

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.

Security recommendations 0

✓ Root user has MFA
Having multi-factor authentication (MFA) for the root user improves security for this account.

✓ Root user has no active access keys

AWS Account
Account ID
058264350511
Account Alias
autohall [Edit](#) | [Delete](#)

Using CloudTrail for user event logging:

cloudtrail Delete Stop logging

General details Edit

Trail logging ✓ Logging	Trail log location aws-cloudtrail-logs-330662919014-dbd2474b/AWSLogs/o-yu2zjqhqb/058264350511	Log file validation Enabled	SNS notification delivery Disabled
Trail name cloudtrail	Last log file delivered April 16, 2025, 16:21:14 (UTC+02:00)	Last file validation delivered April 16, 2025, 15:52:44 (UTC+02:00)	Last SNS notification -
Multi-region trail Yes	Log file SSE-KMS encryption Not enabled		
Apply trail to my organization Enabled for all accounts			

Depending on the user access permission configuration, we present best practices for maintaining user identity security. We maintain the minimum required roles or permissions, setting temporary credentials where applicable for accessing IAM roles. Each Partner administrator user must have dedicated credentials.

For our access to management console we use IAM Identity Center with the principles of least privilege

The customer does not have access to the AWS Account, we manage the account for them

Autohall

Overview

Account name
Autohall

Users and groups (1)

Permission sets (1)

Assigned users and groups (1)

The following users and groups in IAM Identity Center can select this AWS acc

Find users by username, find groups by group name

Username / group name

☐ [Administradores](#)

Based on the methodology and design of the solution, Access management using IAM groups:

- IAM groups aligned with specific roles (e.g., Developers, Administrators, Auditors) were created.
- Each group was associated with IAM policies that follow the principle of least privilege, granting only the necessary permissions for each function.
- Avoided the use of wildcards (*) in policies, using specific actions and resources instead.

Dedicated credentials:

- Each AWS Partner user received unique and personal credentials.
- The use of shared accounts has been disabled to ensure the traceability of actions.

Use of temporary credentials:

- For administrative or support tasks, IAM roles with limited duration have been configured.
- Users temporarily assumed these roles using the console or CLI, using AWS STS (Security Token Service).

Identity Federation:

- Integrated the customer's corporate identity system with AWS using SAML 2.0.
- This allowed users to authenticate with their enterprise credentials and assume roles in AWS without the need to manage multiple passwords.

Additional controls:

- Enabled MFA (Multi-Factor Authentication) for all console accesses.



- CloudTrail and AWS Config alerts have been implemented to detect unauthorized changes to IAM policies.

Results:

- Reduced risk of unauthorized access.
- Improvement in traceability and auditing of access.
- Compliance with internal security policies and regulatory requirements.