Verificar o acesso seguro e a rotação das chaves de depósito do Umbrella S3 (obrigatória a cada 90 dias)

Contents

Introdução

Este documento descreve as etapas de rotação das chaves de Balde S3 como parte das melhorias de segurança e práticas recomendadas da Cisco.

Informações de Apoio

Como parte das melhorias de segurança e práticas recomendadas da Cisco, os administradores do Cisco Umbrella e do Cisco Secure Access com buckets S3 gerenciados pela Cisco para armazenamento de log agora precisam ser girados as chaves IAM para o bucket S3 a cada 90 dias. Anteriormente, não era necessário girar essas chaves. Esse requisito entrará em vigor a partir de 15 de maio de 2025.

Enquanto os dados no bucket pertencem ao administrador, o próprio bucket é de propriedade da Cisco/gerenciado. Para que os usuários da Cisco sigam as práticas recomendadas de segurança, pedimos que nossos Cisco Secure Access e Umbrella revezem suas chaves pelo menos a cada 90 dias. Isso ajuda a garantir que nossos usuários não corram o risco de vazamento de dados ou divulgação de informações e sigam nossas práticas recomendadas de segurança como uma empresa líder em segurança.

Essa restrição não se aplica a buckets de S3 gerenciados que não são da Cisco. Recomendamos que você mude para seu próprio bucket gerenciado, caso essa restrição de segurança crie um problema para você.

Problema

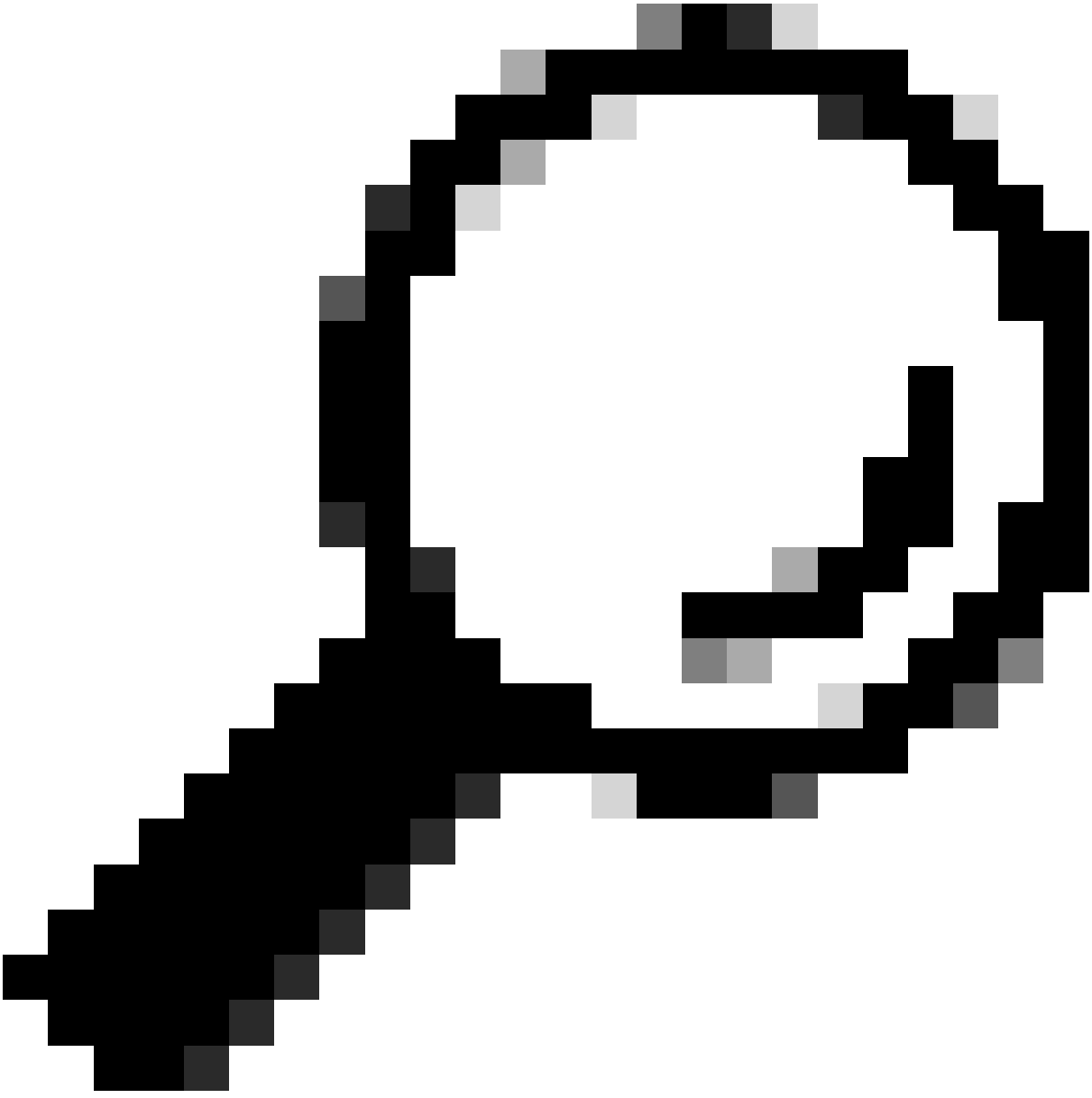
Os usuários que não puderem rotacionar suas chaves dentro de 90 dias não terão mais acesso aos seus buckets S3 gerenciados pela Cisco. Os dados no bucket continuam a ser atualizados

com informações registradas, mas o próprio bucket se torna inacessível.

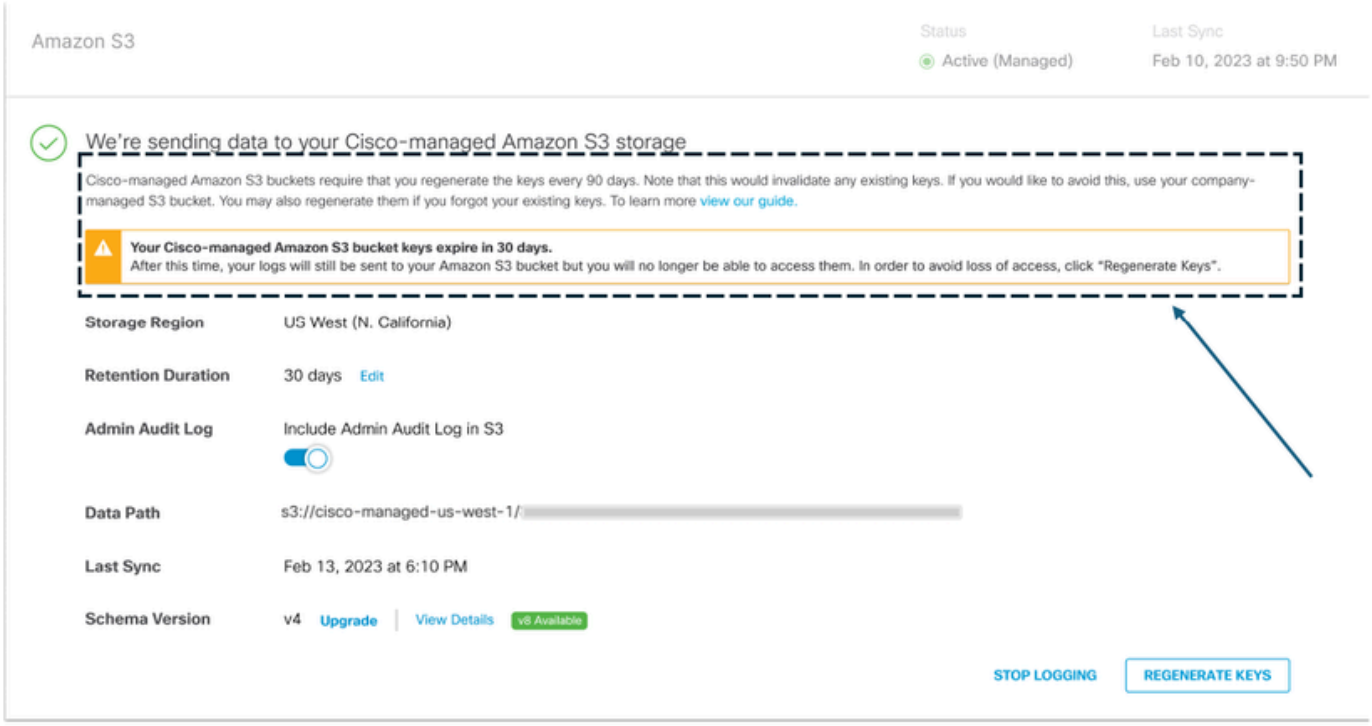
Solução

1. Navegue até Admin > Log Management e na área do Amazon S3 selecione Use a Cisco-managed Amazon S3 bucket

---

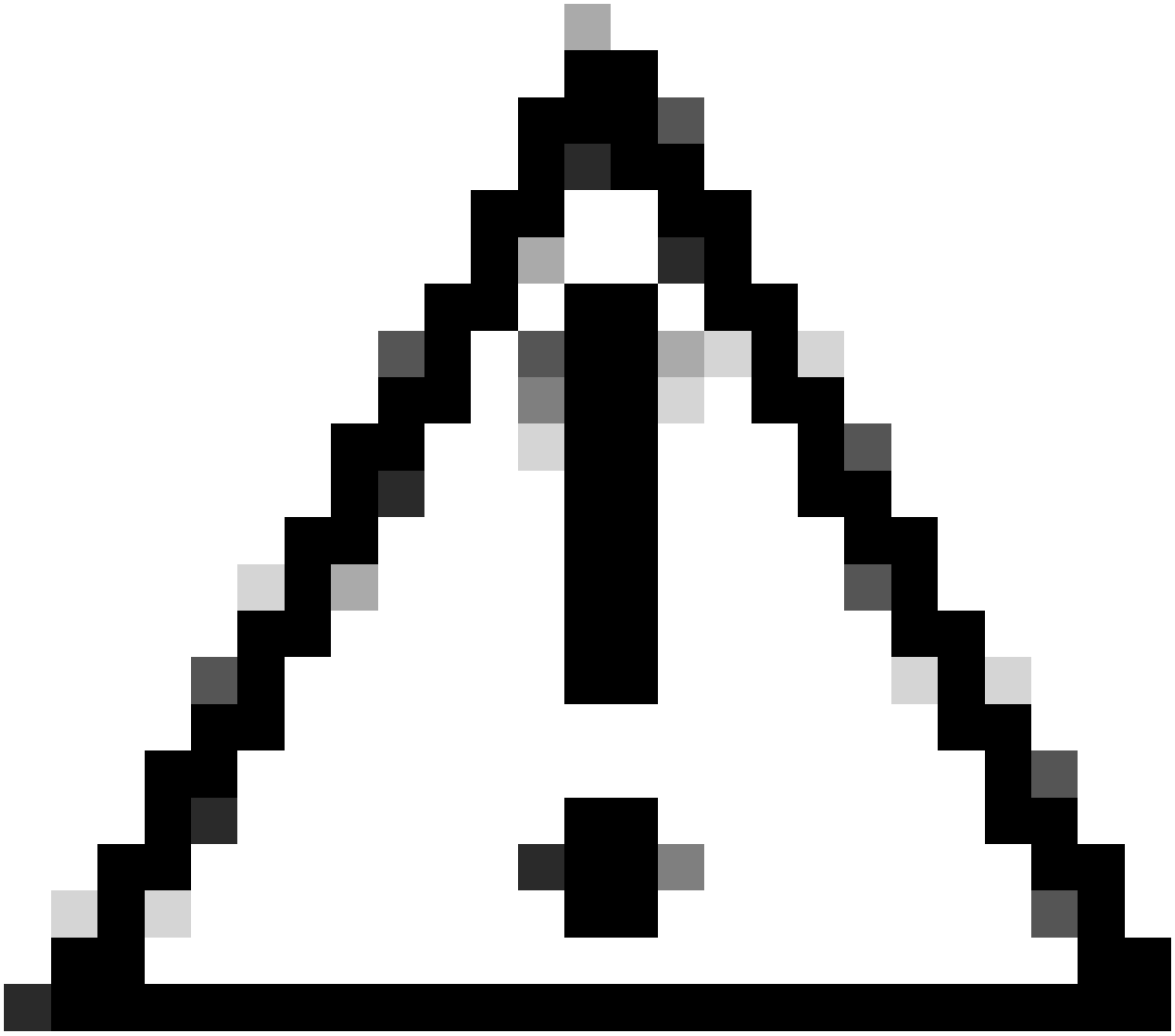


Tip: O novo banner é apresentado com uma mensagem de aviso sobre os novos requisitos de segurança de rotação das chaves de balde S3.

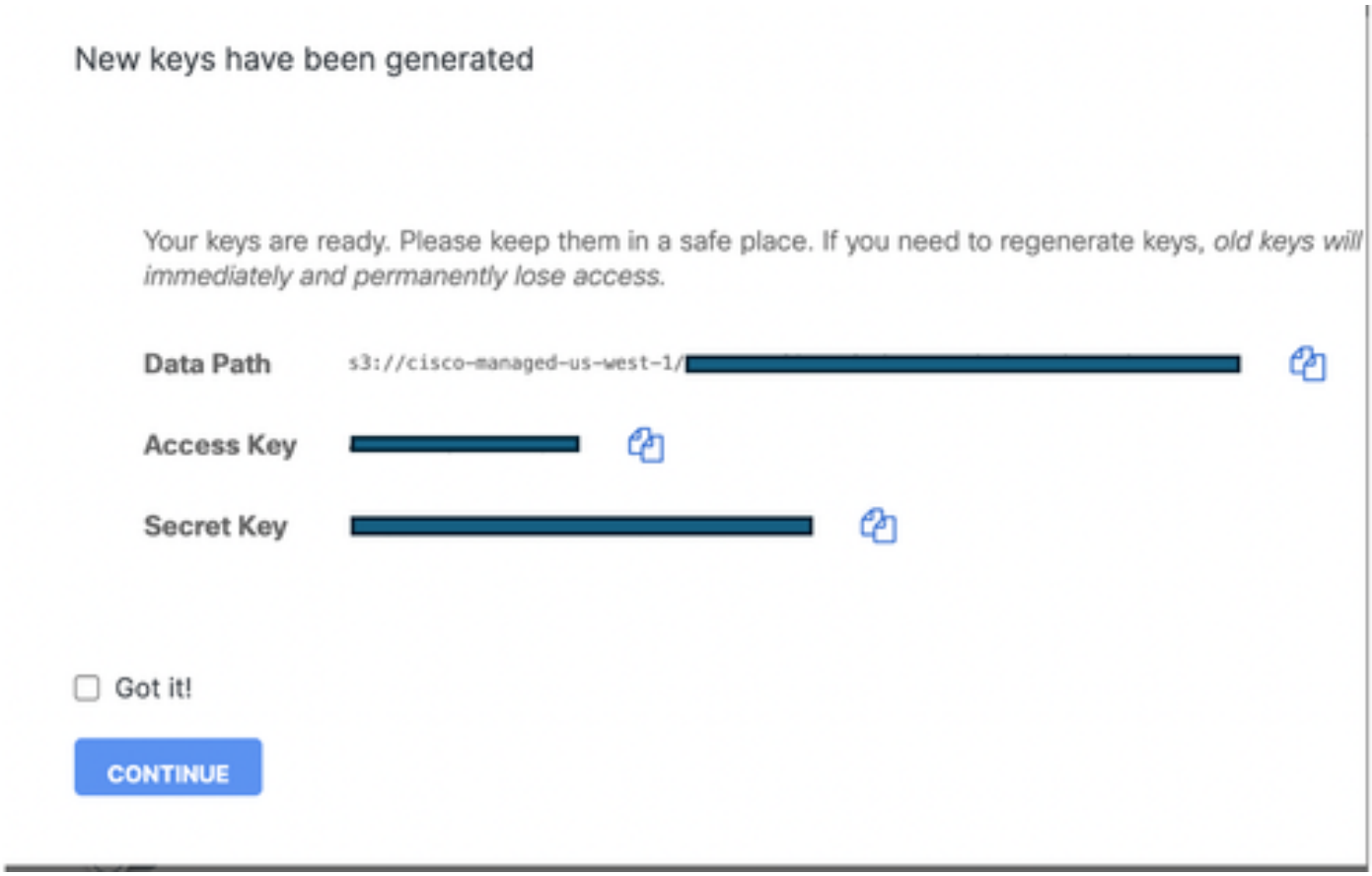


2. Gere suas novas chaves de Balde S3

3. Armazene sua nova chave em local seguro.



Caution: A chave e o segredo podem ser exibidos apenas uma vez e não são visíveis para a equipe de suporte da Cisco.



4. Atualize todos os logs de inclusão de sistema externo do bucket do Cisco-Managed S3 com a nova chave e o novo segredo.

Verifique O Acesso Ao Compartimento S3

Para verificar o Acesso ao seu S3 Bucket, você pode usar o formato de arquivos conforme esclarecido neste exemplo ou no guia de documentação do Secure Access and Umbrella.

1. Configure o AWS CLI com novas chaves geradas.

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


AWS Secret Access Key [None]:


Default region name [None]:


Default output format [None]:
```

2. Liste um dos logs salvos no seu S3-Bucket.

```
$ 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/
```

Informações Relacionadas

- Gerenciar o registro de acesso seguro da Cisco
- Formatos de log e controle de versão

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.