Überprüfen der Drehung der S3-Bucket-Schlüssel für sicheren Zugriff und Umbrella (alle 90 Tage erforderlich)

Inhalt

Einleitung

Hintergrundinformationen

Problem

Lösung

Zugriff auf S3-Bucket überprüfen

Zugehörige Informationen

Einleitung

In diesem Dokument werden die Schritte zum Drehen der S3-Bucket-Schlüssel im Rahmen der Cisco Security- und Best Practice-Verbesserungen beschrieben.

Hintergrundinformationen

Im Rahmen der Verbesserungen von Cisco Sicherheit und Best Practices müssen Cisco Umbrella- und Cisco Secure Access-Administratoren mit von Cisco verwalteten S3-Buckets für die Protokollspeicherung nun alle 90 Tage die IAM-Schlüssel für die S3-Bucket ändern. Bisher war es nicht erforderlich, diese Schlüssel zu drehen. Diese Anforderung trat am 15. Mai 2025 in Kraft.

Die Daten in der Gruppe gehören zwar dem Administrator, die Gruppe selbst gehört jedoch Cisco. Um sicherzustellen, dass Cisco-Benutzer die Best Practices für die Sicherheit einhalten, bitten wir Cisco Secure Access und Umbrella, ihre Schlüssel künftig mindestens alle 90 Tage zu wechseln. Dies trägt dazu bei, dass unsere Benutzer nicht Gefahr laufen, dass Daten verloren gehen oder Informationen offen gelegt werden, und dass sie unsere Best Practices für die Sicherheit als führendes Sicherheitsunternehmen einhalten.

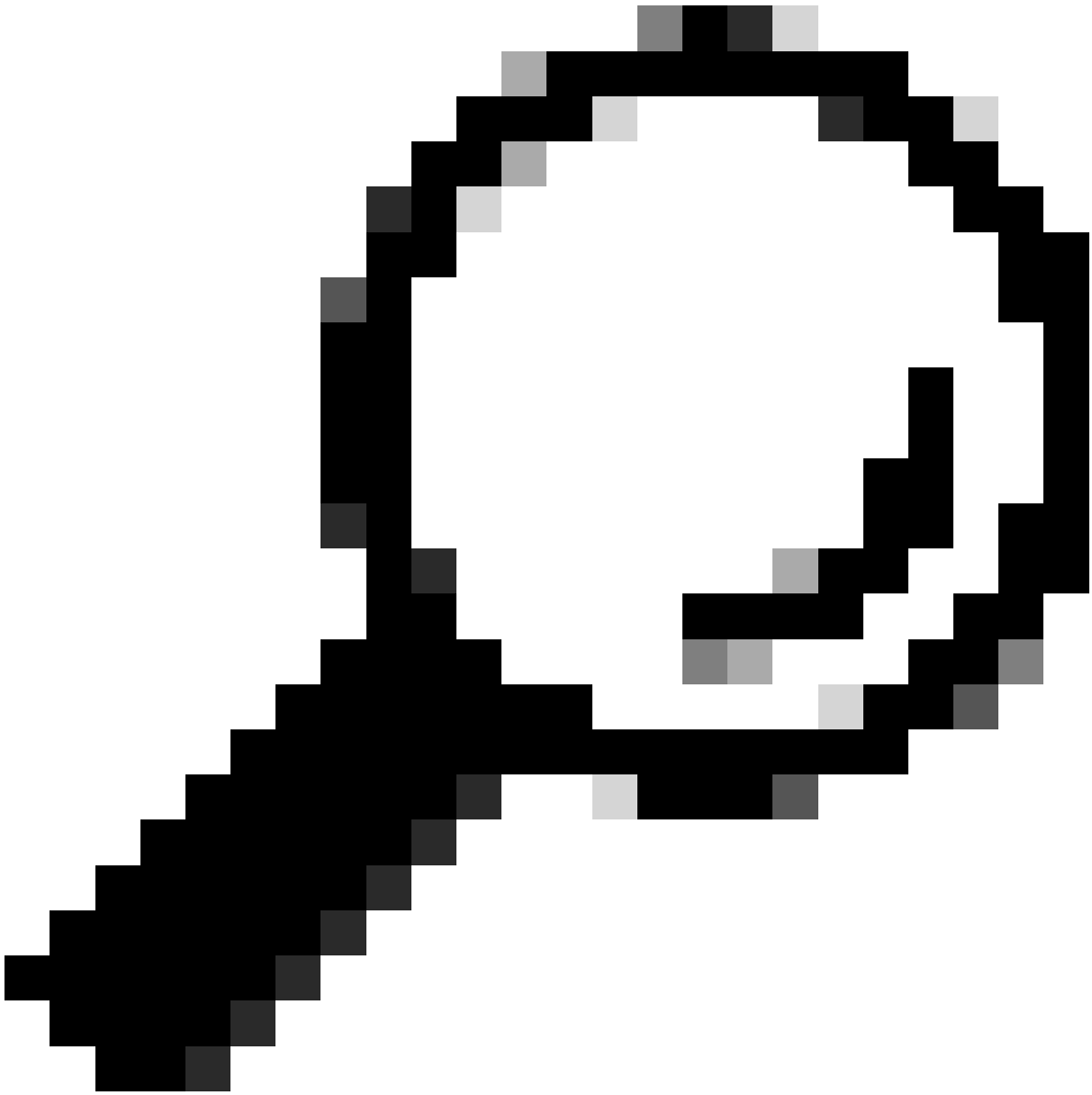
Diese Einschränkung gilt nicht für von anderen Anbietern verwaltete S3-Buckets. Wir empfehlen, zu Ihrem eigenen verwalteten Bucket zu wechseln, da diese Sicherheitseinschränkung für Sie ein Problem darstellt.

Problem

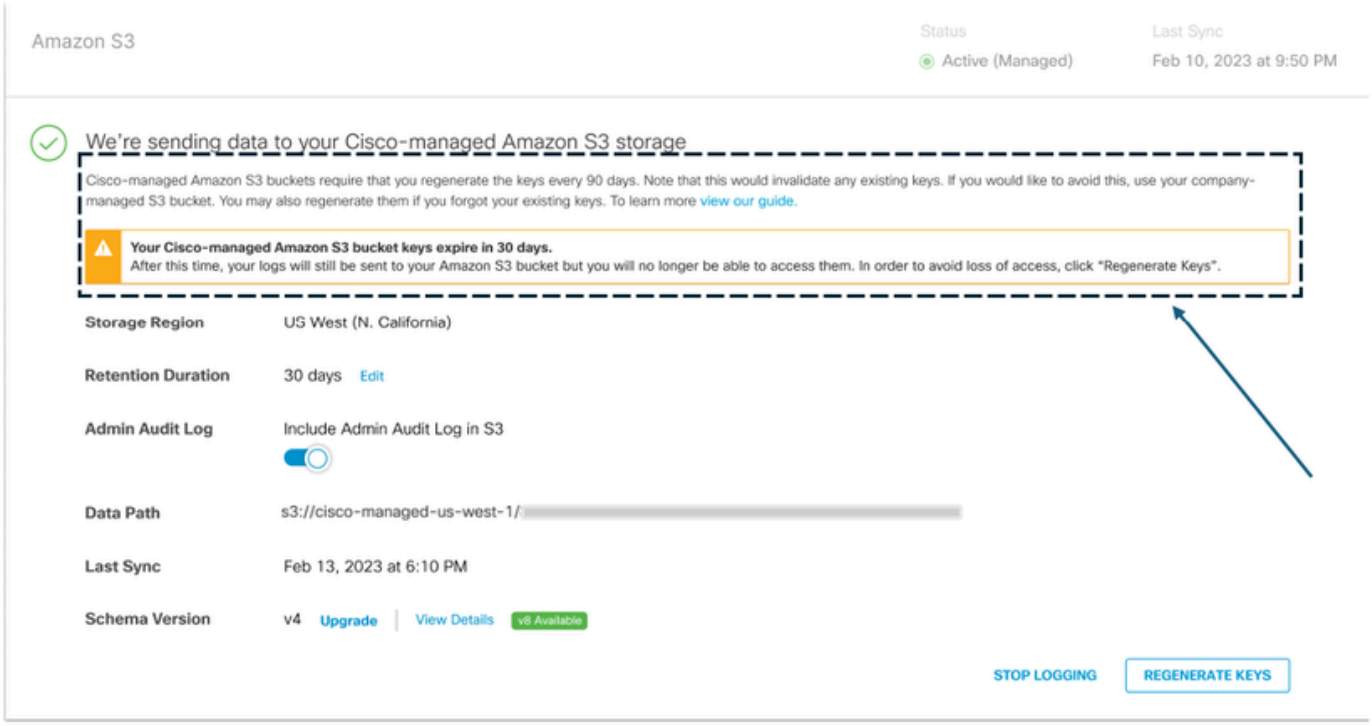
Benutzer, die ihre Schlüssel nicht innerhalb von 90 Tagen drehen können, haben keinen Zugriff mehr auf ihre von Cisco verwalteten S3-Buckets. Die Daten im Bucket werden weiterhin mit protokollierten Informationen aktualisiert, aber der Bucket selbst ist nicht mehr zugänglich.

Lösung

1. Navigieren Sie zu Admin > Log Management, und wählen Sie im Bereich Amazon S3 die Option Use a Cisco-managed Amazon S3 bucket

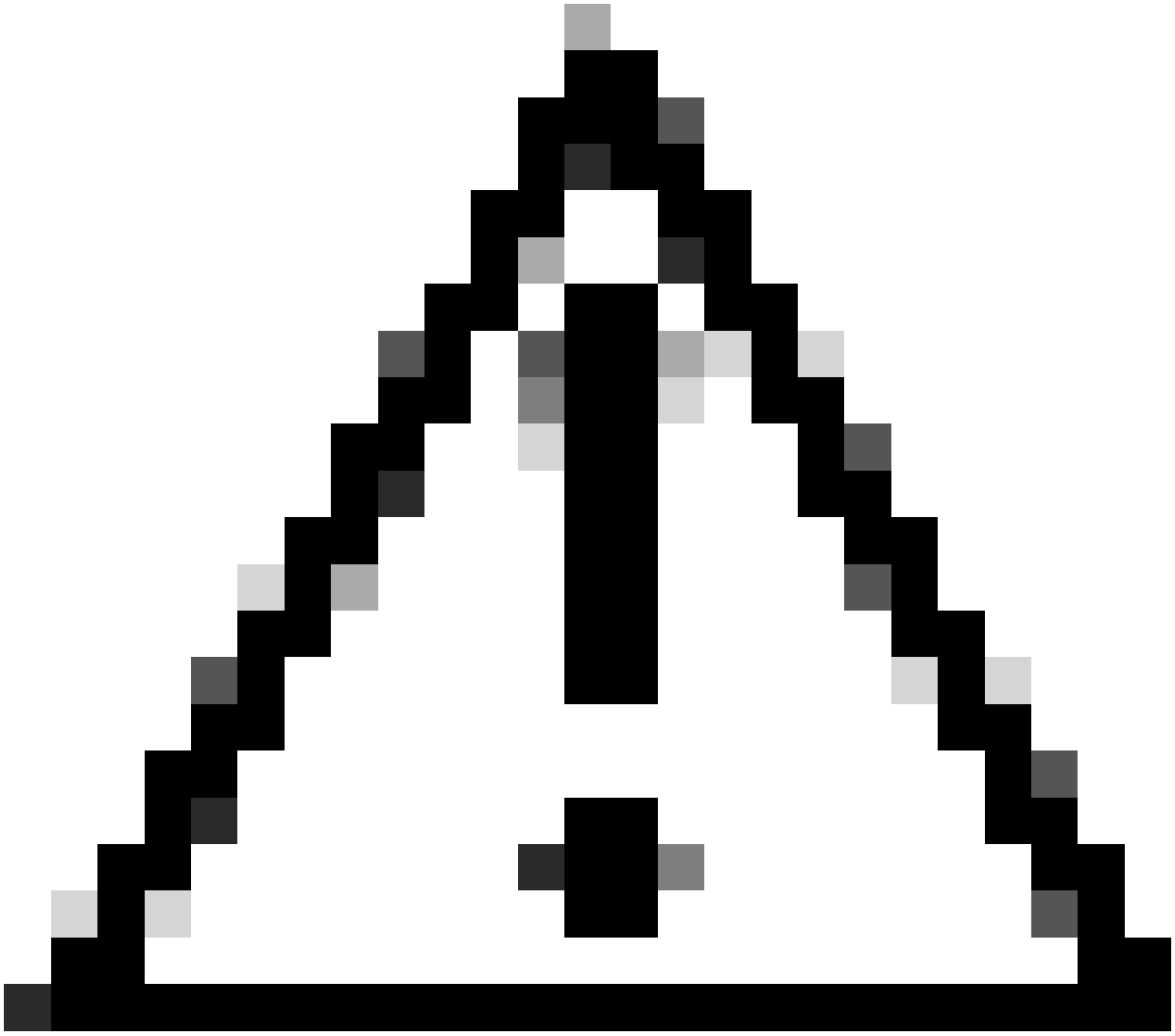


Tipp: Ein neues Banner wird mit einer Warnmeldung über die neuen Sicherheitsanforderungen der Rotation der S3-Eimer-Tasten angezeigt.

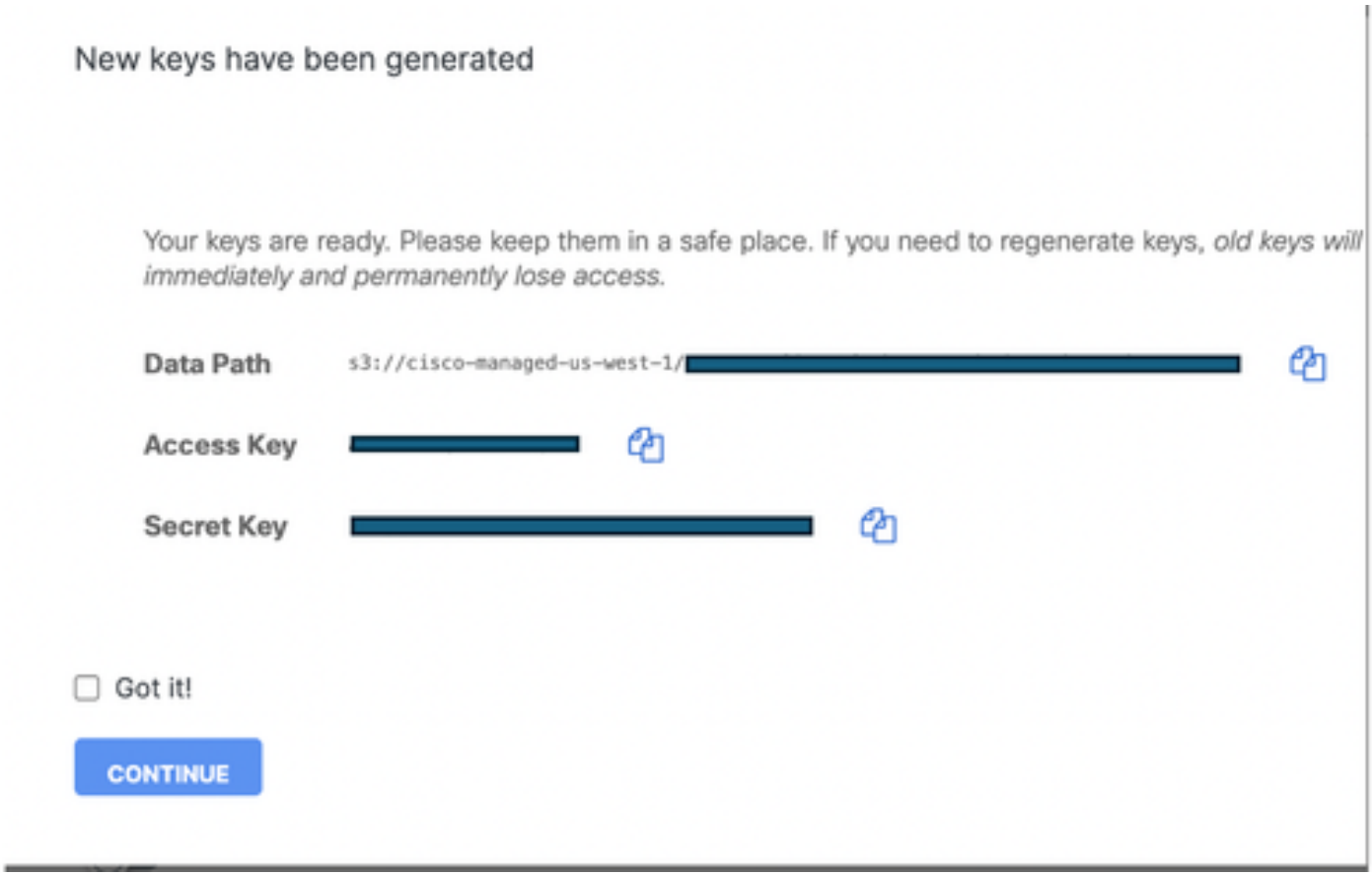


2. Generieren Sie Ihre neuen S3 Bucket Schlüssel

3. Speichern Sie Ihren neuen Schlüssel an einem sicheren Ort.



Vorsicht: Schlüssel und geheimer Schlüssel können nur einmal angezeigt werden und sind für das Cisco Support-Team nicht sichtbar.



4. Aktualisieren Sie alle externen Systeme, die Protokolle von der Cisco Managed S3-Bucket empfangen, mit dem neuen Schlüssel und Schlüssel.

Zugriff auf S3-Bucket überprüfen

Um den Zugriff auf Ihren S3-Bucket zu überprüfen, können Sie das Dateiformat verwenden, wie in diesem Beispiel oder in der Dokumentation zu Secure Access und Umbrella erläutert.

1. Konfigurieren Sie Ihre AWS CLI mit neuen generierten Schlüsseln.

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



AWS Secret Access Key [None]:



Default region name [None]:



Default output format [None]:
```

2. Führen Sie eines der gespeicherten Protokolle in Ihrem S3-Bucket auf.

```
$ 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/
```

Zugehörige Informationen

- Cisco Secure Access-Protokollierung verwalten
- Protokollformate und Versionsverwaltung

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.