

ACCT-001 - Define Secure AWS Account Governance Best Practice

The root user is secured

The Root user has administrative roles, with MFA enabled. Users with access to the Customer's AWS portal have minimal access roles: read only. The CloudTrail application is used to monitor user activity.

IAM Dashboard [Info](#)

Security recommendations 0

- ✔ Root user has MFA
Having multi-factor authentication (MFA) for the root user improves security for this account.
- ✔ You have MFA
Having multi-factor authentication (MFA) for the IAM user improves security for this account.
- ✔ Your user, `castro.carlos@cloudrivers.io`, does not have any active access keys that have been unused for more than a year.
Deactivating or deleting unused access keys improves security.

Using CloudTrail for user event logging:

CloudTrail

Dashboard
Event history
Insights
Lake
Dashboards
Query
Event data stores
Integrations
Trails
Settings
Pricing
Documentation
News

management-events

Delete
Stop logging

General details

Trail logging
Logging

Trail log location
aws-cloudtrail-logs-992382705250-S9e6a0dc/AWSLogs/992382705250

Log file validation
Disabled

Log file validation delivered
-

SNS notification delivery
Disabled

Last SNS notification
-

Trail name
management-events

Multi-region trail
Yes

Apply trail to my organization
Not enabled

Last log file delivered
March 27, 2025, 01:01:09 (UTC-04:00)

Log file SSE-KMS encryption
Not enabled

Edit

CloudWatch Logs

Log group
infinitly-prod-cloudtrail-logs

IAM Role
arn:aws:iam::992382705250:role/cloudtrail-log-role

Edit