

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](#)

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
Forums

management-events

Delete

Stop logging

General details

Trail logging
Logging

Trail name
management-events

Multi-region trail
Yes

Apply trail to my organization
Not enabled

Trail log location
aws-cloudtrail-logs-992382705250-39e6a0dc/AWSLogs/992382705250

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

Log file SSE-KMS encryption
Not enabled

Log file validation
Disabled

Last file validation delivered
-

SNS notification delivery
Disabled

Last SNS notification
-

CloudWatch Logs

Log group
infinity-prod-cloudtrail-logs

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

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.

Account settings [Info](#)Password policy [Info](#)

Configure the password requirements for the IAM users.

[Edit](#)

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
- Lowercase
- Numbers
- Non-alphanumeric characters

Other requirements

- Never expire password
- Must not be identical to your AWS account name or email address

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. If you use regional STS endpoints, no action is required. Session tokens from the global STS endpoint (<https://sts.amazonaws.com>) are valid only in AWS Regions that are 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.

Global endpoint

Valid only in 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.

Security Groups (5) [Info](#)[Actions](#)[Export security groups to CSV](#)[Create security group](#)

< 1 >

<input type="checkbox"/>	Name	Security group ID	Security group name	VPC ID	Description
<input type="checkbox"/>	-	sg-0e4b0ff336395e4a3	default	vpc-0c3362d734f51cc6c	default VPC security group
<input type="checkbox"/>	-	sg-0f7812c9e7acb6c93	infinity-hana-subnet-sg	vpc-0c3362d734f51cc6c	HANA SG
<input type="checkbox"/>	-	sg-082498cd447b0f2e7	infinity-app-subnet-sg	vpc-0c3362d734f51cc6c	SAP APP SG
<input type="checkbox"/>	-	sg-075438b7b0122971f	infinity-ad-subnet-sg	vpc-0c3362d734f51cc6c	infinity-ad-subnet-sg
<input type="checkbox"/>	-	sg-0d134c0571f427cea	infinity-public-subnet-sg	vpc-0c3362d734f51cc6c	infinity-public-subnet-sg