt+S]
Global
Kallola
Billing and Cost Management
Budgets
Create budget
Billing and Cost Management
Choose billing view New
Choose a billing view
Home
Getting Started
Billing and Payments
Bills
Payments
Credits
Purchase Orders
Cost and Usage Analysis
Cost Explorer
Cost Explorer Saved Reports
Cost Anomaly Detection
Free Tier
Step 1
Choose budget type
Step 2
Set your budget
Step 3
Configure alerts
Step 4 - Optional
Attach actions
Step 5
Review
Review Info
Step 1: Choose budget type
Edit
Budget type
Cost budget
Monitor your costs against a specified dollar amount and receive alerts when your user-defined thresholds are met.
Step 2: Set up your budget
Edit
Budget details
Name
SecurityProjectBudget
Period
Monthly
Budget amount
$2.00
Start date
May 2025
End date
-
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com/costmanagement/home?region=us-east-1#/budgets/create/steps/3?validationTrigger=false&stepIndex=2&budget...
Search
[Alt+S]
Global
Kallola
Billing and Cost Management > Budgets > Create budget
Billing and Cost Management
Choose billing view New
Choose a billing view
Home
Getting Started
Billing and Payments
Bills
Payments
Credits
Purchase Orders
Cost and Usage Analysis
Cost Explorer
Cost Explorer Saved Reports
Cost Anomaly Detection
Free Tier
Step 2: Configure alerts
Edit
Alerts
Alert #1
Threshold
75% of budgeted amount
Threshold measured against
Actual costs
Step 3: Attach actions - optional
Edit
Actions
You have no budgets actions
Cancel
Previous
Create budget
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com/costmanagement/home?region=us-east-1#/budgets/overview
Search
[Alt+S]
Global
Kallola
Billing and Cost Management > Budgets > Overview
Billing and Cost Management
Choose billing view New
Choose a billing view
Home
Getting Started
Billing and Payments
Bills
Payments
Credits
Purchase Orders
Cost and Usage Analysis
Cost Explorer
Cost Explorer Saved Reports
Cost Anomaly Detection
Free Tier
Your budget SecurityProjectBudget has been updated successfully.
Budgets (1) Info
Download CSV
Actions
Create budget
Find a budget
Type - Show all budgets
1
Name
Thresholds
Budget
Amount ...
Forecast...
Current vs. budgeted
SecurityProjectBudget
OK
$2.00
$0.00
-
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences







Phase 1: Setup Security Services

✅ Enable CloudTrail

ap-south-1.console.aws.amazon.com/cloudtrailv2/home?region=ap-south-1#/welcome

Search [Alt+S] Asia Pacific (Mumbai) Kallola

Management & Governance

AWS CloudTrail

Continuously log your AWS account activity

Use CloudTrail to meet your governance, compliance, and auditing needs for your AWS accounts.

Create a trail with AWS CloudTrail

Get started with AWS CloudTrail by creating a trail to log your AWS account activity.

Create a trail

Pricing

Pricing

How it works

Getting started

What is AWS CloudTrail?

How AWS CloudTrail works

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

ap-south-1.console.aws.amazon.com/cloudtrailv2/home?region=ap-south-1#/create

Search [Alt+S] Asia Pacific (Mumbai) Kallola

CloudTrail > Create trail

Step 1
Choose trail attributes

Step 2
Choose log events

Step 3
Review and create

Choose trail attributes

General details

A trail created in the console is a multi-region trail. Learn more

Trail name

Enter a display name for your trail.

KK_management_events

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

Enable for all accounts in my organization

To review accounts in your organization, open AWS Organizations. See all accounts

Storage location Info

Create new S3 bucket
Create a bucket to store logs for the trail.

Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

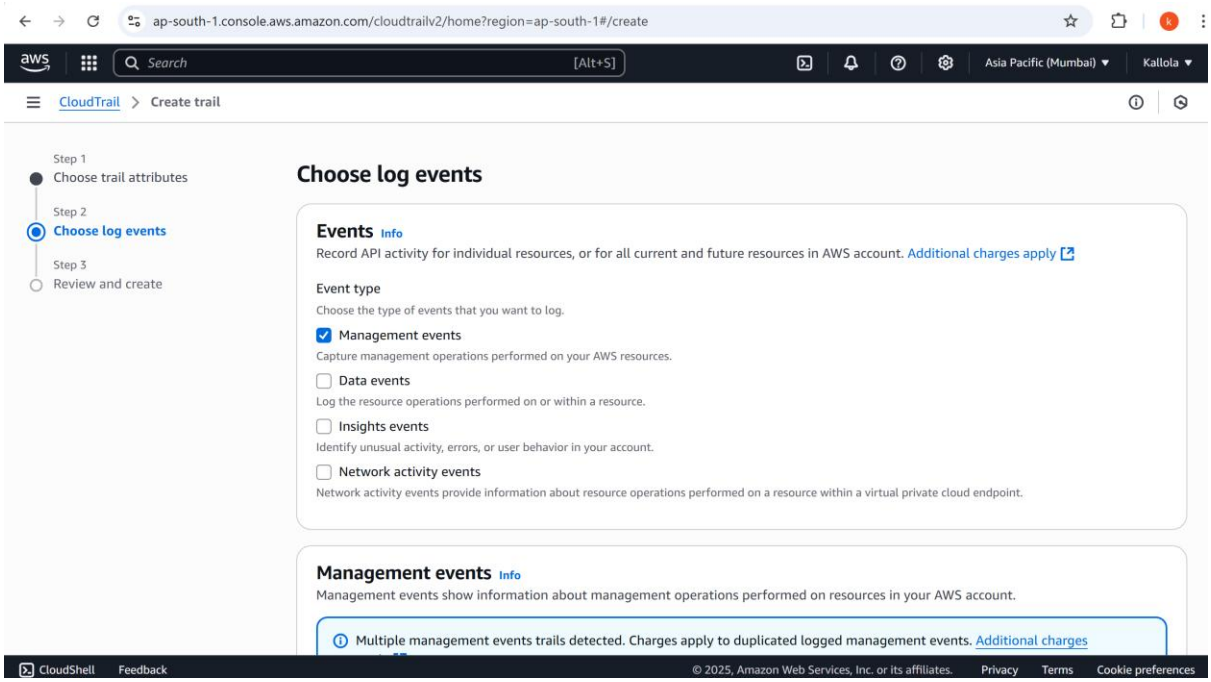
Trail log bucket and folder

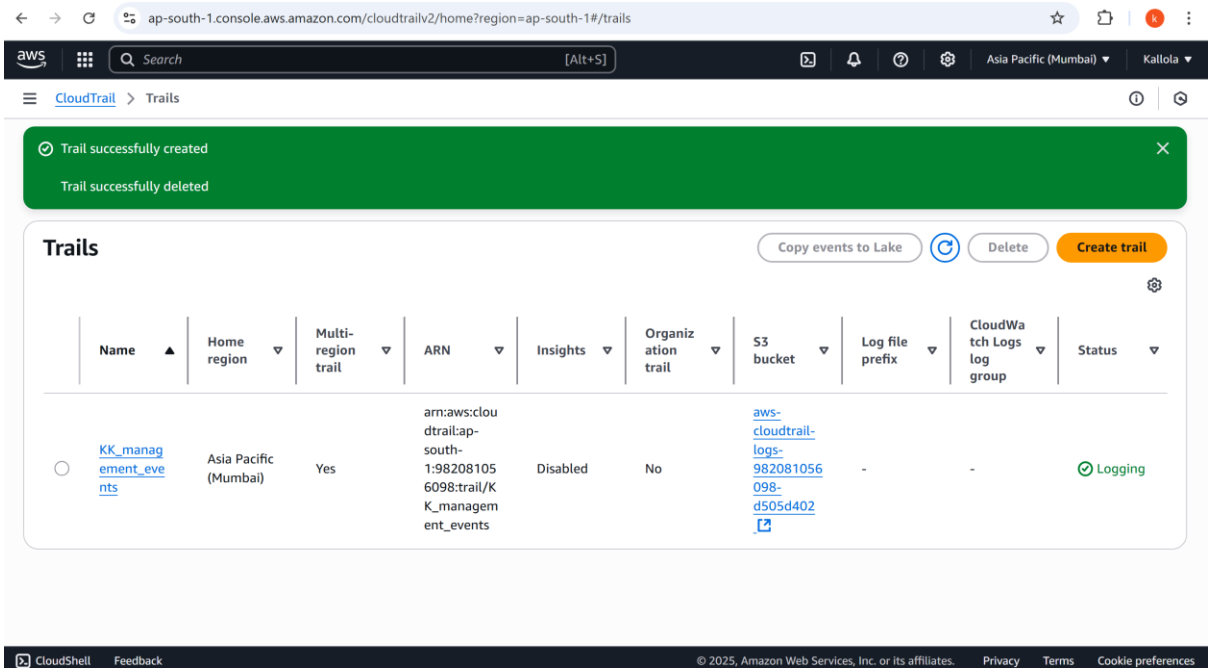
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

aws-cloudtrail-logs-982081056098-d505d402

Logs will be stored in aws-cloudtrail-logs-982081056098-d505d402/AWSLogs/982081056098

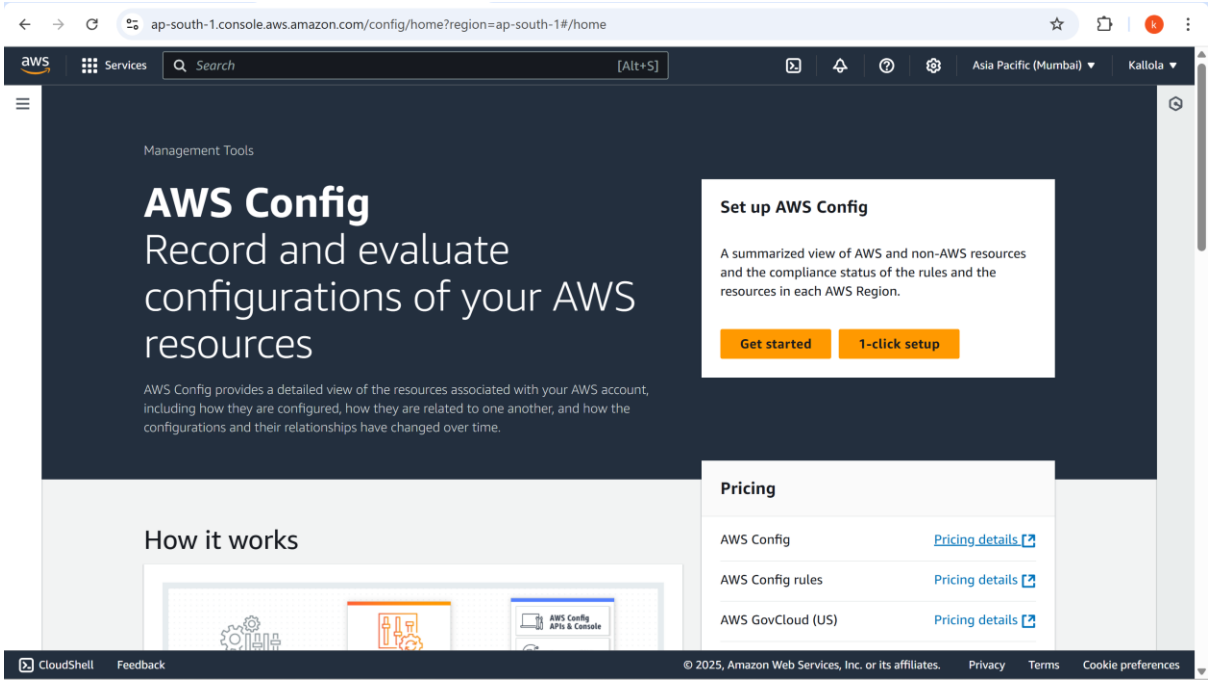
Log file SSE-KMS encryption Info

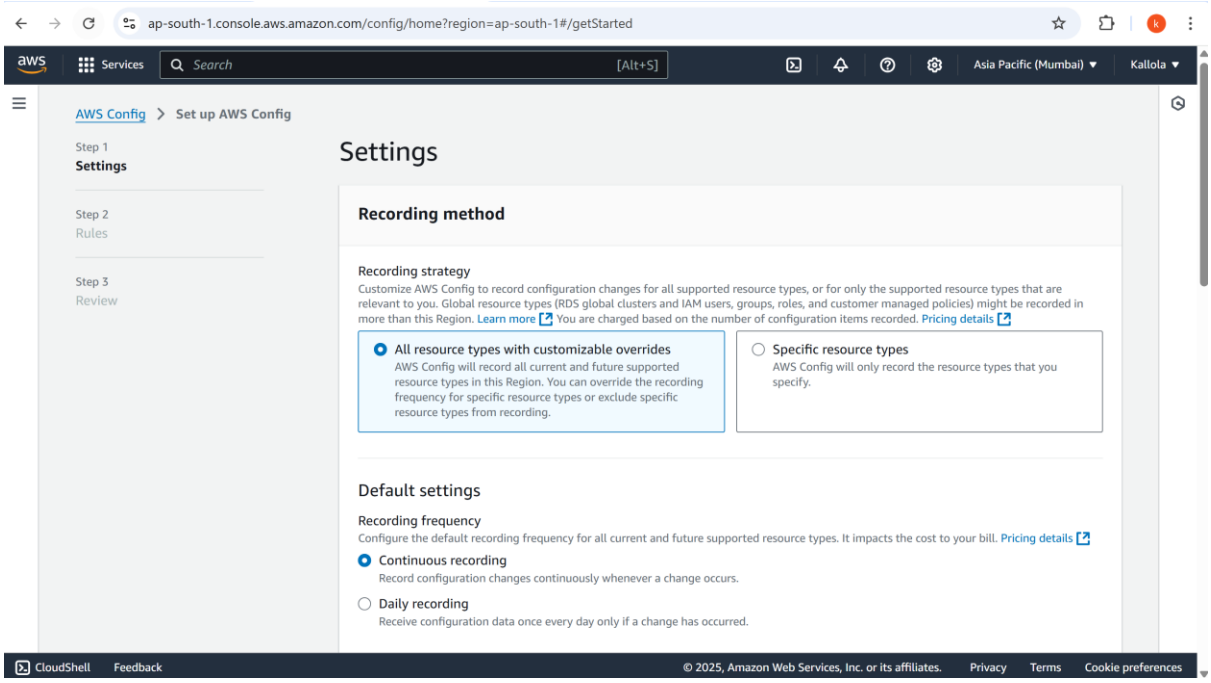


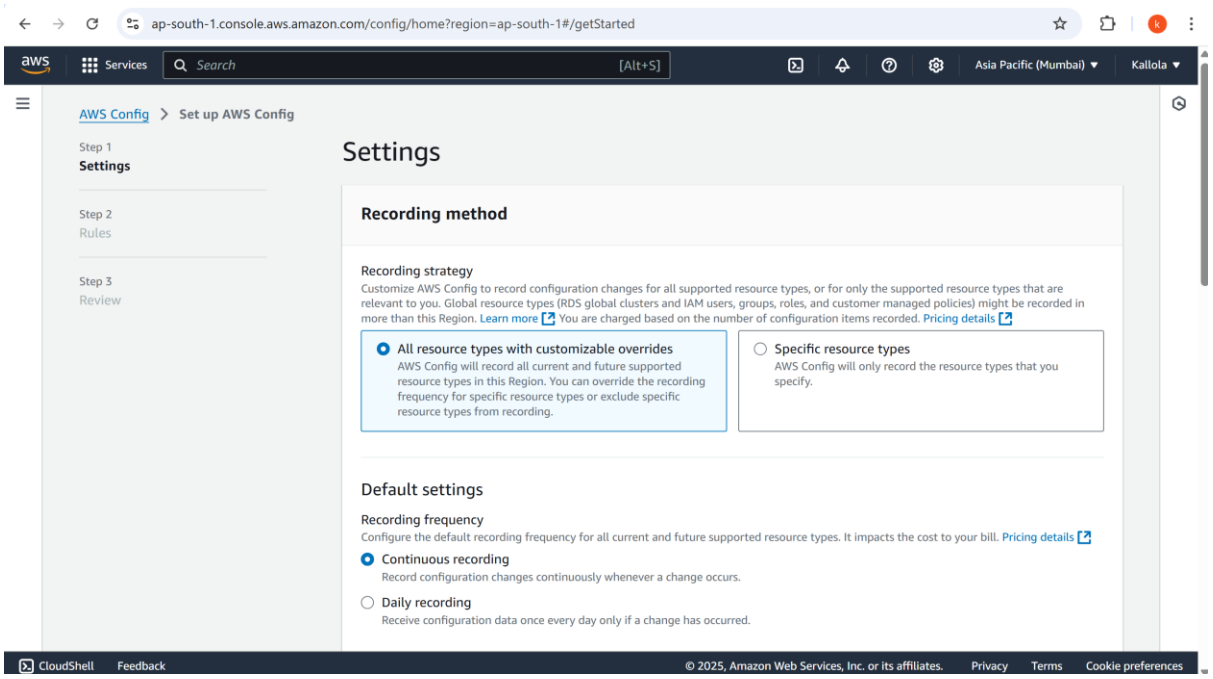


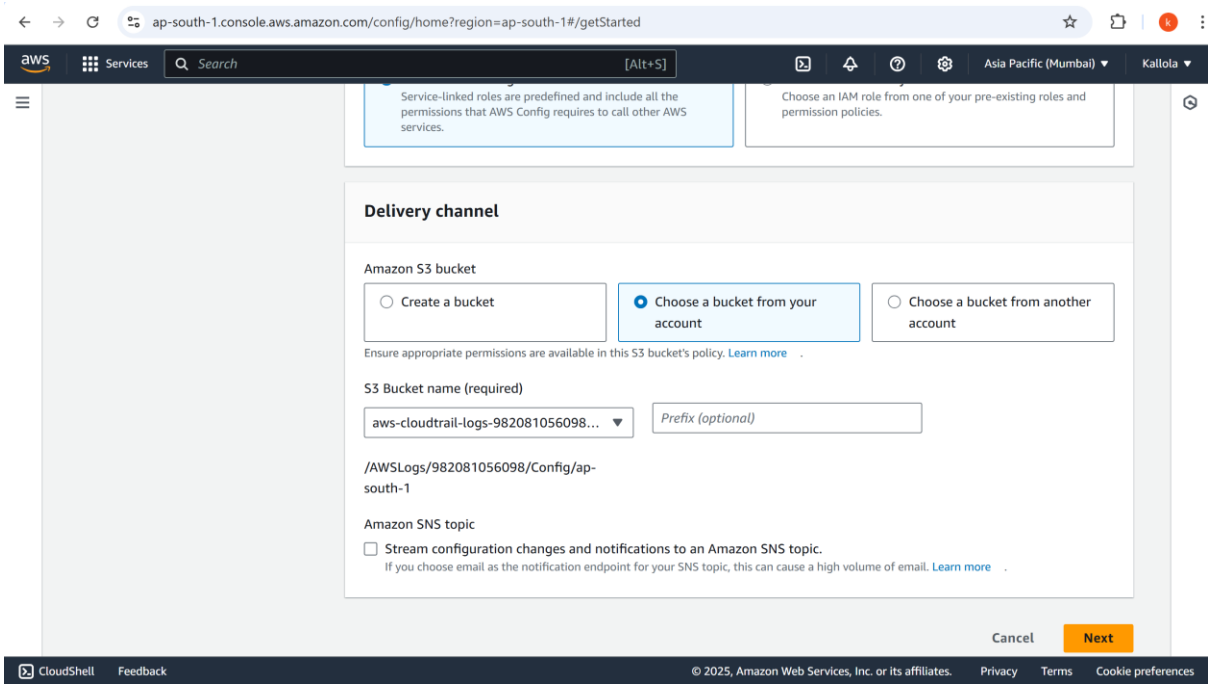
✅ Enable AWS Config

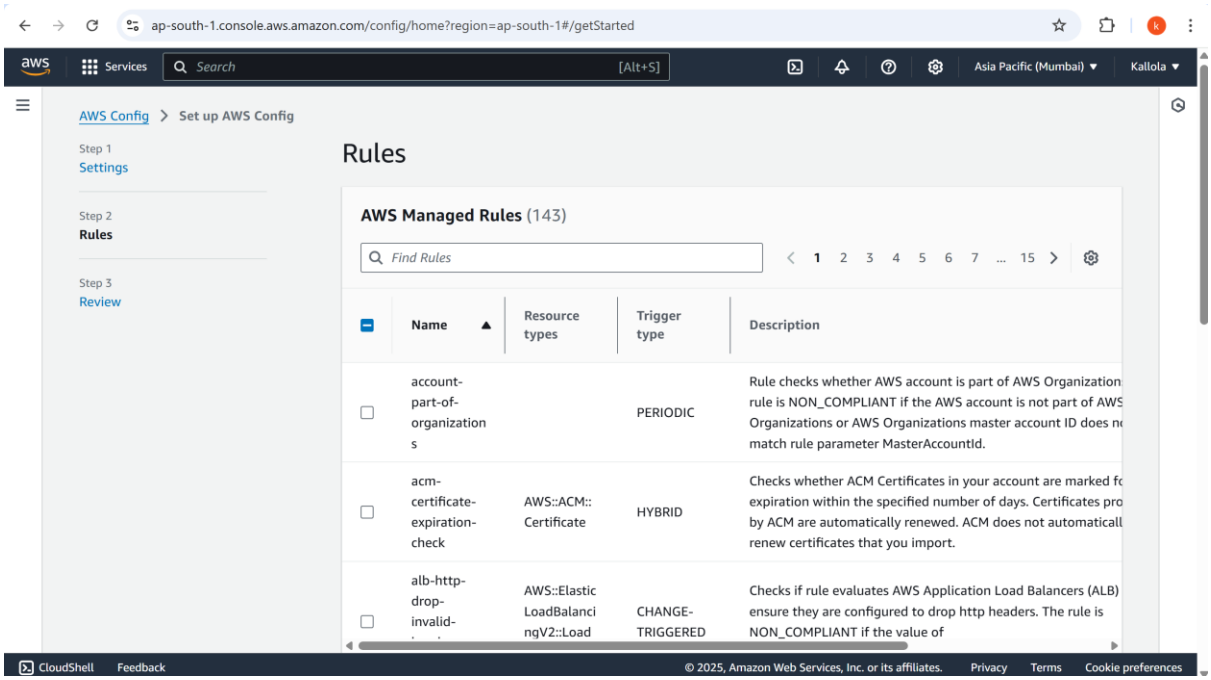
- Go to AWS Config → Set it up for all resources
- Choose the same or a different S3 bucket for Config logs

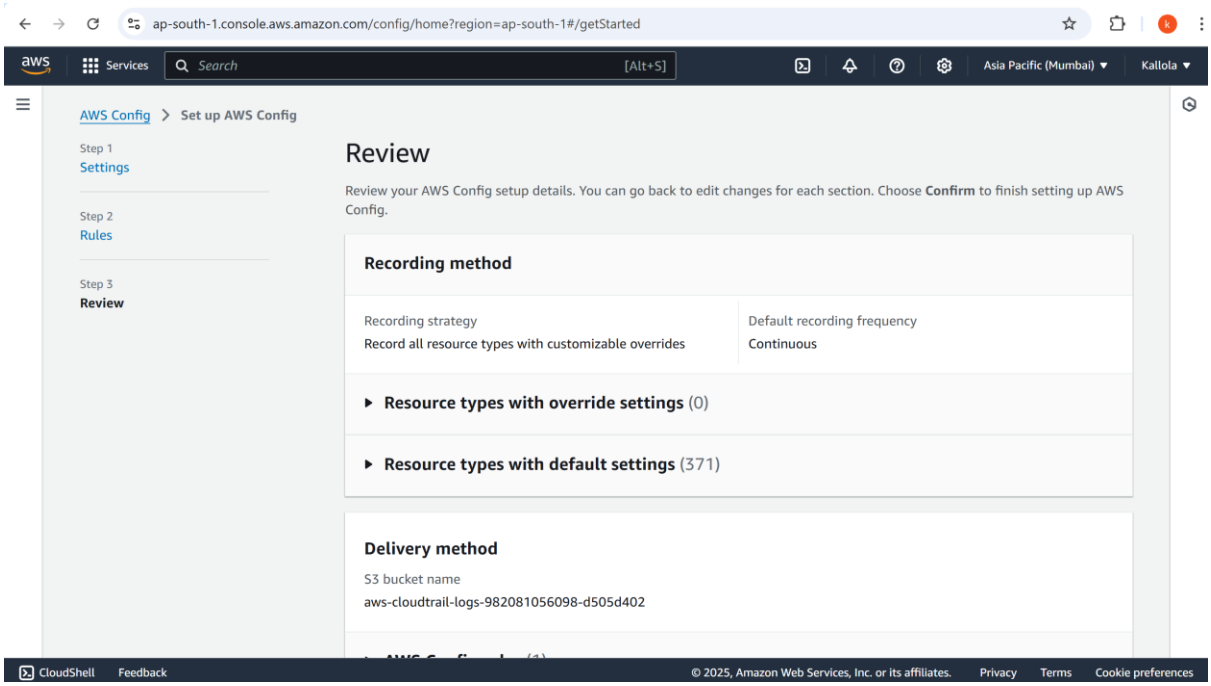

ap-south-1.console.aws.amazon.com/config/home?region=ap-south-1#/home
aws
Services
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
Management Tools
AWS Config
Record and evaluate configurations of your AWS resources
AWS Config provides a detailed view of the resources associated with your AWS account, including how they are configured, how they are related to one another, and how the configurations and their relationships have changed over time.
Set up AWS Config
A summarized view of AWS and non-AWS resources and the compliance status of the rules and the resources in each AWS Region.
Get started
1-click setup
Pricing
AWS Config
Pricing details
AWS Config rules
Pricing details
AWS GovCloud (US)
Pricing details
How it works
AWS Config APIs & Console
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

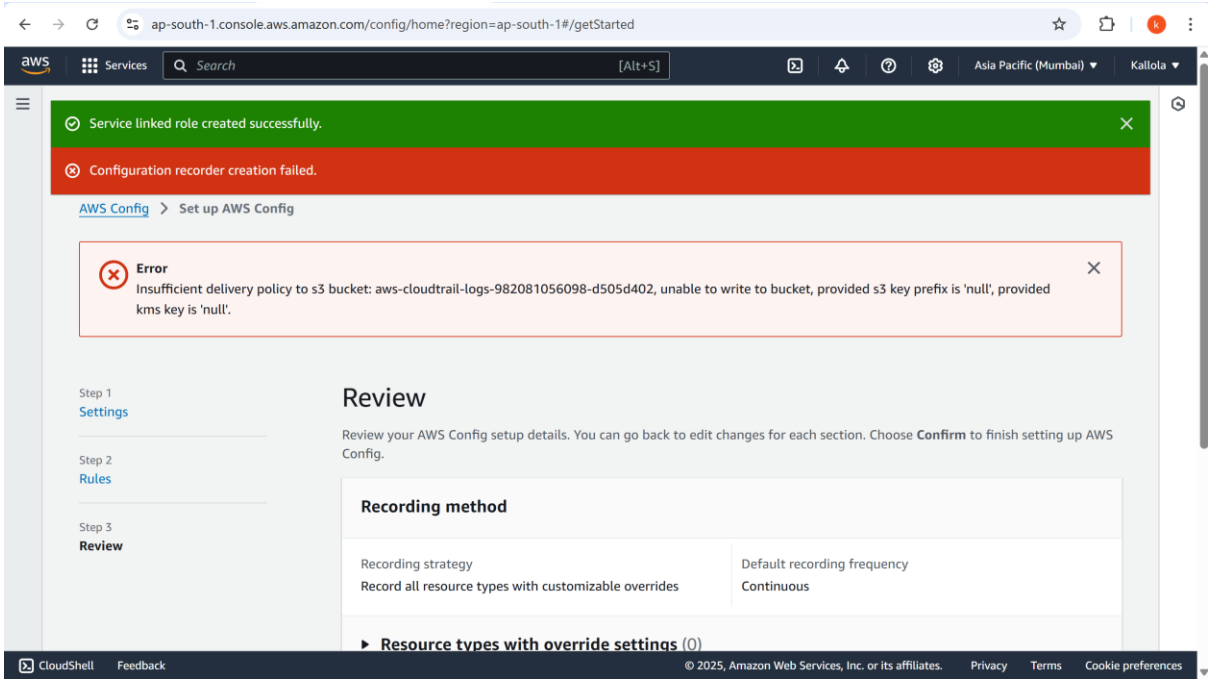

ap-south-1.console.aws.amazon.com/config/home?region=ap-south-1#/getStarted
aws
Services
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
AWS Config
Set up AWS Config
Step 1
Settings
Step 2
Rules
Step 3
Review
Settings
Recording method
Recording strategy
Customize AWS Config to record configuration changes for all supported resource types, or for only the supported resource types that are relevant to you. Global resource types (RDS global clusters and IAM users, groups, roles, and customer managed policies) might be recorded in more than this Region. Learn more You are charged based on the number of configuration items recorded. Pricing details
All resource types with customizable overrides
AWS Config will record all current and future supported resource types in this Region. You can override the recording frequency for specific resource types or exclude specific resource types from recording.
Specific resource types
AWS Config will only record the resource types that you specify.
Default settings
Recording frequency
Configure the default recording frequency for all current and future supported resource types. It impacts the cost to your bill. Pricing details
Continuous recording
Record configuration changes continuously whenever a change occurs.
Daily recording
Receive configuration data once every day only if a change has occurred.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


ap-south-1.console.aws.amazon.com/config/home?region=ap-south-1#/getStarted
Services
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
AWS Config > Set up AWS Config
Step 1
Settings
Step 2
Rules
Step 3
Review
Settings
Recording method
Recording strategy
Customize AWS Config to record configuration changes for all supported resource types, or for only the supported resource types that are relevant to you. Global resource types (RDS global clusters and IAM users, groups, roles, and customer managed policies) might be recorded in more than this Region. Learn more You are charged based on the number of configuration items recorded. Pricing details
All resource types with customizable overrides
AWS Config will record all current and future supported resource types in this Region. You can override the recording frequency for specific resource types or exclude specific resource types from recording.
Specific resource types
AWS Config will only record the resource types that you specify.
Default settings
Recording frequency
Configure the default recording frequency for all current and future supported resource types. It impacts the cost to your bill. Pricing details
Continuous recording
Record configuration changes continuously whenever a change occurs.
Daily recording
Receive configuration data once every day only if a change has occurred.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


ap-south-1.console.aws.amazon.com/config/home?region=ap-south-1#/getStarted
Services
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
Service-linked roles are predefined and include all the permissions that AWS Config requires to call other AWS services.
Choose an IAM role from one of your pre-existing roles and permission policies.
Delivery channel
Amazon S3 bucket
Create a bucket
Choose a bucket from your account
Choose a bucket from another account
Ensure appropriate permissions are available in this S3 bucket's policy. Learn more
S3 Bucket name (required)
aws-cloudtrail-logs-982081056098...
Prefix (optional)
/AWSLogs/982081056098/Config/ap-south-1
Amazon SNS topic
Stream configuration changes and notifications to an Amazon SNS topic.
If you choose email as the notification endpoint for your SNS topic, this can cause a high volume of email. Learn more
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

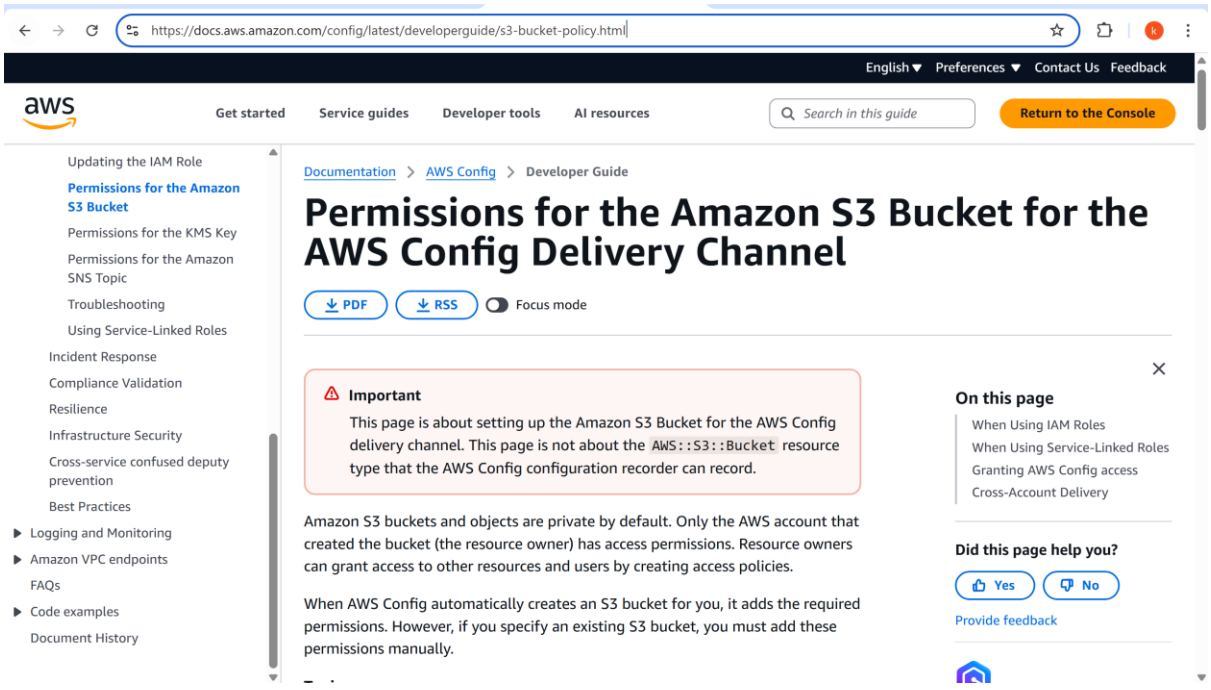

ap-south-1.console.aws.amazon.com/config/home?region=ap-south-1#/getStarted
Services
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
AWS Config > Set up AWS Config
Step 1
Settings
Step 2
Rules
Step 3
Review
Rules
AWS Managed Rules (143)
Find Rules
1 2 3 4 5 6 7 ... 15
Name
Resource types
Trigger type
Description
account-part-of-organizations
PERIODIC
Rule checks whether AWS account is part of AWS Organization
rule is NON_COMPLIANT if the AWS account is not part of AWS
Organizations or AWS Organizations master account ID does n
match rule parameter MasterAccountId.
acm-certificate-expiration-check
AWS::ACM::Certificate
HYBRID
Checks whether ACM Certificates in your account are marked fo
expiration within the specified number of days. Certificates pro
by ACM are automatically renewed. ACM does not automaticall
renew certificates that you import.
alb-http-drop-invalid-
AWS::ElasticLoadBalancingV2::Load
CHANGE-TRIGGERED
Checks if rule evaluates AWS Application Load Balancers (ALB)
ensure they are configured to drop http headers. The rule is
NON_COMPLIANT if the value of
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

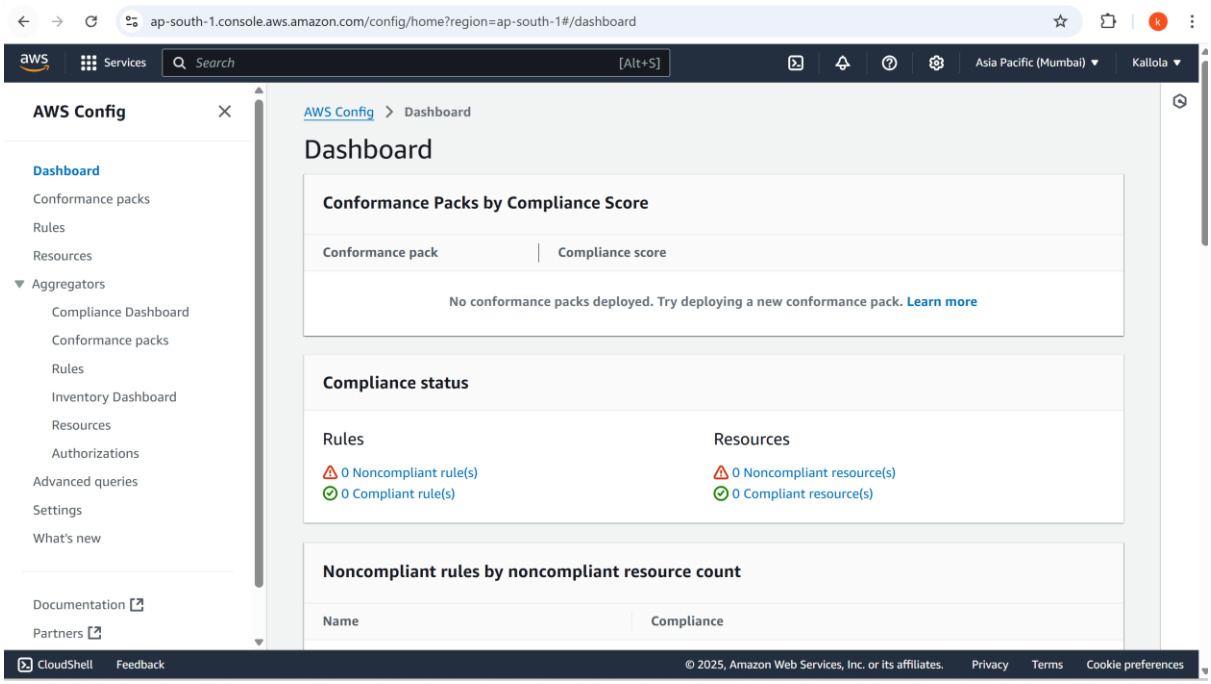

ap-south-1.console.aws.amazon.com/config/home?region=ap-south-1#/getStarted
Services
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
AWS Config > Set up AWS Config
Step 1
Settings
Step 2
Rules
Step 3
Review
Review
Review your AWS Config setup details. You can go back to edit changes for each section. Choose Confirm to finish setting up AWS Config.
Recording method
Recording strategy
Record all resource types with customizable overrides
Default recording frequency
Continuous
Resource types with override settings (0)
Resource types with default settings (371)
Delivery method
S3 bucket name
aws-cloudtrail-logs-982081056098-d505d402
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Checked & found that there is no delivery channel available, implemented the following help document & issue is fixed.

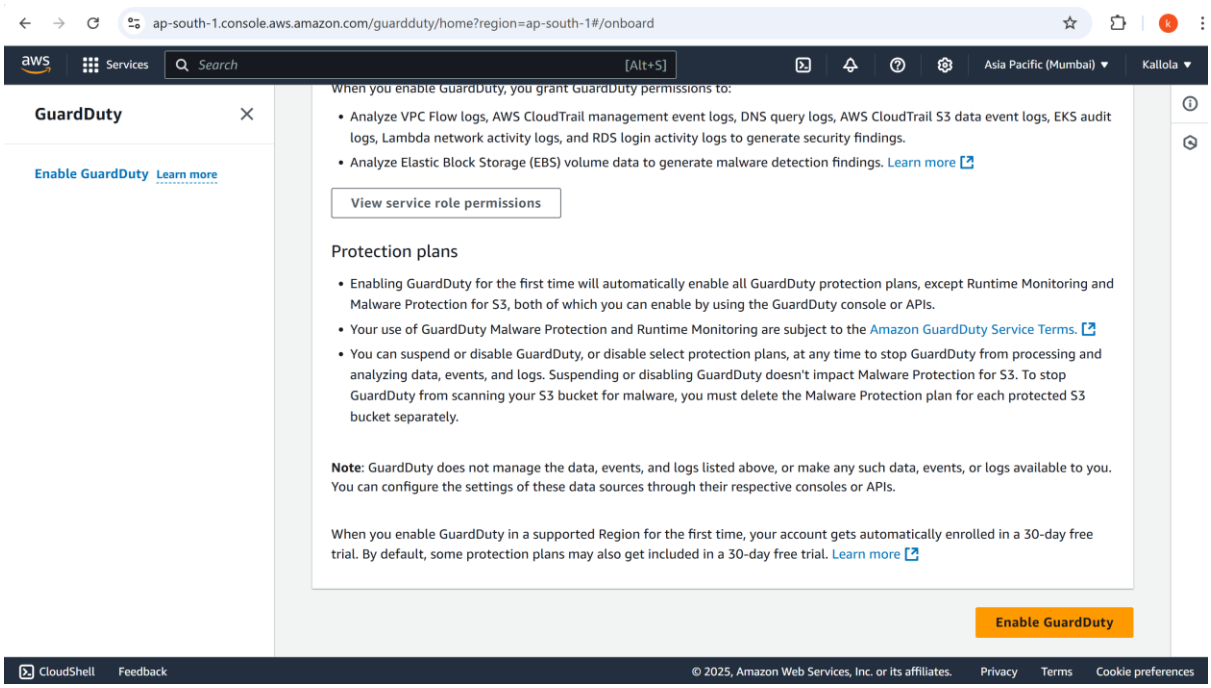
https://docs.aws.amazon.com/config/latest/developerguide/s3-bucket-policy.html

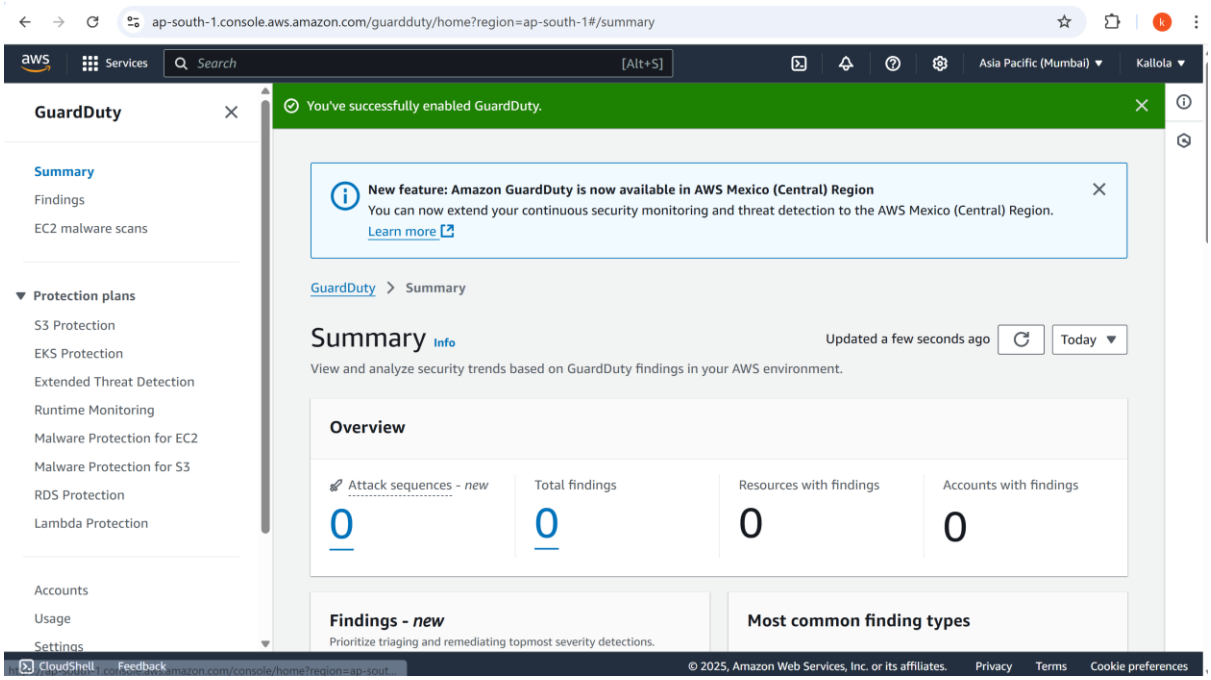




✅ Enable GuardDuty

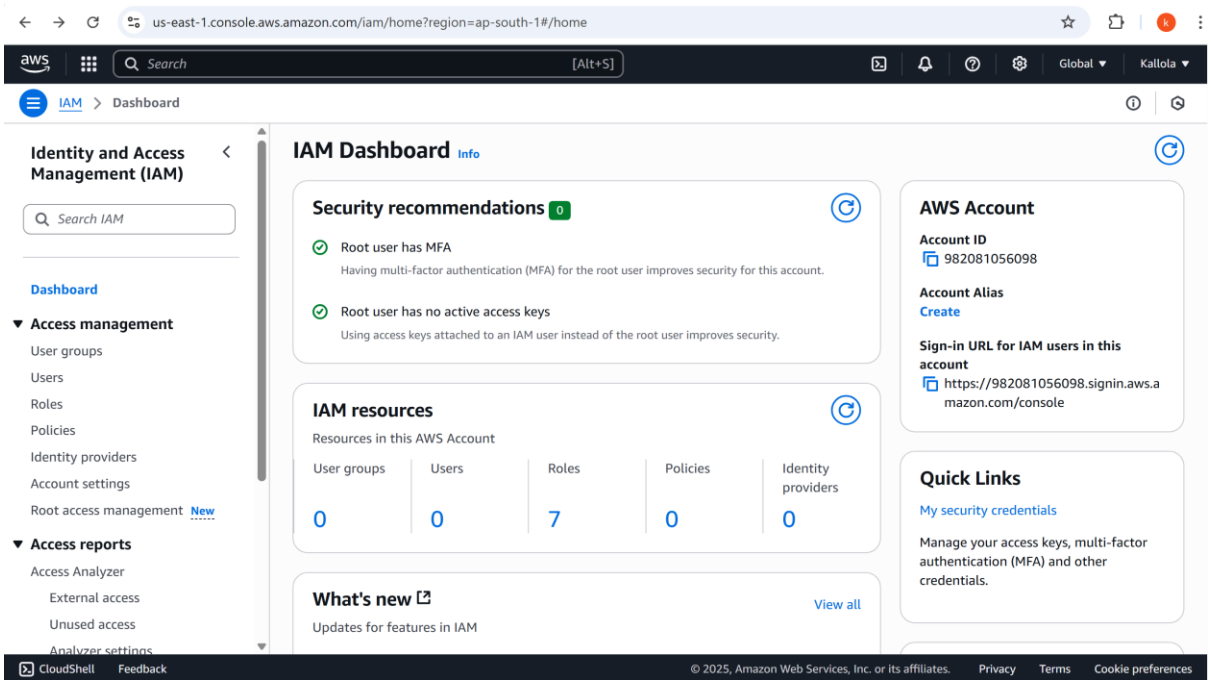
- Go to GuardDuty → Enable
- No extra config needed initially

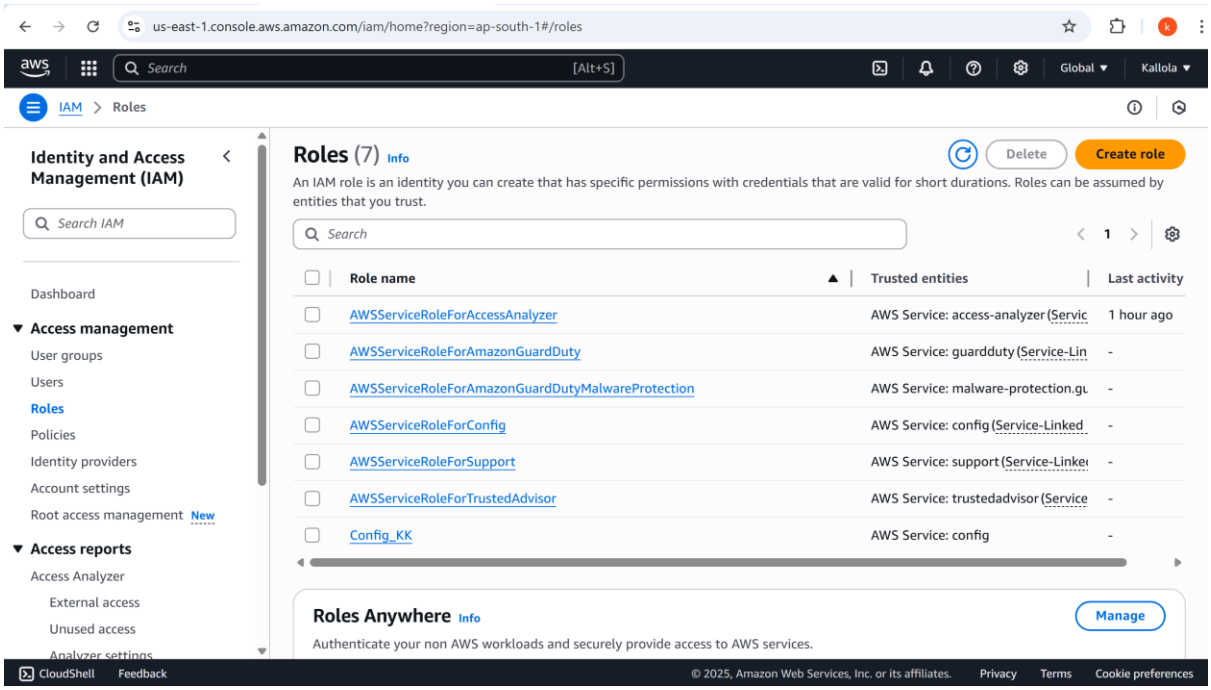


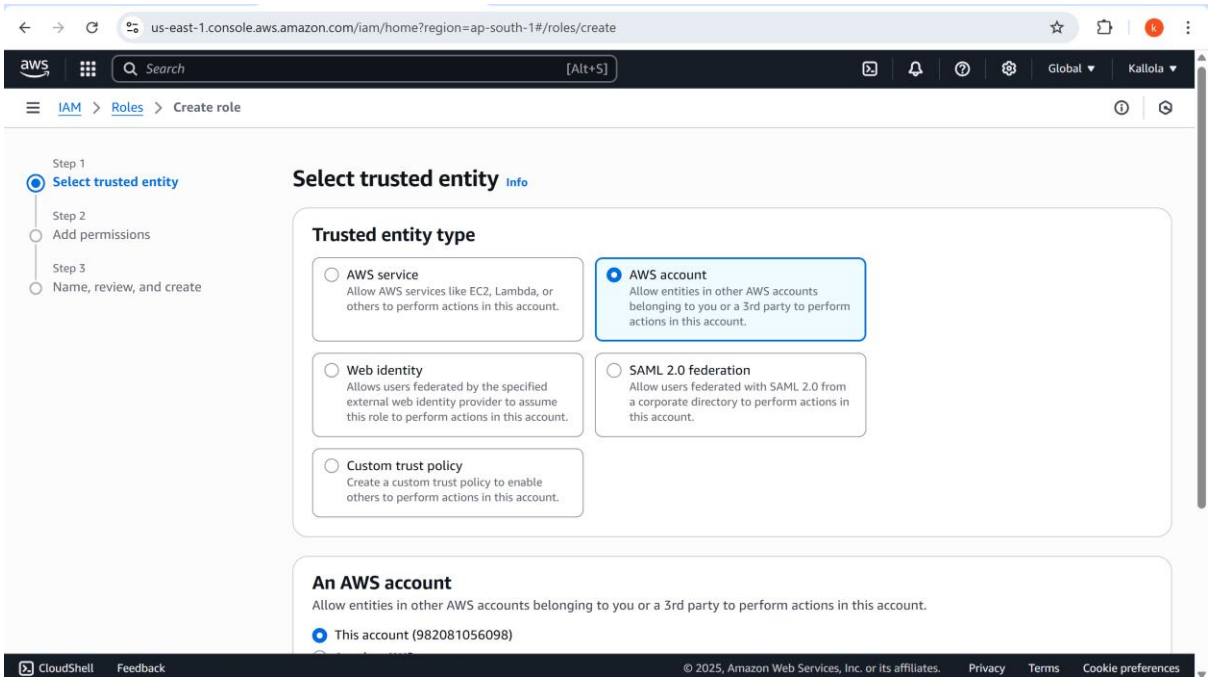


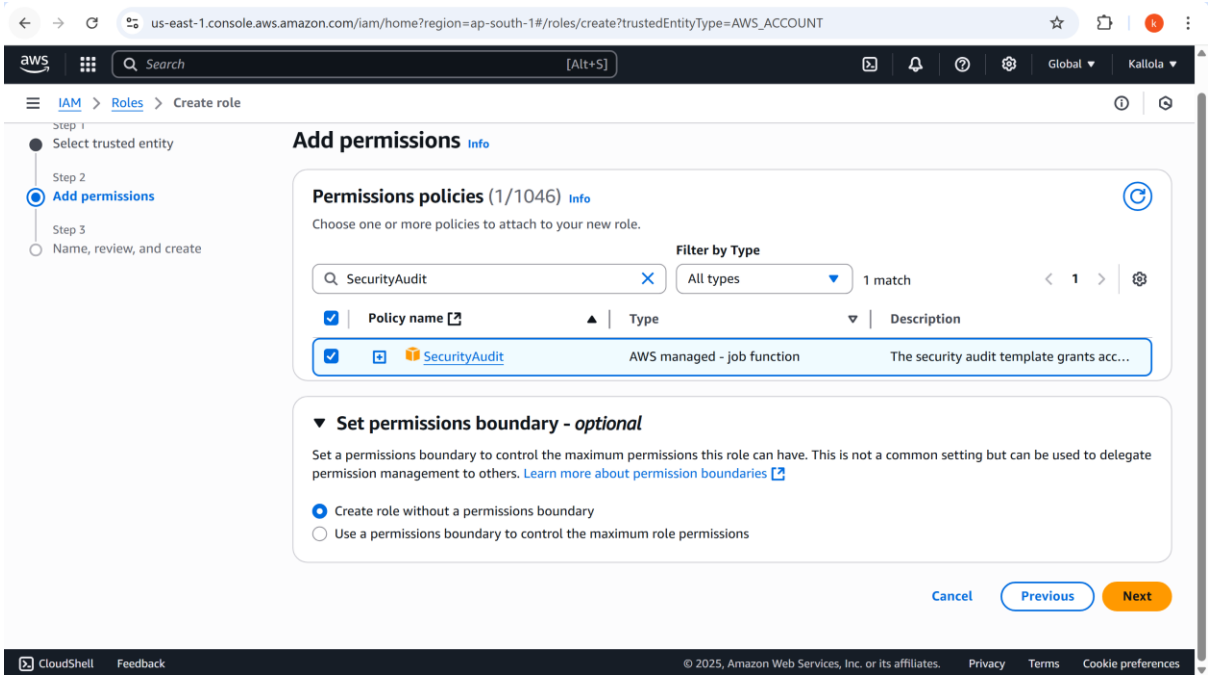
✅ IAM Setup

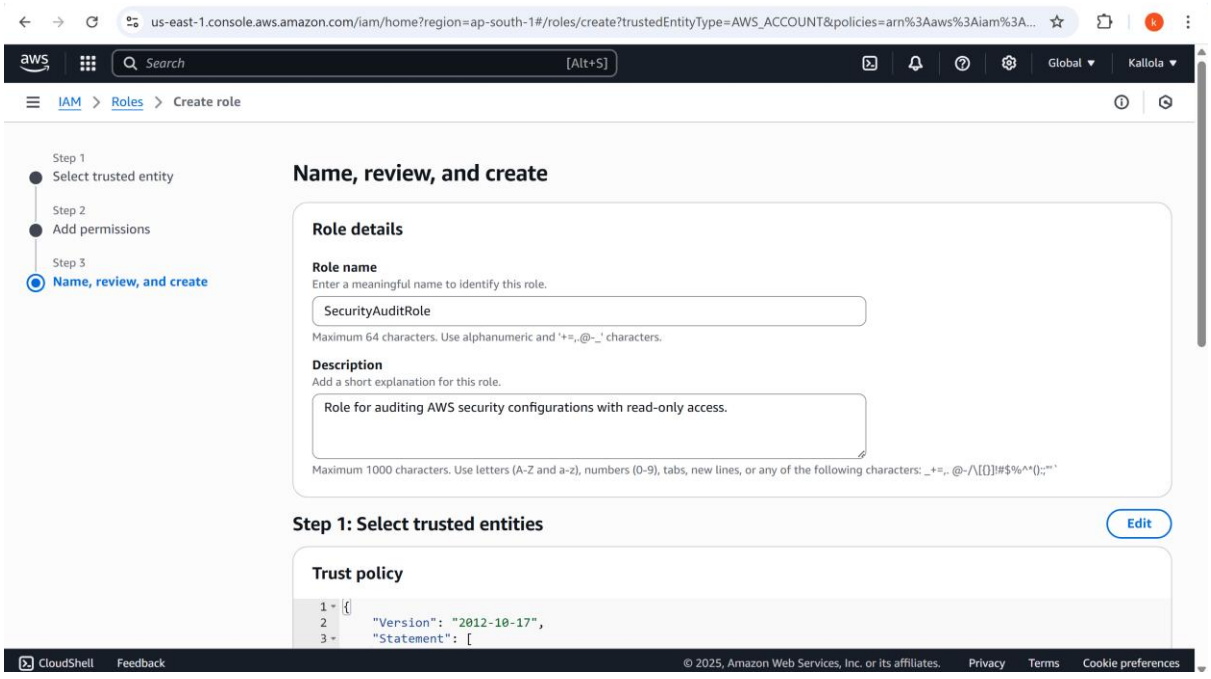
- Create an IAM Role "SecurityAuditRole" (optional) if you want cleaner permissions

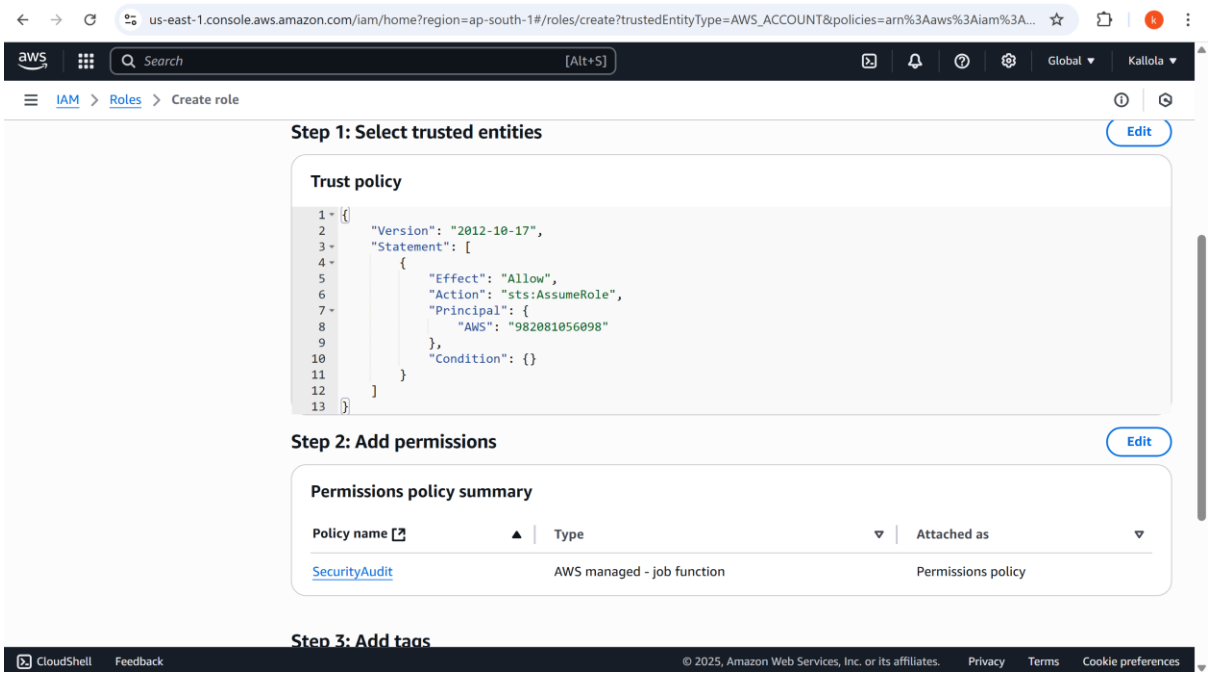


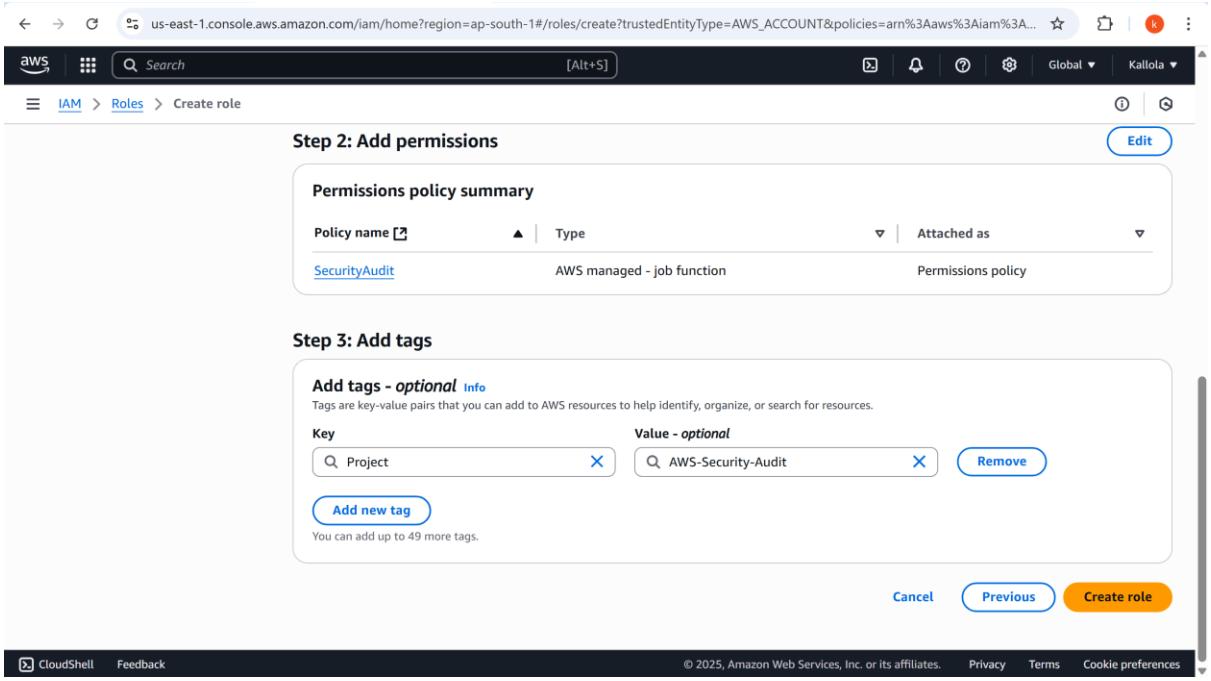

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles
Search
[Alt+S]
Global
Kallola
IAM > Roles
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Roles (7) Info
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Delete
Create role
Search
Role name
Trusted entities
Last activity
AWSServiceRoleForAccessAnalyzer
AWS Service: access-analyzer (Servic
1 hour ago
AWSServiceRoleForAmazonGuardDuty
AWS Service: guardduty (Service-Lin
AWSServiceRoleForAmazonGuardDutyMalwareProtection
AWS Service: malware-protection.gu
AWSServiceRoleForConfig
AWS Service: config (Service-Linked
AWSServiceRoleForSupport
AWS Service: support (Service-Linke
AWSServiceRoleForTrustedAdvisor
AWS Service: trustedadvisor (Service
Config_KK
AWS Service: config
Roles Anywhere Info
Authenticate your non AWS workloads and securely provide access to AWS services.
Manage
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

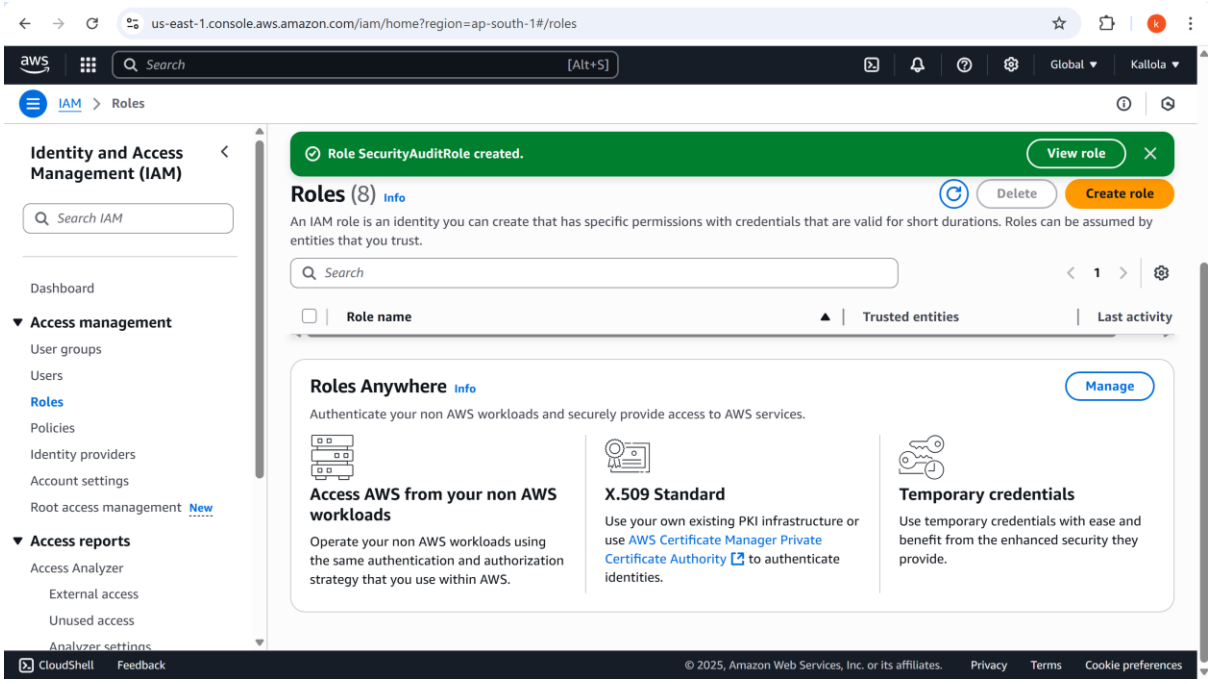

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create
Search
[Alt+S]
Global
Kallola
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Select trusted entity Info
Trusted entity type
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
An AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
This account (982081056098)
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

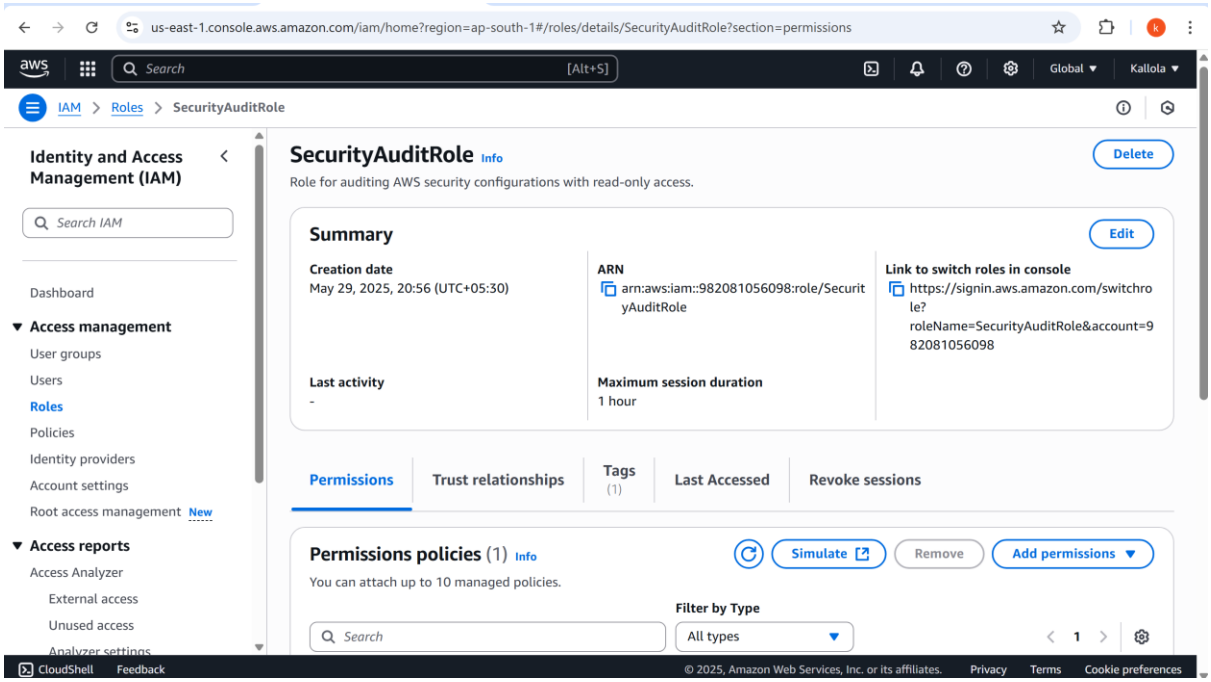

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create?trustedEntityType=AWS_ACCOUNT
Search
[Alt+S]
Global
Kallola
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Add permissions Info
Permissions policies (1/1046) Info
Choose one or more policies to attach to your new role.
Filter by Type
SecurityAudit
All types
1 match
1
Policy name
Type
Description
SecurityAudit
AWS managed - job function
The security audit template grants acc...
Set permissions boundary - optional
Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting but can be used to delegate permission management to others. Learn more about permission boundaries
Create role without a permissions boundary
Use a permissions boundary to control the maximum role permissions
Cancel
Previous
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create?trustedEntityType=AWS_ACCOUNT&policies=arn%3Aaws%3Aiam%3A...
Search
[Alt+S]
Global
Kallola
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
SecurityAuditRole
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Role for auditing AWS security configurations with read-only access.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/\[{}]!#$%^*();:"'`
Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
"Statement": [
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

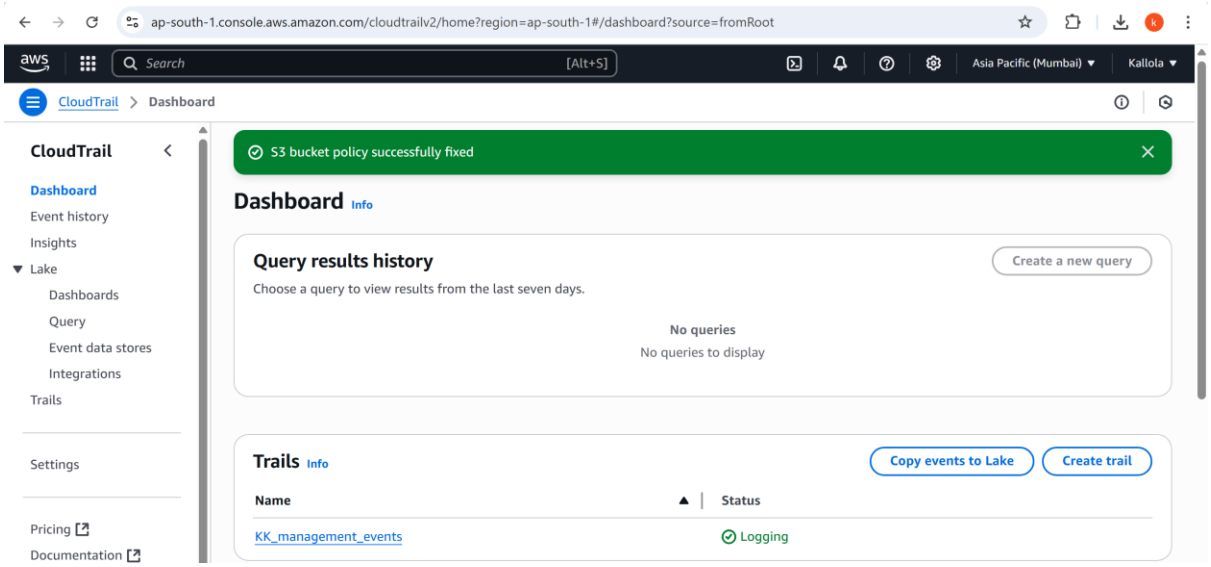

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create?trustedEntityType=AWS_ACCOUNT&policies=arn%3Aaws%3Aiam%3A...
Search
[Alt+S]
Global
Kallola
IAM
Roles
Create role
Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": "sts:AssumeRole",
"Principal": {
"AWS": "982081056098"
},
"Condition": {}
}
]
}
Step 2: Add permissions
Edit
Permissions policy summary
Policy name
Type
Attached as
SecurityAudit
AWS managed - job function
Permissions policy
Step 3: Add tags
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

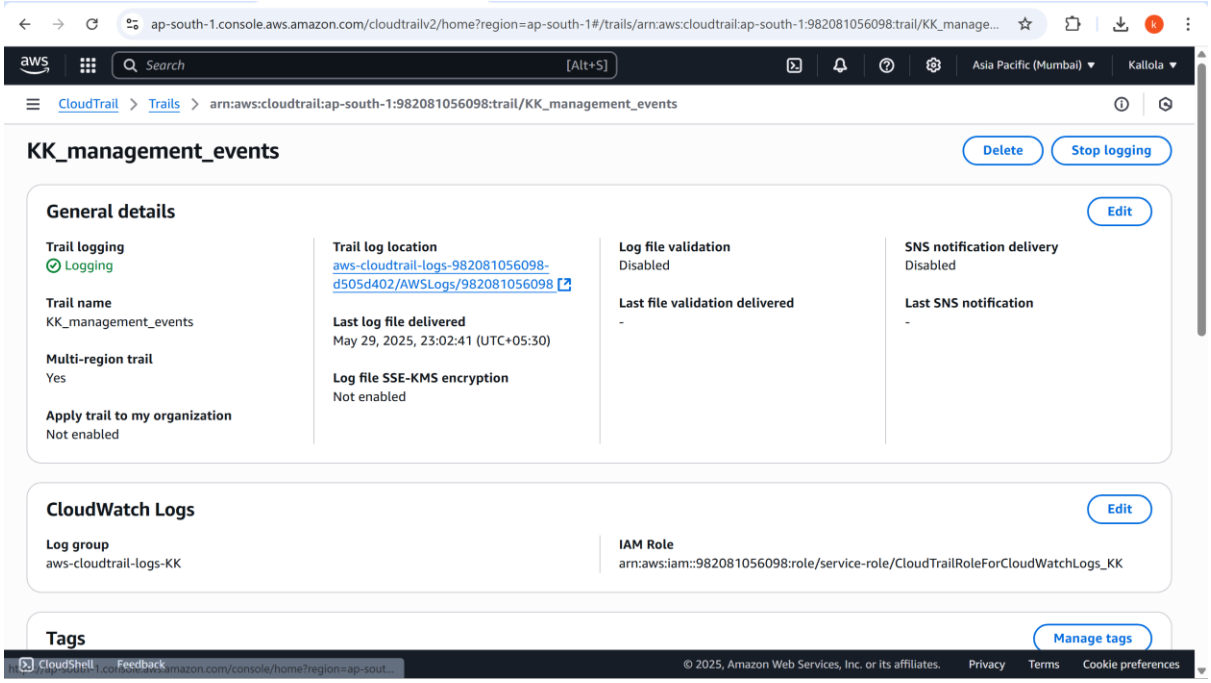

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create?trustedEntityType=AWS_ACCOUNT&policies=arn%3Aaws%3Aiam%3A...
Search
[Alt+S]
Global
Kallola
IAM
Roles
Create role
Step 2: Add permissions
Edit
Permissions policy summary
Policy name
Type
Attached as
SecurityAudit
AWS managed - job function
Permissions policy
Step 3: Add tags
Add tags - optional
Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.
Key
Value - optional
Project
AWS-Security-Audit
Remove
Add new tag
You can add up to 49 more tags.
Cancel
Previous
Create role
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



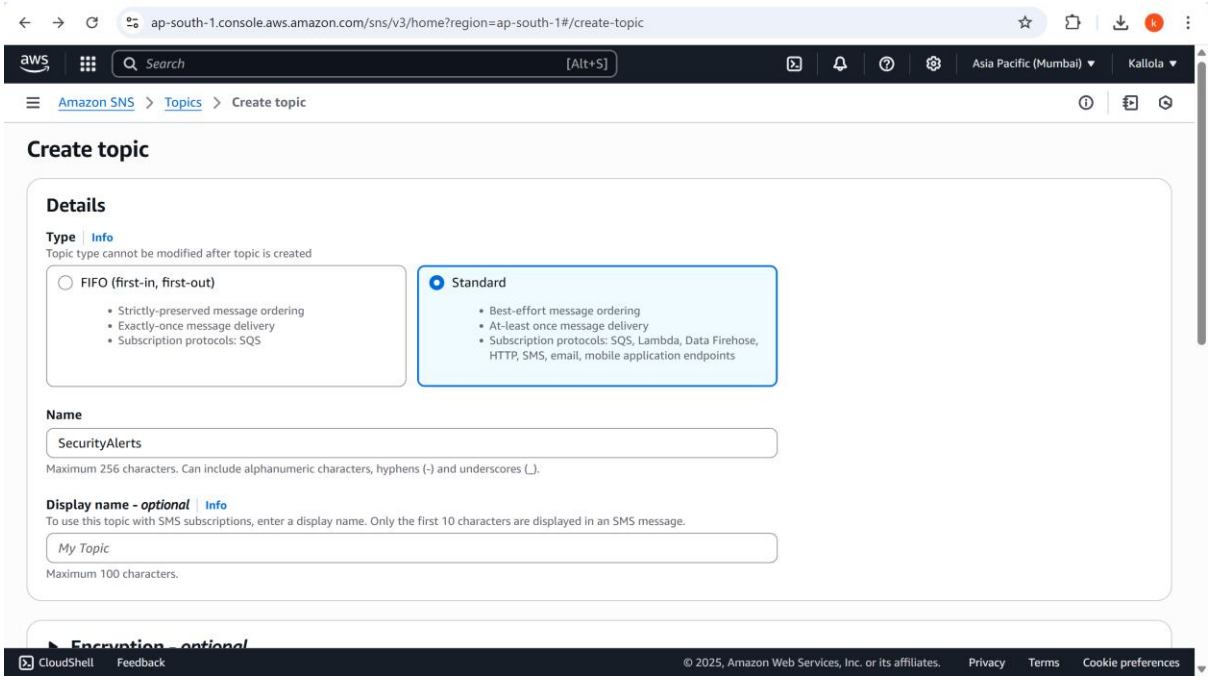


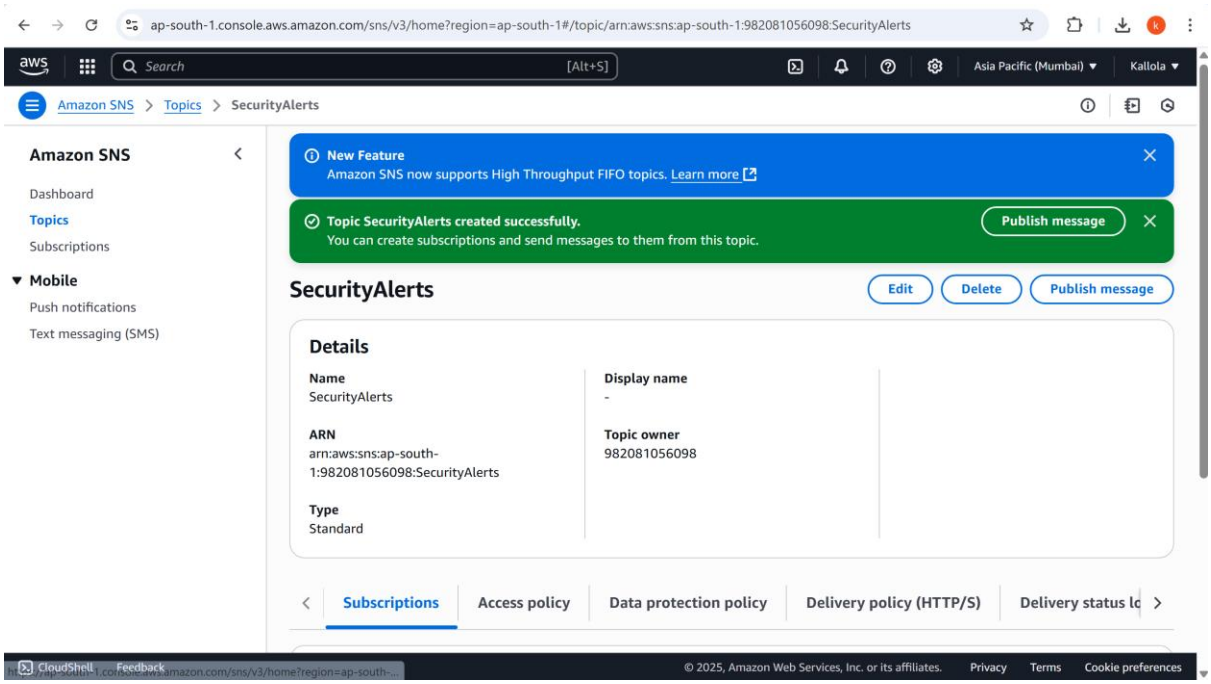
Enable CloudWatch Logs



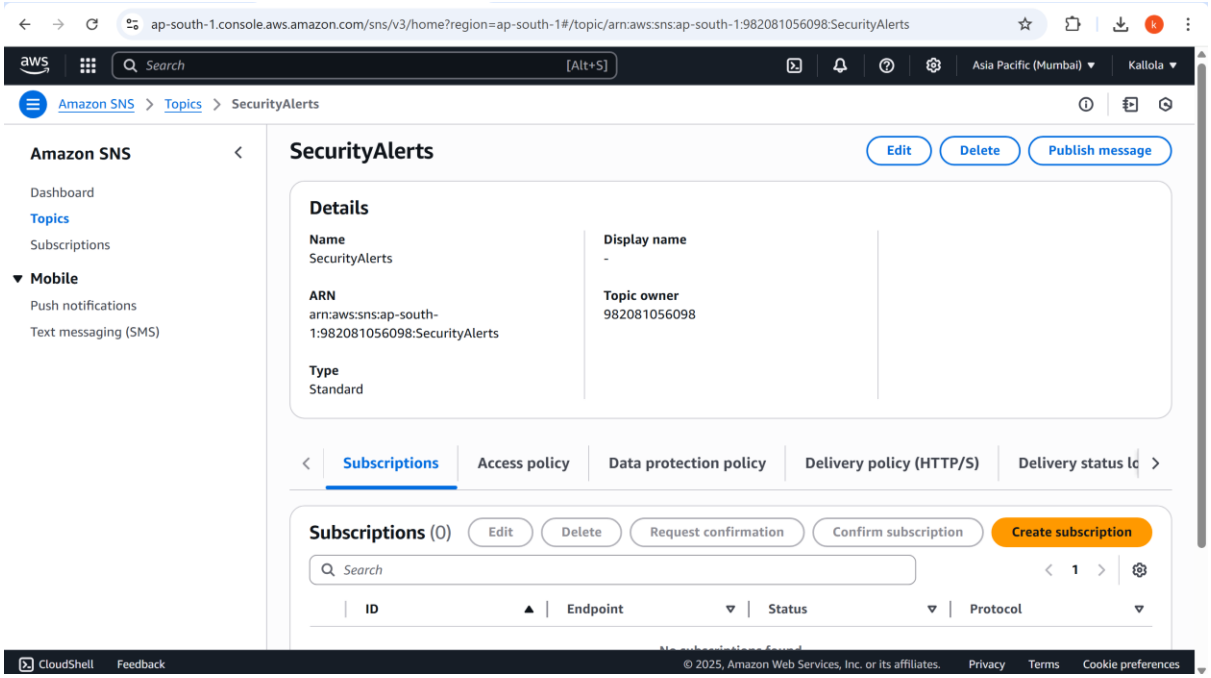


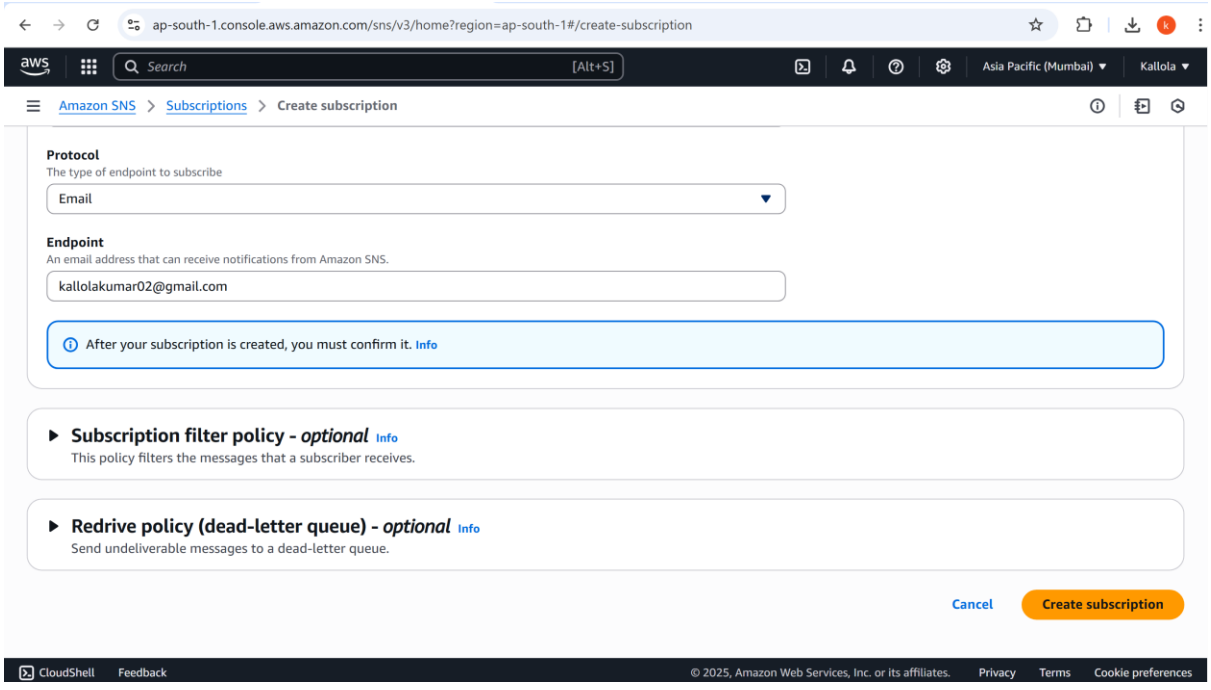
Create an SNS Topic for Alerts

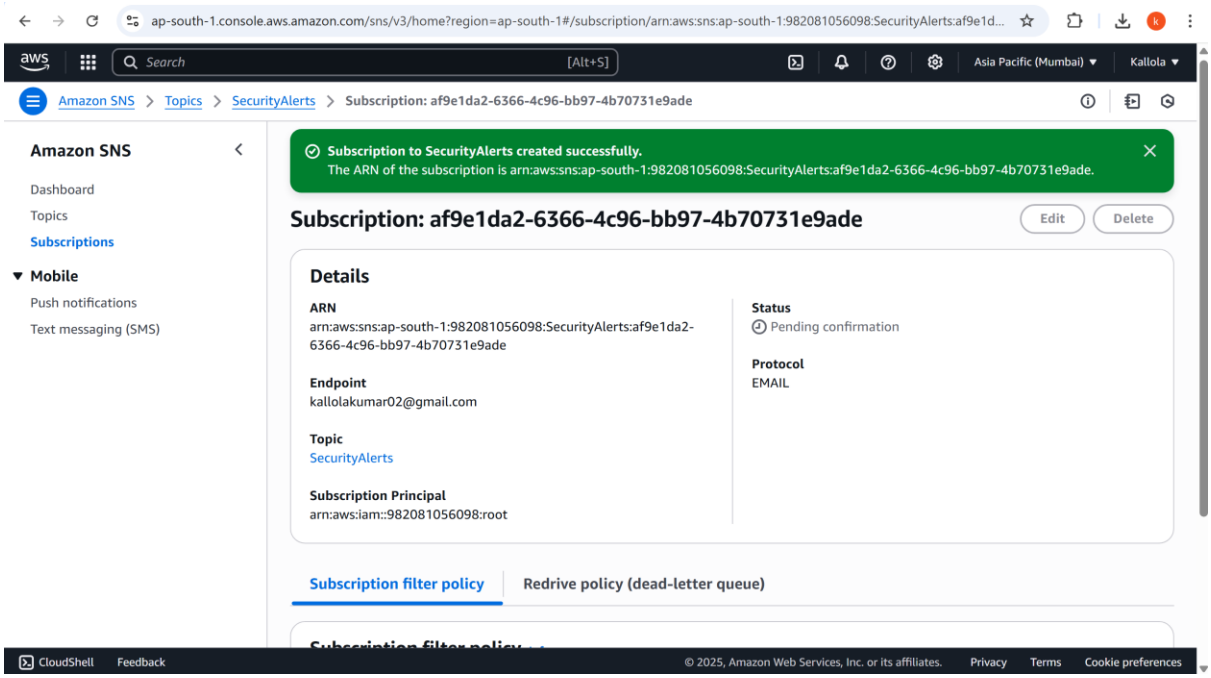


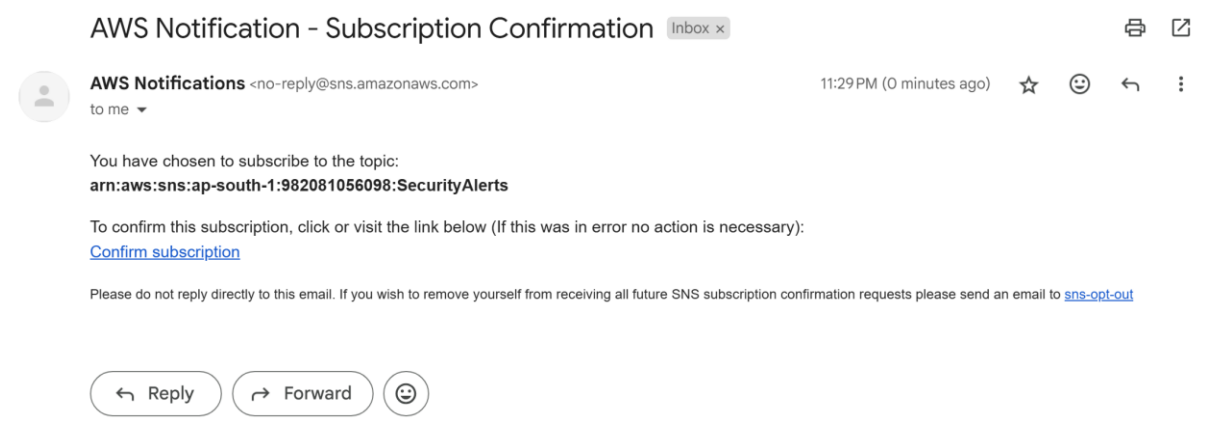


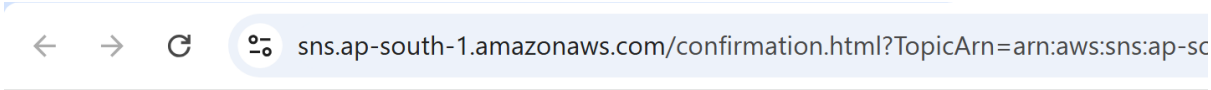
Now create subscription too


ap-south-1.console.aws.amazon.com/sns/v3/home?region=ap-south-1#/topic/arn:aws:sns:ap-south-1:982081056098:SecurityAlerts
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
Amazon SNS > Topics > SecurityAlerts
Amazon SNS
Dashboard
Topics
Subscriptions
Mobile
Push notifications
Text messaging (SMS)
SecurityAlerts
Edit
Delete
Publish message
Details
Name
SecurityAlerts
Display name
-
ARN
arn:aws:sns:ap-south-1:982081056098:SecurityAlerts
Topic owner
982081056098
Type
Standard
Subscriptions
Access policy
Data protection policy
Delivery policy (HTTP/S)
Delivery status lo
Subscriptions (0)
Edit
Delete
Request confirmation
Confirm subscription
Create subscription
Search
ID
Endpoint
Status
Protocol
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


ap-south-1.console.aws.amazon.com/sns/v3/home?region=ap-south-1#/create-subscription
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
Amazon SNS > Subscriptions > Create subscription
Protocol
The type of endpoint to subscribe
Email
Endpoint
An email address that can receive notifications from Amazon SNS.
kallolakumar02@gmail.com
After your subscription is created, you must confirm it. Info
Subscription filter policy - optional Info
This policy filters the messages that a subscriber receives.
Redrive policy (dead-letter queue) - optional Info
Send undeliverable messages to a dead-letter queue.
Cancel
Create subscription
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences







aws

Simple Notification Service

Subscription confirmed!

You have successfully subscribed.

Your subscription's id is:
`arn:aws:sns:ap-south-1:982081056098:SecurityAlerts:af9e1da2-6366-4c96-bb97-4b70731e9ade`

If it was not your intention to subscribe, click here to unsubscribe.

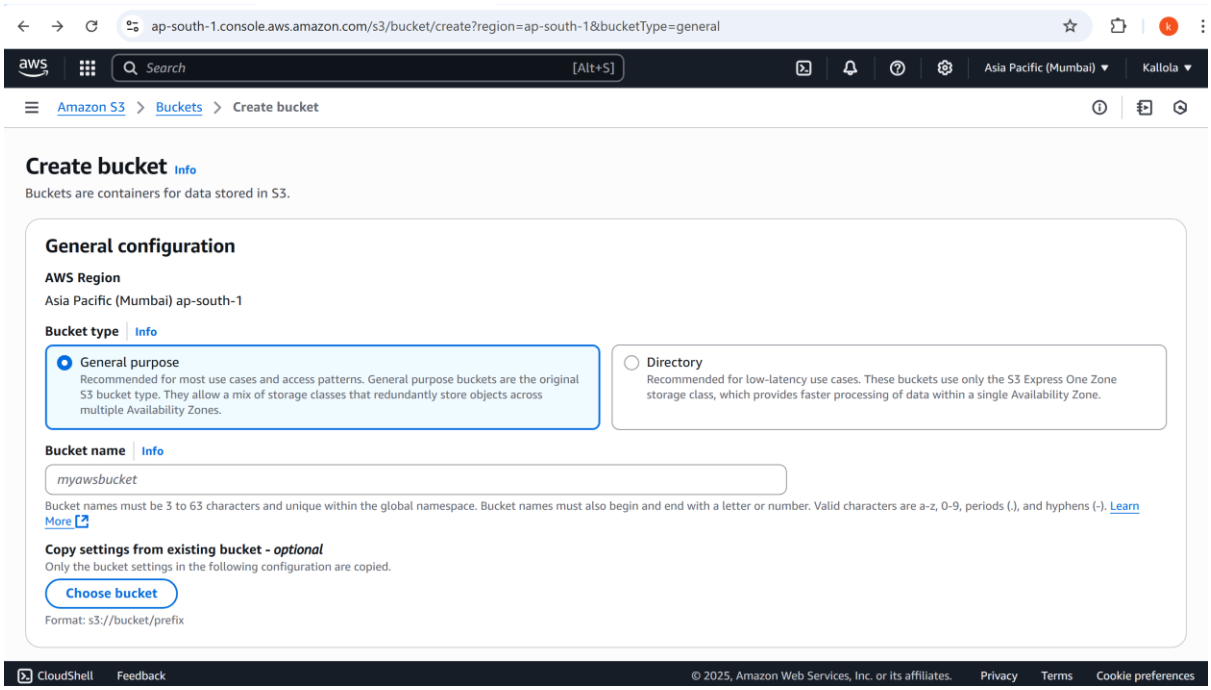
Phase 2 – Create a Simulated Attack & Response Pipeline

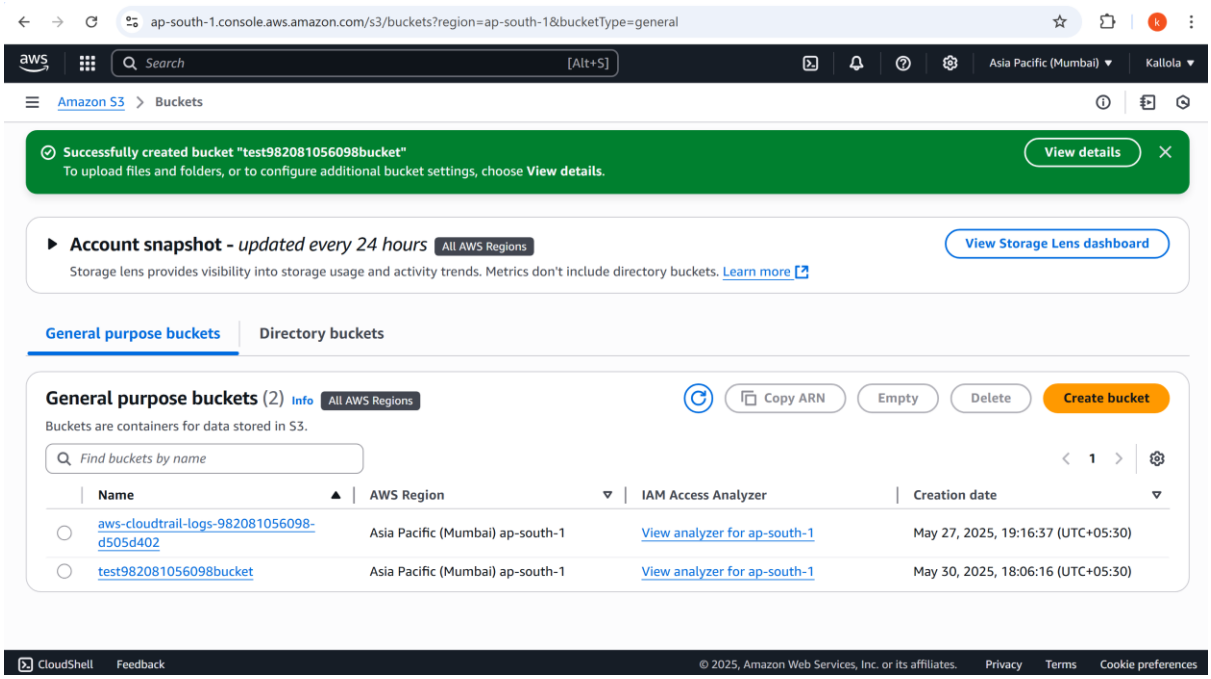
Public S3 Bucket Access

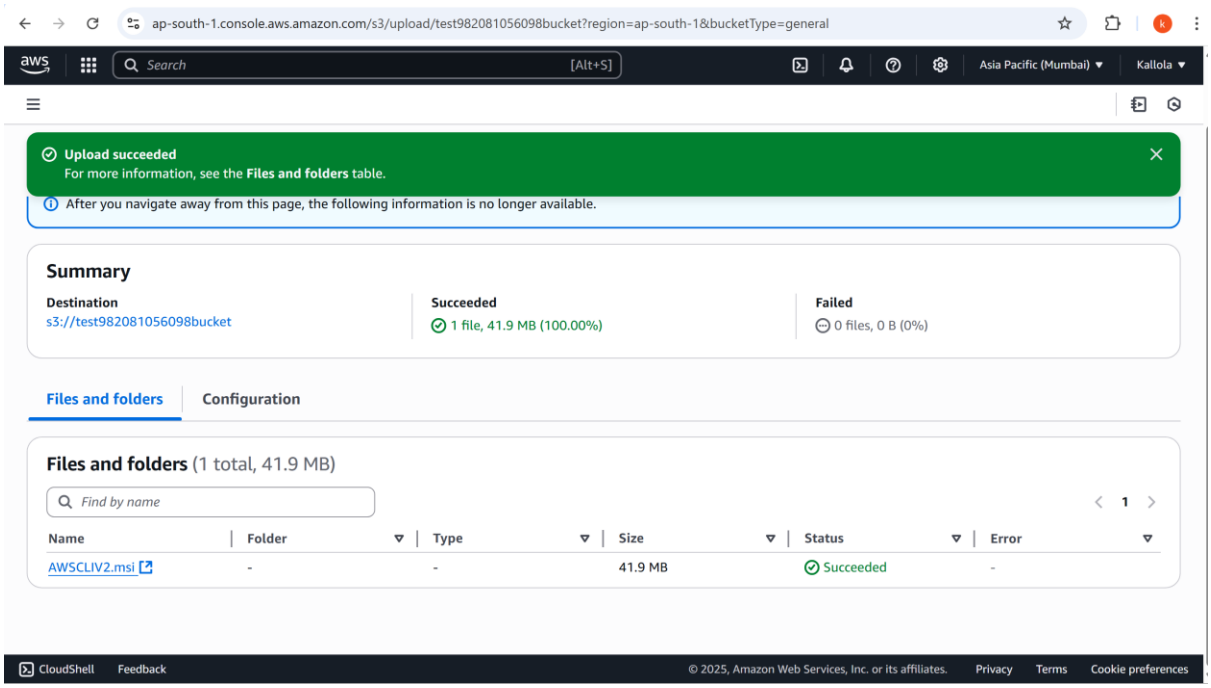
1. Create an S3 bucket and upload a dummy file.
2. Modify bucket policy to make it public.
3. Try accessing the file from a public browser.

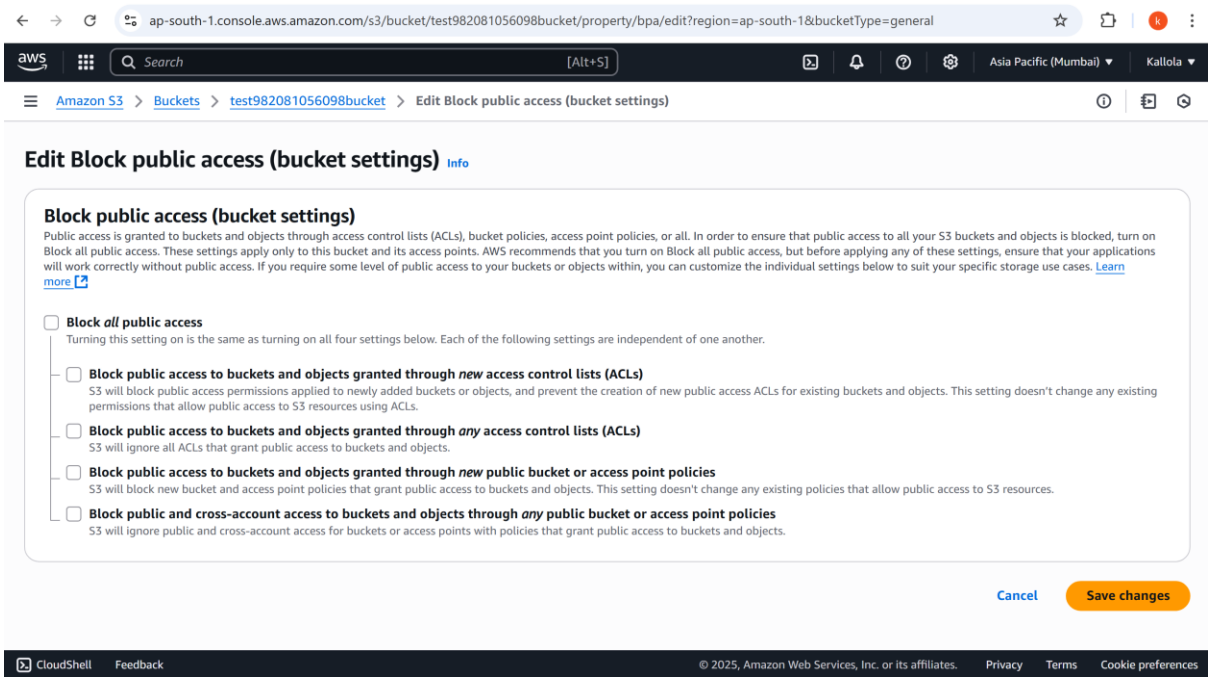
📌 Expected Alerts:

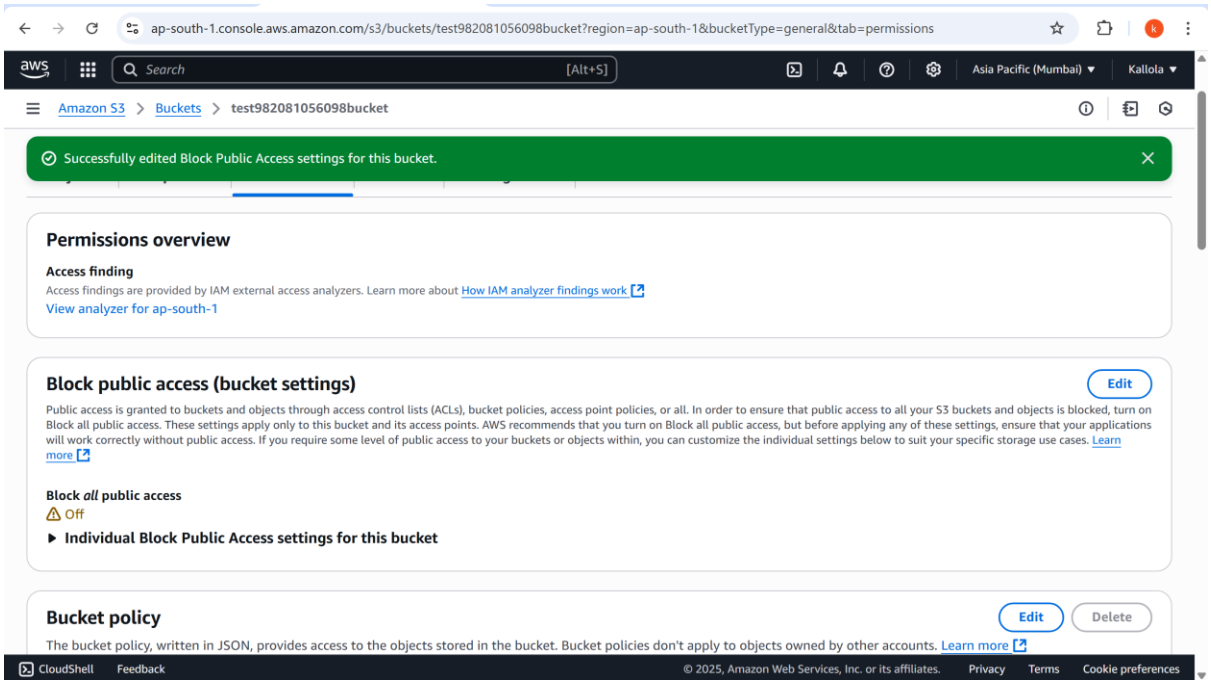
- AWS Config detects non-compliant S3 bucket policy
- GuardDuty may raise Policy:S3/BucketPublicReadAcl or S3/BucketPublicRead

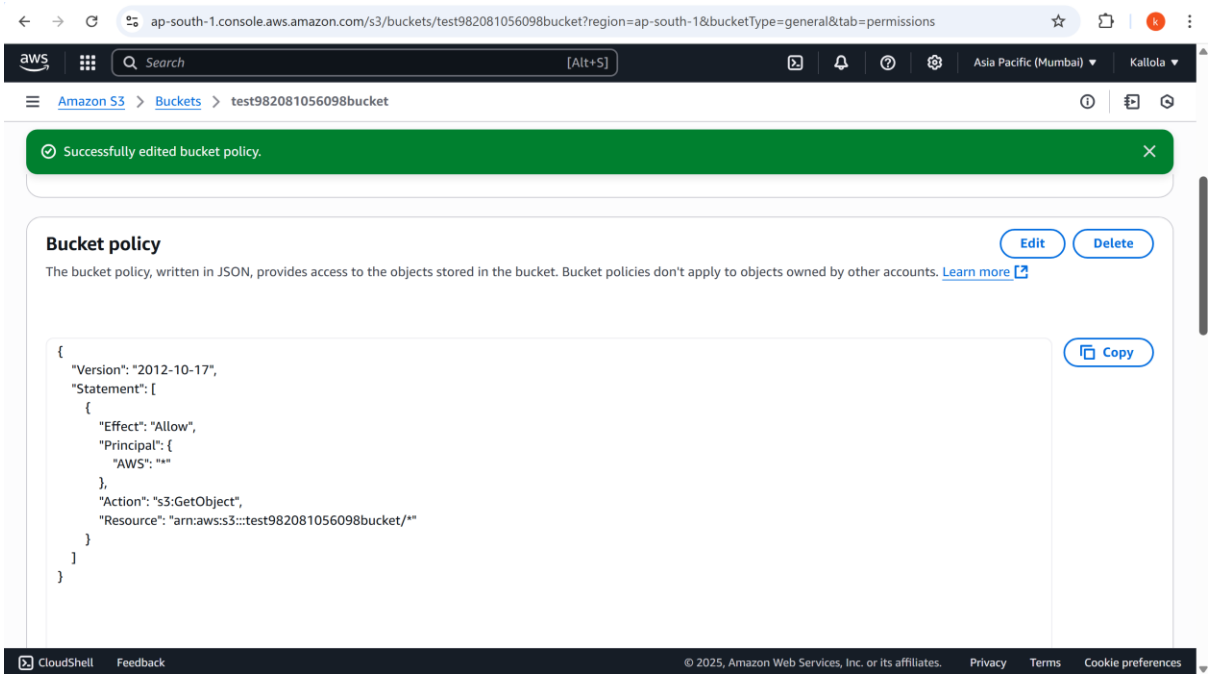


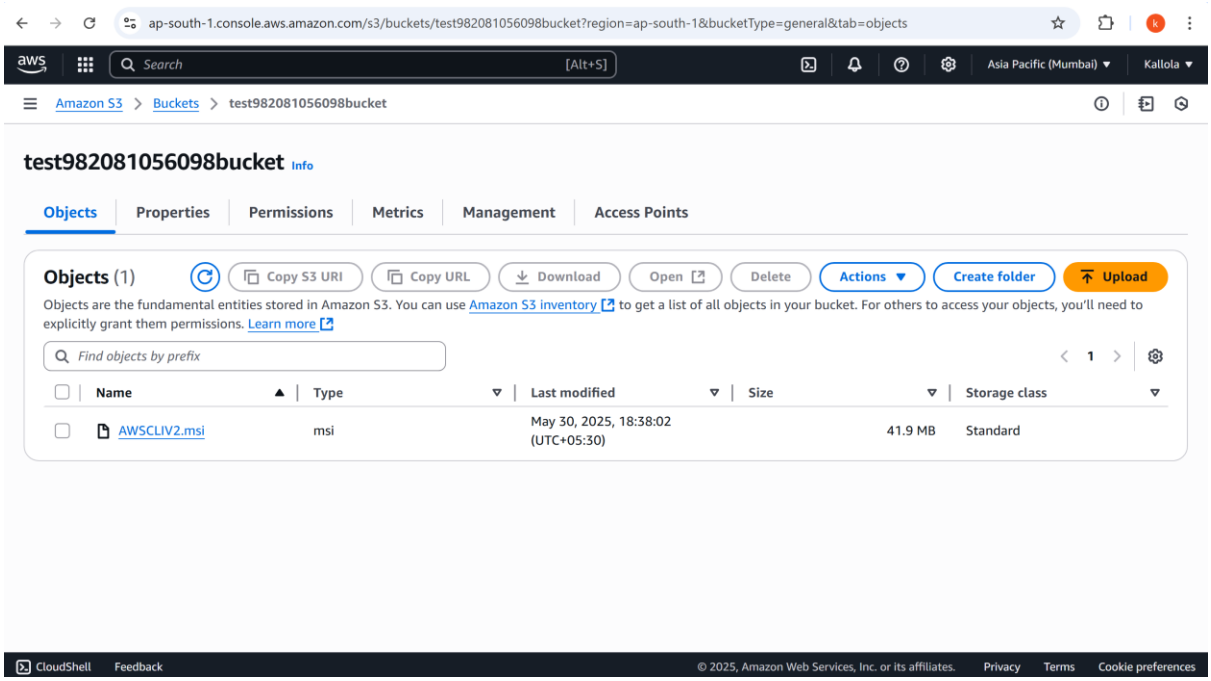

ap-south-1.console.aws.amazon.com/s3/buckets?region=ap-south-1&bucketType=general
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
Amazon S3 > Buckets
Successfully created bucket "test982081056098bucket"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (2) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
aws-cloudtrail-logs-982081056098-d505d402
Asia Pacific (Mumbai) ap-south-1
View analyzer for ap-south-1
May 27, 2025, 19:16:37 (UTC+05:30)
test982081056098bucket
Asia Pacific (Mumbai) ap-south-1
View analyzer for ap-south-1
May 30, 2025, 18:06:16 (UTC+05:30)
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


ap-south-1.console.aws.amazon.com/s3/upload/test982081056098bucket?region=ap-south-1&bucketType=general
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
Upload succeeded
For more information, see the Files and folders table.
After you navigate away from this page, the following information is no longer available.
Summary
Destination
s3://test982081056098bucket
Succeeded
1 file, 41.9 MB (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 total, 41.9 MB)
Find by name
Name
Folder
Type
Size
Status
Error
AWSCLIV2.msi
-
-
41.9 MB
Succeeded
-
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


ap-south-1.console.aws.amazon.com/s3/bucket/test982081056098bucket/property/bpa/edit?region=ap-south-1&bucketType=general
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
Amazon S3 > Buckets > test982081056098bucket > Edit Block public access (bucket settings)
Edit Block public access (bucket settings) Info
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
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

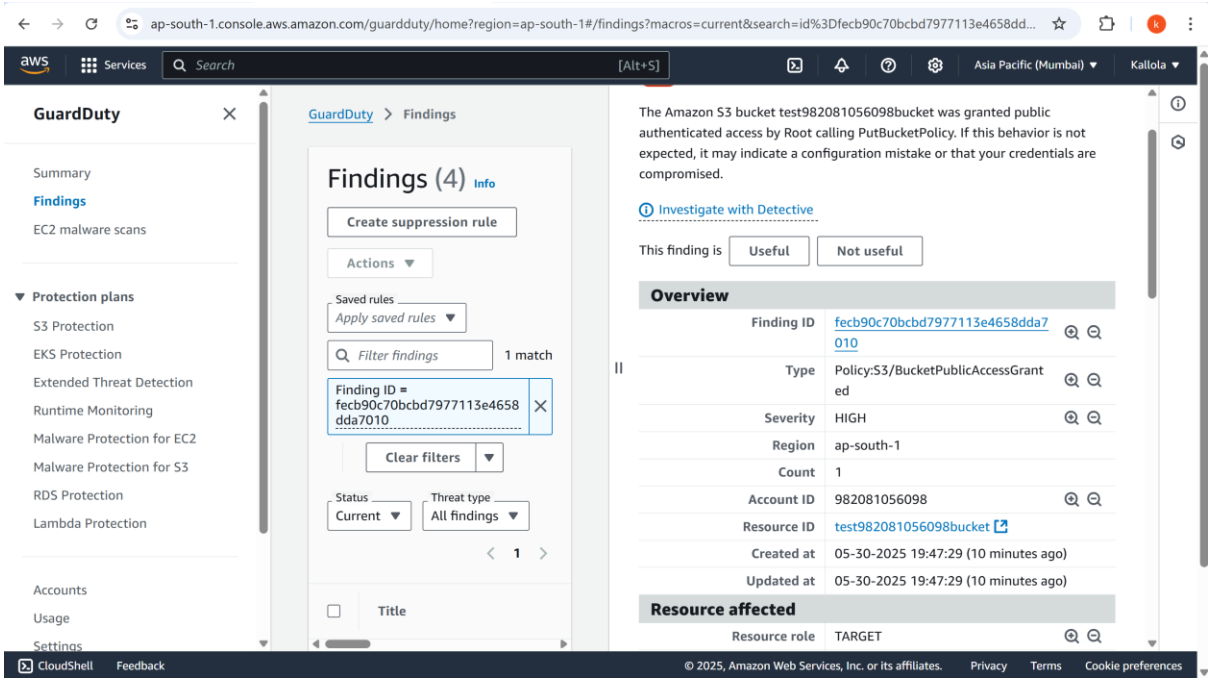

ap-south-1.console.aws.amazon.com/s3/buckets/test982081056098bucket?region=ap-south-1&bucketType=general&tab=permissions
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
Amazon S3 > Buckets > test982081056098bucket
Successfully edited Block Public Access settings for this bucket.
Permissions overview
Access finding
Access findings are provided by IAM external access analyzers. Learn more about How IAM analyzer findings work
View analyzer for ap-south-1
Block public access (bucket settings)
Edit
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
Edit
Delete
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
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

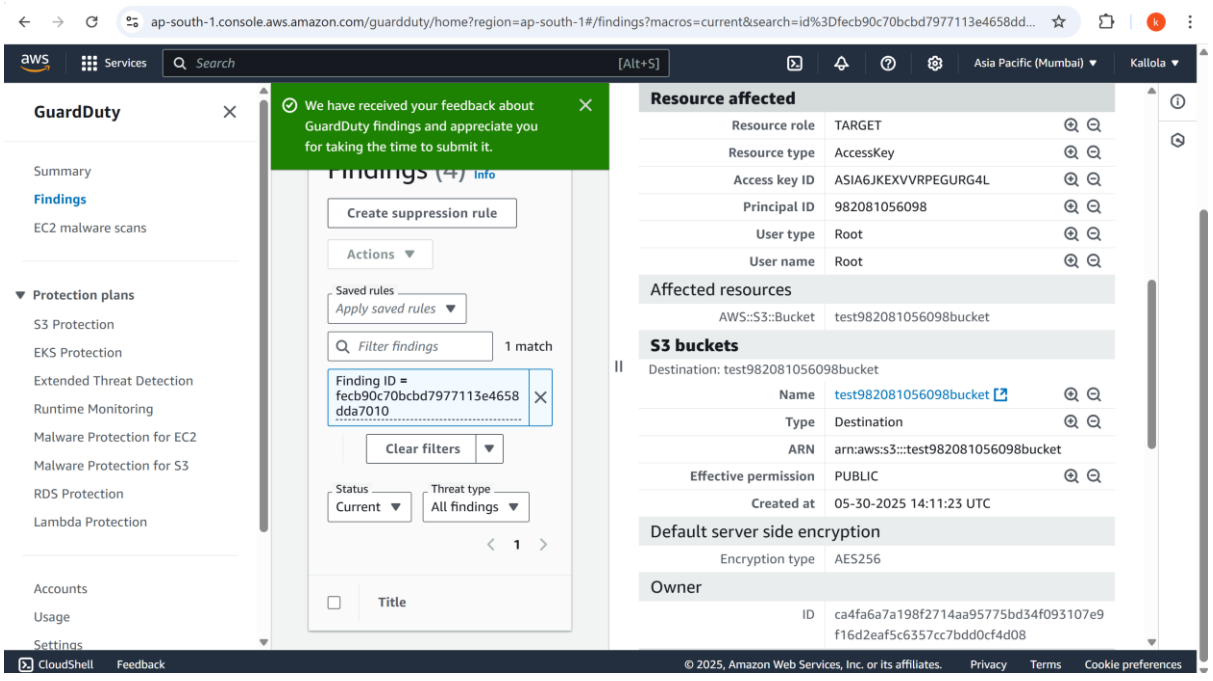




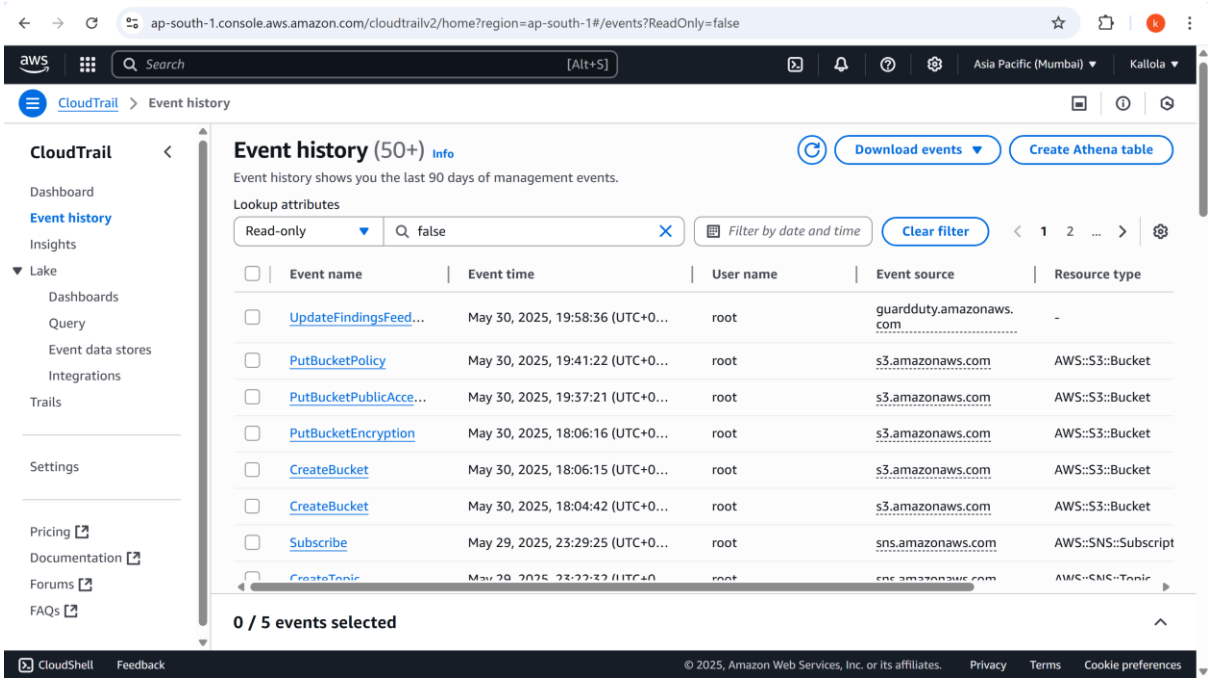
The s3 public access enabled.

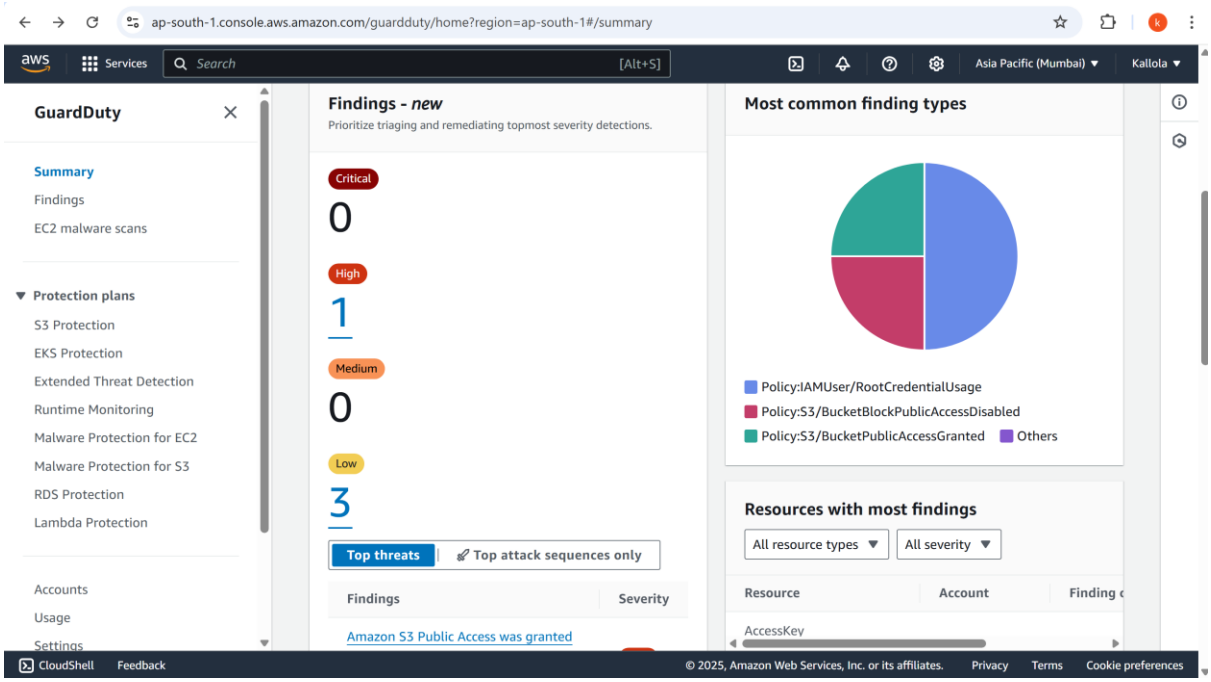
It’s detected by Guard duty with severity level HIGH.

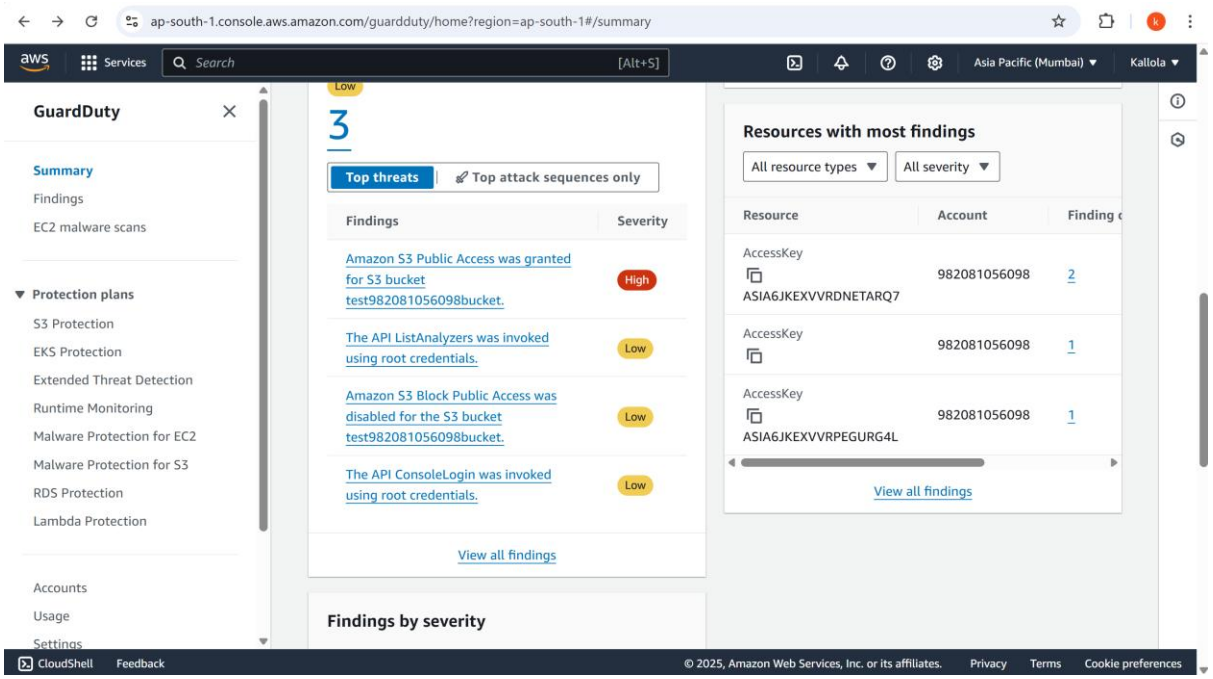

ap-south-1.console.aws.amazon.com/guardduty/home?region=ap-south-1#/findings?macros=current&search=id%3Dfecb90c70bcbd7977113e4658dd...
aws
Services
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
GuardDuty
Summary
Findings
EC2 malware scans
Protection plans
S3 Protection
EKS Protection
Extended Threat Detection
Runtime Monitoring
Malware Protection for EC2
Malware Protection for S3
RDS Protection
Lambda Protection
Accounts
Usage
Settings
GuardDuty > Findings
Findings (4) Info
Create suppression rule
Actions
Saved rules
Apply saved rules
Filter findings
1 match
Finding ID = fecb90c70bcbd7977113e4658dda7010
Clear filters
Status
Current
Threat type
All findings
1
Title
The Amazon S3 bucket test982081056098bucket was granted public authenticated access by Root calling PutBucketPolicy. If this behavior is not expected, it may indicate a configuration mistake or that your credentials are compromised.
Investigate with Detective
This finding is
Useful
Not useful
Overview
Finding ID
fecb90c70bcbd7977113e4658dda7010
Type
Policy:S3/BucketPublicAccessGranted
Severity
HIGH
Region
ap-south-1
Count
1
Account ID
982081056098
Resource ID
test982081056098bucket
Created at
05-30-2025 19:47:29 (10 minutes ago)
Updated at
05-30-2025 19:47:29 (10 minutes ago)
Resource affected
Resource role
TARGET
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


ap-south-1.console.aws.amazon.com/guardduty/home?region=ap-south-1#/findings?macros=current&search=id%3Dfecb90c70bcbd7977113e4658dd...
aws
Services
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
GuardDuty
We have received your feedback about GuardDuty findings and appreciate you for taking the time to submit it.
Summary
Findings
EC2 malware scans
Protection plans
S3 Protection
EKS Protection
Extended Threat Detection
Runtime Monitoring
Malware Protection for EC2
Malware Protection for S3
RDS Protection
Lambda Protection
Accounts
Usage
Settings
Findings (4) Info
Create suppression rule
Actions
Saved rules
Apply saved rules
Filter findings
1 match
Finding ID = fecb90c70bcbd7977113e4658dda7010
Clear filters
Status
Current
Threat type
All findings
1
Title
Resource affected
Resource role
TARGET
Resource type
AccessKey
Access key ID
ASIA6JKEXVVRPEGURG4L
Principal ID
982081056098
User type
Root
User name
Root
Affected resources
AWS::S3::Bucket
test982081056098bucket
S3 buckets
Destination: test982081056098bucket
Name
test982081056098bucket
Type
Destination
ARN
arn:aws:s3:::test982081056098bucket
Effective permission
PUBLIC
Created at
05-30-2025 14:11:23 UTC
Default server side encryption
Encryption type
AES256
Owner
ID
ca4fa6a7a198f2714aa95775bd34f093107e9f16d2eaf5c6357cc7bdd0cf4d08
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Now use cloudTrail to verify sequence of API activity

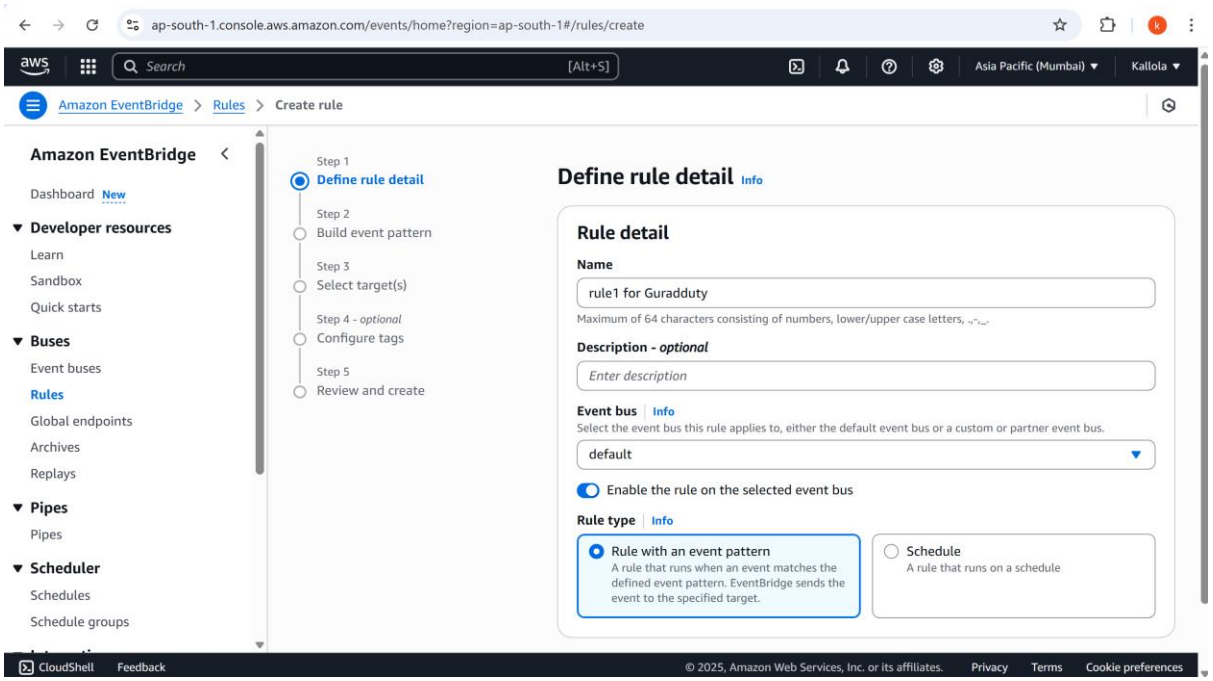


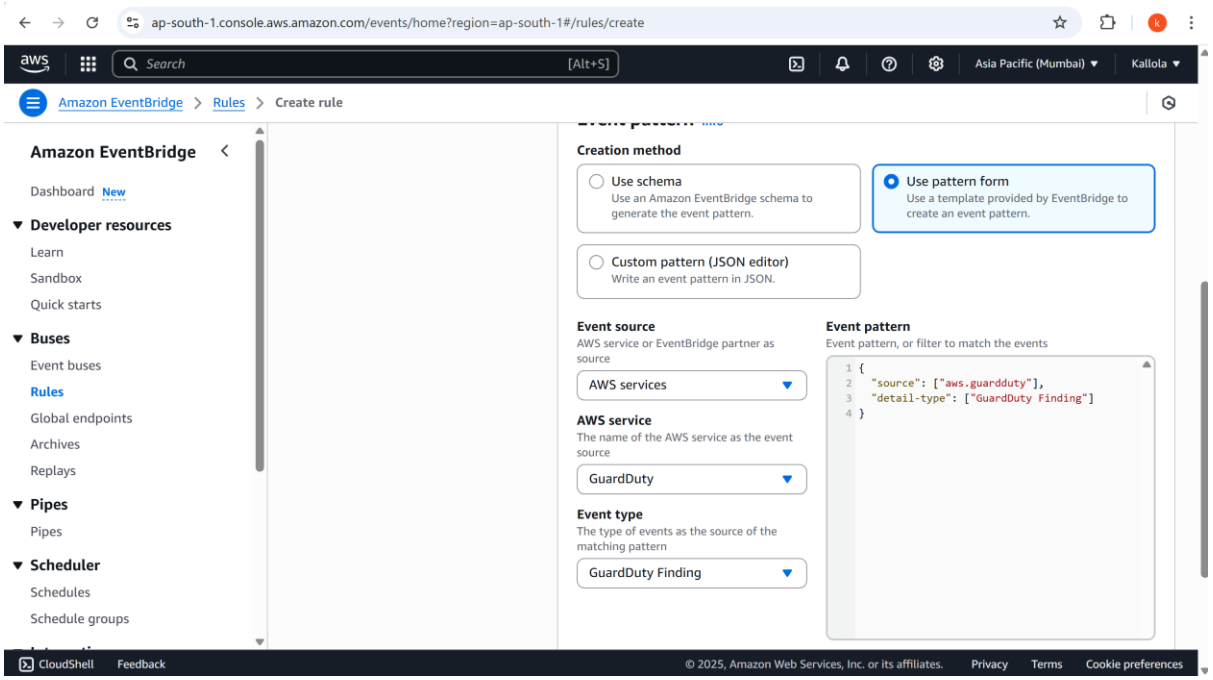


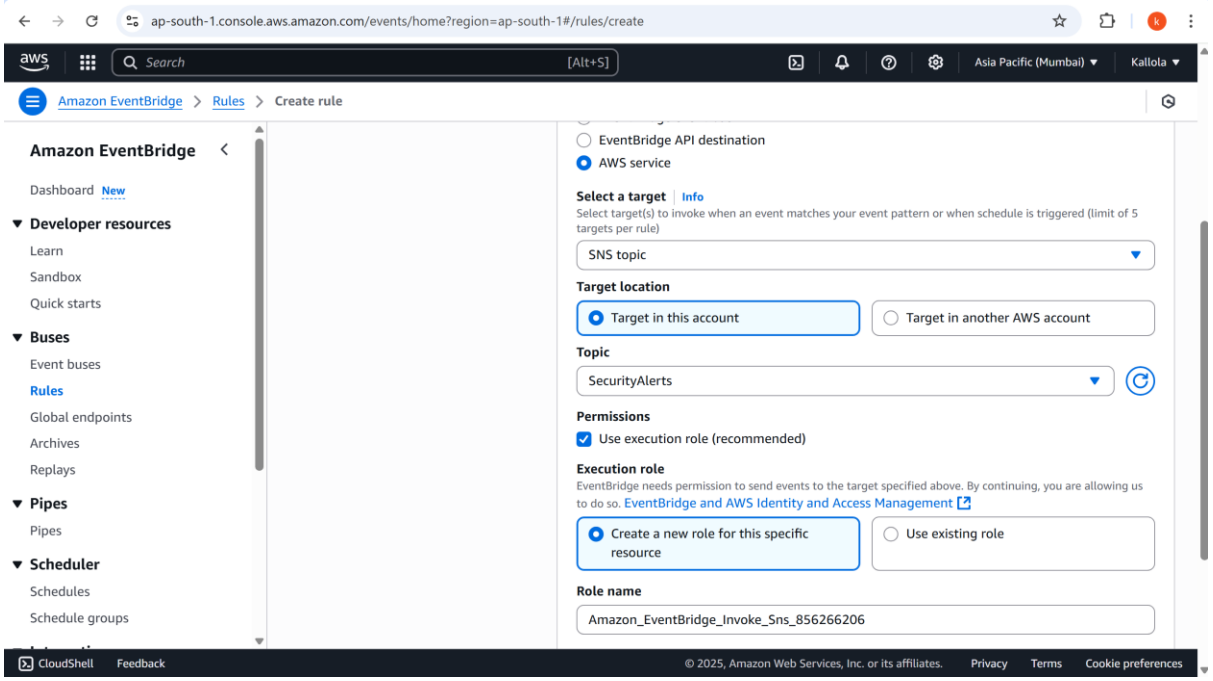


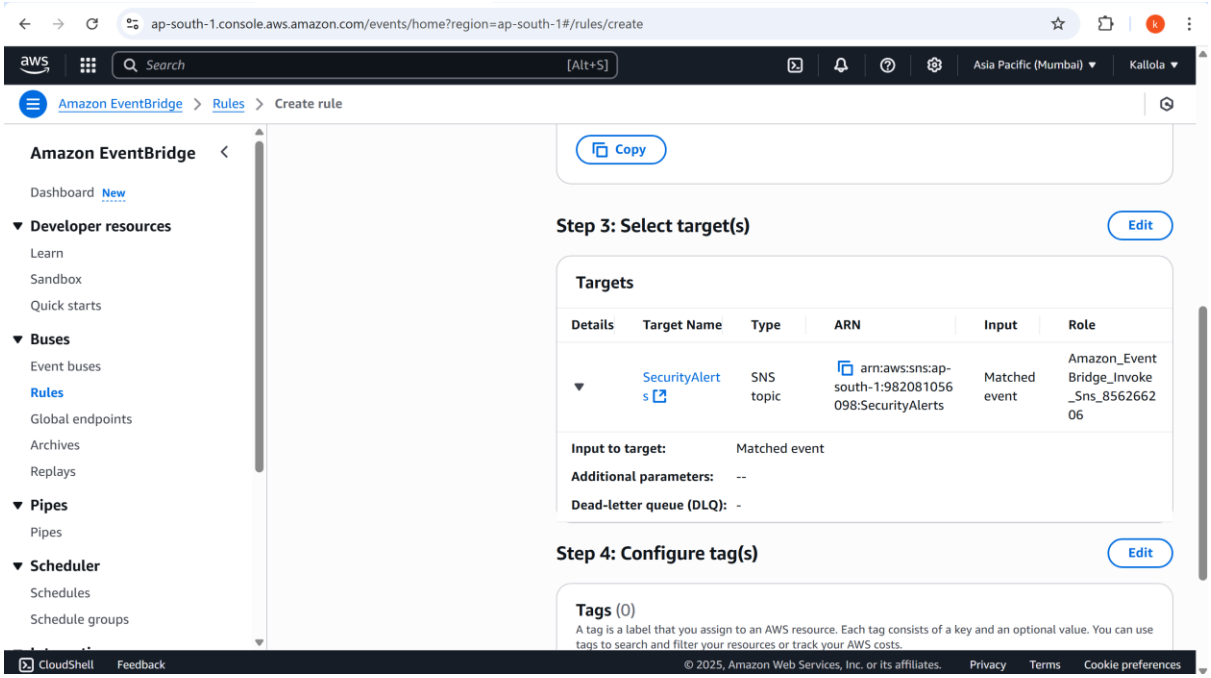
Phase 3: Create Alerts

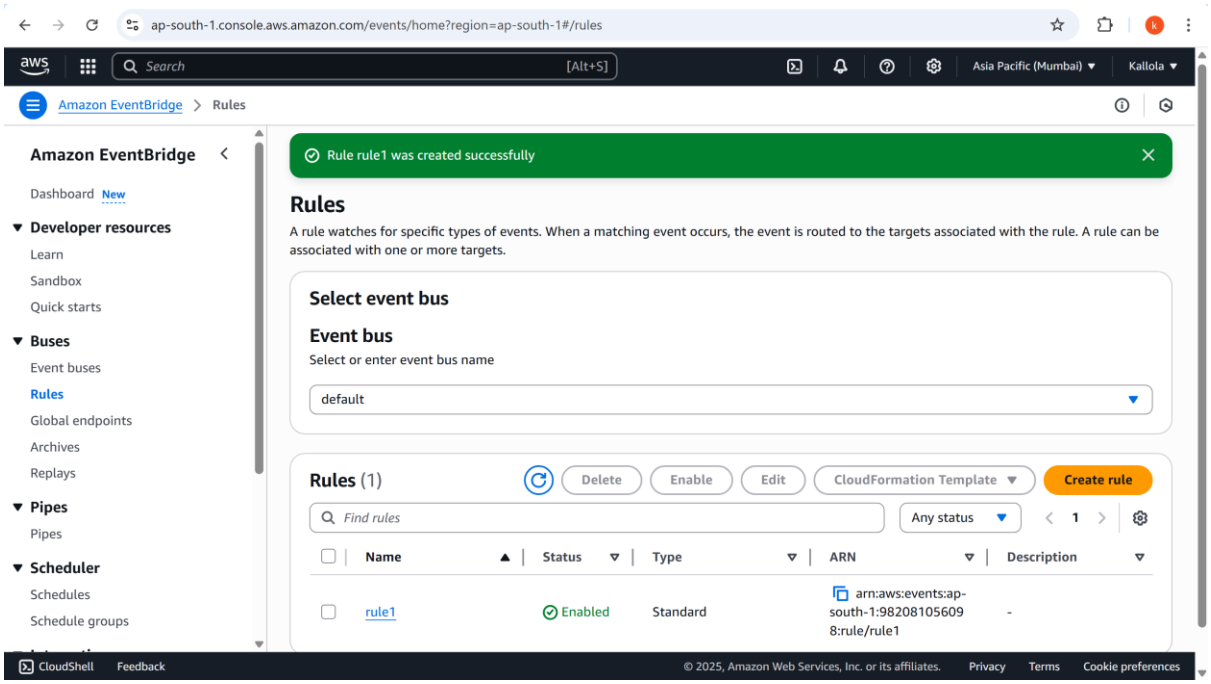
- Use **EventBridge** to listen to GuardDuty findings
- Trigger **SNS Email Alert** to your inbox




ap-south-1.console.aws.amazon.com/events/home?region=ap-south-1#/rules/create
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
Amazon EventBridge
Rules
Create rule
Amazon EventBridge
Dashboard New
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
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
GuardDuty
Event type
The type of events as the source of the matching pattern
GuardDuty Finding
Event pattern
Event pattern, or filter to match the events
{
"source": ["aws.guardduty"],
"detail-type": ["GuardDuty Finding"]
}
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

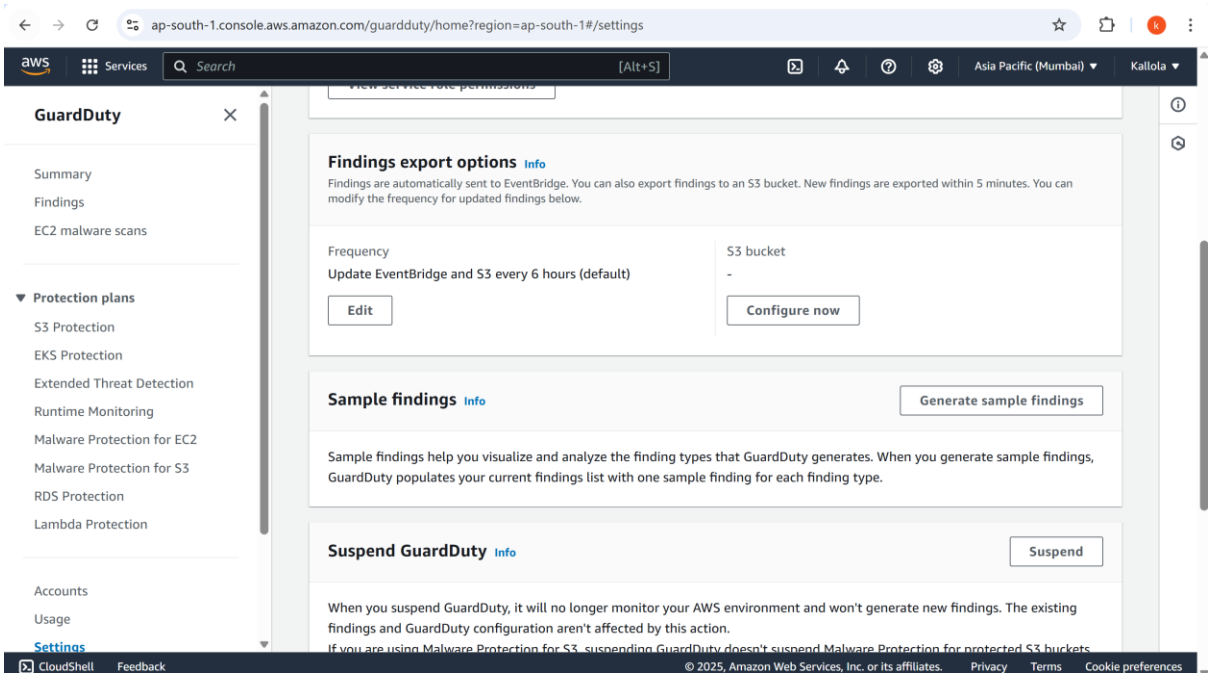

ap-south-1.console.aws.amazon.com/events/home?region=ap-south-1#/rules/create
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
Amazon EventBridge
Rules
Create rule
Amazon EventBridge
Dashboard New
Developer resources
Learn
Sandbox
Quick starts
Buses
Event buses
Rules
Global endpoints
Archives
Replays
Pipes
Pipes
Scheduler
Schedules
Schedule groups
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)
SNS topic
Target location
Target in this account
Target in another AWS account
Topic
SecurityAlerts
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_Sns_856266206
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

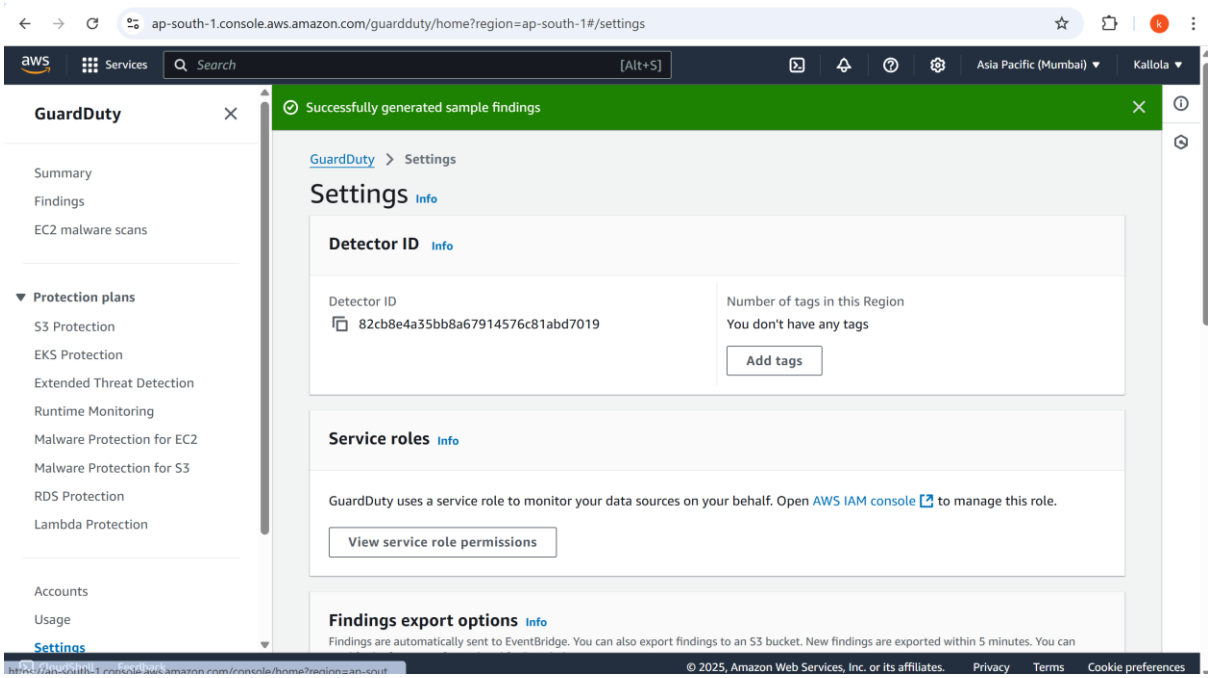




Simulate a GuardDuty Finding to test the above settings:-

Guradduty → settings → Generate sample findings





After this I got mail notification about the sample findings generated by Guardduty.