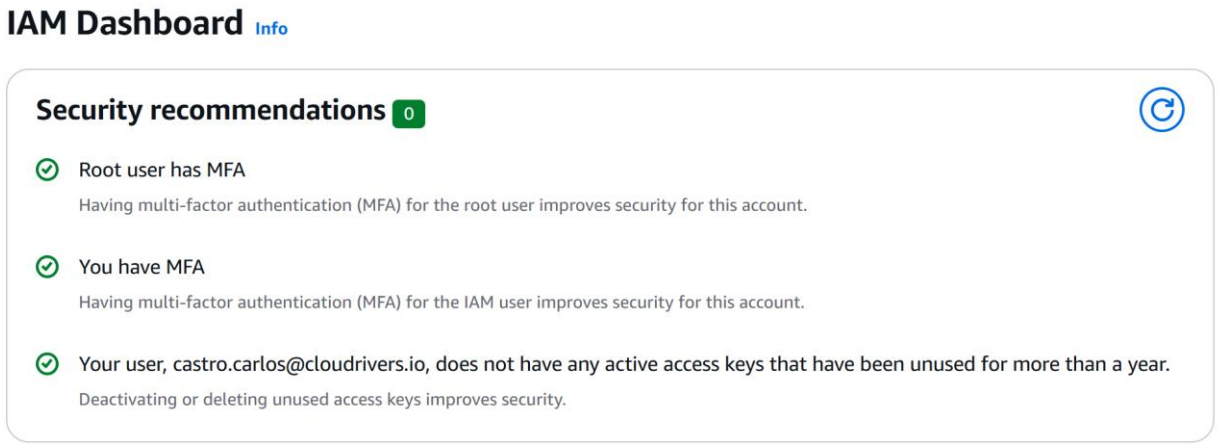
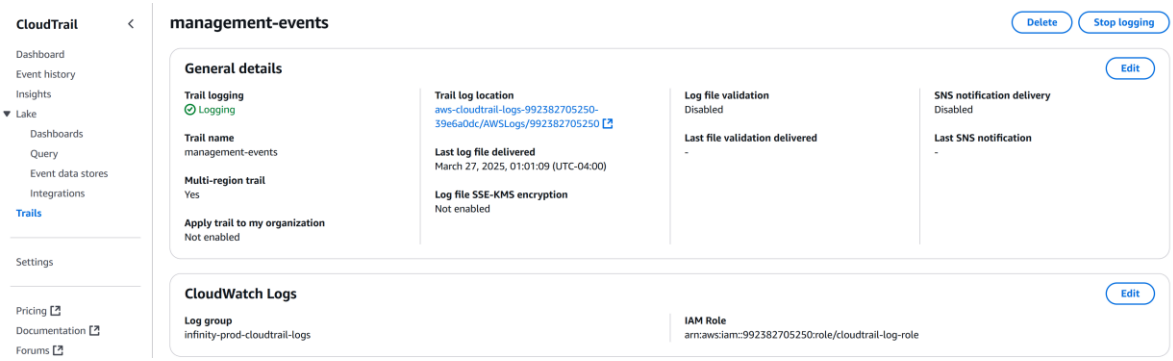
The root user is secured

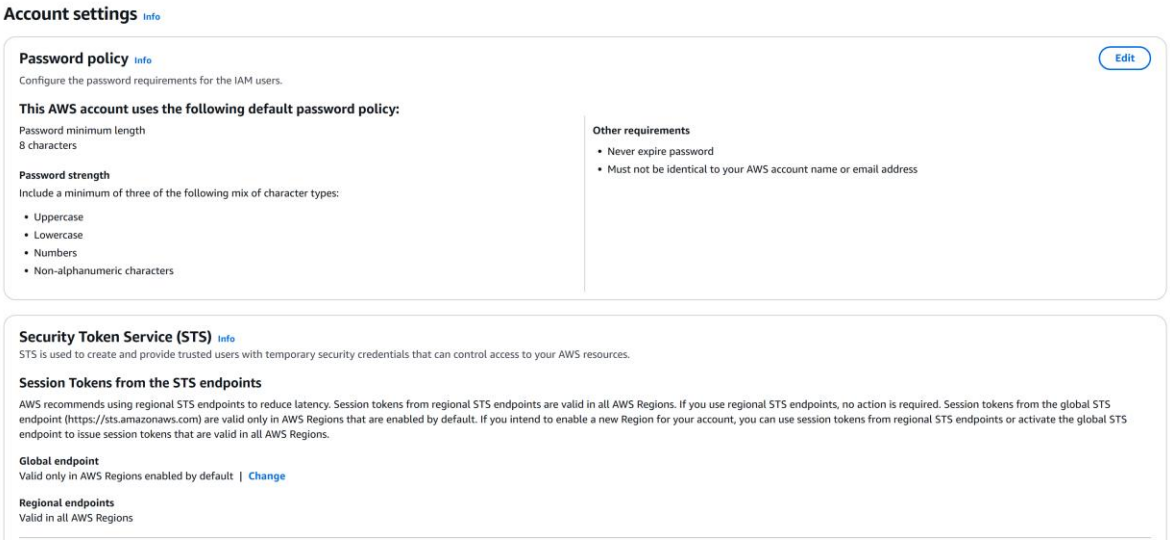
The Root user has the administrative roles, with MFA settings active. Users with access to Customer's AWS portal have minimum access roles, read Only. The CloudTrail application is used to monitor user activities.



Using CloudTrail for user event logging:



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.



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 Seguros Patria workloads.

This definition is done similarly to the on-premises environment, although the use of IAM policies achieves greater control over the assigned privileges.

Based on the methodology and design of the solution, security groups are defined in such a way as to allow traffic only to and from where it belongs.

Considerations:

The entire implemented environment needed a Landing Zone, here we define the VPC to be used and the security groups that will allow us to define the accesses and restrictions of incoming-outgoing traffic. To show a better detail, check the documentation of the network area.

Security groups and access allowed or denied to specific ports on the Infinity Gifts Souvenirs platform.