

Seguridad

Seguridad de la cuenta AWS

AWS Security Hub

Proporciona una visión completa de su estado de seguridad en AWS y lo ayuda a comprobar su entorno con las prácticas recomendadas y los estándares del sector de seguridad. Security Hub recopila datos de seguridad de todas las cuentas de AWS, de los servicios y de los productos de terceros compatibles y le ayuda a analizar sus tendencias de seguridad y a identificar los problemas de seguridad de mayor prioridad.

Status 27/11/2023 Security Score

77%

IAM Access Analyzer

Ayuda a identificar los recursos de su organización y sus cuentas, como buckets de Amazon S3 o roles de IAM, que se comparten con una entidad externa. Esto le permite identificar el acceso no deseado a sus recursos y datos, lo que constituye un riesgo para la seguridad

Status Por implementar

Seguridad de los Usuarios y Accesos

Toda la seguridad se maneja con Grupos, Roles y Políticas de AWS IAM.

Todas las cuentas tiene configurado el MFA

- Cuentas de Desarrolladores 2 cuentas
 - Se crearon políticas y permisos específicos de acceso a los servicios y recursos para un desarrollador recursos para un desarrollador.
 - Servicios
 - S3 (Lectura)
 - Lambda (Lectura)
 - Amplify (Lectura)
 - RDS (Lectura)
 - API Gateway (Lectura)
 - Cognito (Lectura, Creación Usuarios)
- Cuenta Administración 1 cuenta
 - Se creó una cuenta administración con políticas de escritura específicas para los siguientes servicios

- Lambda (Lectura)
- API Gateway (Lectura)
- IAM (Administración de Usuarios)
- S3 (Lectura, Creación de Buckets)
- Amplify (Lectura, Creación de Apps)
- RDS (Lectura, Creación de DB)
- Cognito (Lectura, Creación de Pools y usuarios)

- Cuenta de Deployment 1 cuenta
 - Se creo un usuario con políticas específicas para hacer deployment desde github actions.
- Cuenta ROOT, acceso con MFA Virtual 1 cuenta

Seguridad de la API

Acceso mediante Autenticación de Cognito Implementada

El acceso a la API tiene un sistema de permisología basado en roles (Lend2B, Client, Provider, Lender, Cuenta Ancla) para esto se implemento un control de acceso a la API usando Cognito User Pools. Este servicio provee una interfaz donde se pueden crear, modificar y eliminar usuarios, ademas de las funciones de login y cambio de contraseña usando un [sistema de Tokens](#)

Acceso mediante API KEY Pendiente

Este tipo de acceso se tiene planificado crear para los usuarios de la API como servicio. Ejemplo API REST para que la consuma ABL

Seguridad de los archivos

Seguridad de permisología de S3

En proceso

Seguridad de la Base de Datos

EL acceso a la Base de Datos, solo es permitida desde VPC security groups, donde las Lambdas la pueden consultar. EL resto de puertos y accesos estan restringidos.

Encriptación de Datos

En proceso

Seguridad de la aplicación y código

Desarrollo

Usando el plugin [Serverless Offline](#) y Docker se despliega localmente un ambiente de trabajo completo para cada desarrollador.

API RSET

La Documentación de la API REST se maneja con Postman.

La API REST se maneja con [Postman](#) en el plan Basic con 3 usuarios, donde se gestiona un Workspace privado para la gestión de la documentación y pruebas de las API que se tienen disponibles.

Serverless Framework

Blog post de medidas de seguridad que tiene Serverless Framework en la capa de desarrollo y despliegue

Github Workflows

Para hacer el deploy se usa AWS Credentials **aws-access-key-id/aws-secret-access-key**
<https://github.com/aws-actions/configure-aws-credentials>

Se usan [Github Secrets](#) para almacenar la información de autenticación que se usa para hacer el despliegue de la solución.

OpenID En Proceso

Se planea cambiar la autenticación a OpenID

<https://docs.github.com/en/actions/deployment/security-hardening-your-deployments/configuring-openid-connect-in-amazon-web-services>

--

Recomendaciones de seguridad de AWS

<https://docs.aws.amazon.com/prescriptive-guidance/latest/aws-startup-security-baseline/welcome.html>

IAM Access Analyzer

https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/what-is-access-analyzer.html