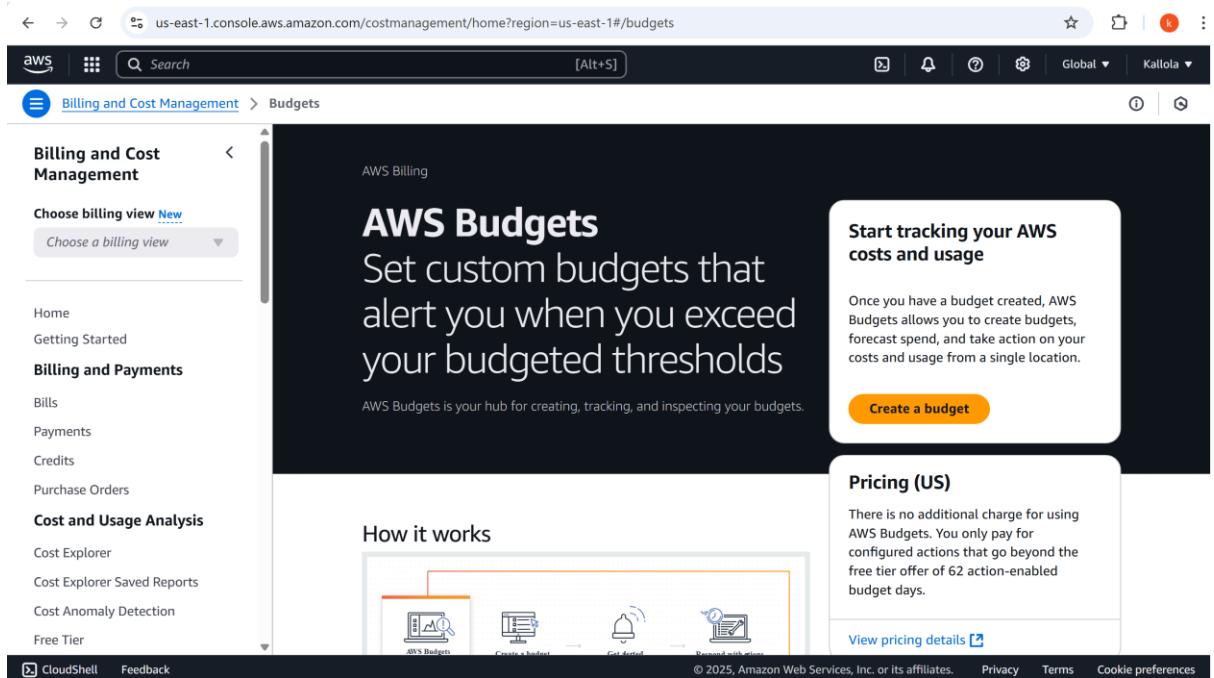


AWS Security Monitoring & Alerting Project

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... k

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)

Savings and Commitments
Cost Optimization Hub

Savings Plans
Overview
Inventory
Recommendations

CloudShell Feedback

Choose budget type

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

Budget setup

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.

Use a template (simplified)
Use the recommended configurations. You can change some configuration options after the budget is created.

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.

© 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... k

Billing and Cost Management > **Budgets** > Create budget

Billing and Payments
Bills
Payments
Credits
Purchase Orders

Cost and Usage Analysis
Cost Explorer
Cost Explorer Saved Reports
Cost Anomaly Detection
Free Tier

CloudShell Feedback

Set your budget

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.

© 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...

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

Details

Budget name
Provide a descriptive name for this budget.

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.

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

Budgeting method [Info](#)

Create a budget that tracks against a single monthly budgeted amount.

© 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...

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](#)

Create a budget that tracks against a single monthly budgeted amount.

Enter your budgeted amount (\$)
Last month's cost: \$0.00

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.

© 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... Remove

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

Set alert threshold

Threshold
When should this alert be triggered?
 % of budgeted amount

Trigger
How should this alert be triggered?

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.

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... Remove

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

Set alert threshold

Threshold
When should this alert be triggered?
 % of budgeted amount

Trigger
How should this alert be triggered?

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.

Maximum number of email recipients is 10.

► [Amazon SNS Alerts - Optional Info](#)

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... ☆ 🔍 🌐 ⚙️ Global ▾ Kallola ▾

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
kallo02@gmail.com
Amazon SNS
Not configured

Add action

Cancel Previous Next

© 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... ☆ 🔍 🌐 ⚙️ Global ▾ Kallola ▾

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

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

Budget details

Name	SecurityProjectBudget	Start date	May 2025
Period	Monthly	End date	-
Budget amount		\$2.00	

© 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...

Billing and Cost Management > Budgets > Create budget

Step 2: Configure alerts

Alerts

Alert #1

Threshold
75% of budgeted amount

Threshold measured against
Actual costs

Step 3: Attach actions - optional

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

Billing and Cost Management > Budgets > Overview

Your budget **SecurityProjectBudget** has been updated successfully.

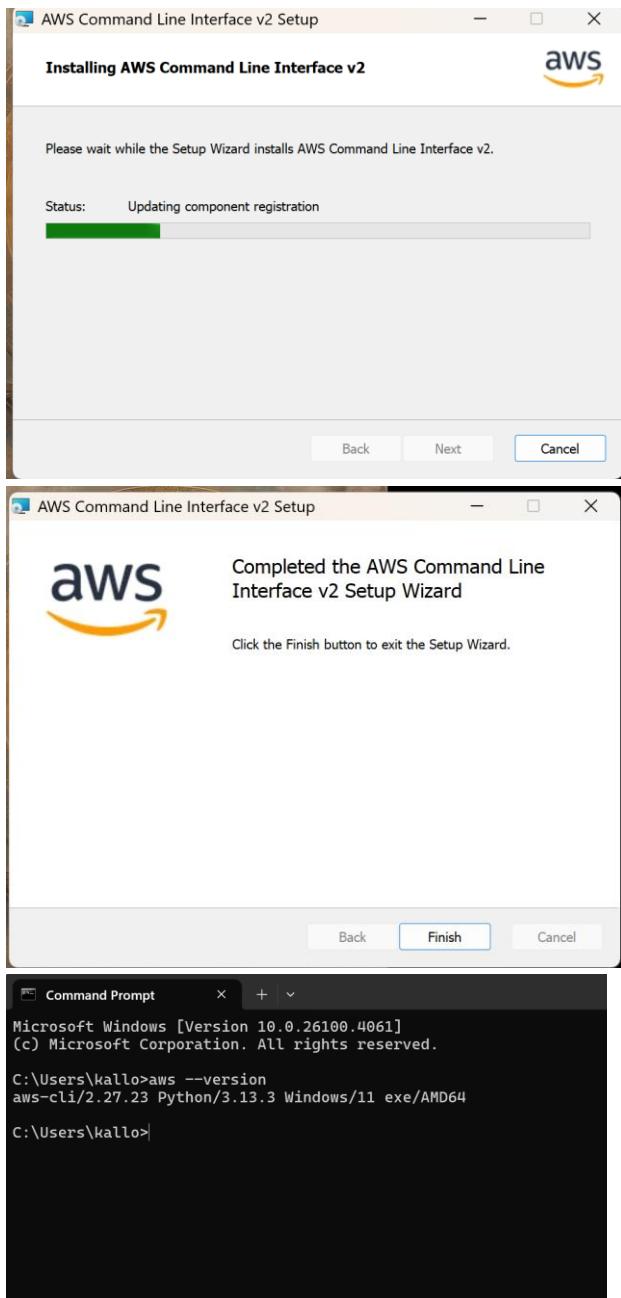
Budgets (1) Info

Download CSV Actions Create budget

Name	Thresholds	Budget	Amount ...	Forecast...	Current vs. budgeted
SecurityProjectBudget	OK	\$2.00	\$0.00		0.

Find a budget Type - Show all budgets 1

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

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

AWS CloudTrail

Continuously log your AWS account activity

Management & Governance

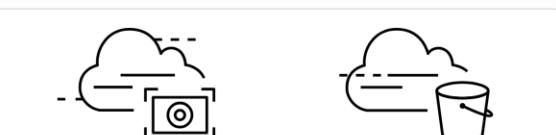
Use CloudTrail to meet your governance, compliance, and auditing needs for your AWS accounts.

Create a trail with AWS CloudTrail

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

Create a trail

How it works



Pricing

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

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

Log file SSE-KMS encryption [Info](#)

© 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

aws 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 log events

Events Info
 Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#)

Event type
 Choose the type of events that you want to log.

Management events
 Capture management operations performed on your AWS resources.

Data events
 Log the resource operations performed on or within a resource.

Insights events
 Identify unusual activity, errors, or user behavior in your account.

Network activity events
 Network activity events provide information about resource operations performed on a resource within a virtual private cloud endpoint.

Management events Info
 Management events show information about management operations performed on resources in your AWS account.

Multiple management events trails detected. Charges apply to duplicated logged management events. [Additional charges](#)

← → ⌂ ap-south-1.console.aws.amazon.com/cloudtrailv2/home?region=ap-south-1#/trails

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

CloudTrail > Trails

Trail successfully created
 Trail successfully deleted

Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
KK_management_events	Asia Pacific (Mumbai)	Yes	arn:aws:cloudtrail:ap-south-1:982081056098:trail/KK_management_events	Disabled	No	aws-cloudtrail-logs-982081056098-d505d402	-	-	<input checked="" type="checkbox"/> Logging

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](#)

How it works

Pricing

AWS Config	Pricing details
AWS Config rules	Pricing details
AWS GovCloud (US)	Pricing details

© 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.

© 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

aws 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

aws 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)

Name	Resource types	Trigger type	Description
account-part-of-organization		PERIODIC	Rule checks whether AWS account is part of AWS Organizations rule is NON_COMPLIANT if the AWS account is not part of AWS Organizations or AWS Organizations master account ID does not match rule parameter MasterAccountId.
acm-certificate-expiration-check	AWS::ACM::Certificate	HYBRID	Checks whether ACM Certificates in your account are marked for expiration within the specified number of days. Certificates proxy by ACM are automatically renewed. ACM does not automatically renew certificates that you import.
alb-http-drop-invalid-headers	AWS::ElasticLoadBalancingV2::LoadBalancer	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

aws 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

AWS Config (1)

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

The screenshot shows the AWS Config setup process. A green success message at the top states "Service linked role created successfully." Below it, an error message in a red box states "Configuration recorder creation failed." The error details are: "Error Insufficient delivery policy to s3 bucket: aws-cloudtrail-logs-982081056098-d505d402, unable to write to bucket, provided s3 key prefix is 'null', provided kms key is 'null'." On the left, a sidebar shows steps: Step 1 Settings, Step 2 Rules, and Step 3 Review. The Review section is active. It contains a "Recording method" table with one row: Recording strategy "Record all resource types with customizable overrides" and Default recording frequency "Continuous". At the bottom, there's a link to "Resource types with override settings (0)". The footer includes links to CloudShell, Feedback, and various AWS terms.

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>

The screenshot shows the AWS developer guide for "Permissions for the Amazon S3 Bucket for the AWS Config Delivery Channel". The page title is "Permissions for the Amazon S3 Bucket for the AWS Config Delivery Channel". It features an "Important" callout box stating: "This page is about setting up the Amazon S3 Bucket for the AWS Config delivery channel. This page is not about the AWS::S3::Bucket resource type that the AWS Config configuration recorder can record." Below this, there's a note: "Amazon S3 buckets and objects are private by default. Only the AWS account that created the bucket (the resource owner) has access permissions. Resource owners can grant access to other resources and users by creating access policies." Another note below it says: "When AWS Config automatically creates an S3 bucket for you, it adds the required permissions. However, if you specify an existing S3 bucket, you must add these permissions manually." On the left, a sidebar lists various AWS services and documentation sections. On the right, there are "On this page" and "Did this page help you?" sections, along with a feedback link and a home icon.

The screenshot shows the AWS Config Dashboard. On the left, there's a sidebar with 'AWS Config' selected. Under 'Dashboard', it lists 'Conformance packs', 'Rules', 'Resources', and 'Aggregators'. Under 'Aggregators', it lists 'Compliance Dashboard', 'Conformance packs', 'Rules', 'Inventory Dashboard', 'Resources', 'Authorizations', 'Advanced queries', 'Settings', and 'What's new'. Below the sidebar, there are three main sections: 'Conformance Packs by Compliance Score' (empty), 'Compliance status' (empty), and 'Noncompliant rules by noncompliant resource count' (empty). At the bottom, there are links for 'Documentation', 'Partners', 'CloudShell', 'Feedback', and copyright information.

✓ Enable GuardDuty

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

The screenshot shows the 'GuardDuty' enablement page. It starts with a note about granting permissions: 'When you enable GuardDuty, you grant GuardDuty permissions to:'. It lists two bullet points: 'Analyze VPC Flow logs, AWS CloudTrail management event logs, DNS query logs, AWS CloudTrail S3 data event logs, EKS audit logs, Lambda network activity logs, and RDS login activity logs to generate security findings.' and 'Analyze Elastic Block Storage (EBS) volume data to generate malware detection findings.' Below this is a 'View service role permissions' button. The next section is 'Protection plans', which contains a bulleted list: 'Enabling GuardDuty for the first time will automatically enable all GuardDuty protection plans, except Runtime Monitoring and Malware Protection for S3, both of which you can enable by using the GuardDuty console or APIs.', 'Your use of GuardDuty Malware Protection and Runtime Monitoring are subject to the [Amazon GuardDuty Service Terms](#).', and 'You can suspend or disable GuardDuty, or disable select protection plans, at any time to stop GuardDuty from processing and analyzing data, events, and logs. Suspending or disabling GuardDuty doesn't impact Malware Protection for S3. To stop GuardDuty from scanning your S3 bucket for malware, you must delete the Malware Protection plan for each protected S3 bucket separately.' A note below states: 'Note: GuardDuty does not manage the data, events, and logs listed above, or make any such data, events, or logs available to you. You can configure the settings of these data sources through their respective consoles or APIs.' At the bottom, it says 'When you enable GuardDuty in a supported Region for the first time, your account gets automatically enrolled in a 30-day free trial. By default, some protection plans may also get included in a 30-day free trial.' A large orange 'Enable GuardDuty' button is at the bottom right.

The screenshot shows the AWS GuardDuty console. A green banner at the top says "You've successfully enabled GuardDuty." Below it, a blue box contains a message: "New feature: Amazon GuardDuty is now available in AWS Mexico (Central) Region. You can now extend your continuous security monitoring and threat detection to the AWS Mexico (Central) Region." A "Learn more" link is provided. The main "Summary" page shows zero findings, total findings, resources with findings, and accounts with findings, all at 0. The left sidebar includes sections for Summary, Protection plans (S3, EKS, Extended Threat Detection, Runtime Monitoring, Malware Protection for EC2, S3, RDS, Lambda), Accounts, Usage, and Settings.

✓ IAM Setup

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

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar lists Identity and Access Management (IAM) features: Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management), and Access reports (Access Analyzer, External access, Unused access, Analyzer settings). The main area displays "Security recommendations" (Root user has MFA, Root user has no active access keys), "IAM resources" (User groups: 0, Users: 0, Roles: 7, Policies: 0, Identity providers: 0), and "What's new" (Updates for features in IAM). A "View all" link is present. To the right, there are three boxes: "AWS Account" (Account ID: 982081056098, Account Alias: Create, Sign-in URL: https://982081056098.signin.aws.amazon.com/console), and "Quick Links" (My security credentials, Manage your access keys, multi-factor authentication (MFA) and other credentials).

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles

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

CloudShell Feedback

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.

Role name	Trusted entities	Last activity
AWSServiceRoleForAccessAnalyzer	AWS Service: access-analyzer (Service-Linked)	1 hour ago
AWSServiceRoleForAmazonGuardDuty	AWS Service: guardduty (Service-Linked)	-
AWSServiceRoleForAmazonGuardDutyMalwareProtection	AWS Service: malware-protection.gu...	-
AWSServiceRoleForConfig	AWS Service: config (Service-Linked)	-
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linker)	-
Config_KK	AWS Service: config	-

Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Manage

© 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

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 Allows 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

Add permissions

Step 1: Select trusted entity
Step 2: Add permissions (selected)
Step 3: Name, review, and create

Add permissions

Permissions policies (1/1046)

Choose one or more policies to attach to your new role.

Filter by Type: All types (1 match)

Policy name: SecurityAudit

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...

Name, review, and create

Step 1: Select trusted entity
Step 2: Add permissions
Step 3: Name, review, and create (selected)

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

Trust policy

```
1: [{}]
2:   "Version": "2012-10-17",
3:   "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...

Step 1: Select trusted entities

Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": "sts:AssumeRole",  
7       "Principal": {  
8         "AWS": "982081056098"  
9       },  
10      "Condition": {}  
11    }  
12  ]  
13 }
```

Step 2: Add permissions

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...

Step 2: Add permissions

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

Add new tag
You can add up to 49 more tags.

Cancel Previous Create role

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles

Identity and Access Management (IAM)

Roles (8) 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.

Roles Anywhere [Info](#)

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard

Use your own existing PKI infrastructure or use [AWS Certificate Manager Private Certificate Authority](#) to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

View role **Delete** **Create role**

CloudShell Feedback

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/SecurityAuditRole)section=permissions

Identity and Access Management (IAM)

SecurityAuditRole [Info](#)

Role for auditing AWS security configurations with read-only access.

Summary

Creation date
May 29, 2025, 20:56 (UTC+05:30)

ARN
[arn:aws:iam::982081056098:role/SecurityAuditRole](#)

Last activity
-

Maximum session duration
1 hour

Link to switch roles in console
<https://signin.aws.amazon.com/switchrole?roleName=SecurityAuditRole&account=982081056098>

Edit

Permissions **Trust relationships** **Tags (1)** **Last Accessed** **Revoke sessions**

Permissions policies (1) Info

You can attach up to 10 managed policies.

Filter by Type [Search](#) [All types](#)

Simulate **Remove** **Add permissions**

CloudShell Feedback

Enable CloudWatch Logs

← → ⌂ ap-south-1.console.aws.amazon.com/clouptrailv2/home?region=ap-south-1#/dashboard?source=fromRoot

CloudTrail > Dashboard

S3 bucket policy successfully fixed

Dashboard Info

Query results history

Choose a query to view results from the last seven days.

No queries
No queries to display

Create a new query

Trails Info

Copy events to Lake **Create trail**

Name	Status
KK_management_events	Logging

← → ⌂ ap-south-1.console.aws.amazon.com/clouptrailv2/home?region=ap-south-1#/trails/arn:aws:clouptrail:ap-south-1:982081056098:trail/KK_manage...

CloudTrail > Trails > arn:aws:clouptrail:ap-south-1:982081056098:trail/KK_management_events

KK_management_events

Delete **Stop logging**

General details

Trail logging Logging	Trail log location aws-clouptrail-logs-982081056098-d505d402/AWSLogs/982081056098	Log file validation Disabled	SNS notification delivery Disabled
Trail name KK_management_events	Last log file delivered May 29, 2025, 23:02:41 (UTC+05:30)	Last file validation delivered -	Last SNS notification -
Multi-region trail Yes	Log file SSE-KMS encryption Not enabled	Edit	
Apply trail to my organization Not enabled			

CloudWatch Logs

Edit

Log group aws-clouptrail-logs-KK	IAM Role arn:aws:iam::982081056098:role/service-role/CloudTrailRoleForCloudWatchLogs_KK
-------------------------------------	--

Tags

Manage tags

CloudShell Feedback

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

Create an SNS Topic for Alerts

← → ⌂ ap-south-1.console.aws.amazon.com/sns/v3/home?region=ap-south-1#/create-topic

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

Amazon SNS > Topics > Create topic

Create topic

Details

Type | Info Topic type cannot be modified after topic is created

FIFO (first-in, first-out)

- Strictly-preserved message ordering
- Exactly-once message delivery
- Subscription protocols: SQS

Standard

- Best-effort message ordering
- At-least once message delivery
- Subscription protocols: SQS, Lambda, Data Firehose, HTTP, SMS, email, mobile application endpoints

Name Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (_).

Display name - optional | Info To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message.

Maximum 100 characters.

Encryption - optional

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#/topic/arn:aws:sns:ap-south-1:982081056098:SecurityAlerts

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

Amazon SNS > Topics > SecurityAlerts

Amazon SNS

- Dashboard
- Topics
- Subscriptions

▼ Mobile

- Push notifications
- Text messaging (SMS)

SecurityAlerts

New Feature Amazon SNS now supports High Throughput FIFO topics. [Learn more](#)

Topic SecurityAlerts created successfully. You can create subscriptions and send messages to them from this topic. [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

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

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

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

Amazon SNS > Topics > SecurityAlerts

Amazon SNS < SecurityAlerts

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 ↗

Subscriptions (0) Edit Delete Request confirmation Confirm subscription Create subscription

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

aws 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

← → ⌂ ap-south-1.console.aws.amazon.com/sns/v3/home?region=ap-south-1#/subscription/arn:aws:sns:ap-south-1:982081056098:SecurityAlerts:af9e1da... ☆ 🔍 📁 📲 📽 Kallola

Amazon SNS > Topics > SecurityAlerts > Subscription: af9e1da2-6366-4c96-bb97-4b70731e9ade

Subscription: af9e1da2-6366-4c96-bb97-4b70731e9ade

Details

ARN arn:aws:sns:ap-south-1:982081056098:SecurityAlerts:af9e1da2-6366-4c96-bb97-4b70731e9ade	Status Pending confirmation
Endpoint kallolakumar02@gmail.com	Protocol EMAIL
Topic SecurityAlerts	
Subscription Principal arn:aws:iam::982081056098:root	

Subscription filter policy Redrive policy (dead-letter queue)

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

AWS Notification - Subscription Confirmation Inbox 🖨️ 📎

AWS Notifications <no-reply@sns.amazonaws.com> 11:29 PM (0 minutes ago) ☆ 😊 ⏪ ⏴

to me ▾

You have chosen to subscribe to the topic:
arn:aws:sns:ap-south-1:982081056098:SecurityAlerts

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

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [sns-opt-out](#)

Reply Forward Smile

← → ⌂ sns.ap-south-1.amazonaws.com/confirmation.html?TopicArn=arn:aws:sns:ap-south-1:982081056098:SecurityAlerts:af9e1da2-6366-4c96-bb97-4b70731e9ade



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

The screenshot shows the 'Create bucket' configuration page in the AWS S3 console. The URL in the address bar is `ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general`. The page title is 'Create bucket'. The 'General configuration' section is active. Under 'Bucket type', 'General purpose' is selected. The 'Bucket name' field contains 'myawsbucket'. The 'Copy settings from existing bucket - optional' section is present but empty. At the bottom, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates.' and 'Privacy Terms Cookie preferences'.

← → ⌂ ap-south-1.console.aws.amazon.com/s3/buckets?region=ap-south-1&bucketType=general

aws | 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.

▶ 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

General purpose buckets Directory buckets

General purpose buckets (2) Info All AWS Regions

Buckets are containers for data stored in S3.

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)

Copy ARN Empty Delete Create bucket

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

aws | 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	Succeeded	Failed
s3://test982081056098bucket	1 file, 41.9 MB (100.00%)	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

Screenshot of the 'Edit Block public access (bucket settings)' page in the AWS S3 console.

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**

Screenshot of the 'Permissions overview' and 'Block public access (bucket settings)' pages in the AWS S3 console.

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)

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

Screenshot of the 'Bucket policy' page in the AWS S3 console.

Bucket policy

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

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

The screenshot shows the AWS S3 Bucket Policy editor. A green success message at the top says "Successfully edited bucket policy." Below it, the "Bucket policy" section displays a JSON policy document:

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": {"AWS": "*"}, "Action": "s3:GetObject", "Resource": "arn:aws:s3:::test982081056098bucket/*" } ] }
```

Buttons for "Edit" and "Delete" are visible. A "Copy" button is located in the top right corner of the policy editor area.

The screenshot shows the AWS S3 Objects page for the bucket "test982081056098bucket". The "Objects" tab is selected. A single object, "AWSCLIV2(msi)", is listed in the table:

Name	Type	Last modified	Size	Storage class
AWSCLIV2(msi)	msi	May 30, 2025, 18:38:02 (UTC+05:30)	41.9 MB	Standard

The s3 public access enabled.

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

GuardDuty > Findings

Findings (4) Info

Create suppression rule

Actions ▾

Saved rules Apply saved rules ▾

Filter findings 1 match

Finding ID = **fecb90c70bcd7977113e4658dda7010** X

Clear filters ▾

Status Current Threat type All findings

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	fecb90c70bcd7977113e4658dda7010
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
Resource role	TARGET
Resource type	AccessKey
Access key ID	ASIA6JKEXVVRPEGURG4L
Principal ID	982081056098
User type	Root
User name	Root

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

GuardDuty > Findings

Findings (4) Info

Create suppression rule

Actions ▾

Saved rules Apply saved rules ▾

Filter findings 1 match

Finding ID = **fecb90c70bcd7977113e4658dda7010** X

Clear filters ▾

Status Current Threat type All findings

Title

We have received your feedback about GuardDuty findings and appreciate you for taking the time to submit it.

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
Name	test982081056098bucket
Type	Destination
ARN	arn:aws:s3:::test982081056098bucket
Effective permission	PUBLIC
Created at	05-30-2025 14:11:23 UTC

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
----	--

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

Now use cloudTrail to verify sequence of API activity

The screenshot shows the AWS CloudTrail Event history page. The left sidebar includes options like Dashboard, Event history (selected), Insights, Lake (Dashboards, Query, Event data stores, Integrations), Trails, Settings, Pricing, Documentation, Forums, and FAQs. The main area displays a table of events with columns: Event name, Event time, User name, Event source, and Resource type. The table lists several events from May 30, 2025, such as 'UpdateFindingsFeed...', 'PutBucketPolicy', 'PutBucketPublicAcce...', 'PutBucketEncryption', 'CreateBucket', 'CreateBucket', 'Subscribe', and 'CreateTopic'. A search bar at the top allows filtering by event name and date.

The screenshot shows the AWS GuardDuty home page. The left sidebar includes 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, and Settings. The main area features a 'Findings - new' section with counts for Critical (0), High (1), Medium (0), and Low (3) severity findings. It also includes a pie chart titled 'Most common finding types' and a table for 'Resources with most findings'.

The screenshot shows the AWS GuardDuty console. On the left, there's a sidebar with 'GuardDuty' selected. Under 'Summary', it lists 'Findings' and 'EC2 malware scans'. Under 'Protection plans', it lists various services like S3 Protection, EKS Protection, etc. In the center, there's a summary card with 'Top threats' (3 findings) and a table of findings. One finding is highlighted: 'Amazon S3 Public Access was granted for S3 bucket test982081056098bucket.' (Severity: High). To the right, there's a table titled 'Resources with most findings' showing AccessKeys and their counts.

Phase 3: Create Alerts

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

The screenshot shows the AWS EventBridge console. On the left, there's a sidebar with 'Amazon EventBridge' selected. Under 'Developer resources', it lists 'Rules'. The main area shows a flowchart with 5 steps: Step 1 (Define rule detail), Step 2 (Build event pattern), Step 3 (Select target(s)), Step 4 - optional (Configure tags), and Step 5 (Review and create). Step 1 is currently active. On the right, there's a detailed view of 'Define rule detail' with fields for 'Name' (rule1 for Guraduty), 'Description - optional' (Enter description), 'Event bus' (default), and 'Rule type' (selected 'Rule with an event pattern').

← → ⌂ ap-south-1.console.aws.amazon.com/events/home?region=ap-south-1#/rules/create

aws 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

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

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

```
1 {  
2   "source": ["aws.guardduty"],  
3   "detail-type": ["GuardDuty Finding"]  
4 }
```

← → ⌂ ap-south-1.console.aws.amazon.com/events/home?region=ap-south-1#/rules/create

aws 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

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

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

The screenshot shows the 'Create rule' wizard in the Amazon EventBridge console. The current step is 'Step 3: Select target(s)'. A table lists a single target named 'SecurityAlerts' (SNS topic, ARN: arn:aws:sns:ap-south-1:982081056098:SecurityAlerts). The input type is 'Matched event'. Below the table, there are fields for 'Input to target', 'Additional parameters', and 'Dead-letter queue (DLQ)'.

The screenshot shows the 'Rules' page in the Amazon EventBridge console. A green success message at the top states 'Rule rule1 was created successfully'. The main area displays the 'Select event bus' configuration, where the event bus 'default' is selected. Below this, the 'Rules (1)' table shows one rule named 'rule1' (Enabled, Standard type, ARN: arn:aws:events:ap-south-1:982081056098:rule/rule1).

Simulate a GuardDuty Finding to test the above settings:-

Gurardduty → settings → Generate sample findings

The screenshot shows the AWS GuardDuty Settings page. On the left, a sidebar lists various sections like Summary, Findings, EC2 malware scans, Protection plans (S3, EKS, Extended Threat Detection, Runtime Monitoring, Malware Protection for EC2, S3, RDS, Lambda), Accounts, Usage, and Settings. The main content area is titled 'Findings export options' and includes a sub-section 'Frequency' set to 'Update EventBridge and S3 every 6 hours (default)'. It also features a 'Sample findings' section with a 'Generate sample findings' button and a 'Suspend GuardDuty' section with a 'Suspend' button.

The screenshot shows the AWS GuardDuty Settings page after generating sample findings. A green banner at the top states 'Successfully generated sample findings'. The main content area shows the 'Detector ID' section with the ID '82cb8e4a35bb8a67914576c81abd7019' and a note about tags. It also includes 'Service roles' and 'Findings export options' sections.

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