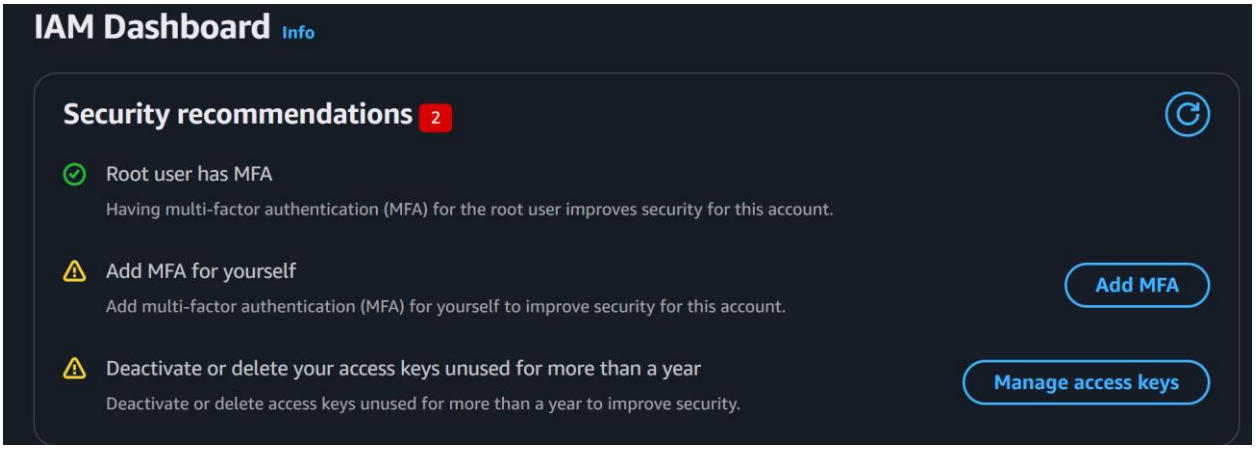
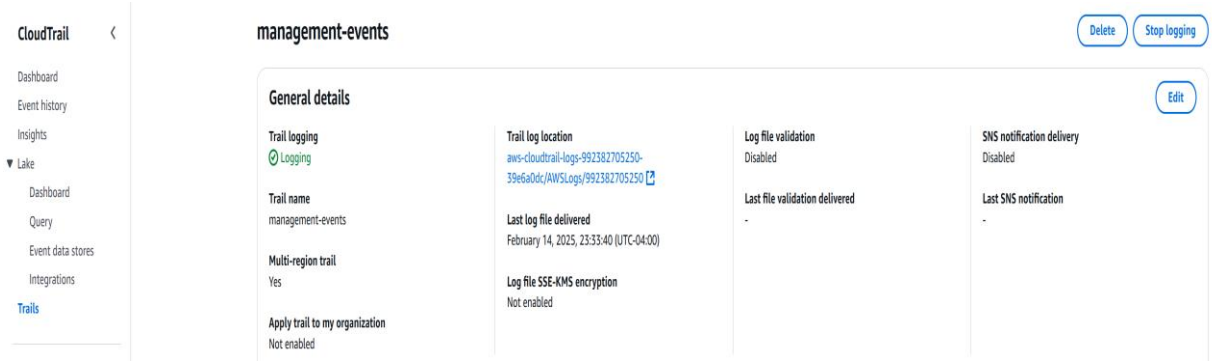
SEC-002 - Prevention of Public Access of Cloud Resources

The root user is secured

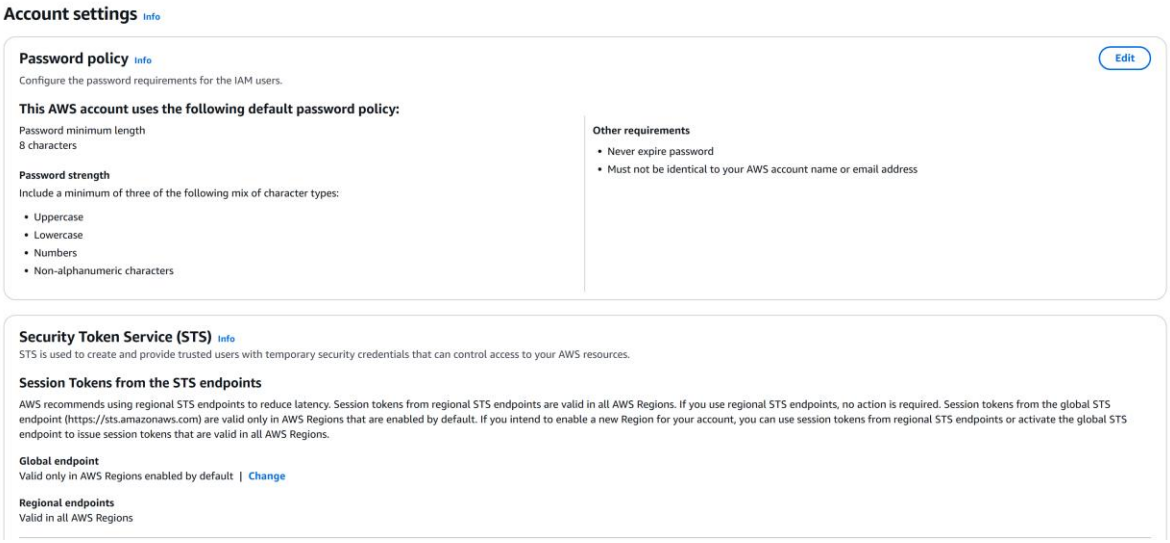
The Root user has administrative roles, with MFA enabled. Users with access to the Customer's AWS portal have minimal access roles: read only. The CloudTrail application is used to monitor user activity.



Using CloudTrail for user event logging:



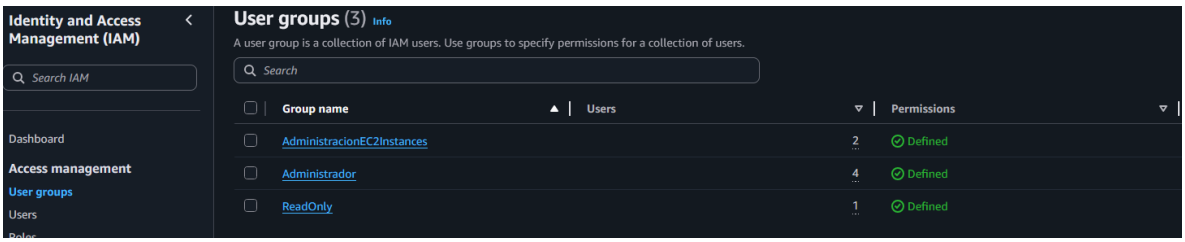
Depending on the user access permission configuration, we present best practices for maintaining user identity security. We maintain the minimum required roles or permissions, setting temporary credentials where applicable for accessing IAM roles. Each Partner administrator user must have dedicated credentials.



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.

Implementation of user groups for assigning permissions.



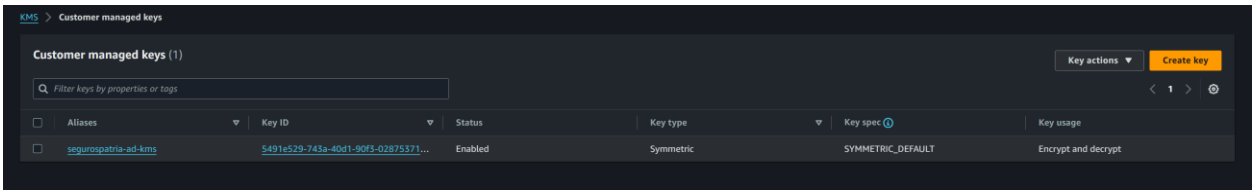
Based on the methodology and design of the solution, security groups are defined in such a way as to allow traffic only to and from where it belongs.

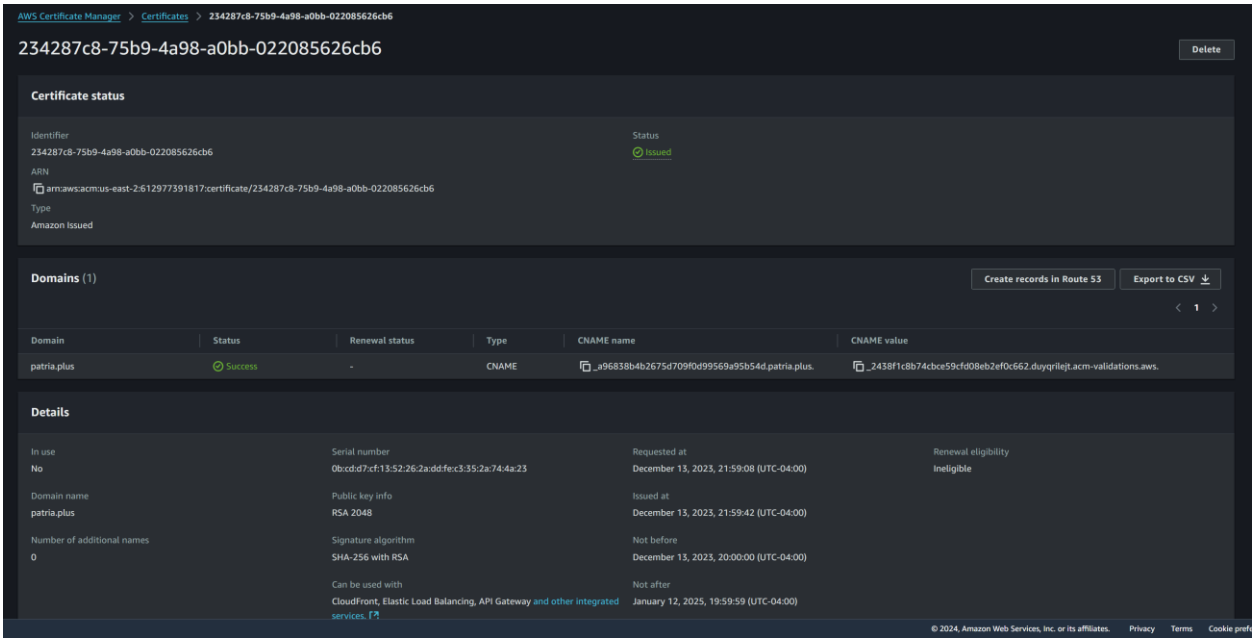
Considerations:

The entire implemented environment required a Landing Zone. Here we defined the VPC to be used and the security groups that would allow us to define access and restrictions for incoming and outgoing traffic. For more details, please review the networking documentation.

Security groups and permitted or denied access to specific ports on the Seguros Patria platform.

The Directory services are implemented using certificates issued by the Certificate Manager service are associated. The Organization using Customer manager Keys.





Data stores are in private subnets.

Cryptographic keys are managed securely

Encryption keys are controlled by the client.