セキュアアクセスとUmbrella S3バケットキーローテーションの確認（90日ごとに必要）

内容

はじめに

背景説明

問題

解決方法

S3バケットへのアクセスの確認

関連情報

はじめに

このドキュメントでは、シスコのセキュリティとベストプラクティスの改善の一部として、S3バケットキーを回転させる手順について説明します。

背景説明

シスコのセキュリティとベストプラクティスの改善の一環として、ログストレージにシスコ管理のS3バケットを使用するCisco UmbrellaおよびCisco Secure Access管理者は、90日ごとにS3バケットのIAMキーをローテーションする必要があります。以前は、これらのキーを回転させる必要はありませんでした。 この要件は、2025年5月15日から有効になります。

バケット内のデータは管理者に属していますが、バケット自体はシスコ所有/管理対象です。シスコのユーザがセキュリティのベストプラクティスに従うようにするため、シスコはCisco Secure AccessとUmbrellaに対して、最低90日ごとにキーをローテーションするように要請しています。 これは、当社のユーザがデータ漏洩や情報漏洩のリスクを抱えないようにし、セキュリティのリーディングカンパニーとしてのセキュリティのベストプラクティスに従うことを保証するのに役立ちます。

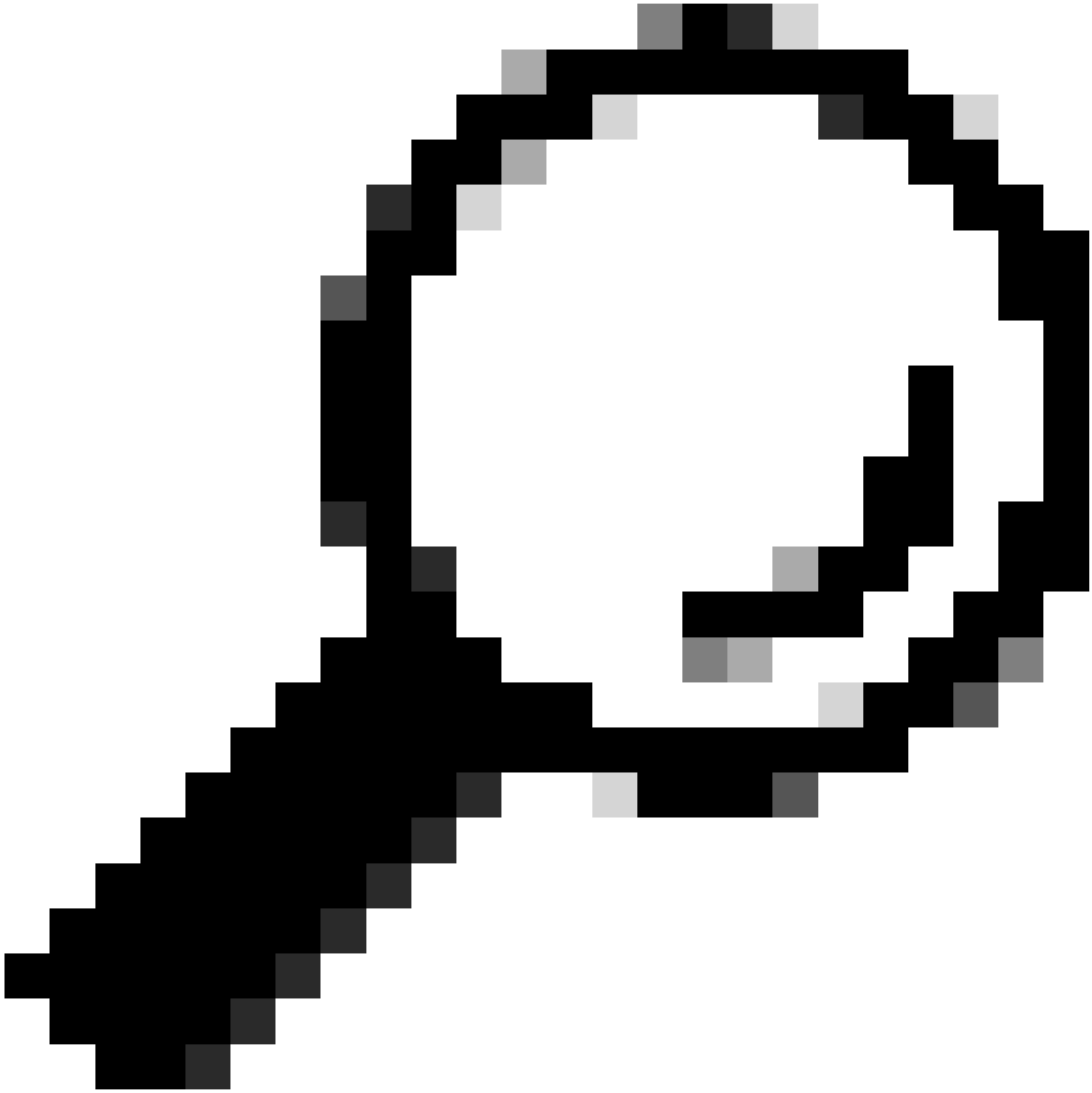
この制限は、シスコが管理する以外のS3バケットには適用されません。独自の管理バケットに移動することをお勧めします。このセキュリティの制限によって問題が発生します。

問題

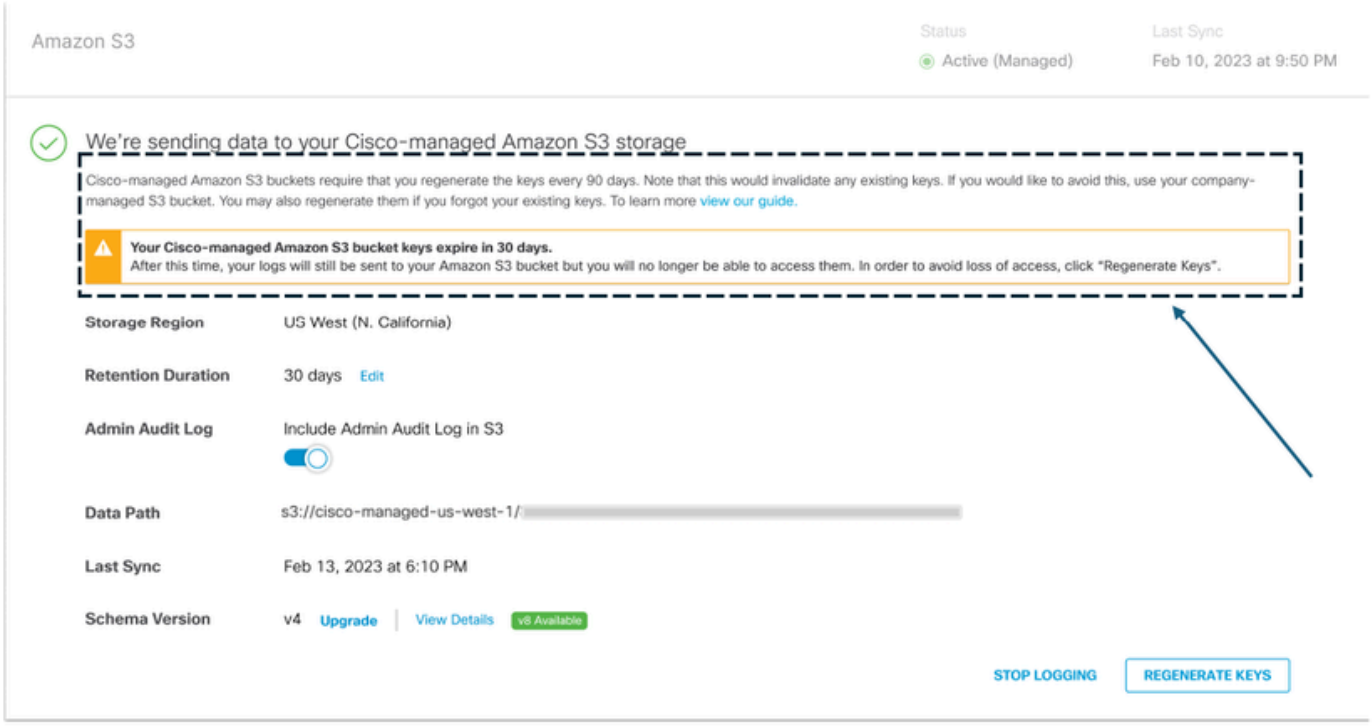
90日以内にキーをローテーションできないユーザは、シスコが管理するS3バケットにアクセスできなくなります。 バケット内のデータは、ログに記録された情報で引き続き更新されますが、バケット自体にはアクセスできなくなります。

解決方法

1. Admin > Log Managementに移動し、Amazon S3エリアでUse a Cisco-managed Amazon S3 bucketを選択します

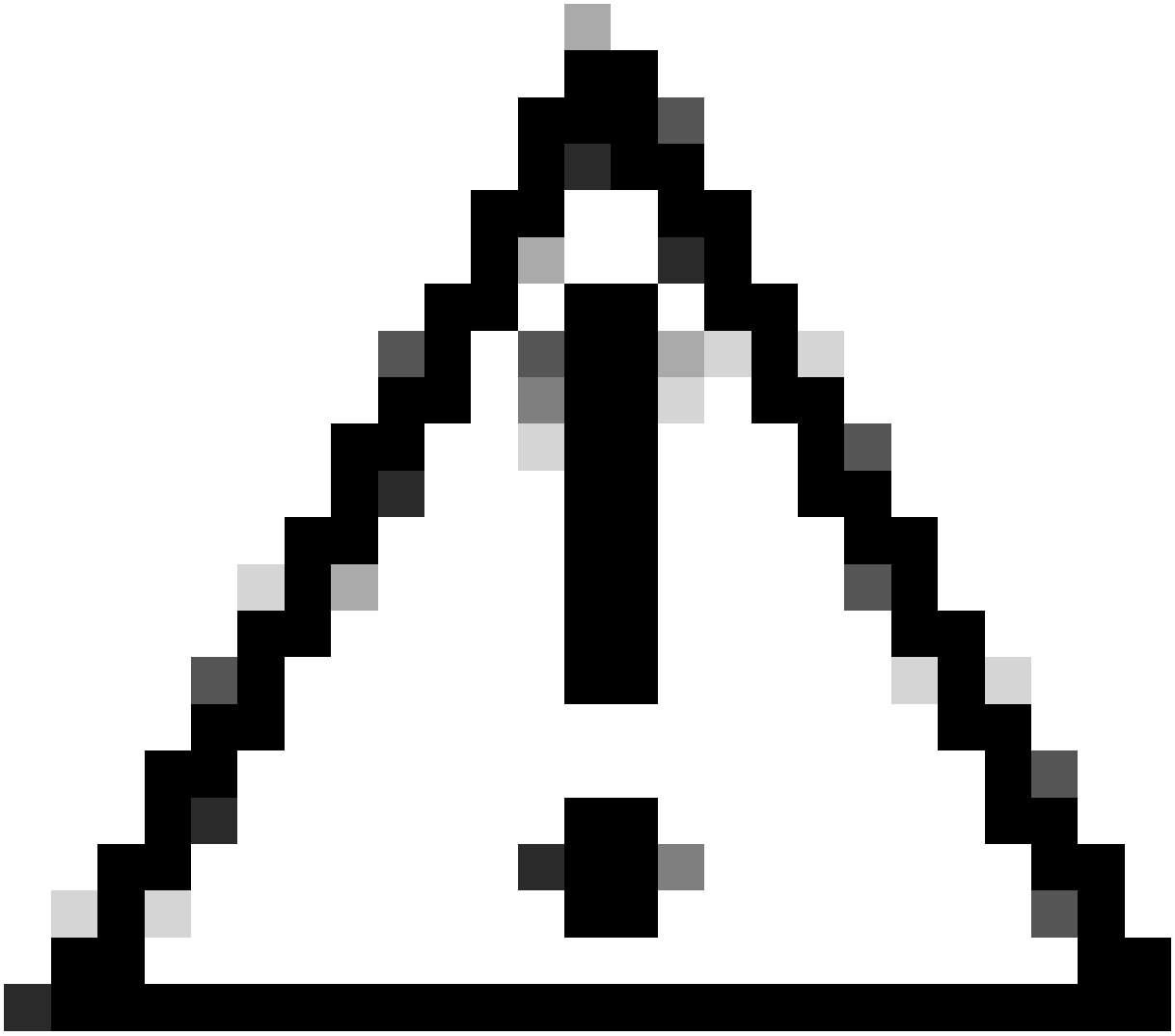


ヒント：新しいバナーに、S3バケットキーのローテーションに関する新しいセキュリティ要件に関する警告メッセージが表示されます。

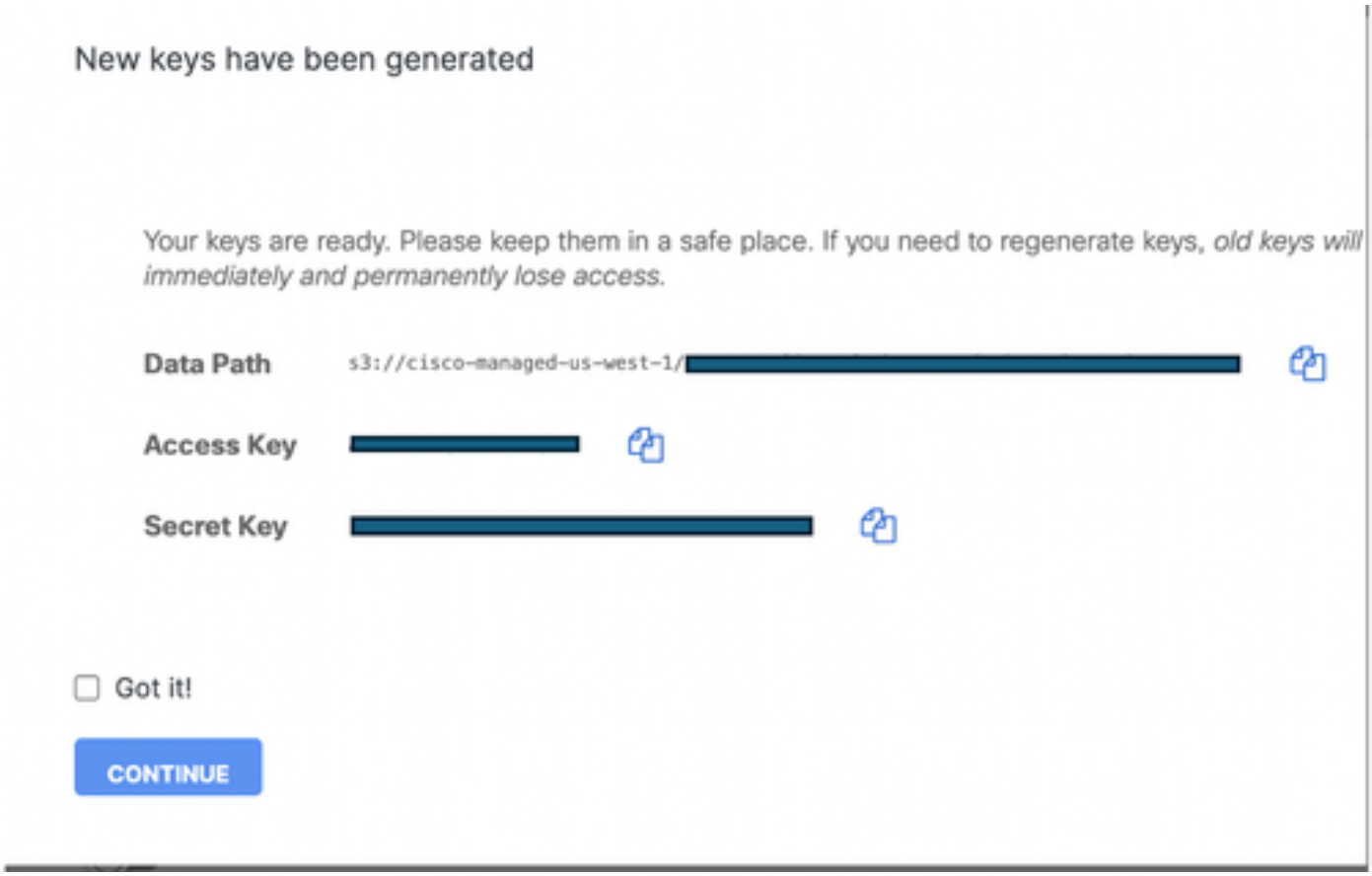


2. 新しいS3バケットキーを生成します

3. 新しい鍵を安全な場所に保管します。



注意：これらのキーとシークレットは1回だけ表示でき、シスコサポートチームには表示されません。



4. シスコが管理するS3バケットのログを取り込むすべての外部システムを、新しいキーとシークレットで更新します。

S3バケットへのアクセスの確認

S3バケットへのアクセスを確認するには、この例で説明されているファイル形式、または『Secure Access and Umbrellaドキュメントガイド』で説明されているファイル形式を使用できます。

1. 新しく生成されたキーを使用してAWS CLIを設定します。

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


AWS Secret Access Key [None]:


Default region name [None]:


Default output format [None]:
```

2. S3-Bucketに保存されている口グの1つをリストします。

```
$ 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/
```

関連情報

- Cisco Secure Access口ギングの管理
- 口グ形式とバージョン管理

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。