Verificar acceso seguro y rotación de claves de depósito Umbrella S3 (obligatorio cada 90 días)

Contenido

Introducción

Este documento describe los pasos de rotación de las claves de depósito S3 como parte de las mejoras de las prácticas recomendadas y la seguridad de Cisco.

Antecedentes

Como parte de las mejoras en las prácticas recomendadas y la seguridad de Cisco, ahora es necesario que los administradores de Cisco Umbrella y Cisco Secure Access con depósitos S3 gestionados por Cisco para el almacenamiento de registros roten las claves IAM del depósito S3 cada 90 días. Anteriormente, no había ningún requisito de rotación de estas claves, que entró en vigor el 15 de mayo de 2025.

Aunque los datos de la cubeta pertenecen al administrador, la cubeta en sí es propiedad/está gestionada por Cisco. Para que los usuarios de Cisco cumplan con las prácticas recomendadas de seguridad, pedimos a Cisco Secure Access y Umbrella que roten sus claves al menos cada 90 días en el futuro. Esto ayuda a garantizar que nuestros usuarios no corran el riesgo de filtración de datos o divulgación de información y que se adhieran a nuestras prácticas recomendadas de seguridad como empresa de seguridad líder.

Esta restricción no se aplica a los depósitos S3 gestionados que no son de Cisco y le recomendamos que cambie a su propio depósito gestionado si esta restricción de seguridad le crea un problema.

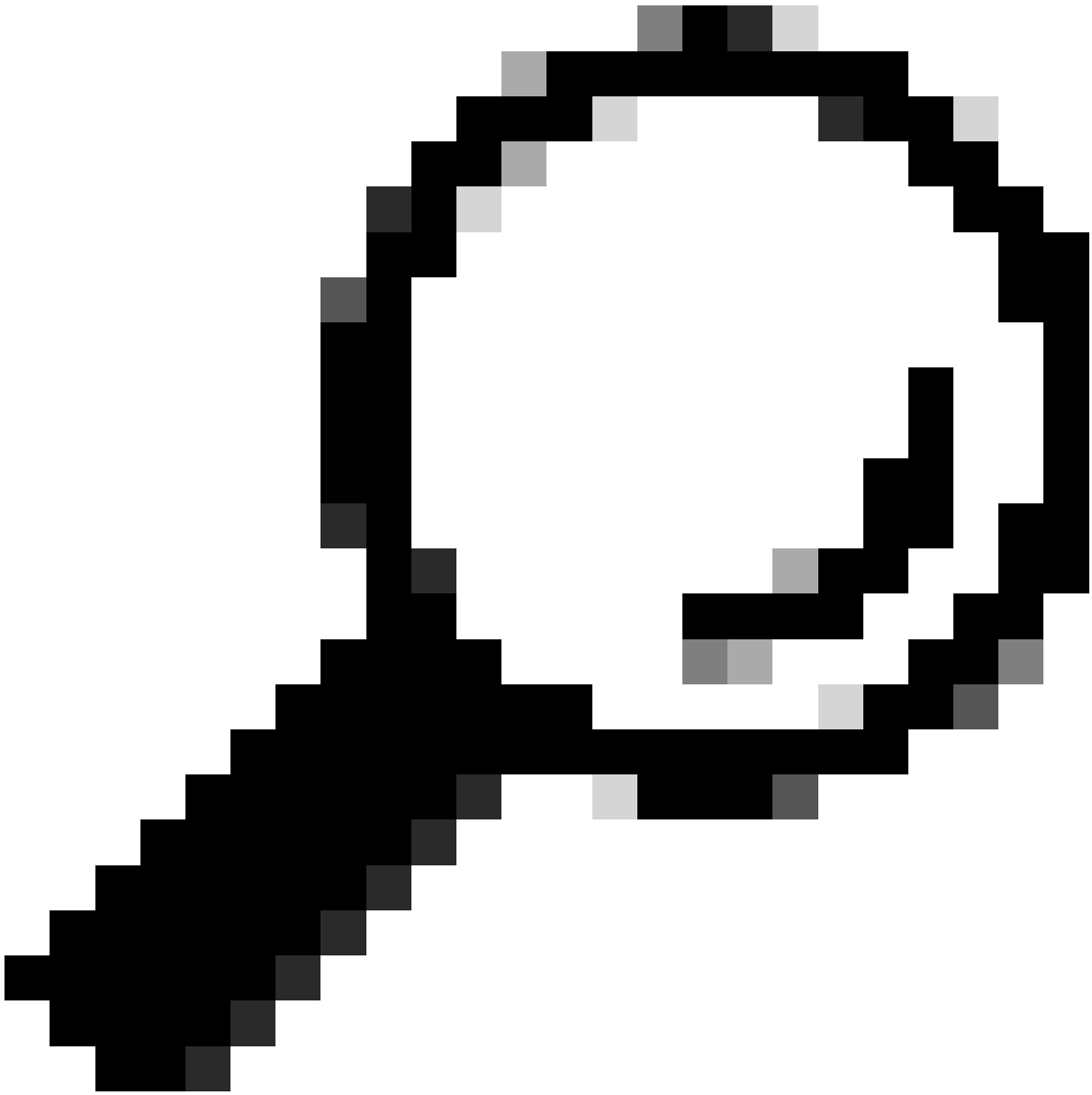
Problema

Los usuarios que no puedan rotar sus claves en 90 días ya no tendrán acceso a sus depósitos S3 gestionados por Cisco. Los datos de la cubeta se siguen actualizando con la información registrada, pero la cubeta en sí se vuelve inaccesible.

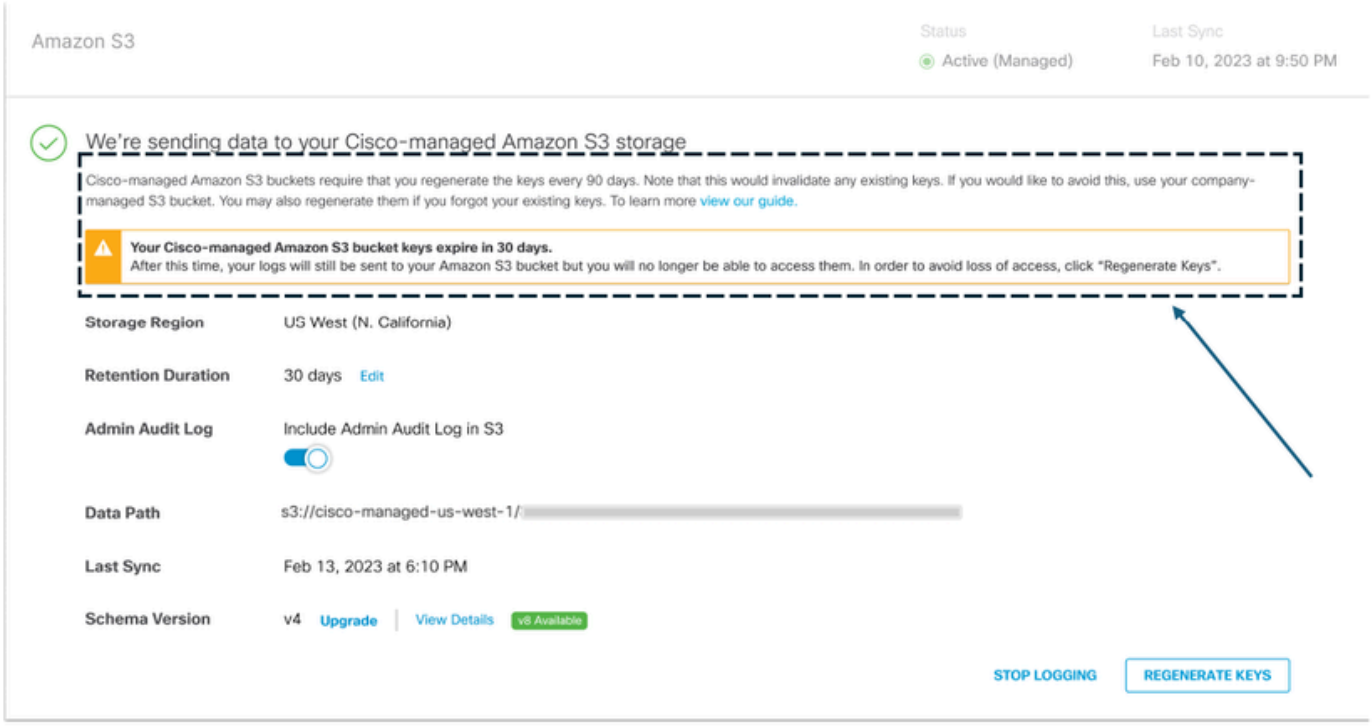
Solución

1. Navegue hasta Admin > Log Management y en el área Amazon S3 seleccione Use a Cisco-managed Amazon S3 bucket

---

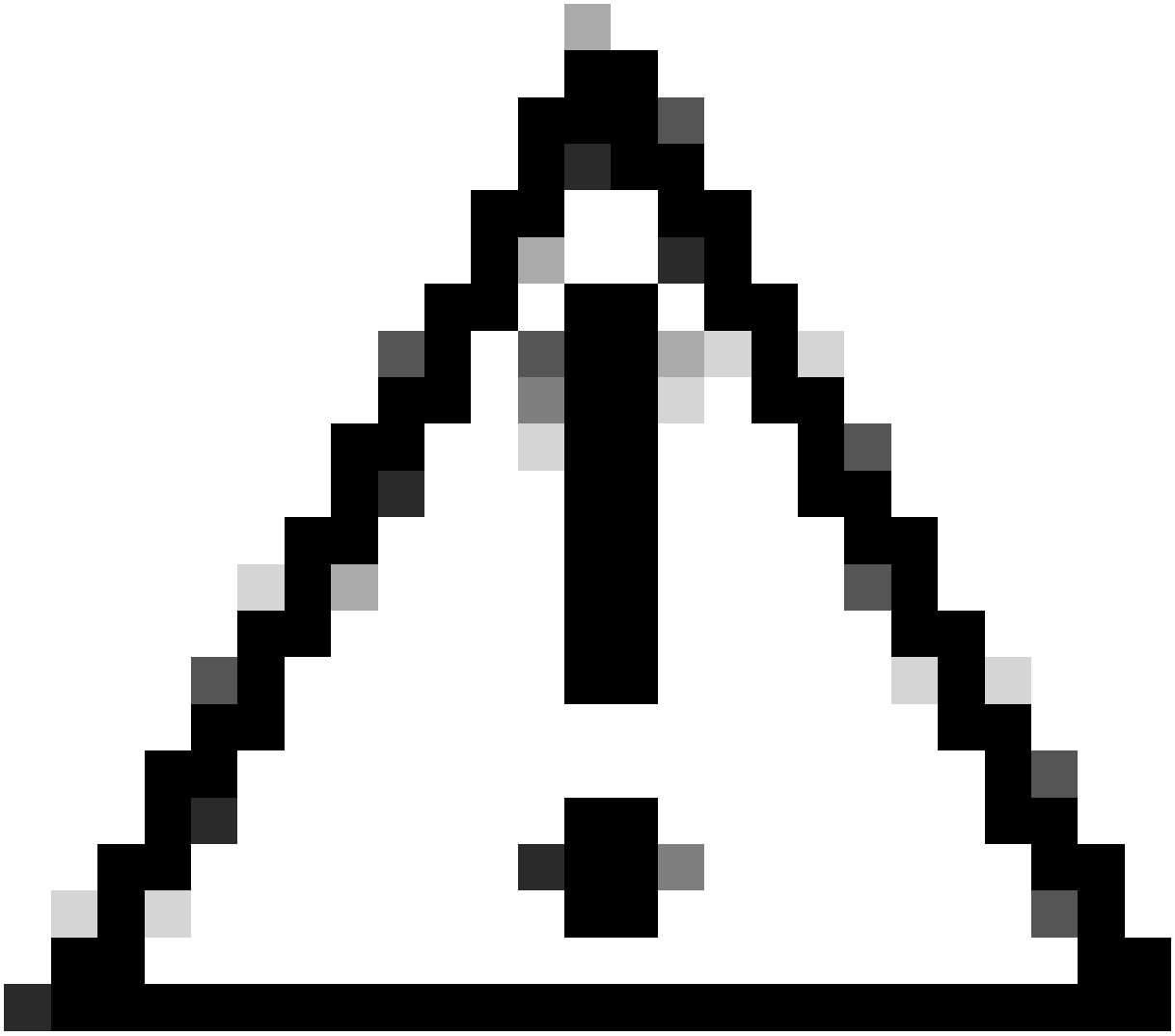


Consejo: El nuevo banner se presenta con un mensaje de advertencia con respecto a los nuevos requisitos de seguridad de la rotación de las claves de cubeta S3.

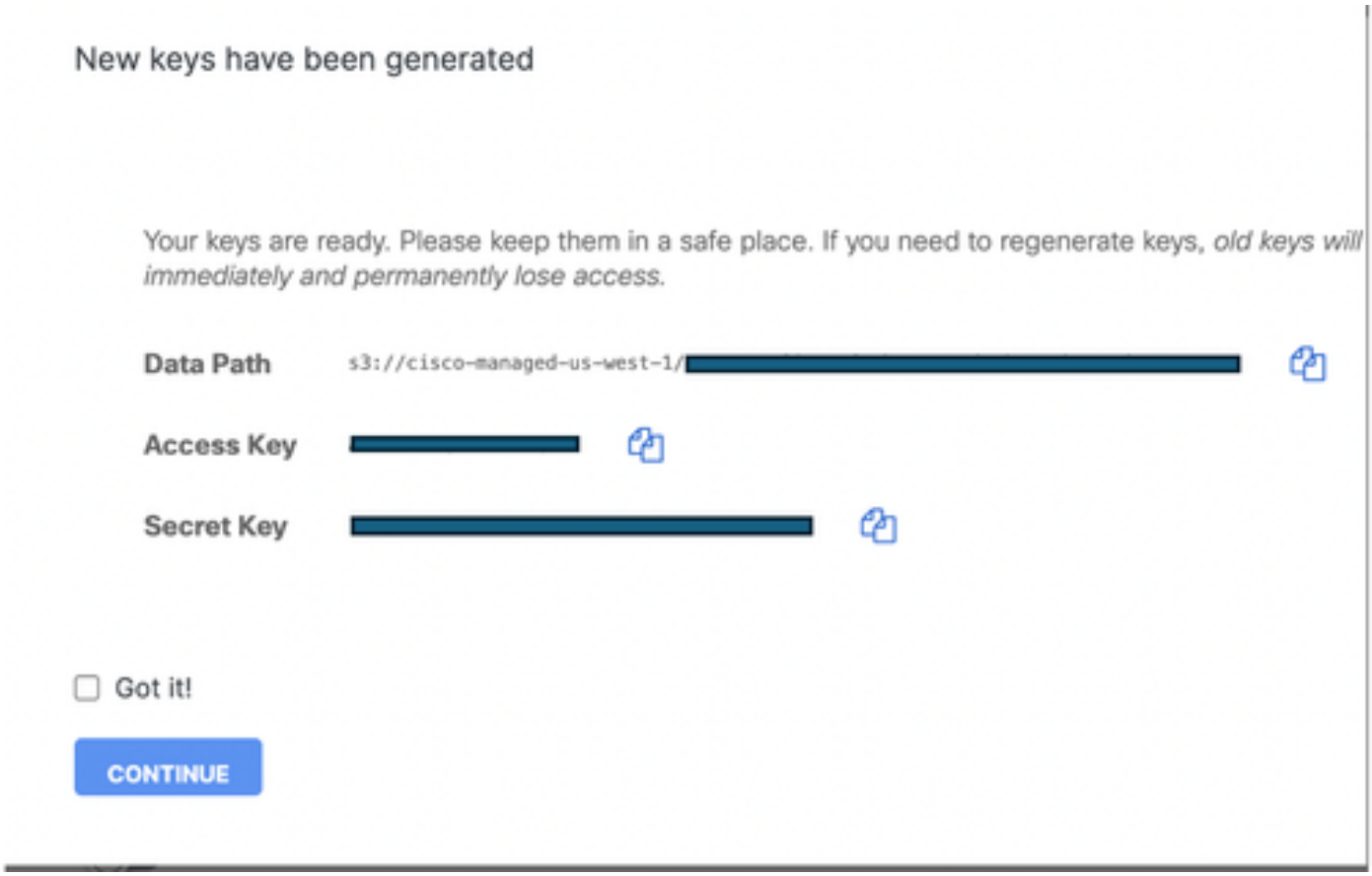


2. Genere las nuevas claves de depósito S3

3. Guarde la nueva clave en un lugar seguro.



Precaución: La clave y el secreto solo pueden mostrarse una vez y no son visibles para el equipo de soporte técnico de Cisco.



4. Actualice cualquier registro de ingesta de sistema externo de la cubeta S3 gestionada por Cisco con la nueva clave y el secreto.

Verificar El Acceso A La Cubeta S3

Para verificar el acceso a su cubo S3, puede utilizar el formato de archivos que se explica en este ejemplo o en la guía de documentación de Secure Access y Umbrella.

1. Configure la CLI de AWS con nuevas claves generadas.

```
$ aws configure
AWS Access Key ID [None]:


AWS Secret Access Key [None]:


Default region name [None]:


Default output format [None]:
```

2. Enumere uno de los logs guardados en su S3-Bucket.

```
$ aws s3 ls s3://cisco-managed-us-west-1/[org_id]_[s3-bucket-instance]/dnslogs
                           PRE dnslogs/
$ aws s3 ls s3://cisco-managed-us-west-1/[org_id]_[s3-bucket-instance]/auditlogs
                           PRE auditlogs/
```

Información Relacionada

- Administrar registro de Cisco Secure Access
- Formatos de registro y control de versiones

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).