Jojo267

Email not verified
Users must first verify their email address before they can begin to use certain features such as completing email-based two-step verification during sign-in.

General information

Profile | Groups (1) | AWS accounts | Applications | MFA devices (0) | Active sessions (1)

Group memberships (1)

To grant permission to this user, add the user to a group that has access to AWS accounts or cloud applications. Learn more

Search for group name starting with...

Group name
Admin

aws-reserved/sso.amazonaws.com/us-east-2/AWSReservedSSO_AdministratorAccess_c0c9e8f454c8b4f1 Info

Resource details and findings for this resource across analyzers

Resource details

ARN
arn:aws:iam::784074784420:role/aws-reserved/sso.amazonaws.com/us-east-2/AWSReservedSSO_AdministratorAccess_c0c9e8f454c8b4f1

Type
IAM role

Owner account
784074784420

Analyzers for these findings
Analyzer: AccountAnalyzer

Active findings (1)

Actions

Search findings

Filter access type
All types

1

Finding ID	Access type	Principal	Condition	Shared through	Access level	Resource cont...	Service contro...	Last updated
de600b2c-610a-4916-9735-41dc801c5f56	External access	Federated User arn:aws:iam::7...	-	-	Write, Tagging	Not applicable	-	181 days ago

General details

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

Trail name

Enter a display name for your trail.

AccountTrail1

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-784074784420-79cf6ca1

Logs will be stored in aws-cloudtrail-logs-784074784420-79cf6ca1/AWSLogs/784074784420

Log file SSE-KMS encryption | Info

☐ Enabled

▼ Additional settings

Log file validation | Info

☑ Enabled

SNS notification delivery | Info

☑ Enabled

Create a new SNS topic

◉ New

○ Existing

SNS topic

aws-cloudtrail-logs-784074784420-c5d81ee2

Edit arn:aws:cloudtrail:us-east-2:784074784420:trail/AccountTrail1

General details

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

Trail name

Enter a display name for your trail.

AccountTrail1

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 name

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

aws-cloudtrail-logs-784074784420-79cf6ca1 ✕ Browse

Prefix - *optional*

prefix

Logs will be stored in aws-cloudtrail-logs-784074784420-79cf6ca1/AWSLogs/784074784420

Log file SSE-KMS encryption | Info

☑ Enabled

Customer managed AWS KMS key

- (•) New
- ( ) Existing

AWS KMS alias

cloudtrail-key

KMS key and S3 bucket must be in the same region.

▼ Additional settings

Log file validation | Info

☑ Enabled

SNS notification delivery | Info

☐ Enabled

Cancel Save changes

Edit arn:aws:cloudtrail:us-east-2:784074784420:trail/AccountTrail1

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.

- [x] Management events

Capture management operations performed on your AWS resources.

Management events Info

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

No additional charges apply to log management events on this trail because this is your first copy of management events.

API activity

Choose the activities you want to log.

- [x] Read
- [x] Write
- [ ] Exclude AWS KMS events
- [ ] Exclude Amazon RDS Data API events

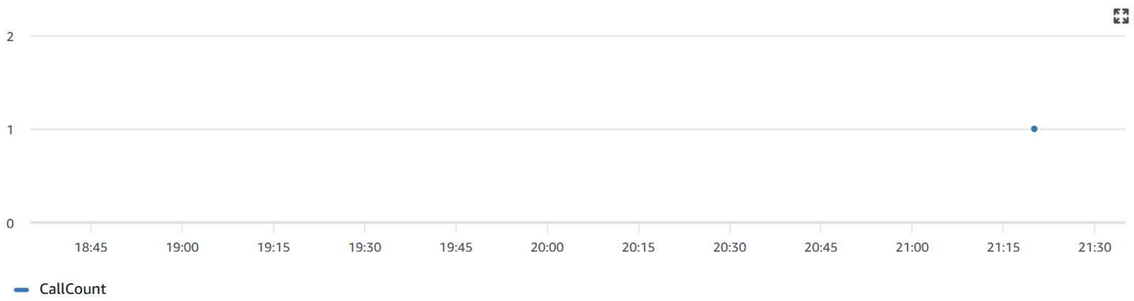
Cancel Save changes

Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add alarm details
Step 4
Preview and create

Specify metric and conditions

Metric

Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.



Namespace
AWS/Usage

Metric name
CallCount

Type
API

Resource
StartLogging

Service
CloudTrail

Class
None

Statistic
Sum

Period
5 minutes

Conditions

Threshold type

- (●) Static — Use a value as a threshold
- ( ) Anomaly detection — Use a band as a threshold

Whenever CallCount is...
Define the alarm condition.

- (●) Greater — > threshold
- ( ) Greater/Equal — >= threshold
- ( ) Lower/Equal — <= threshold
- ( ) Lower — < threshold

than...
Define the threshold value.

Configure actions

Notification

Alarm state trigger
Define the alarm state that will trigger this action.

Remove

- (●) In alarm
  The metric or expression is outside of the defined threshold.
- ( ) OK
  The metric or expression is within the defined threshold.
- ( ) Insufficient data
  The alarm has just started or not enough data is available.

Send a notification to the following SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.

- ( ) Select an existing SNS topic
- (●) Create new topic
- ( ) Use topic ARN to notify other accounts

Create a new topic...
The topic name must be unique.

CloudTrail-API-Activity-Alarm

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

Email endpoints that will receive the notification...
Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

jodelis65@gmail.com

user1@example.com, user2@example.com

Create topic

Add notification

Lambda action

Dashboard

Conformance Packs by Compliance Score

Conformance pack	Compliance score

No conformance packs deployed. Try deploying a new conformance pack. Learn more

Compliance status

Rules

1 Noncompliant rule(s)
3 Compliant rule(s)

Resources

1 Noncompliant resource(s)
2 Compliant resource(s)

Noncompliant rules by noncompliant resource count

Name	Compliance
iam-password-policy	1 Noncompliant resource(s)

View all noncompliant rules

Resource inventory (58)

Stacks (1)

Search by stack name

Filter status: Active

View nested

Stack name	Status	Created time	Description
config-security-rules	CREATE_COMPLETE	2025-08-28 17:17:30 UTC-0400	AWS Account Governance - Basic AWS Config Rules for Lab 1

Stacks (1)

Filter status

Search by stack name

Active

View nested

1

Stacks

config-security-rules
2025-08-28 17:17:30 UTC-0400
CREATE_COMPLETE

config-security-rules

Delete stack | Update stack | Stack actions | Create stack

Stack info | Events | Resources | Outputs | Parameters | Template | Change sets | Git sync

Overview

Stack ID
arn:aws:cloudformation:us-east-2:784074784420:stack/config-security-rules/681c9bb0-8454-11f0-ab49-0a67fa145073

Description
AWS Account Governance - Basic AWS Config Rules for Lab 1

Status
CREATE_COMPLETE

Detailed status
-

Status reason
-

Root stack
-

Parent stack
-

Created time
2025-08-28 17:17:30 UTC-0400

Updated time
-

Deleted time
-

Drift status
NOT_CHECKED

Last drift check time
-

Termination protection
Deactivated

IAM role
-

Successfully enabled standard: PCI DSS v3.2.1

Regions: All Linked Regions

Summary Info

Reset to default layout | + Add widget

Choose a filter set | Filter data

Workflow status = NEW | Workflow status = NOTIFIED | Record state = ACTIVE | Clear filters

Introducing the new AWS Security Hub

The new Security Hub is your unified cloud security solution featuring:

- Prioritized risk detection correlating security signals across AWS
- Potential attack path visualization for each identified exposure
- Centralized management of security capabilities
- Cost optimization through unified pricing of security services including Security Hub CSPM, GuardDuty, and Inspector

Compare pricing | Try Security Hub

Security standards Info

Track your cloud security posture with a summary security score and standard security scores. This widget always shows complete, unfiltered data.

Security score

No standard found for the account

Standard	Passed	Failed	Score
AWS Foundational Security Best Practices v1.0.0	0	0	0%
CIS AWS Foundations Benchmark v1.4.0	0	0	0%
PCI DSS v3.2.1	0	0	0%

Assets with the most findings Info

Prioritize and evaluate your assets that are most at risk.

Resources | Accounts | Applications

Resources	By severity	By resource type	Total findings
784074784420			2

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.

▶ **Billing View - *optional***
Select a billing view you want to create this data export for. This will not be editable after create. If no view is selected, this export will be created for your account data (primary view).

Templates - *new*

Choose a template that best matches your use case.

- ( ) Zero spend budget
  Create a budget that notifies you once your spending exceeds $0.01.
- (●) Monthly cost budget
  Create a monthly budget that notifies you if you exceed, or are forecasted to exceed, the budget amount.
- ( ) Daily Savings Plans coverage budget
  Create a coverage budget for your Savings Plans that notifies you when you fall below the defined target.
- ( ) Daily reservation utilization budget
  Create a utilization budget for your reservations that notifies you when you fall below the defined target.

Monthly cost budget - Template

Budget name
Provide a descriptive name for this budget.

My Monthly Cost Budget

Names must be between 1-100 characters.

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

100

Email recipients
Specify the email recipients you want to notify when the threshold has exceeded.

Separate email addresses using commas

Maximum number of email recipients is 10.

Scope
All AWS services are in scope in this budget.

ⓘ You will be notified when 1) your **actual spend** reaches 85% 2) your **actual spend** reaches 100% 3) if your **forecasted spend** is expected to reach 100%.