

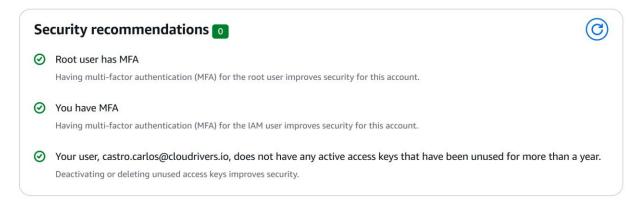


SEC-002 - Prevention of Public Access of Cloud Resources

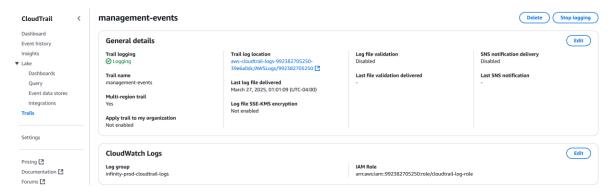
The root user is secured

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.

IAM Dashboard Info



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.





Password policy time Configure the password requirements for the IAM users. This AWS account uses the following default password policy: Password minimum length 8 characters Password strength Include a minimum of three of the following mix of character types: Uppercase Nom-alphanumeric characters Security Token Service (STS) Info STS is used to create and provide trusted users with temporary security credentials that can control access to your AWS resources. Session Tokens from the STS endpoints AWS recommends using regional STS endpoints to reduce latency. Session tokens from regional STS endpoints are valid in all AWS Regions in the are valid in all AWS Regions on action is required. Session tokens from regional STS endpoints or activate the global STS endpoint to issue session tokens that are valid in all AWS Regions enabled by default. If you intend to enable a new Region for your account, you can use session tokens from regional STS endpoints or activate the global STS endpoint to issue session tokens that are valid in all AWS Regions enabled by default. | Change Regional endpoints Valid in all AWS Regions

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.

