Controleer beveiligde toegang en paraplu S3 emmer toetsen rotatie (elke 90 dagen vereist)

Inhoud

Inleiding

Dit document beschrijft de stappen van het roteren van de S3 Bucket toetsen als deel van Cisco Security en best practices verbeteringen.

Achtergrondinformatie

Als onderdeel van de verbeteringen in Cisco Security en best practices moeten Cisco Umbrella en Cisco Secure Access-beheerders met Cisco-beheerde S3-emmers voor logopslag nu elke 90 dagen worden gedraaid in de IAM-toetsen voor de S3-emmer. Vroeger was er geen verplichting om deze sleutels te draaien, dit vereiste wordt van kracht vanaf 15 mei 2025.

Terwijl de gegevens in de emmer aan de beheerder toebehoren, is de emmer zelf Cisco-bezeten/beheerd. Om ervoor te zorgen dat Cisco-gebruikers zich houden aan de best practice op het gebied van beveiliging, vragen we onze Cisco Secure Access en Umbrella om hun sleutels ten minste elke 90 dagen te draaien. Dit helpt ervoor te zorgen dat onze gebruikers geen risico lopen op lekkage van gegevens of informatieopenbaarmaking en dat ze zich houden aan onze best practices op het gebied van beveiliging als toonaangevend beveiligingsbedrijf.

Deze beperking is niet van toepassing op niet-Cisco beheerde S3-emmers en we raden u aan naar uw eigen beheerde emmer te verhuizen. Deze beveiligingsbeperking creëert een probleem voor u.

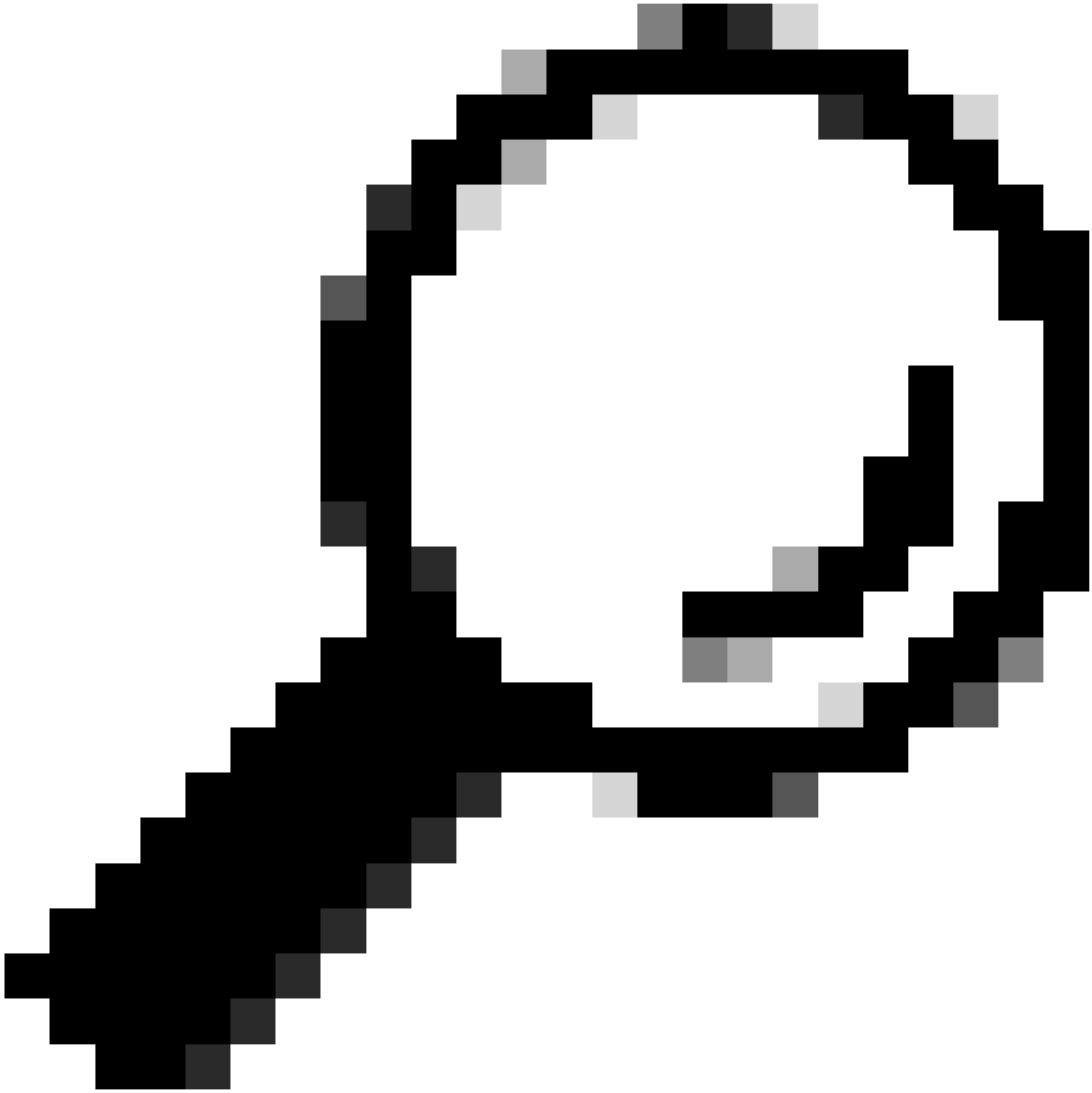
Probleem

Gebruikers die hun sleutels niet binnen 90 dagen kunnen draaien, hebben geen toegang meer tot hun door Cisco beheerde S3-emmers. De gegevens in de emmer worden nog steeds bijgewerkt met gelogde informatie, maar de emmer zelf wordt ontoegankelijk.

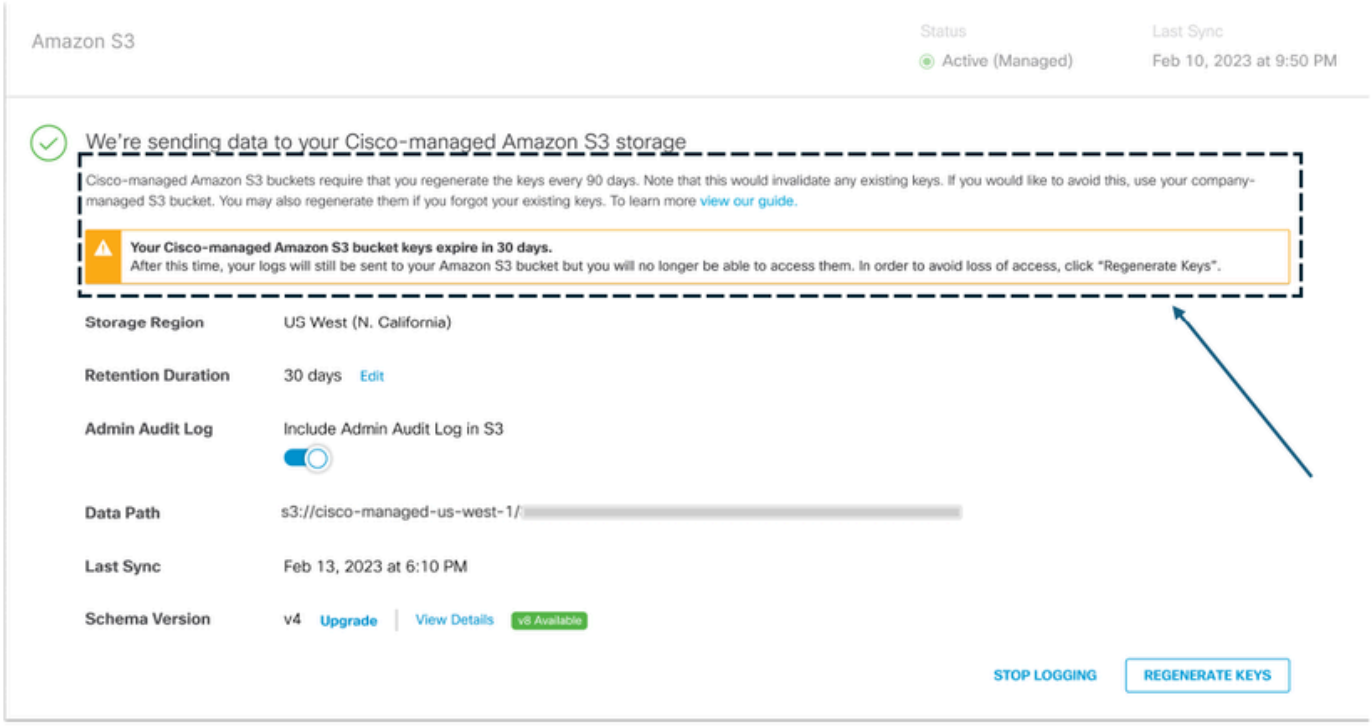
Oplossing

1. Navigeren naar Admin > Log Management en in het Amazon S3 gebied selecteren Gebruik een Cisco-beheerde Amazon S3 emmer

---

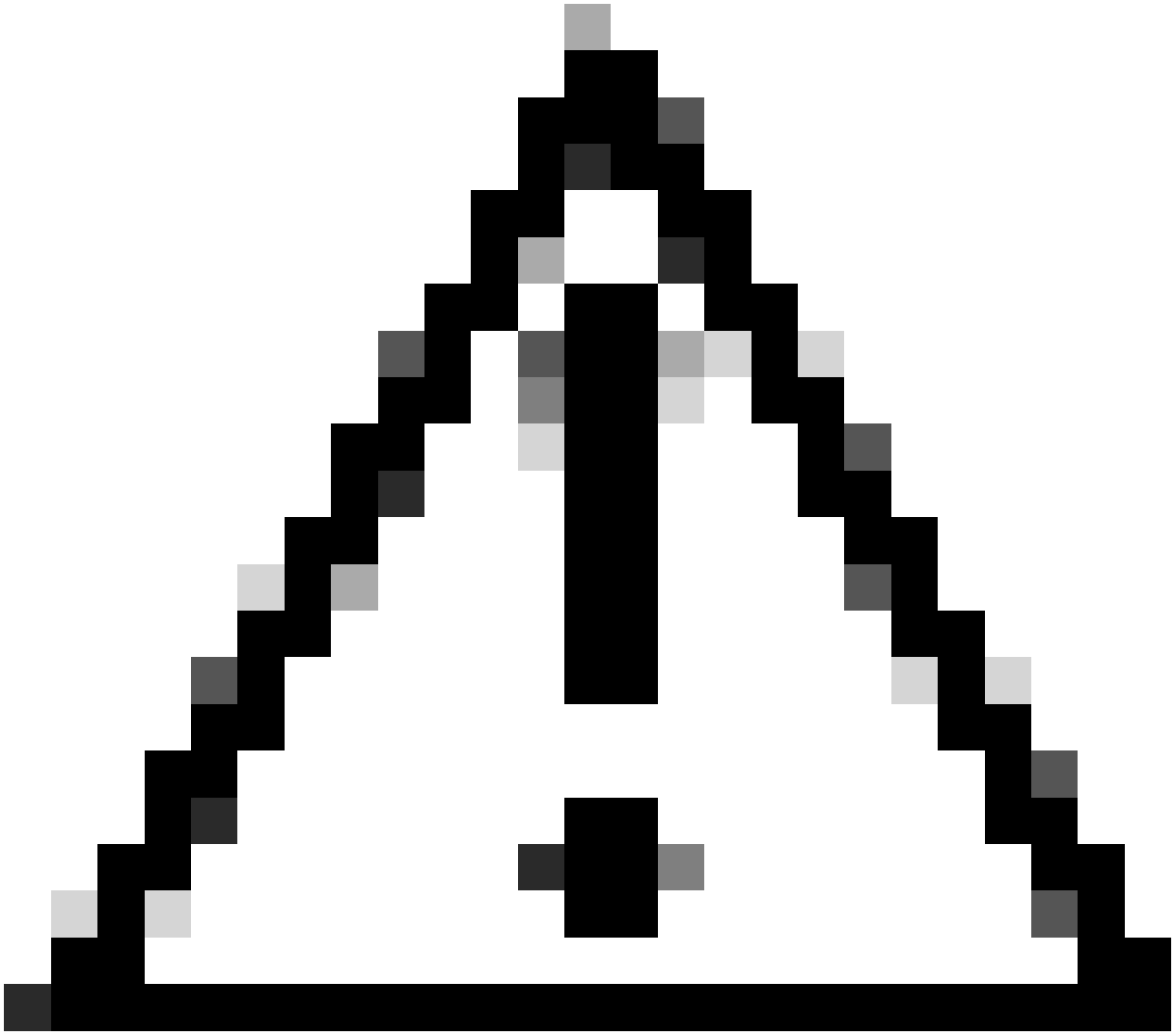


Tip: Nieuwe banner wordt gepresenteerd met een waarschuwingsbericht met betrekking tot de nieuwe veiligheidseisen van het draaien van de S3 Bucket toetsen.

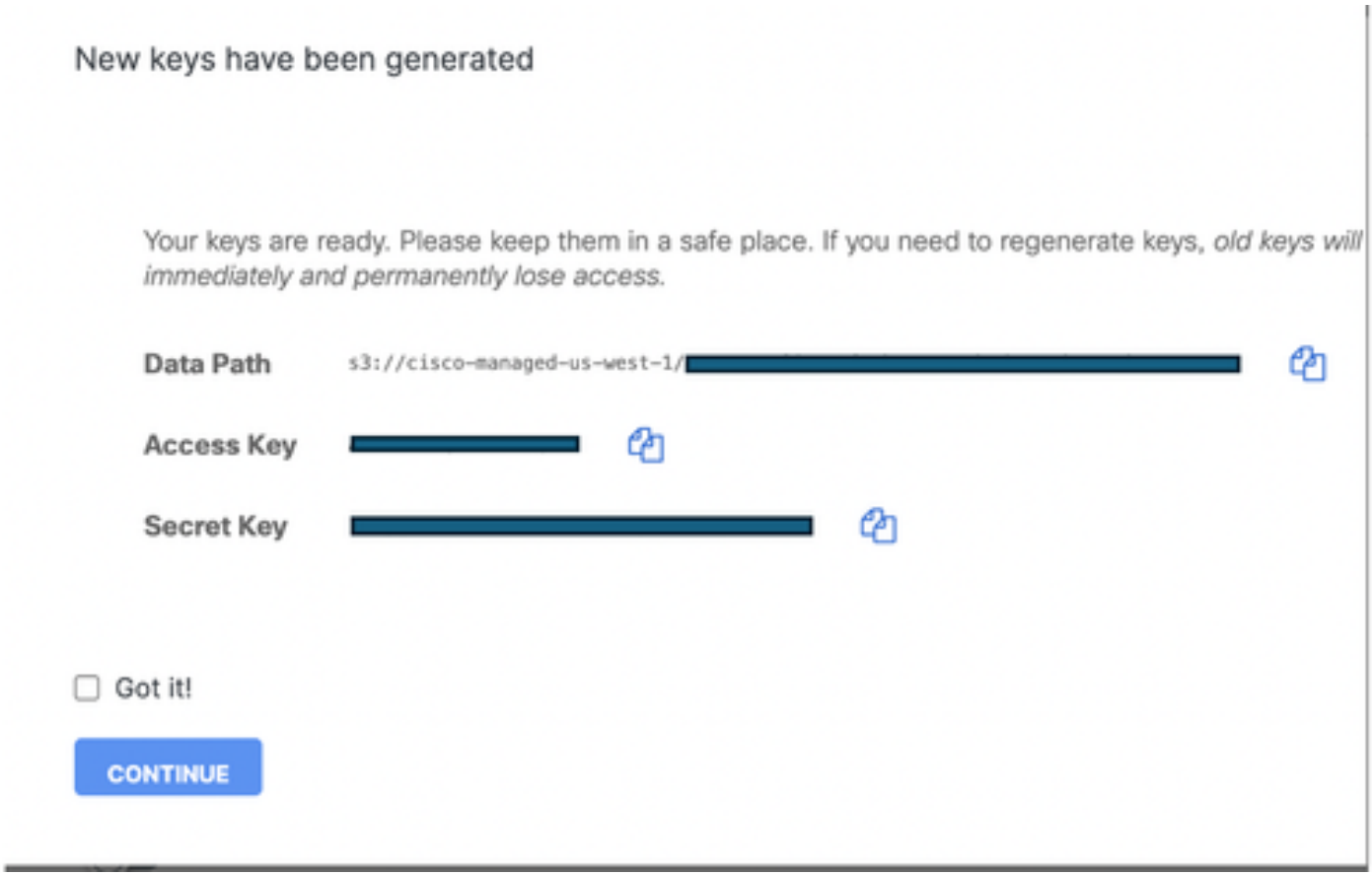


2. Genereer uw nieuwe S3 Bucket toetsen

3. Bewaar uw nieuwe sleutel op een veilige plaats.



Voorzichtig: Hun sleutel en geheim kunnen slechts eenmaal worden weergegeven en zijn niet zichtbaar voor het Cisco-ondersteuningsteam.



4. Update alle externe systemen die logs uit Cisco-beheerde S3-emmer opnemen met de nieuwe sleutel en het nieuwe geheim.

Controleer de toegang tot S3 emmer

Om de toegang tot uw S3 Bucket te verifiëren kunt u de bestandsindeling gebruiken zoals in dit voorbeeld of in de documentatie van Secure Access en Umbrella wordt verduidelijkt.

1. Configureer uw AWS CLI met nieuwe gegenereerde toetsen.

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



AWS Secret Access Key [None]:



Default region name [None]:



Default output format [None]:
```

2. Maak een lijst van de opgeslagen logs in uw S3-emmer.

```
$ 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/
```

Gerelateerde informatie

- Cisco Secure Access-vastlegging beheren
- Log indelingen en versies

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.