Verifica accesso sicuro e rotazione chiavi bucket Umbrella S3 (obbligatorio ogni 90 giorni)

Sommario

Introduzione

In questo documento vengono descritti i passaggi della rotazione delle chiavi Bucket S3 come parte dei miglioramenti alla sicurezza e alle best practice di Cisco.

Premesse

Nell'ambito dei miglioramenti apportati alla sicurezza e alle best practice di Cisco, gli amministratori di Cisco Umbrella e Cisco Secure Access con bucket S3 gestiti da Cisco per lo storage dei log devono ora ruotare le chiavi IAM per il bucket S3 ogni 90 giorni. In precedenza, non era necessario ruotare questi tasti. Questo requisito ha effetto a partire dal 15 maggio 2025.

Mentre i dati nel bucket appartengono all'amministratore, il bucket stesso è di proprietà di Cisco/gestito da Cisco. Per garantire la conformità degli utenti Cisco alle best practice sulla sicurezza, chiediamo ai nostri Cisco Secure Access e Umbrella di ruotare le loro chiavi almeno ogni 90 giorni. In questo modo possiamo evitare che i nostri utenti siano esposti al rischio di perdita di dati o di divulgazione di informazioni e rispettare le nostre best practice sulla sicurezza in quanto azienda leader nel settore della sicurezza.

Questa restrizione non si applica ai bucket S3 non gestiti da Cisco e si consiglia di passare al proprio bucket gestito se la restrizione di sicurezza crea un problema.

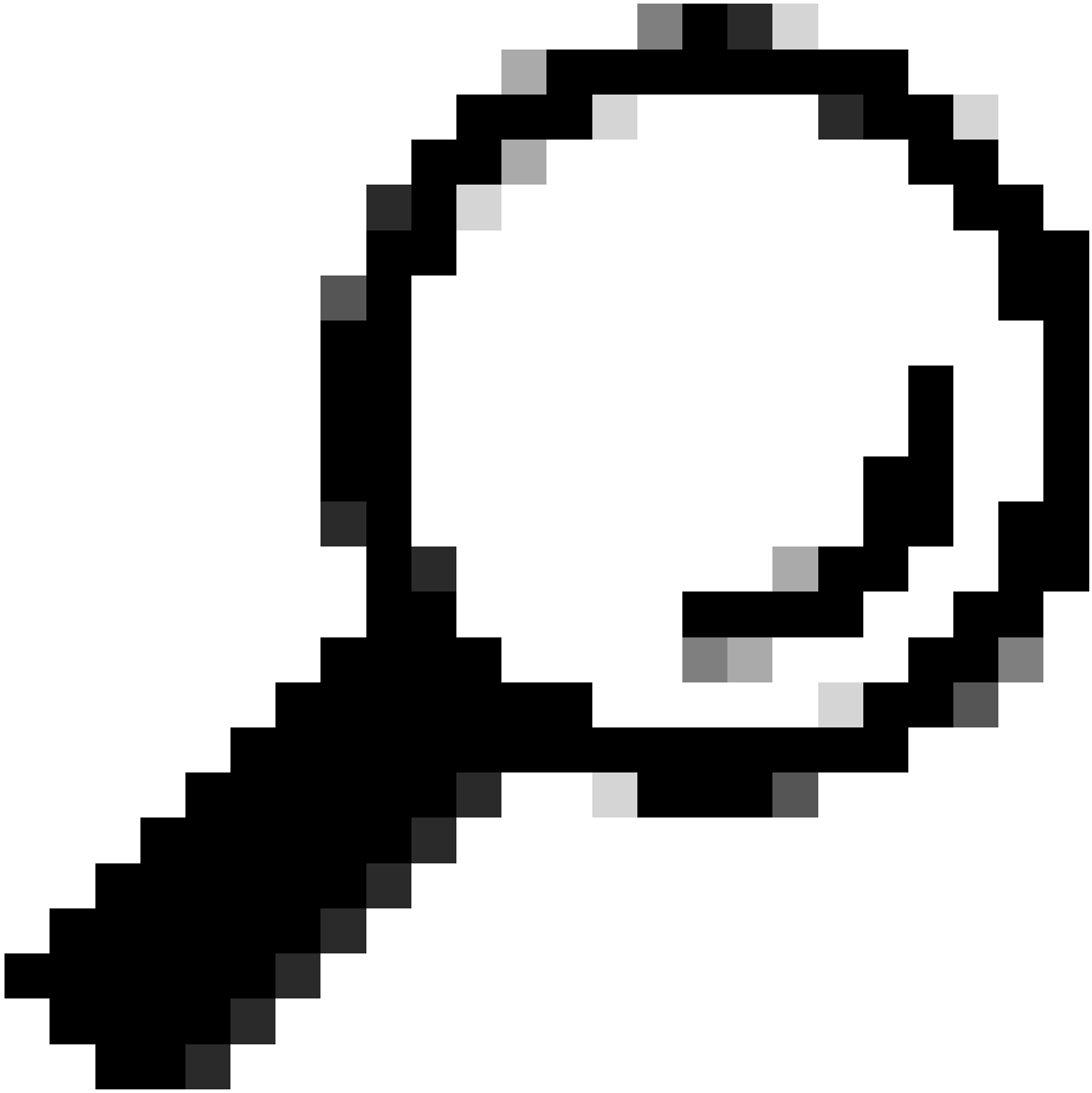
Problema

Gli utenti che non possono ruotare le chiavi entro 90 giorni non hanno più accesso ai bucket S3 gestiti da Cisco. I dati nel bucket continuano ad essere aggiornati con le informazioni registrate, ma il bucket stesso diventa inaccessibile.

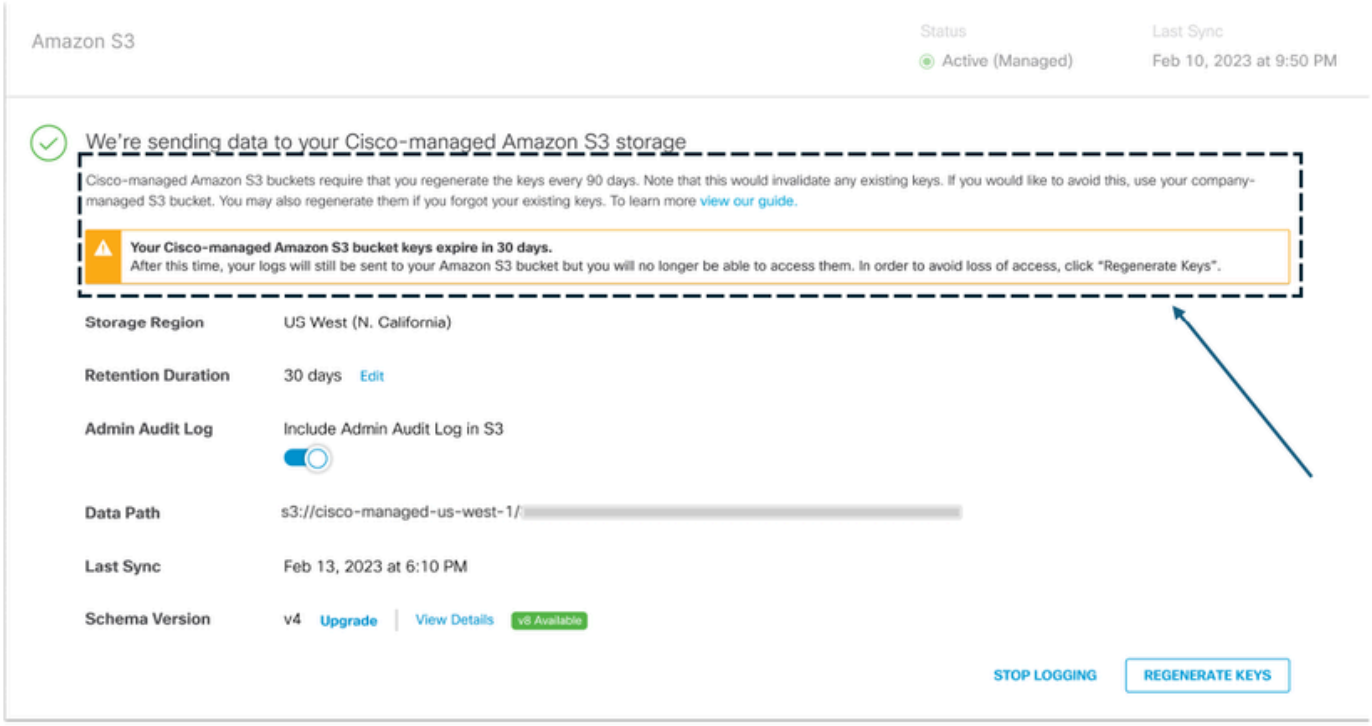
Soluzione

1. Passare a Admin > Log Management e nell'area Amazon S3 selezionare Use a Cisco-managed Amazon S3 bucket

---

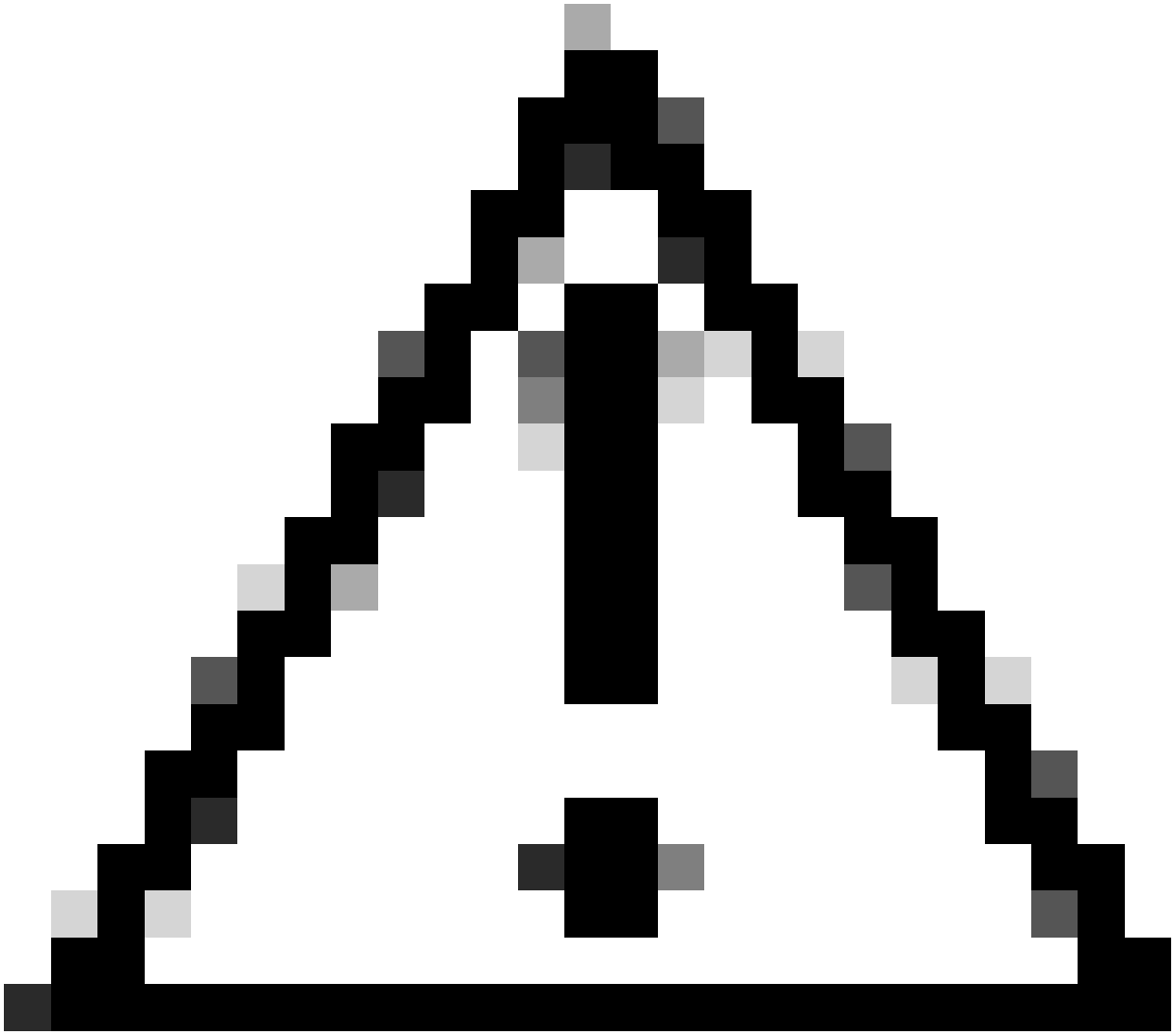


Suggerimento: Sul nuovo banner viene visualizzato un messaggio di avvertenza relativo ai nuovi requisiti di sicurezza per la rotazione delle chiavi Bucket S3.

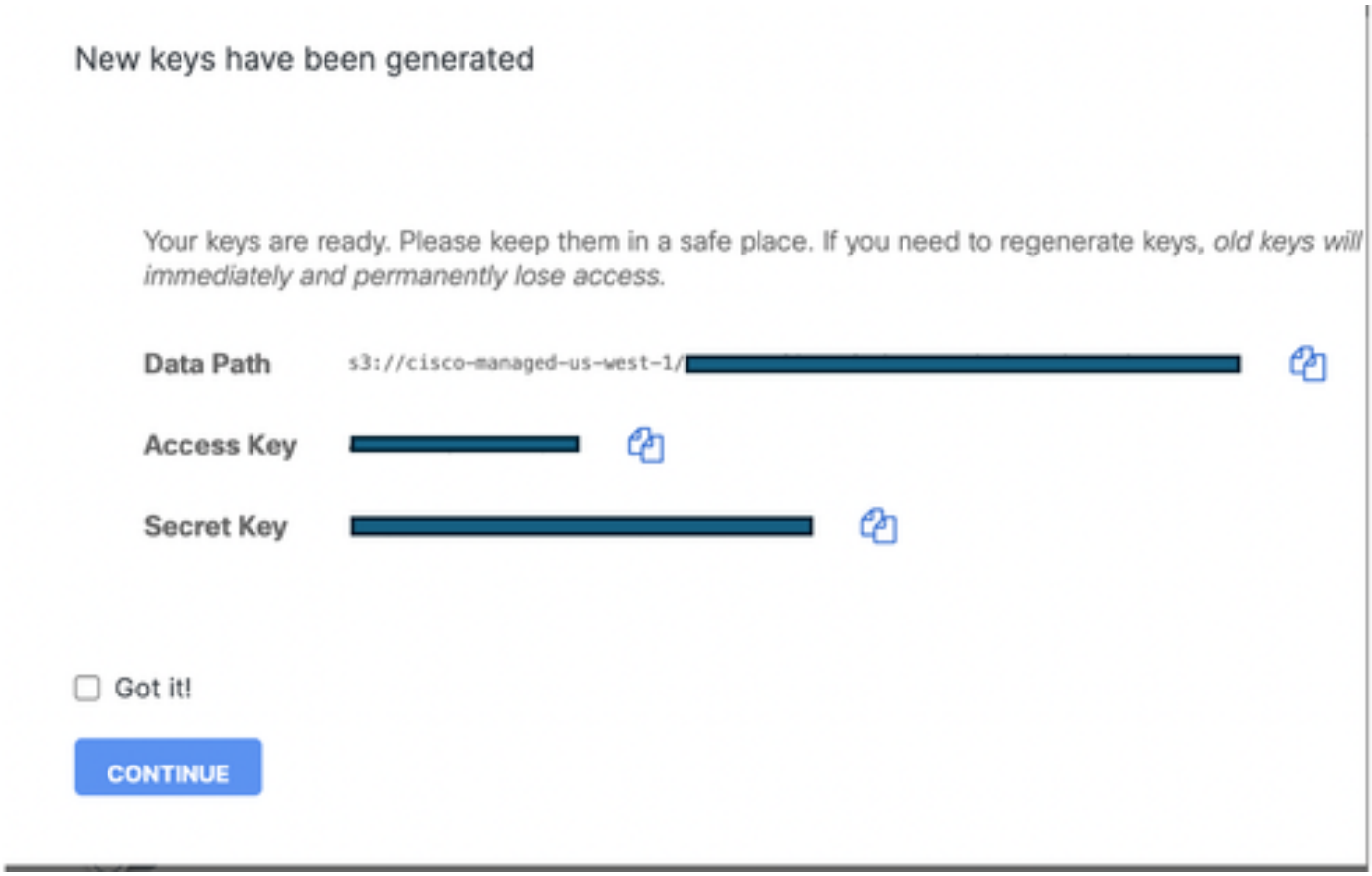


2. Generare le nuove chiavi del periodo fisso S3

3. Conservare la nuova chiave in un luogo sicuro.



Attenzione: Chiave e segreto possono essere visualizzati una sola volta e non sono visibili al team di supporto Cisco.



4. Aggiorna tutti i log di acquisizione del sistema esterno dal bucket S3 gestito da Cisco con la nuova chiave e il nuovo segreto.

Verifica L'Accesso Al Bucket S3

Per verificare l'accesso al bucket S3, è possibile utilizzare il formato di file specificato in questo esempio o nella guida alla documentazione di Secure Access and Umbrella.

1. Configurare la CLI di AWS con le nuove chiavi generate.

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



AWS Secret Access Key [None]:



Default region name [None]:



Default output format [None]:
```

2. Elencare uno dei log salvati nel bucket S3.

```
$ 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/
```

Informazioni correlate

- Gestisci registrazione accesso sicuro Cisco
- Formati di log e controllo delle versioni

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).