Télécharger les journaux depuis la gestion des journaux Umbrella à l'aide de l'ILC AWS

Table des matières

Introduction

Ce document décrit comment télécharger des journaux à partir d'Umbrella Log Management à l'aide de l'interface de ligne de commande AWS.

Aperçu

Une fois que votre gestion des journaux dans l'Amazon S3 a été configuré, vous pouvez souhaiter tester les fichiers journaux sont en cours d'écriture et sont téléchargeables.

Pour ce faire, nous avons présenté une approche utilisant l'interface de ligne de commande AWS d'Amazon

Pour des méthodes alternatives, veuillez consulter ici.

Conditions préalables

- Téléchargez et installez l'interface de ligne de commande AWS depuis https://aws.amazon.com/cli/
- Créez votre compartiment géré Cisco comme décrit ici
- Vous pouvez également configurer la journalisation pour utiliser votre propre compartiment S3, comme décrit ici

Configuration de vos informations de sécurité dans AWS CLI

Sur la ligne de commande, saisissez :

```
aws configure
```

Ces quatre questions vous sont présentées. Si vous avez créé un groupement géré par Cisco, les trois premiers ont été fournis lorsque vous avez créé le groupement. Pour les regroupements gérés Cisco, le nom de la région par défaut est indiqué dans votre nom de regroupement. Par exemple, la région pour « cisco-managed-us-west-2 » est « us-west-2 ». Pour votre propre bucket, la région est définie en fonction de vos paramètres S3. Pour une liste complète des régions d'Amazon S3, veuillez consulter ici.

Vous pouvez réexécuter cette configuration à tout moment et elle affiche une version réduite de vos informations d'identification, par exemple :

ID de clé d'accès AWS [**********HVBA] :

Clé d'accès secrète AWS [**********OutFw] :

Nom de la région par défaut [us-west-2] :

Format de sortie par défaut [Aucun] :

Synchroniser le contenu du compartiment dans le dossier local

Entrez cette commande, en remplaçant par "votrenom de compartiment" et "préfixe" par les détails de votre compartiment.

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

Le préfixe est facultatif pour les compartiments appartenant à l'administrateur et obligatoire pour les compartiments gérés par Cisco. Exemple :

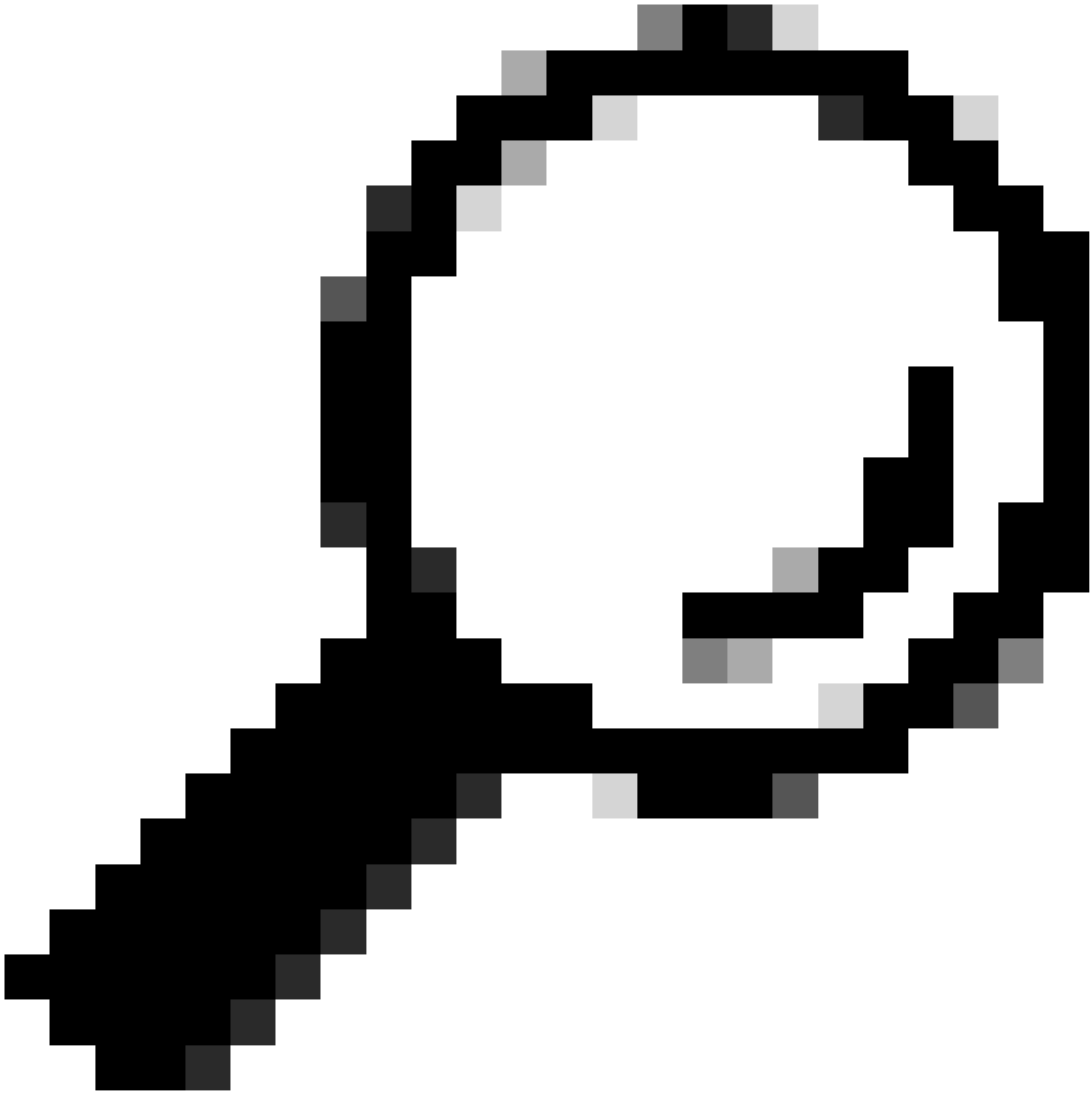
```
aws s3 sync s3://cisco-managed-us-west-2/2293370_96b88e0e21ac0136373b7009a340dc5f/ c:\temp\
```

Vous voyez un résultat comme ceci :

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

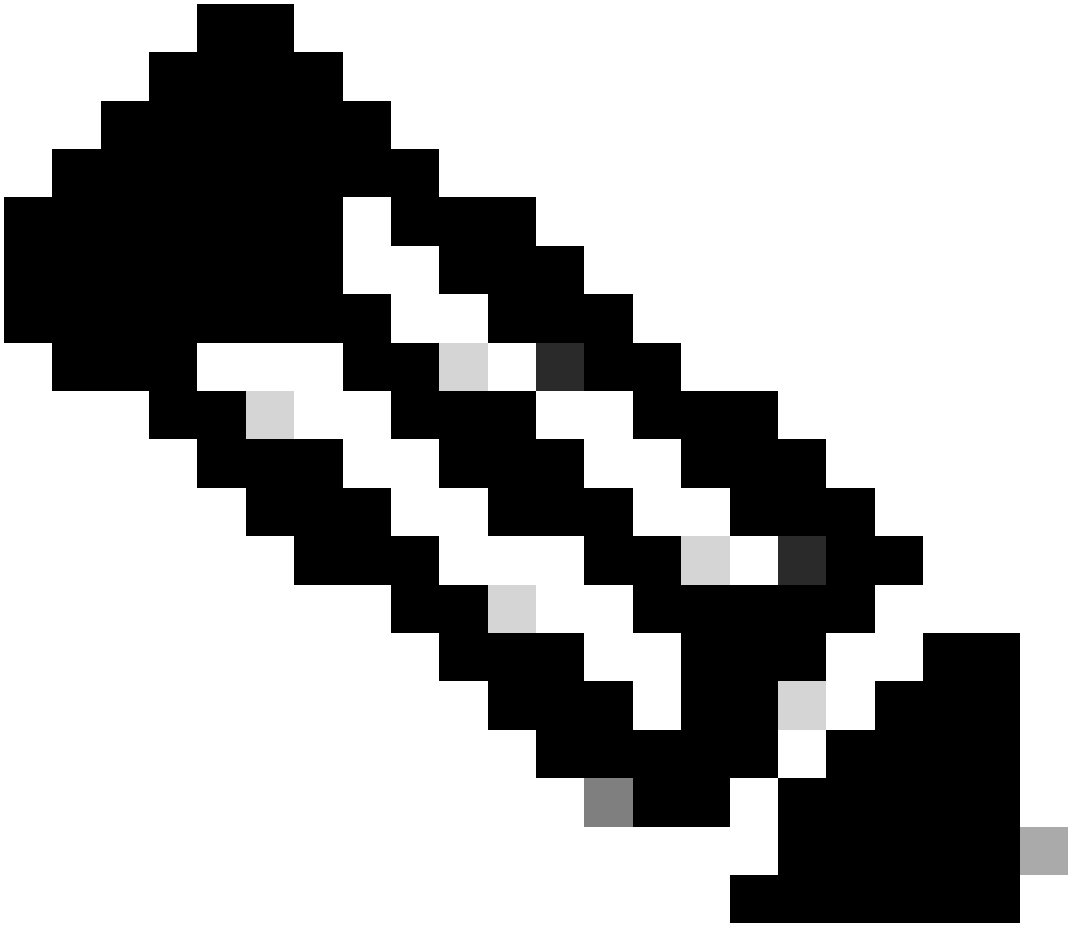
téléchargement : s3://ccisco-managed-us-west-2/2293370_96b88e0e21ac0136373b7009a340dc5f/dnslogs/2018-05-01/2018-05-01-12-40-0e41.csv.gz à dnslogs\2018-05-01\2018-05-01-12-40-0e41.csv.gz

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



Conseil : Toute tentative d'énumération du contenu d'une racine de bucket gérée par Cisco génère généralement une erreur, car le niveau d'accès fourni ne dispose pas des droits nécessaires pour énumérer le contenu de la racine de bucket. Vous pouvez cependant lister le contenu du préfixe et des dossiers dans le bucket en utilisant une commande similaire à celle-ci :

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



Remarque : La documentation complète de l'interface de ligne de commande est disponible sur Amazon ici.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.