Scaricare i log da Umbrella Log Management utilizzando la CLI di AWS

Sommario

Introduzione

Questo documento descrive come scaricare i log da Umbrella Log Management utilizzando la CLI di AWS.

Panoramica

Una volta che la gestione dei log in Amazon S3 è stata configurata, si potrebbe desiderare di testare i file di log in fase di scrittura e sono scaricabili.

A tale scopo, abbiamo delineato un approccio che utilizza l'interfaccia della riga di comando AWS di Amazon

Per i metodi alternativi, vedere qui.

Prerequisiti

- Scaricare e installare AWS CLI da https://aws.amazon.com/cli/
- Creare il bucket gestito con Cisco come descritto qui
- In alternativa, configurare la registrazione in modo che utilizzi il proprio bucket S3 come descritto qui

Configurazione delle credenziali di sicurezza nella CLI di AWS

Nella riga di comando, immettere:

```
aws configure
```

Vi vengono poste queste quattro domande. Se è stato creato un bucket gestito da Cisco, i primi

tre sono stati forniti al momento della creazione del bucket. Per i bucket gestiti con Cisco, il 'Nome area predefinito' è elencato nel nome del bucket. Ad esempio, la regione per "cisco-managed-us-west-2" è "us-west-2". Per il proprio periodo fisso, l'area viene impostata in base alle impostazioni S3. Per un elenco completo delle regioni amazzoniche S3, si prega di vedere qui.

È possibile eseguire di nuovo la configurazione in qualsiasi momento e verrà visualizzata una versione ridotta delle credenziali, ad esempio:

ID chiave di accesso AWS [**********HVBA]:

Chiave di accesso segreto AWS [**********Fuori sede]:

Nome area predefinita [us-west-2]:

Default output format [None]:

Sincronizza il contenuto del bucket con la cartella locale

Immettere questo comando, sostituendo con "nomebucket" e "prefisso" con i dettagli del bucket.

```
aws s3 sync s3://<yourbucketname>/<prefix>/ <your local folder path>
```

Il prefisso è facoltativo per i bucket di proprietà dell'amministratore e obbligatorio per quelli gestiti da Cisco. Ad esempio:

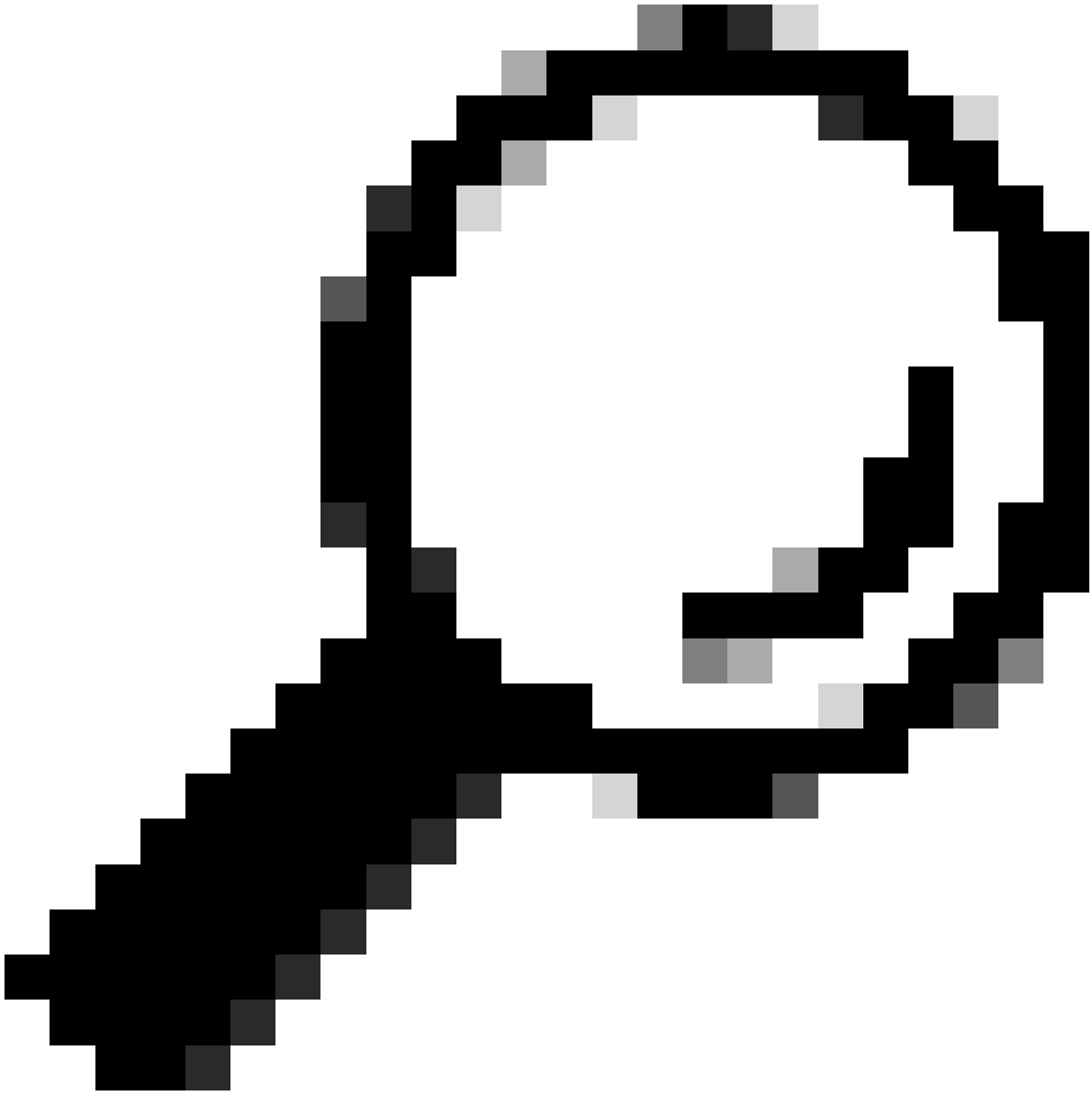
```
aws s3 sync s3://cisco-managed-us-west-2/2293370_96b88e0e21ac0136373b7009a340dc5f/ c:\temp\
```

Viene visualizzato un output simile al seguente:

scarica: s3://cisco-managed-us-west-2/2293370_96b88e0e21ac0136373b7009a340dc5f/dnslogs/2018-05-01/2018-05-01-12-30-0e41.csv.gz to dnslogs\2018-05-01\2018-05-01-12-30-0e41.csv.gz

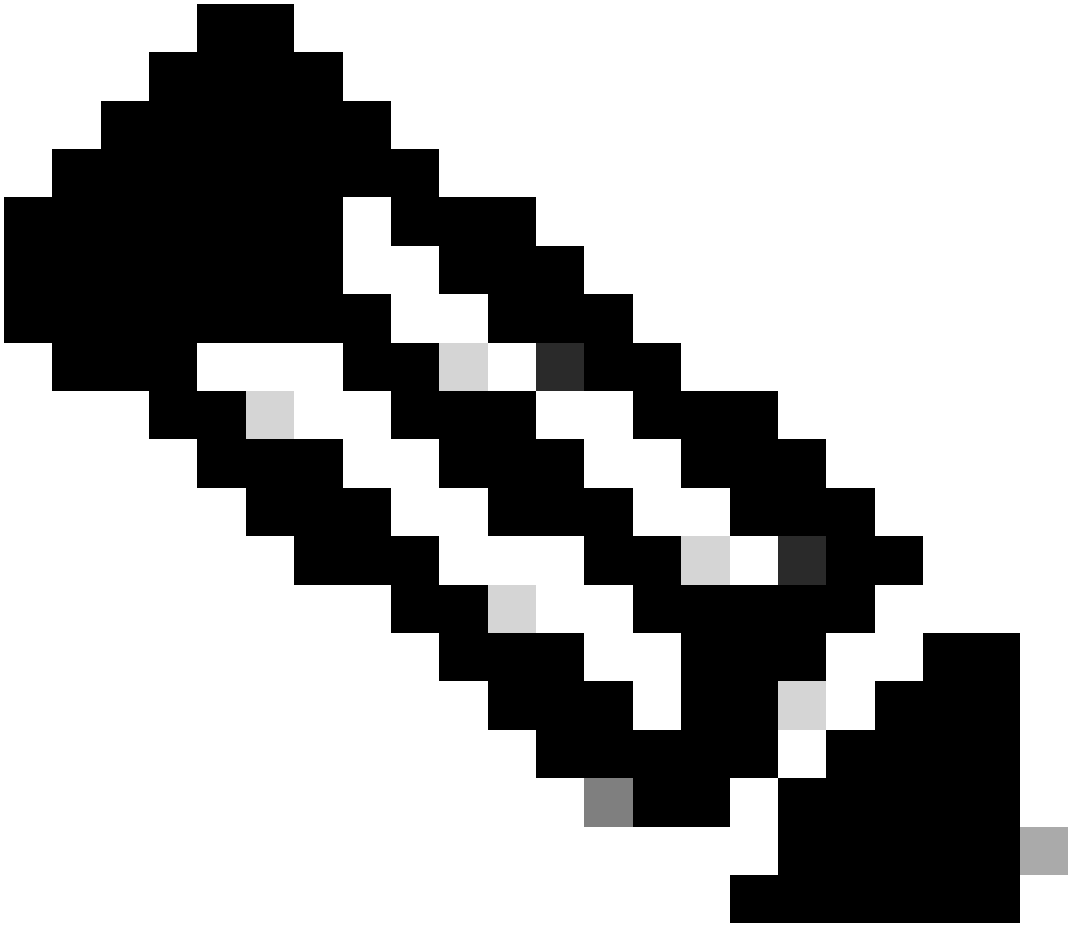
scarica: s3://ccisco-managed-us-west-2/2293370_96b88e0e21ac0136373b7009a340dc5f/dnslogs/2018-05-01/2018-05-01-12-40-0e41.csv.gz to dnslogs\2018-05-01\2018-05-01-12-40-0e41.csv.gz

scarica: s3://cisco-managed-us-west-2/2293370_96b88e0e21ac0136373b7009a340dc5f/dnslogs/2018-05-01/2018-05-01-12-30-b3ab.csv.gz in dnslogs\2018-05-01\2018-05-01-12-30-b3ab.csv.gz



Suggerimento: Il tentativo di elencare il contenuto di una radice bucket gestita da Cisco in genere genera un errore poiché il livello di accesso fornito non dispone dei diritti per elencare il contenuto della radice bucket. È tuttavia possibile elencare il contenuto del prefisso e delle cartelle all'interno del bucket utilizzando un comando simile al seguente:

```
aws s3 Is s3:////dnslogs
```



Nota: La documentazione completa relativa all'interfaccia della riga di comando è disponibile qui in Amazon.

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).