

Vérification de la rotation des clés de compartiment S3 d'Umbrella et d'accès sécurisé (obligatoire tous les 90 jours)

Table des matières

[Introduction](#)

[Informations générales](#)

[Problème](#)

[Solution](#)

[Vérification De L'Accès Au Compartiment S3](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes de la rotation des clés de compartiment S3 dans le cadre des améliorations apportées à la sécurité et aux meilleures pratiques de Cisco.

Informations générales

Dans le cadre des améliorations apportées à la sécurité et aux meilleures pratiques de Cisco, les administrateurs Cisco Umbrella et Cisco Secure Access disposant de compartiments S3 gérés par Cisco pour le stockage des journaux doivent désormais faire pivoter les clés IAM du compartiment S3 tous les 90 jours. Auparavant, il n'était pas nécessaire de faire pivoter ces touches, cette exigence prenant effet le 15 mai 2025.

Bien que les données du compartiment appartiennent à l'administrateur, le compartiment lui-même appartient à Cisco. Afin que les utilisateurs Cisco respectent les meilleures pratiques en matière de sécurité, nous demandons à Cisco Secure Access et à Cisco Umbrella de faire pivoter leurs clés au moins tous les 90 jours. Cela permet de garantir que nos utilisateurs ne courent aucun risque de fuite de données ou de divulgation d'informations et de respecter nos meilleures pratiques en matière de sécurité en tant que société leader dans le domaine de la sécurité.

Cette restriction ne s'applique pas aux compartiments S3 non gérés par Cisco et nous vous recommandons de passer à votre propre compartiment géré, car cette restriction de sécurité crée un problème pour vous.

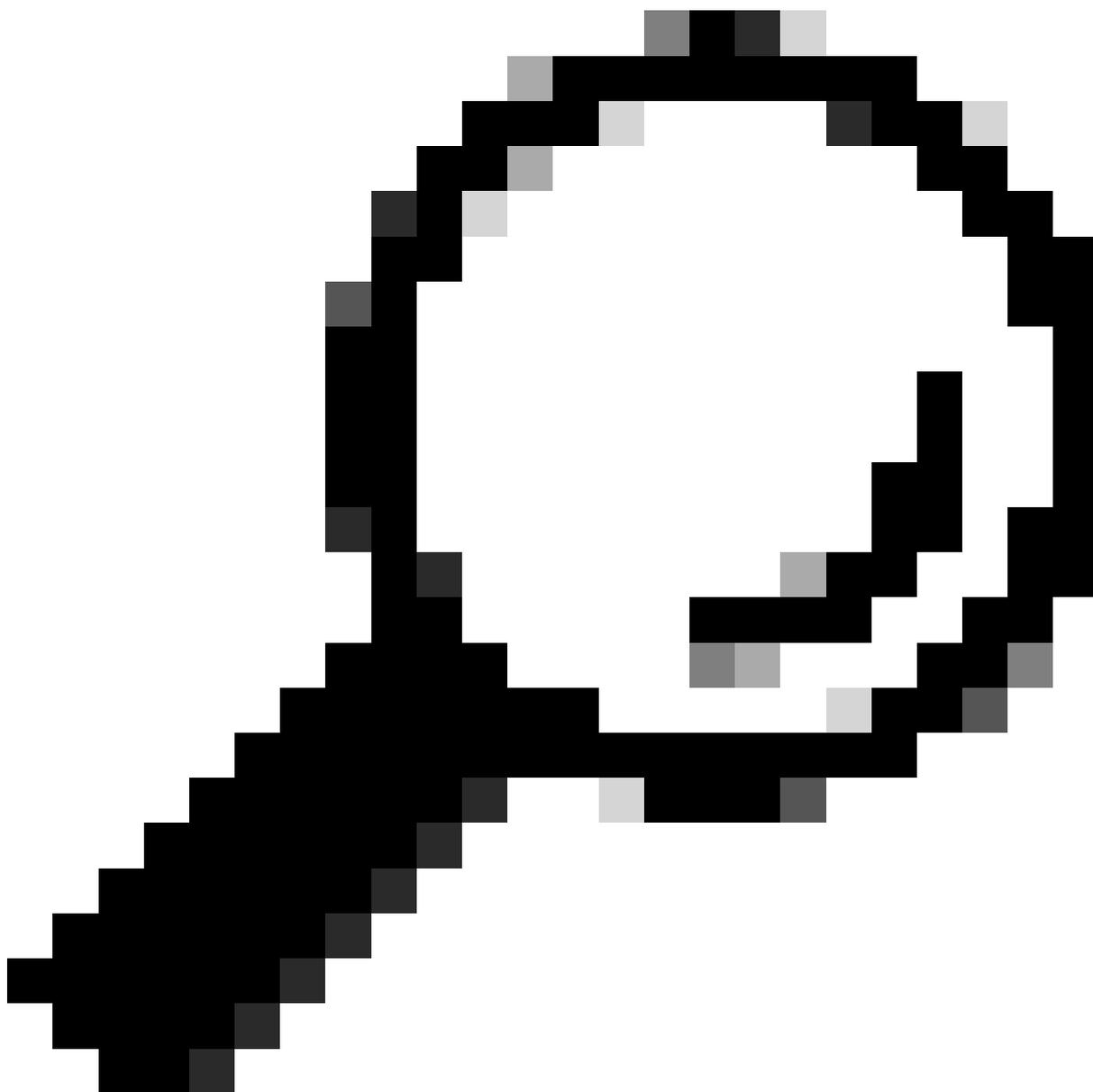
Problème

Les utilisateurs qui ne peuvent pas faire pivoter leurs clés dans les 90 jours ne peuvent plus accéder à leurs compartiments S3 gérés par Cisco. Les données du compartiment continuent

d'être mises à jour avec les informations consignées, mais le compartiment lui-même devient inaccessible.

Solution

1. Accédez à Admin > Log Management et dans la zone Amazon S3, sélectionnez Use a Cisco-managed Amazon S3 bucket



Conseil : Une nouvelle bannière est présentée avec un message d'avertissement concernant les nouvelles exigences de sécurité de la rotation des clés de compartiment S3.

 We're sending data to your Cisco-managed Amazon S3 storage

Cisco-managed Amazon S3 buckets require that you regenerate the keys every 90 days. Note that this would invalidate any existing keys. If you would like to avoid this, use your company-managed S3 bucket. You may also regenerate them if you forgot your existing keys. To learn more [view our guide](#).

**Your Cisco-managed Amazon S3 bucket keys expire in 30 days.**

After this time, your logs will still be sent to your Amazon S3 bucket but you will no longer be able to access them. In order to avoid loss of access, click "Regenerate Keys".

Storage Region US West (N. California)

Retention Duration 30 days [Edit](#)

Admin Audit Log Include Admin Audit Log in S3



Data Path s3://cisco-managed-us-west-1/

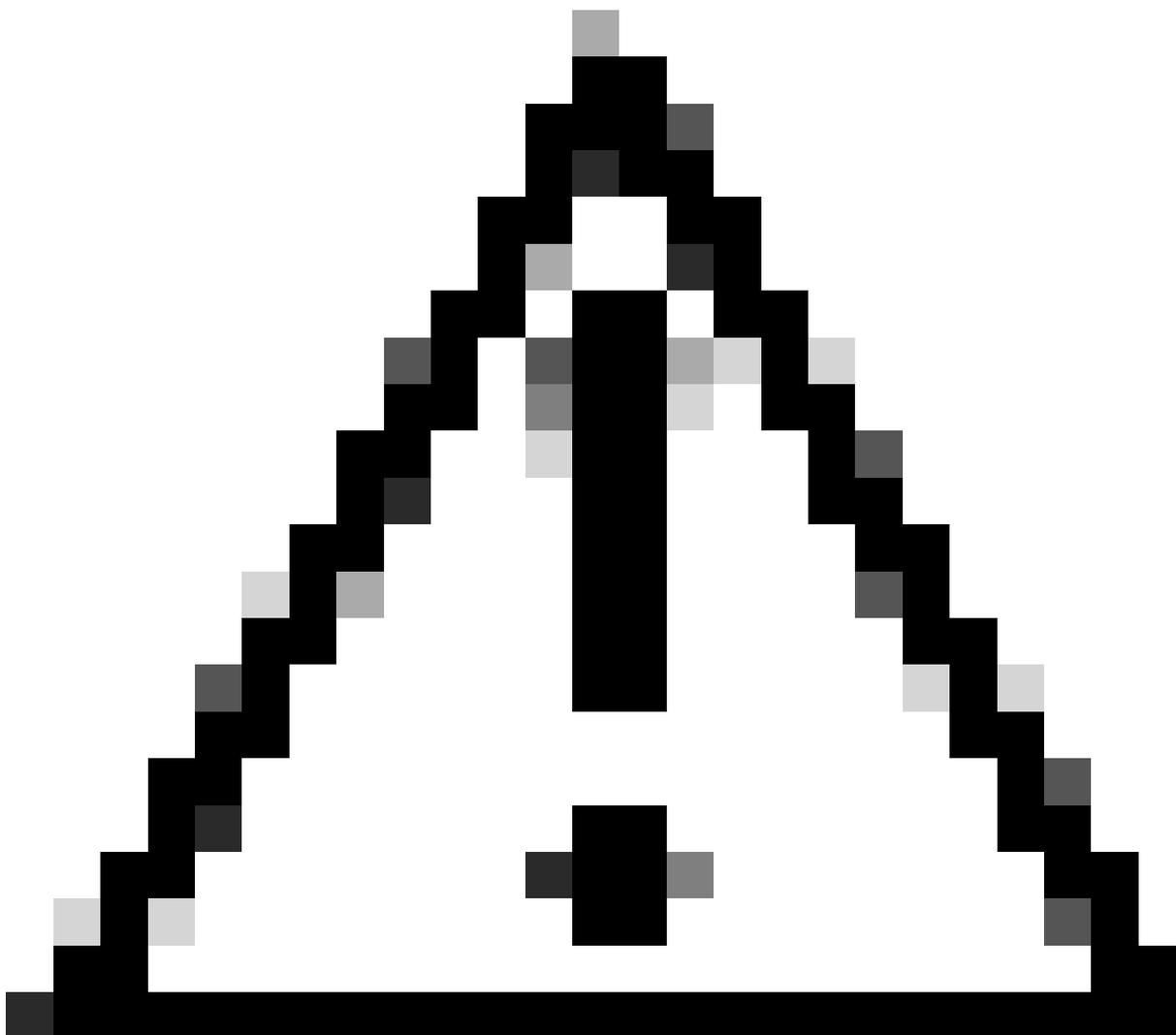
Last Sync Feb 13, 2023 at 6:10 PM

Schema Version v4 [Upgrade](#) | [View Details](#) v6 Available

[STOP LOGGING](#)[REGENERATE KEYS](#)

2. Générez vos nouvelles clés de compartiment S3

3. Conservez votre nouvelle clé en lieu sûr.



Mise en garde : La clé et le secret ne peuvent être affichés qu'une seule fois et ne sont pas visibles par l'équipe d'assistance Cisco.

New keys have been generated

Your keys are ready. Please keep them in a safe place. If you need to regenerate keys, *old keys will immediately and permanently lose access.*

Data Path s3://cisco-managed-us-west-1/ [redacted] 

Access Key [redacted] 

Secret Key [redacted] 

Got it!

CONTINUE

4. Mettez à jour tous les journaux d'acquisition de système externe à partir du compartiment S3 géré par Cisco avec la nouvelle clé et le nouveau secret.

Vérification De L'Accès Au Compartiment S3

Pour vérifier l'accès à votre compartiment S3, vous pouvez utiliser le format de fichier tel que précisé dans cet exemple ou dans le guide de documentation Secure Access and Umbrella.

1. Configurez votre CLI AWS avec les nouvelles clés générées.

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

```
AWS Secret Access Key [None]:
```

```
Default region name [None]:
```

```
Default output format [None]:
```

2. Répertoriez l'un des journaux enregistrés dans votre compartiment S3.

```
$ 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/
```

Informations connexes

- [Gérer la consignation Cisco Secure Access](#)
- [Formats de journaux et contrôle de version](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.