验证安全访问和Umbrella S3桶密钥轮替（每90天需要一次）

目录

简介

本文档介绍作为思科安全和最佳实践改进的一部分旋转S3 Bucket密钥的步骤。

背景信息

作为思科安全和最佳实践改进的一部分，Cisco Umbrella和Cisco Secure Access管理员使用思科管理的S3存储桶进行日志存储，现在需要每90天轮换S3存储桶的IAM密钥。以前，这些密钥无需轮替，此要求自2025年5月15日起生效。

当桶中的数据属于管理员时，桶本身由思科拥有/管理。为了让思科用户遵守安全最佳实践，我们要求我们的思科安全访问和Umbrella以后至少每90天轮换一次密钥。这有助于确保我们的用户不会面临数据泄露或信息泄露的风险，并遵守我们作为领先安全公司的安全最佳实践。

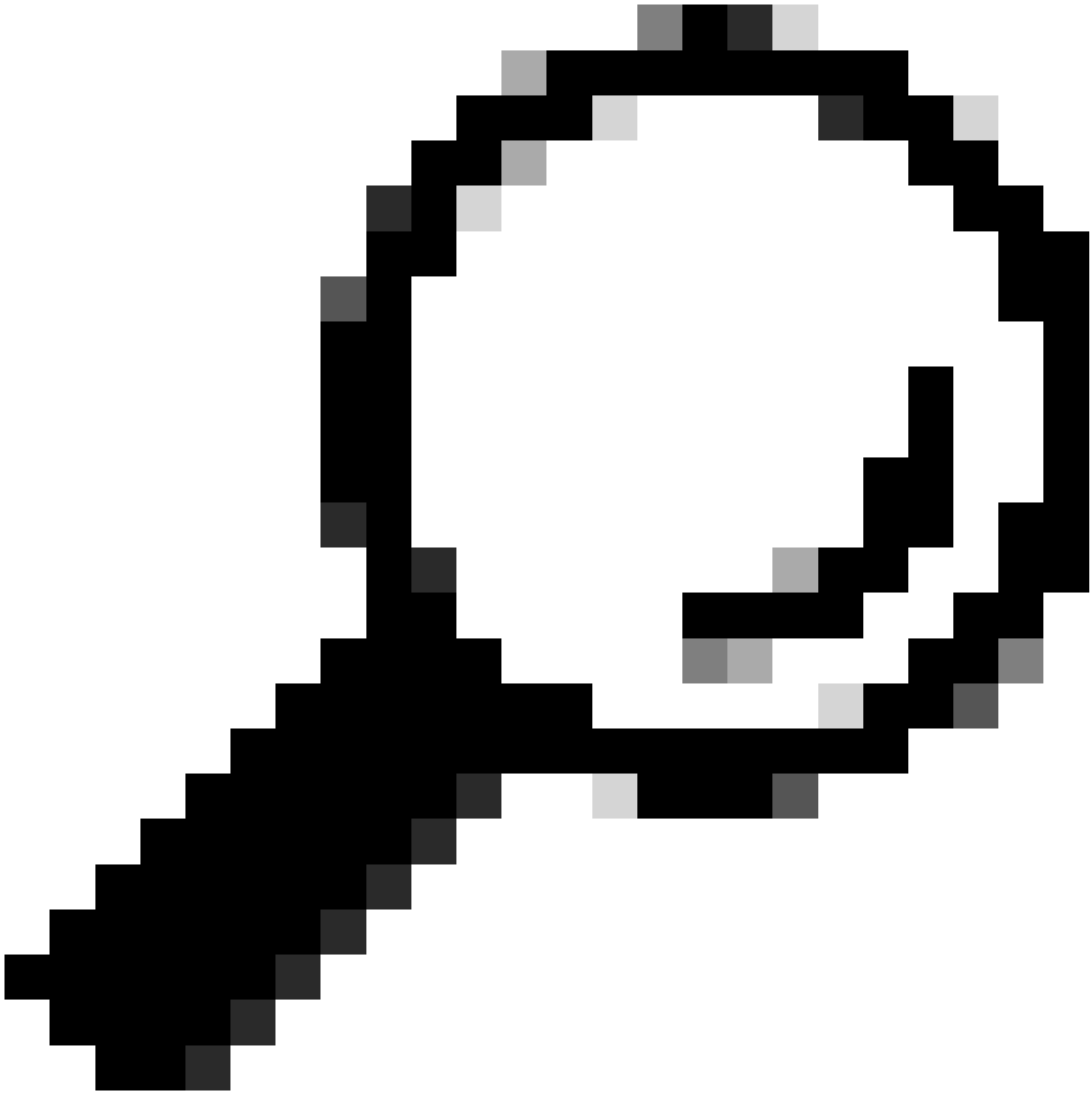
此限制不适用于非思科托管的S3存储桶，我们建议您迁移到自己的托管存储桶，因为此安全限制会给您带来问题。

问题

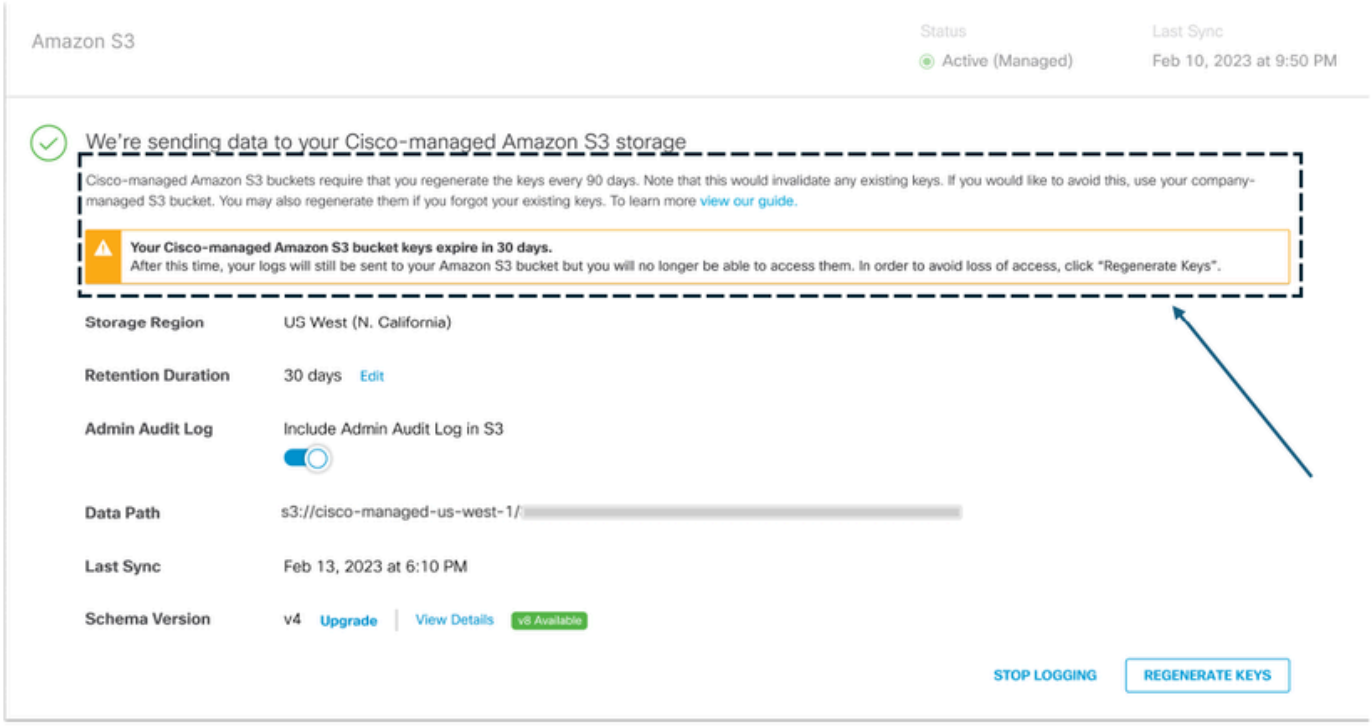
在90天内无法轮换密钥的用户将无法再访问其思科托管的S3存储桶。 存储桶中的数据继续使用已记录的信息进行更新，但存储桶本身变得不可访问。

解决方案

1.导航到Admin > Log Management，然后在Amazon S3区域中选择Use a Cisco管理的Amazon S3存储桶

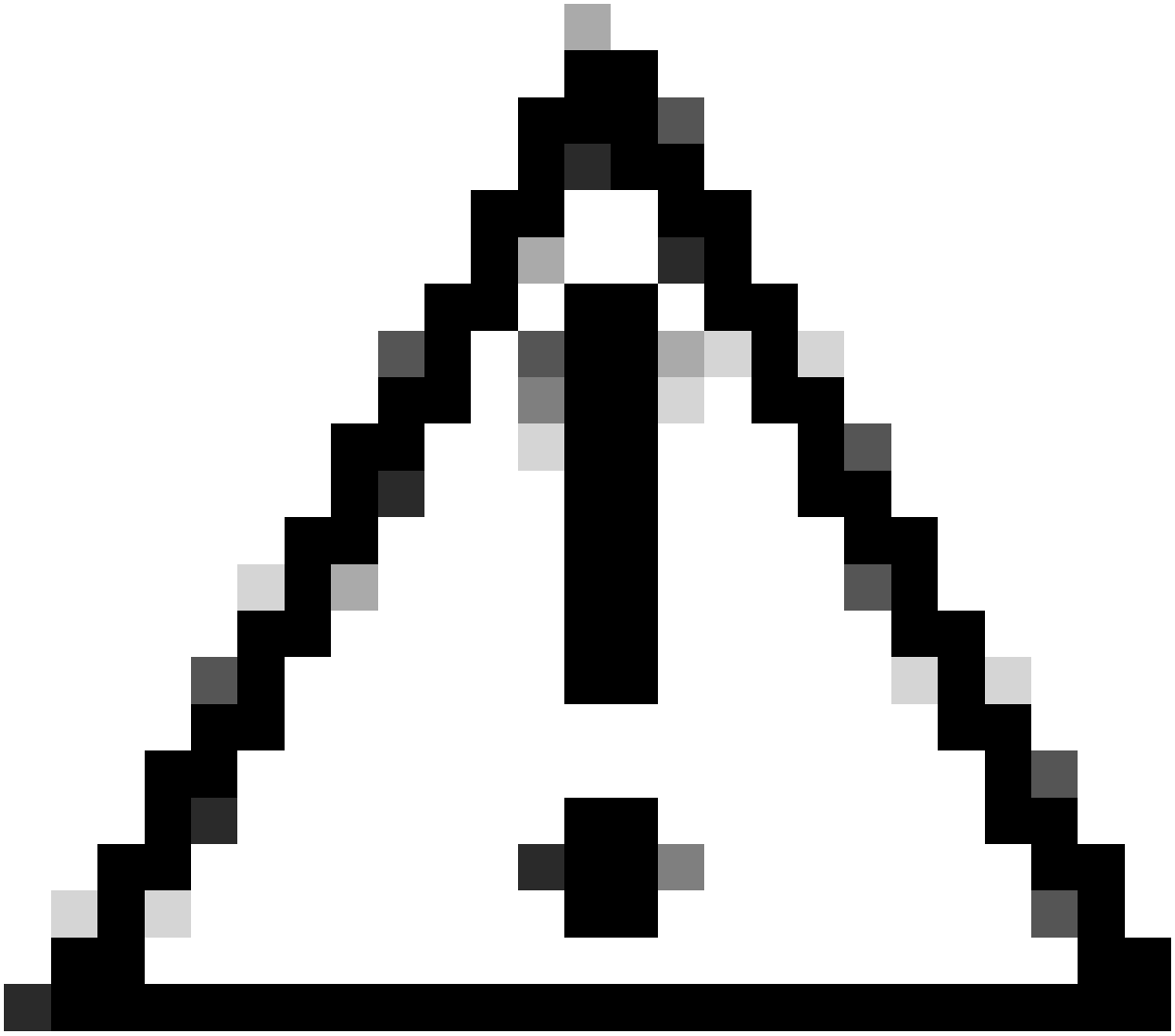


提示：新横幅上会显示有关轮换S3 Bucket密钥的新安全要求的警告消息。

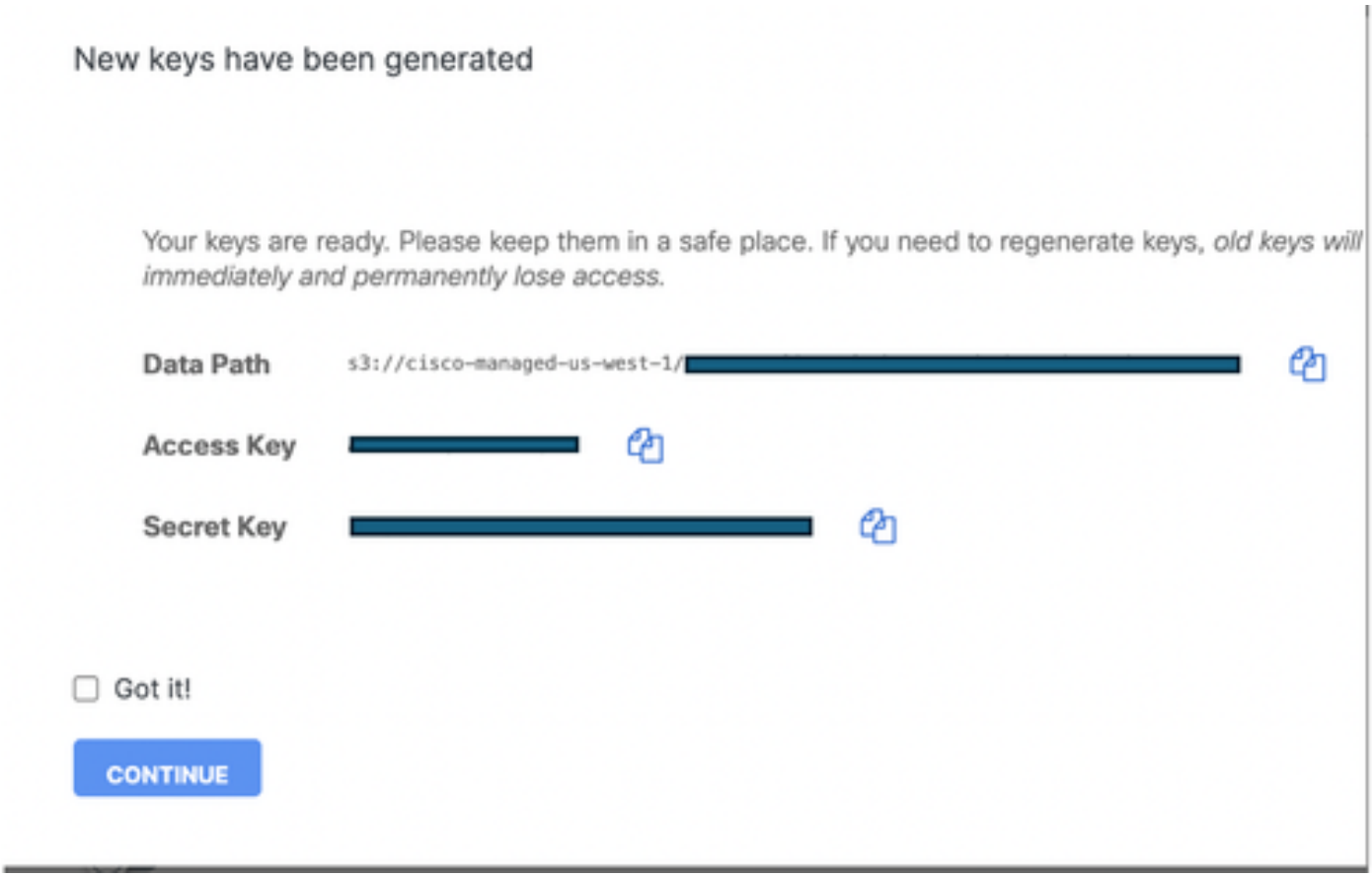


2.生成新的S3存储桶密钥

3.将您的新密钥存储在安全位置。



警告：它们密钥和密钥只能显示一次，且对思科支持团队不可见。



4.使用新密钥和密钥更新任何外部系统从Cisco管理的S3存储桶接收日志。

检验对S3存储桶的访问

要验证对S3存储桶的访问，您可以使用本示例或《安全访问和Umbrella文档指南》中说明的文件格式。

1.使用新生成的密钥配置AWS CLI。

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


AWS Secret Access Key [None]:


Default region name [None]:


Default output format [None]:
```

2.在S3-Bucket中列出一个已保存的日志。

```
$ 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/
```

相关信息

- 管理思科安全访问日志记录
- 日志格式和版本控制

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。