COLOMBIA POTENCIA DE LA VIDA

TIC

LECCIÓN 5: PRÁCTICAS RECOMENDADAS PARA LA PROTECCIÓN DE DATOS Y SERVICIOS ADICIONALES EN AMAZON S3

TALENTO TECH | AZ PROYECTOS EDUCATIVOS | UTP Universidad Tecnológica de Pereira

URL PREFIRMADAS

- Genere una URL prefirmada de S3 y utilícela para cargar archivos (objetos).

- Una URL prefirmada utiliza tres parámetros para limitar el acceso de los usuarios:

Bucket: bucket en el que está el objeto (o lo estará).

Key: nombre del objeto

Expires: periodo de validez de la URL.

De forma predeterminada, todos los objetos en un bucket de S3 son privados. Solo el propietario del objeto tiene permisos para acceder a estos objetos. Sin embargo, el propietario del objeto tiene la opción de compartir objetos con otros mediante la creación de una URL prefirmada, utilizando sus propias credenciales de seguridad, a fin de otorgar permisos por tiempo limitado para cargar o descargar los objetos.

Una URL prefirmada brinda acceso temporal a un objeto de S3 específico. Al usar la URL, un usuario puede leer, escribir o actualizar el objeto. Por ejemplo, si tiene un video en su bucket y tanto el bucket como el video son privados, puede compartir el video con otros usuarios al generar una URL prefirmada.

De manera similar, si desea recibir un objeto de un usuario sin una cuenta de AWS, puede cargar un objeto con una URL prefirmada que comparte con él.

Para más información, consulte “Generating a Presigned URL to Upload an Object (Generación de una URL prefirmada para cargar un objeto)” en la Guía del usuario de Amazon Simple Storage Service en https://docs.aws.amazon.com/AmazonS3/latest/userguide/PresignedUrlUploadObject.html

CONSIDERACIONES DE SEGURIDAD Y PRÁCTICAS RECOMENDADAS (1 DE 2)

- Considere el cifrado de datos en reposo y aplique el cifrado de datos en tránsito.

- Asegúrese de que sus buckets de S3 usen las políticas correctas y no sean de acceso público.

- Utilice el principio de mínimo privilegio.

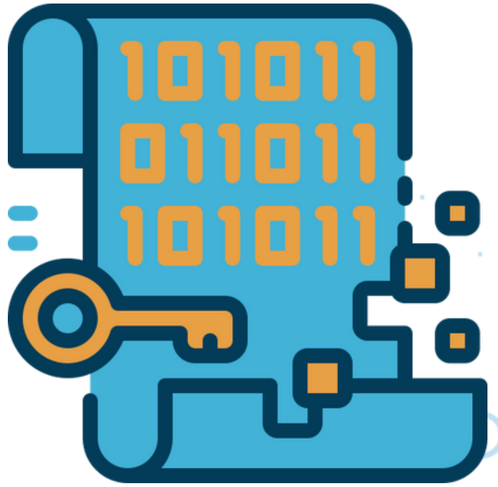
- Habilite la eliminación con MFA para los buckets.

- Aplique el cifrado para cada solicitud PUT.

- Utilice URL prefirmadas para aplicaciones que se refieran a objetos de Amazon S3.

PARA ASEGURARSE DE OFRECER EL EQUILIBRIO ADECUADO ENTRE SEGURIDAD Y FLEXIBILIDAD OPERATIVA, AWS SUGIERE REALIZAR LAS SIGUIENTES PRÁCTICAS RECOMENDADAS AL USAR AMAZON S3:

Utilice el cifrado como un control de acceso adicional para complementar los controles de acceso orientados a la identidad, los recursos y la red ya descritos. AWS ofrece una serie de funciones que pueden ayudarlo a cifrar datos y administrar claves fácilmente. Todos los servicios de AWS ofrecen la capacidad de cifrar datos en reposo y en tránsito.



COLOMBIA POTENCIA DE LA VIDA

TIC

Utilice políticas de bucket junto con políticas de IAM para proteger los recursos del acceso no autorizado y evitar la divulgación de información, el peligro para la integridad de los datos o la eliminación.

Establezca políticas de bucket y de IAM con los privilegios mínimos. Por ejemplo, si se espera que una aplicación cargue objetos, el rol de IAM correspondiente no debería tener permisos de lectura para el objeto ni ningún otro permiso.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Active la eliminación con MFA para buckets habilitados para el control de versiones a fin de asegurarse de que los archivos no se puedan eliminar ni alterar.

Aplique el SSE para cada solicitud PUT. Esto daría lugar a una denegación en los casos en que el usuario final no solicite el SSE.

Use direcciones URL prefirmadas para aplicaciones que se refieren a objetos de S3 con acceso anónimo; por ejemplo, la descarga de contenido restringido. La autenticación y la autorización deben realizarse en la aplicación.

CONSIDERACIONES DE SEGURIDAD Y PRÁCTICAS RECOMENDADAS (2 DE 2)

Para cifrar todos los objetos, establezca el cifrado predeterminado en un bucket.

Si utiliza Object Lock de S3, use el modo de retención apropiado.

Use Block Public Access de S3.

Cargue datos en Amazon S3 con el protocolo de transferencia de archivos SSH (SFTP) a través de AWS Transfer para SFTP

Habilite el control de versiones de S3

COLOMBIA POTENCIA DE LA VIDA

TIC

LAS SIGUIENTES SON PRÁCTICAS RECOMENDADAS ADICIONALES PARA EL USO DE AMAZON S3:

Establezca el cifrado predeterminado en un bucket si desea que todos los objetos se cifren una vez que estén almacenados en el bucket.

TALENTO TECH

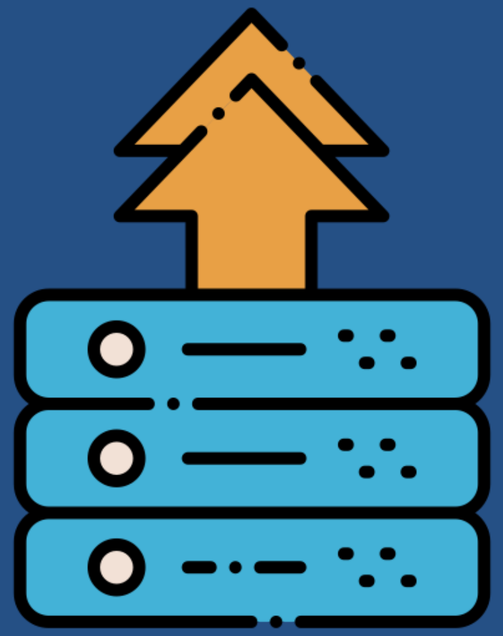
AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

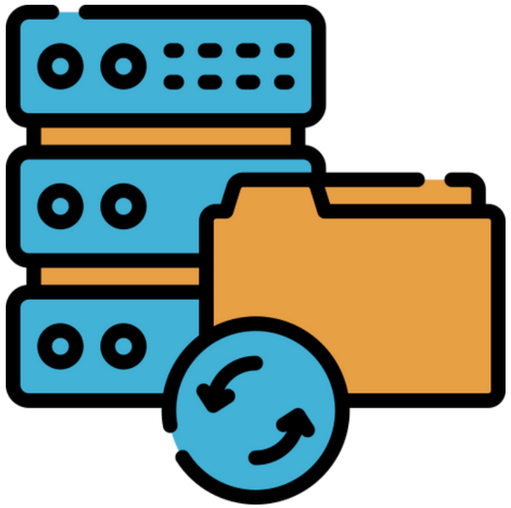
Mientras usa Object Lock de S3, utilice el modo de retención apropiado (modo de gobernanza o modo de cumplimiento). Estos modos de retención aplican diferentes niveles de protección a los objetos. Puede aplicar cualquier modo de retención a cualquier versión del objeto protegida por Object Lock de S3.

Utilice la configuración de Block Public Access de S3 para establecer que los buckets no permitan el acceso público a los datos.

Cargue datos en Amazon S3 con el protocolo de transferencia de archivos SSH (SFTP) con AWS Transfer para SFTP. Este servicio completamente administrado proporciona transferencia de archivos a través de SFTP directamente dentro y fuera de Amazon S3. El uso de este servicio elimina la necesidad de administrar la infraestructura relacionada con el SFTP. Con los datos en Amazon S3, puede integrarlos fácilmente en cargas de trabajo que utilizan una amplia gama de servicios de AWS.



Utilice el control de versiones de S3 para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de S3.



COLOMBIA POTENCIA DE LA VIDA

TIC

SERVICIOS ADICIONALES QUE PUEDEN AYUDARLO A PROTEGER SUS DATOS.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

AWS SECRETS MANAGER

Es un método seguro y escalable para administrar el acceso a los datos confidenciales.

Ofrece una manera de satisfacer los requisitos normativos y de cumplimiento.

Rota los datos confidenciales de manera segura sin desglosar las aplicaciones.

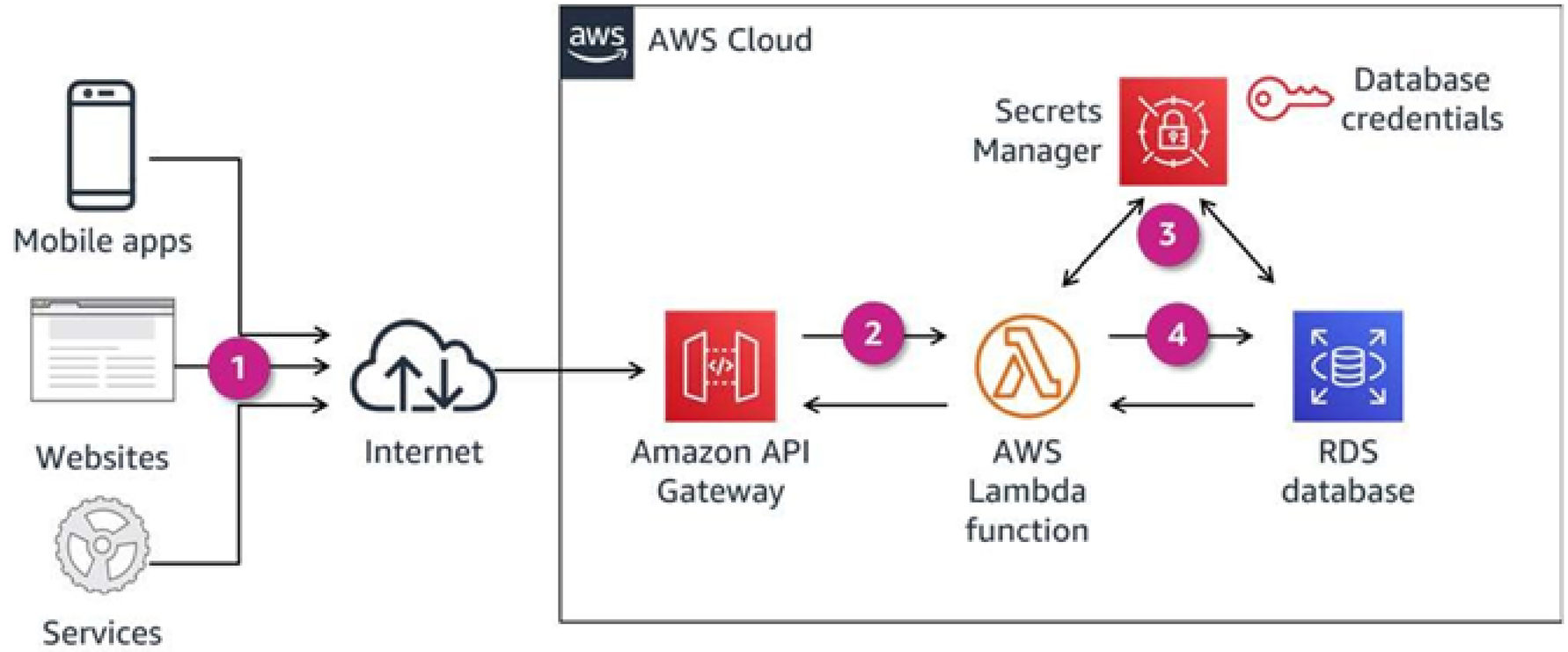
Audita y supervisa el ciclo de vida de los datos confidenciales.

Lo ayuda a evitar poner los datos confidenciales en archivos de código o configuración.

AWS Secrets Manager es un servicio que simplifica la administración de datos confidenciales. Los datos confidenciales pueden ser credenciales de base de datos, contraseñas, claves de API de terceros e incluso texto arbitrario. Puede almacenar y controlar el acceso a estos datos confidenciales de forma centralizada con la consola, la CLI de AWS o la API y los SDK.

Con Secrets Manager, puede eliminar las credenciales codificadas de forma rígida (incluidas las contraseñas) de su código fuente y evitar almacenar las credenciales en un archivo de configuración. En su lugar, utiliza una llamada API a Secrets Manager para recuperar el dato confidencial mediante programación. Esto ayuda a garantizar que los datos confidenciales no puedan ser vulnerados si alguien examina el código, ya que simplemente no están ahí. Además, puede configurar Secrets Manager de forma que rote los datos confidenciales automáticamente de acuerdo con la programación que especifique. Por lo tanto, puede reemplazar datos confidenciales a largo plazo por datos confidenciales a corto plazo, lo que ayuda a reducir significativamente el riesgo de que haya una vulneración.

USO DE SECRETS MANAGER



COLOMBIA POTENCIA DE LA VIDA

TIC

Este diagrama muestra cómo utilizar Secrets Manager para proteger las credenciales de base de datos. El enfoque utiliza una función de AWS Lambda, que a la vez usa credenciales de Secrets Manager para conectarse y consultar la base de datos de Amazon Relational Database Service (Amazon RDS) de backend. Esto se hace sin codificar de forma rígida los datos confidenciales en el código ni pasarlos a través de variables de entorno. Este enfoque ayuda a proteger los datos confidenciales de última milla y las bases de datos de backend.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

COLOMBIA POTENCIA DE LA VIDA

TIC

LOS PASOS DE ESTE FLUJO DE TRABAJO SE DESCRIBEN A CONTINUACIÓN:

LOS CLIENTES LLAMAN A LA API DE RESTFUL ALOJADA EN AMAZON API GATEWAY.

La API Gateway ejecuta la función de Lambda.

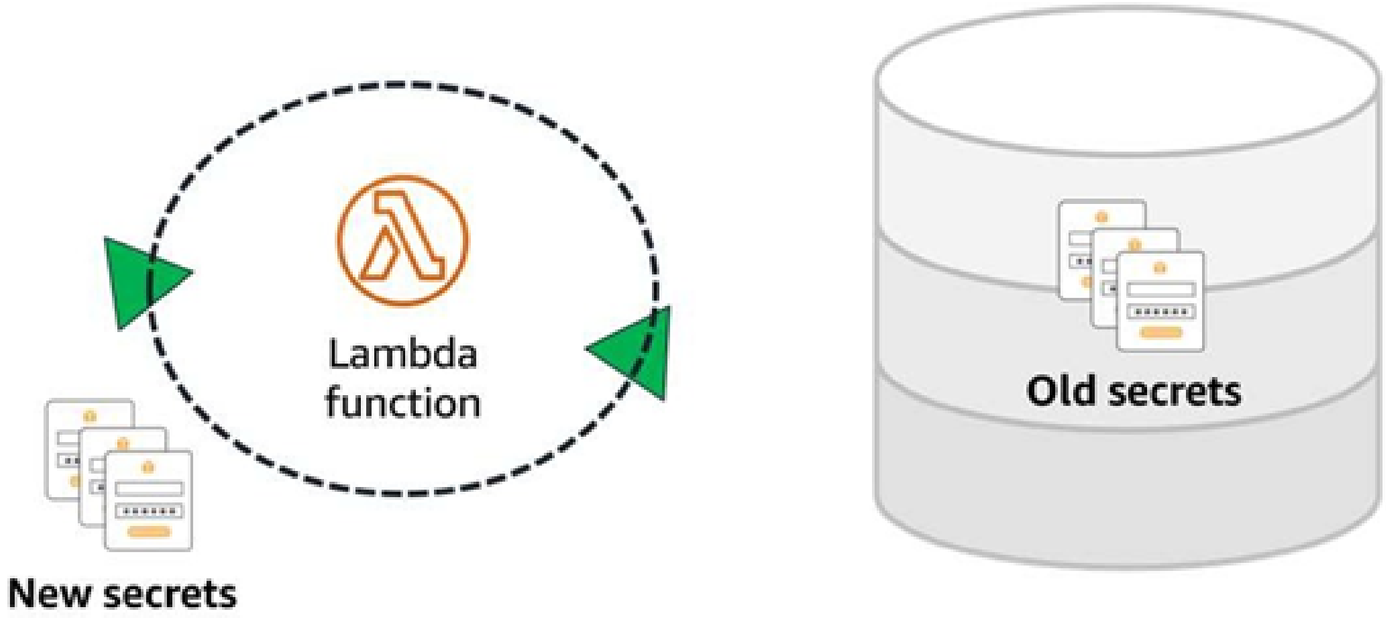
La función de Lambda recupera los datos confidenciales de la base de datos mediante la API de Secrets Manager. Secrets Manager recupera el dato confidencial, descifra el texto protegido del dato confidencial y lo devuelve a la función mediante un canal seguro.

La función de Lambda se conecta a la base de datos de Amazon RDS mediante datos confidenciales de base de datos de Secrets Manager y devuelve los resultados de la consulta.

Para obtener más información, consulte “How to Securely Provide Database Credentials to Lambda Functions by Using AWS Secrets Manager (Cómo brindar de forma segura las credenciales de base de datos a las funciones de Lambda mediante el uso de AWS Secrets Manager)” en el Blog de seguridad de AWS en

https://aws.amazon.com/blogs/security/how-to-securely-provide-database-credentials-to-lambda-functions-by- using-aws-secrets-manager.

ROTACIÓN DE DATOS CONFIDENCIALES



Built-in Lambda function for Amazon RDS DB engine credentials
Custom Lambda function for other credentials

Con Secrets Manager, puede rotar automáticamente las contraseñas de las bases de datos de Amazon Aurora, MySQL, MariaDB, PostgreSQL y Oracle alojadas en AWS. Para activar la rotación automática, necesita permisos de administrador. Esta rotación se realiza sin intervención humana mediante una función de Lambda, ya sea en un horario que usted especifique o según sea necesario. Para las credenciales del motor de base de datos de Amazon RDS, esta función de Lambda ya existe, pero si tiene otras credenciales con un vencimiento, como un usuario de SAML, es posible que desee crear una función personalizada para utilizarla con Secrets Manager.

La función de rotación realiza la tarea de rotar el secreto. El proceso para rotar un dato confidencial tiene cuatro pasos, que corresponden a cuatro pasos de la función de rotación de Lambda.

Secrets Manager usa etiquetas provisionales para etiquetar versiones de datos confidenciales durante la rotación:

La función se pone en contacto con la base de datos para obtener nuevas credenciales.

Secrets Manager almacena las credenciales nuevas con la etiqueta AWSPENDING.

Se prueban las nuevas credenciales.

Las nuevas credenciales se predeterminan con la etiqueta AWSCURRENT.

AMAZON MACIE

Reconoce la información confidencial, como la información de identificación personal (PII), la información financiera, las claves de cifrado y las credenciales.

- Admite tipos de datos personalizados.

- Protege los datos almacenados en Amazon S3 al supervisar las políticas de recursos y las ACL.

- Proporciona una cobertura API completa para la administración.

- Se integra en AWS Organizations.

Amazon Macie es un servicio de seguridad que utiliza el machine learning para descubrir, clasificar y proteger de forma automática la información confidencial en AWS. Macie reconoce la información de identificación personal (PII), como los números de pasaporte, de identificación médica y de identificación tributaria. Macie también reconoce información financiera, claves de cifrado y credenciales. Además, le brinda la posibilidad de agregar tipos de datos personalizados mediante expresiones regulares para permitir que Macie descubra información confidencial de propiedad o exclusiva para su negocio.

Actualmente, Macie protege los datos almacenados en Amazon S3 únicamente y está disponible en la mayoría de las regiones de AWS. Macie también cuenta con paneles y alertas que ofrecen visibilidad del acceso a los datos mediante el análisis de políticas basadas en recursos de Amazon S3 y ACL durante la recuperación de información confidencial. El servicio supervisa de forma continua los datos y genera alertas detalladas cuando detecta riesgo de acceso no autorizado o fugas de datos inadvertidas.

Con Macie, tiene el control total del servicio a través del conjunto de API de Macie y puede administrar Macie de forma centralizada para varias cuentas. Macie se integra con AWS Organizations, lo que significa que puede administrar hasta 5000 cuentas de Macie para una sola organización de AWS. También puede seguir usando las funciones nativas de Macie para administrar varias cuentas, lo que le permite administrar hasta 1000 cuentas de miembros con una sola cuenta de administrador de Macie.

CLASIFICACIÓN DE DATOS Y SUPERVISIÓN DE SUS PERMISOS DE ACCESO

- **Macie escanea y evalúa los objetos del bucket en busca de incumplimientos de políticas e información confidencial.**

- **Macie genera hallazgos en tiempo real para lo siguiente:**

BUCKETS QUE SON PÚBLICOS

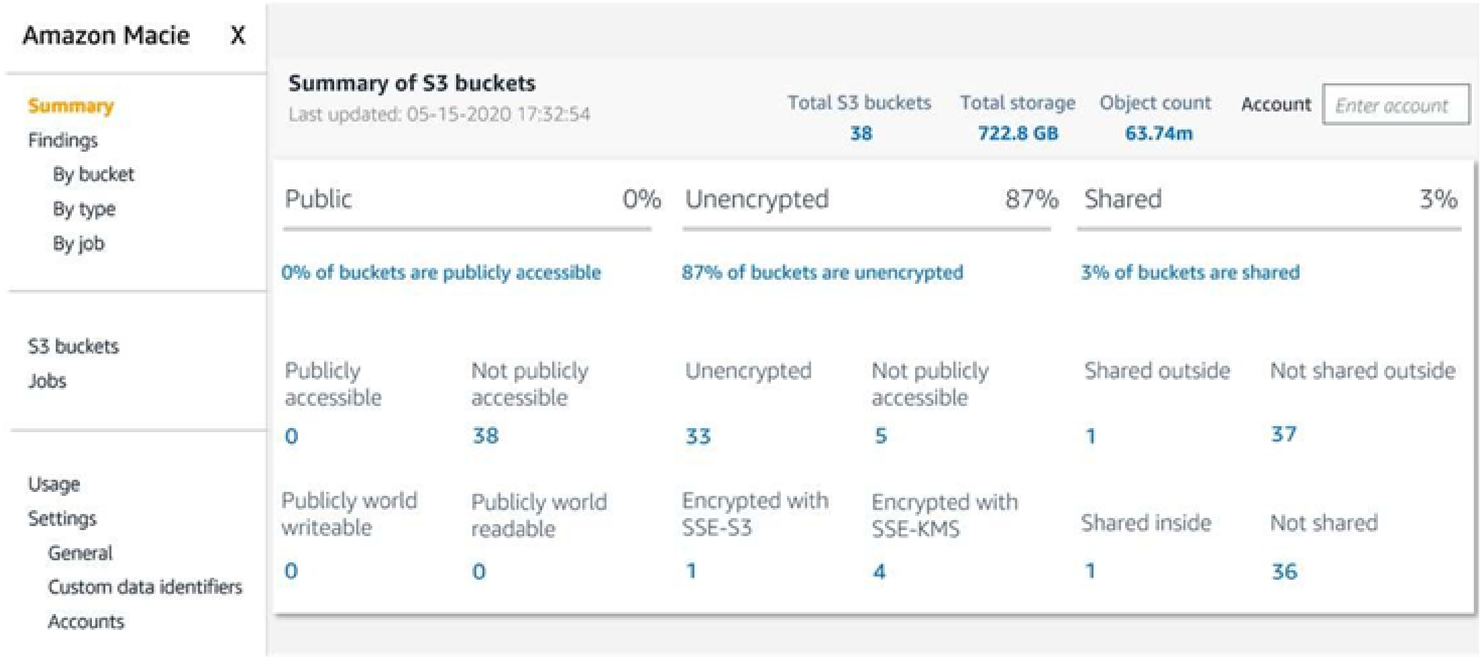
BUCKETS QUE NO ESTÁN CIFRADOS

BUCKETS COMPARTIDOS O REPLICADOS

Macie puede ayudarlo a clasificar sus datos confidenciales y críticos del negocio en el nivel del bucket de S3. Macie analiza todos los objetos compatibles encontrados y los evalúa en busca de información confidencial que cumpla con el criterio del trabajo. Puede configurar aún más estos trabajos de detección de información confidencial; por ejemplo, puede clasificar solo documentos PDF o todos los objetos excepto aquellos con un prefijo particular.

De forma predeterminada, Macie supervisará continuamente todos los buckets en cualquier cuenta en que esté activado. Los hallazgos se generan para cualquier bucket que sea público, no cifrado, compartido o replicado con cuentas de AWS fuera de la organización de un cliente. Estos resultados se informan casi en tiempo real.

RESUMEN DE MACIE



La página de resumen de Macie de la consola proporciona una descripción general de los buckets que han pasado por el proceso de detección de Macie. Como se mencionó, los buckets se supervisan para permitir el acceso público, no se cifran y se comparten o replican fuera de su cuenta.

HALLAZGOS DE MACIE

Showing 791 of 791 | 254 | 343 | 194

Findings

Actions

This table lists findings for your organization. Select a finding to show its details. You can also filter, group, and sort findings based on specific fields and field values.

Saved filters/Auto-archive

Current | Add filter criteria

Finding type	Resources affected	Updated at	Count
SensitiveData:S3Object/Financial	mybucket/123456789012/us-east-1/0a2eac77…jsonl.gz	5 minutes ago	1
SensitiveData:S3Object/Financial	mybucket /123456789012/us-east-1/123ec7e3…jsonl.gz	an hour ago	1
SensitiveData:S3Object/Financial	mybucket /123456789012/us-east-1/b42eac70…jsonl.gz	2 hours ago	1
SensitiveData:S3Object/Financial	mybucket /123456789012/us-east-1/0e11ac6a…jsonl.gz	3 hours ago	1
SensitiveData:S3Object/Financial	mybucket /123456789012/us-east-1/7ae54y00…jsonl.gz	4 hours ago	1
SensitiveData:S3Object/Credentials	mybucket /123456789012/us-east-1/z45w834…jsonl.gz	6 hours ago	1

Los trabajos de Macie analizan datos en buckets de S3 específicos en busca de información confidencial. Cada trabajo usa los identificadores de datos administrados que proporciona Macie y, opcionalmente, los identificadores de datos personalizados que usted crea.

El servicio brinda la capacidad de ejecutar trabajos únicos, diarios, semanales o mensuales de detección de información confidencial para todos o un subconjunto de objetos en un bucket de S3. Para los trabajos de detección de información confidencial, Macie realiza el seguimiento automático de los cambios al bucket y solo evalúa los objetos nuevos o modificados en el tiempo.