[Publish] - 2. Habilitar MFA Delete en el Bucket de CloudTrail

El hallazgo de seguridad **"Habilitar MFA Delete en el Bucket de CloudTrail"** apunta a un control de seguridad crítico diseñado para proteger la integridad de tus registros de auditoría en AWS. AWS CloudTrail registra cada llamada a la API realizada en tu cuenta, sirviendo como la fuente principal de verdad para saber "quién hizo qué y cuándo". Estos registros son indispensables para investigaciones de seguridad, respuesta a incidentes y auditorías de cumplimiento.

Un atacante que obtenga acceso administrativo podría intentar cubrir sus huellas eliminando estos registros. La función **MFA (Autenticación Multifactor) Delete** es una característica de seguridad para los buckets de S3 que proporciona una potente capa de protección contra esta amenaza. Cuando está habilitada, requiere un segundo factor de autenticación (un código de un dispositivo MFA) para eliminar permanentemente cualquier versión de un objeto, lo que hace significativamente más difícil que un atacante borre su actividad.

Análisis de los Recursos de CloudTrail Reportados

Los siguientes trails de CloudTrail están almacenando sus registros en buckets de S3 que no tienen habilitada la función de MFA Delete.

Nombre de CloudTrail	Número de Cuenta
trail/PRD_SA	398984081329
trail/Rackspace	005344269008
trail/Rackspace	174771279728
trail/Rackspace	498798756906
trail/Rackspace	613703092215
trail/Rackspace	890342916428
trail/Rackspace	996126991518
trail/ValesElectronicos	002670977573

Preguntas para tu Equipo (Acción Requerida)

Implementar este cambio requiere coordinación, ya que solo puede ser realizado por el **usuario raíz (root user)** de la cuenta de AWS.

1. **Identificar Acceso al Usuario Raíz:** ¿Han identificado a las personas que tienen acceso a las credenciales del usuario raíz y al dispositivo MFA asociado para cada una de las cuentas listadas?
2. **Programar el Cambio:** ¿Pueden programar un horario con los dueños del usuario raíz para realizar esta configuración de seguridad crítica? Debido a la sensibilidad del acceso raíz, esta acción debe ser planeada y documentada.

Consideraciones de Costo

Es importante entender la estructura de costos asociada con esta función.

- **Función MFA Delete:** No hay un **costo directo** por la función MFA Delete en sí.
- **Versionamiento de S3 (Prerrequisito):** MFA Delete requiere que el versionamiento del bucket de S3 esté habilitado. El versionamiento almacena todas las versiones de un objeto (incluyendo los marcadores de eliminación), lo que significa que tu uso de almacenamiento en S3 aumentará con el tiempo si no tienes una política de ciclo de vida de datos.
- **Almacenamiento en S3:** Se te facturará por el almacenamiento de todas las versiones de tus archivos de registro de CloudTrail.

Conclusión sobre Costos:

El aumento de costos por habilitar el versionamiento suele ser mínimo para los registros de CloudTrail, pero es un balance necesario por el inmenso valor de seguridad que aporta al proteger tu auditoría contra manipulación o eliminación. Es una buena práctica configurar una política de Ciclo de Vida de S3 (S3 Lifecycle policy) para mover las versiones más antiguas de los registros a niveles de almacenamiento más económicos (como S3 Glacier) para gestionar los costos de manera efectiva.

Cómo Solucionarlo: Habilitando MFA Delete

Esta configuración no se puede realizar a través de la consola estándar de AWS y **debe ser ejecutada usando la AWS CLI por el usuario raíz de la cuenta.**

Prerrequisitos:

- Acceso a las credenciales del **usuario raíz** para la cuenta de AWS.
- Un dispositivo **MFA** físico o virtual configurado para el usuario raíz.
- La **AWS CLI** instalada y configurada con las claves de acceso del usuario raíz.

Pasos:

1. **Identificar el Bucket de S3:** Primero, identifica el nombre exacto del bucket de S3 donde se entregan los registros de CloudTrail para cada trail. Puedes encontrar esto en la consola de

CloudTrail.

2. **Habilitar el Versionamiento:** Si aún no está habilitado, ejecuta el siguiente comando para habilitar el versionamiento en el bucket.

```
aws s3api put-bucket-versioning --bucket TU_BUCKET_DE_CLOUDTRAIL
--versioning-configuration Status=Enabled


```

3. **Habilitar MFA Delete:** Ejecuta el siguiente comando, reemplazando el nombre del bucket, el ARN del dispositivo MFA (o número de serie para un dispositivo de hardware) y el código MFA actual.

```
aws s3api put-bucket-versioning --bucket TU_BUCKET_DE_CLOUDTRAIL
--versioning-configuration Status=Enabled,MFADelete=Enabled
--mfa "arn:aws:iam::ID_DE_CUENTA:mfa/root-account-mfa-device 123456"


```

(Reemplaza `TU_BUCKET_DE_CLOUDTRAIL`*,* `ID_DE_CUENTA`*, el ARN y el código MFA* `123456` *con tus datos específicos.)*

4. **Repetir:** Este proceso debe repetirse para el bucket de CloudTrail en cada una de las cuentas identificadas.

Recomendación

Se recomienda que prioricen la habilitación de MFA Delete en los buckets de S3 para todos los trails de CloudTrail listados. La integridad de tus registros de CloudTrail es importante en tu postura de seguridad y cumplimiento. Esta acción proporciona una salvaguarda crítica contra la eliminación y manipulación no autorizadas.

Referencias

Configuring MFA delete - Amazon Simple Storage Service