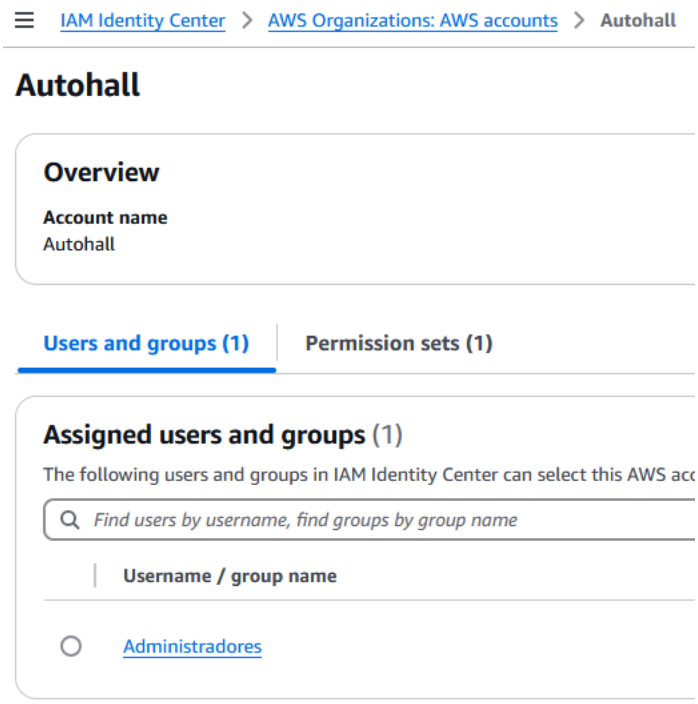
ACCT-002 - Define identity security best practice on how to access customer environment by leveraging IAM

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



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.

Grant least privileges

IAM users are defined and classified into groups based on the role or activities they can run in the console for the management and operation of current Autohall workloads.