

驗證安全訪問和Umbrella S3儲存桶金鑰輪替（每90天需要一次）

目錄

[簡介](#)

[背景資訊](#)

[問題](#)

[解決方案](#)

[驗證對S3儲存桶的訪問](#)

[相關資訊](#)

簡介

本文檔介紹作為思科安全和最佳實踐改進的一部分旋轉S3 Bucket金鑰的步驟。

背景資訊

作為思科安全和最佳實踐改進的一部分，現在要求為日誌儲存使用思科管理的S3儲存桶的Cisco Umbrella和Cisco Secure Access管理員每90天輪換S3儲存桶的IAM金鑰。以前，這些鍵無需旋轉。此要求從2025年5月15日起生效。

當儲存桶中的資料屬於管理員時，儲存桶本身由思科擁有/管理。為了讓思科使用者遵守安全最佳實踐，我們要求我們的思科安全訪問和Umbrella至少每90天輪換一次金鑰。這有助於確保我們的使用者不會面臨資料洩露或資訊洩露的風險，並遵守我們作為領先安全公司的安全最佳實踐。

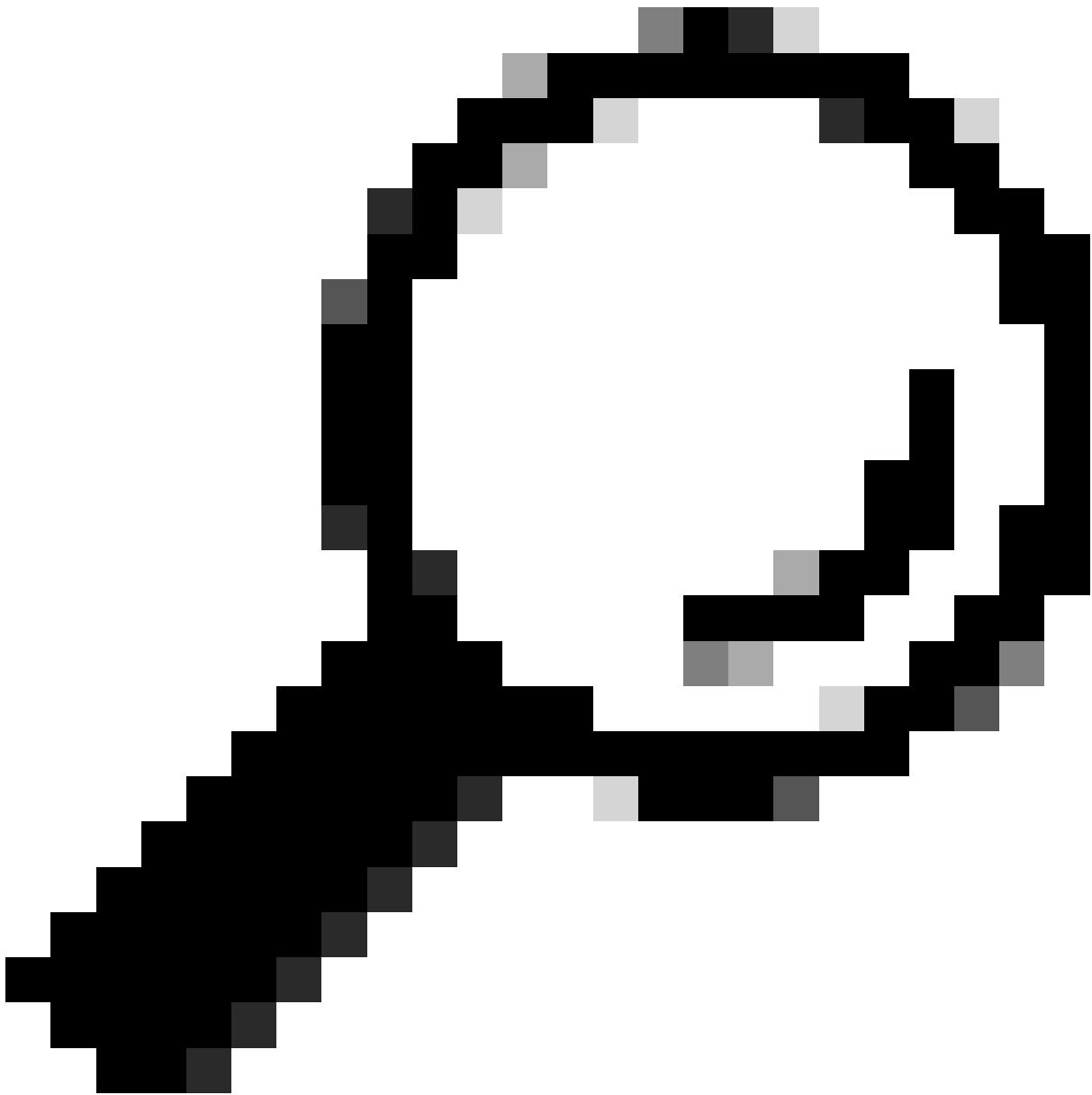
此限制不適用於非思科管理的S3儲存桶，我們建議您移動到您自己的管理儲存桶，因為此安全限制會為您帶來問題。

問題

在90天內無法輪換金鑰的使用者，不再能夠訪問其思科管理的S3儲存桶。儲存桶中的資料繼續使用記錄的資訊更新，但儲存桶本身變得不可訪問。

解決方案

1. 導航到Admin > Log Management，然後在Amazon S3區域選擇Use a Cisco管理的Amazon S3儲存桶



提示：新橫幅上會顯示有關旋轉S3 Bucket金鑰的新安全要求的警告消息。

Amazon S3

Status

Active (Managed)

Last Sync

Feb 10, 2023 at 9:50 PM

✔

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

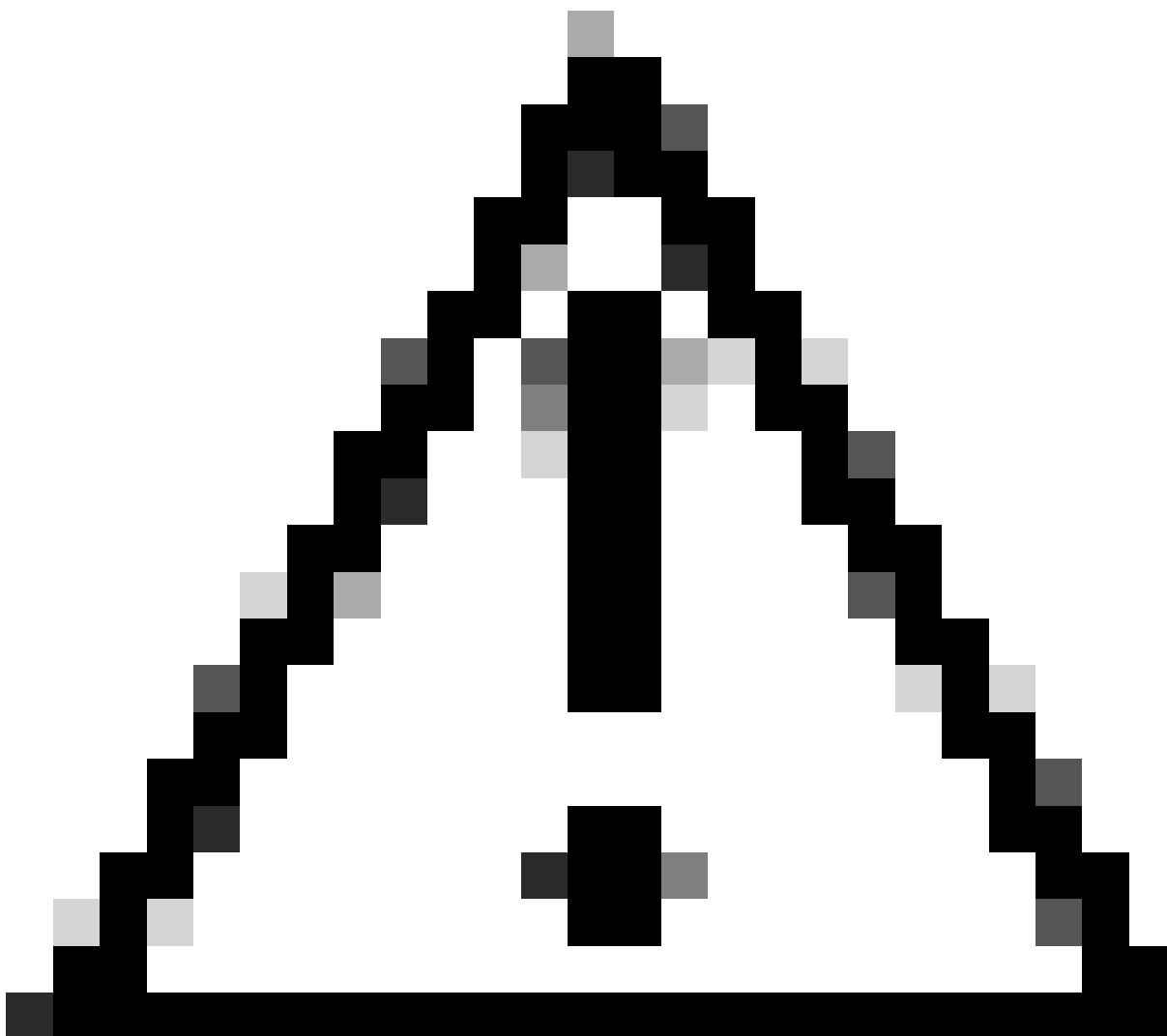
v4 [Upgrade](#) | [View Details](#) v6 Available

STOP LOGGING

REGENERATE KEYS

2.生成新的S3儲存桶金鑰

3.將您的新金鑰儲存在安全位置。



注意：「金鑰」和「金鑰」只能顯示一次，思科支援團隊看不到它們。

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/ 

Access Key 

Secret Key 

☐ Got it!

CONTINUE

4. 使用新的金鑰和金鑰更新從思科管理的S3儲存桶接收的任何外部系統日誌。

驗證對S3儲存桶的訪問

要驗證對S3儲存桶的訪問，您可以使用本示例或Secure Access and Umbrella文檔指南中說明的檔案格式。

1. 使用新生成的密鑰配置您的AWS CLI。

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

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

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

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

2. 列出您的S3-Bucket中儲存的一個日誌。

```
$ 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/
```

相關資訊

- [管理思科安全存取記錄](#)
- [日誌格式和版本控制](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。