Télécharger les journaux à partir de la gestion des journaux Umbrella dans AWS S3

Table des matières

Introduction

Ce document décrit comment télécharger des journaux à partir de la Gestion des journaux Umbrella dans AWS S3.

Aperçu

Une fois que vous avez configuré et testé le bon fonctionnement de la gestion des journaux dans l'Amazon S3, vous pouvez commencer à télécharger et à stocker automatiquement les journaux dans votre infrastructure réseau, soit pour les conserver, soit pour les consommer (ou les deux).

Pour ce faire, nous avons défini une approche utilisant s3tools à partir de http://s3tools.org. s3tools utilise l'utilitaire de ligne de commande s3cmd pour Linux ou OS/X. D'autres outils peuvent accomplir une fonction similaire pour les utilisateurs Windows :

- Pour un outil de ligne de commande, vous pouvez télécharger un petit exécutable de ligne de commande ici.
- Si vous préférez une interface graphique, consultez S3 Browser (https://s3browser.com/), bien que nous ne décrivions pas comment l'utiliser parce que l'interface graphique n'est pas scriptable pour automatiser le processus. Cet article vous explique comment configurer les deux outils de ligne de commande. Vous pouvez utiliser les informations de l'étape 1 pour configurer l'application s3browser si vous le souhaitez.

Commencez par télécharger l'outil correspondant au système d'exploitation que vous souhaitez utiliser. Pour l'instant, nous couvrons juste s3cmd pour OS/X et Linux, bien que les étapes pour accéder à votre bucket et télécharger les données sont effectivement les mêmes pour Windows.

Accédez au programme d'installation à partir de s3tools ici.

Le programme d'installation n'exige pas que vous installiez le programme pour exécuter la ligne de commande. Il vous suffit donc d'extraire le package que vous avez téléchargé.

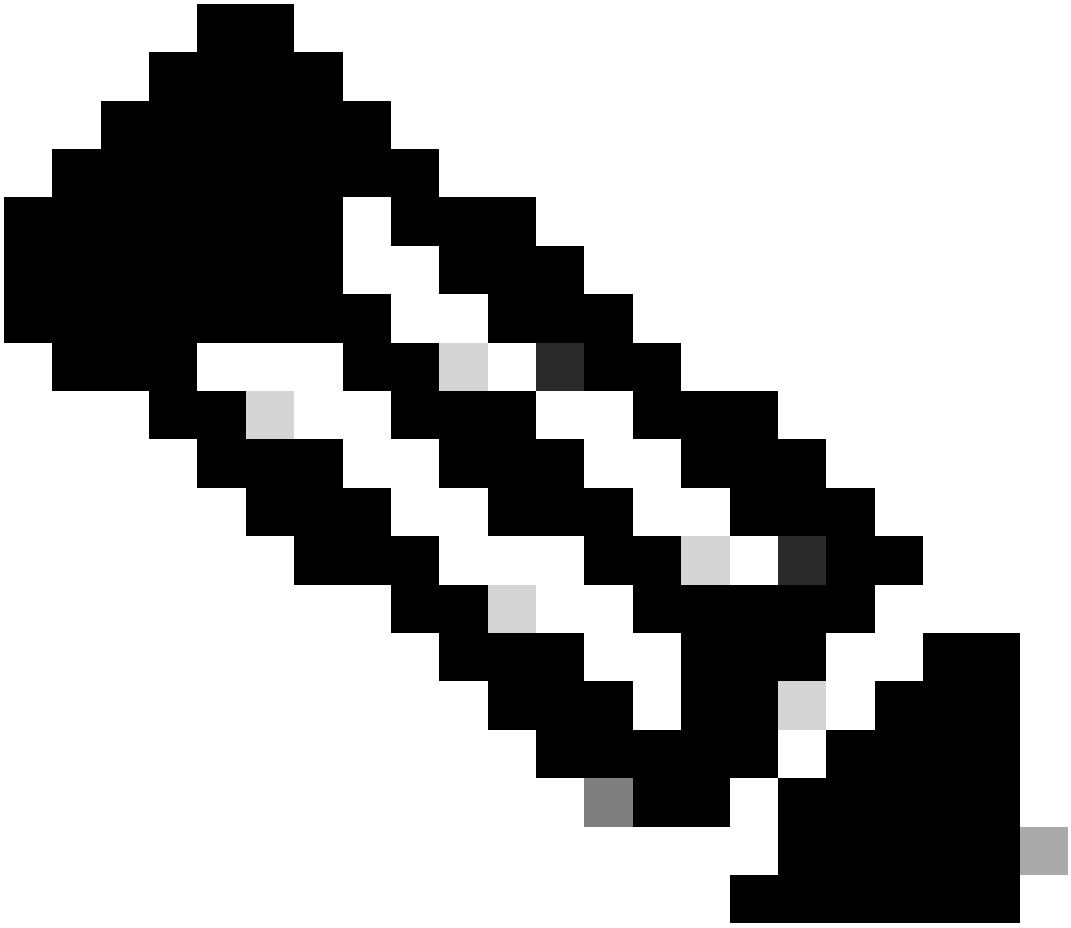
Étape 1 : Configuration de vos informations d'identification de sécurité dans AWS

Étape 1

1. Ajoutez une clé d'accès à votre compte Amazon Web Services pour activer l'accès à distance à votre outil local et la possibilité de télécharger, télécharger et modifier des fichiers dans S3. Connectez-vous à AWS et cliquez sur le nom de votre compte dans l'angle supérieur droit. Dans la liste déroulante, sélectionnez Security Credentials.
2. Une invite vous demande d'utiliser les Méthodes Recommandées d'Amazon et de créer un utilisateur IAM (Identity and Access Management) AWS. En substance, un utilisateur IAM s'assure que le compte que s3cmd utilise pour accéder à votre bucket n'est pas le compte principal (par exemple, votre compte) pour l'ensemble de votre configuration S3. En créant des utilisateurs IAM individuels pour les personnes accédant à votre compte, vous pouvez attribuer à chaque utilisateur IAM un ensemble unique d'informations d'identification de sécurité. Vous pouvez également accorder différentes autorisations à chaque utilisateur IAM. Si nécessaire, vous pouvez modifier ou révoquer les autorisations d'un utilisateur IAM à tout moment.
   Pour plus d'informations sur les utilisateurs IAM et les meilleures pratiques AWS, consultez ici.

Étape 2

1. Cliquez sur Get Started with IAM Users pour créer un utilisateur IAM ayant accès à votre compartiment S3. Accédez à un écran dans lequel vous pouvez créer un utilisateur IAM.
2. Cliquez sur Create New Users et renseignez les champs.
3. Après avoir créé le compte d'utilisateur, vous n'avez qu'une seule occasion d'obtenir deux informations critiques contenant vos informations d'identification de sécurité utilisateur Amazon. Nous vous suggérons fortement de les télécharger en utilisant le bouton en bas à droite pour les sauvegarder. Ils ne sont pas disponibles après cette étape de la configuration. Veillez à noter votre ID de clé d'accès et votre clé d'accès secrète, car nous en aurons besoin dans une étape ultérieure.



Remarque : Le compte d'utilisateur ne peut pas contenir d'espaces.

Étape 3

1. Ensuite, vous souhaitez ajouter une stratégie pour votre utilisateur IAM afin qu'il ait accès à votre compartiment S3. Cliquez sur l'utilisateur que vous venez de créer, puis faites défiler les propriétés des utilisateurs vers le bas jusqu'à ce que le bouton Attacher une stratégie s'affiche.
2. Cliquez sur Attacher une stratégie, puis entrez « s3 » dans le filtre de type de stratégie. Cela devrait montrer deux résultats "AmazonS3FullAccess" et "AmazonS3ReadOnlyAccess".
3. Sélectionnez AmazonS3FullAccess, puis cliquez sur Attacher une stratégie.

Étape 2 : Configuration d'un outil pour télécharger les journaux DNS à partir du compartiment

s3cmd pour MacOS et Linux

1. Accédez au chemin d’accès que vous avez extrait de s3cmd à l’étape précédente et, à partir de Terminal, tapez :

```
./s3cmd --configure
```

   Cela devrait vous amener à une invite vous demandant de fournir vos informations d'identification de sécurité :

Saisissez de nouvelles valeurs ou acceptez les valeurs par défaut entre crochets avec la touche Entrée.

Reportez-vous au manuel d'utilisation pour une description détaillée de toutes les options.

La clé d'accès et la clé secrète sont vos identifiants pour Amazon S3. Laissez-les vides pour utiliser les variables env.

Clé d'accès [VOTRE CLÉ D'ACCÈS] :

Clé secrète [VOTRE CLÉ SECRÈTE] :

2. Ensuite, vous serez invité à répondre à une série de questions sur la façon dont vous souhaitez configurer l'accès à votre compartiment. Dans ce cas, nous ne configurons pas de mot de passe de cryptage (GPG) et nous n'utilisons pas HTTPS ni de serveur proxy. Si votre réseau ou vos préférences diffèrent, renseignez les champs obligatoires :

Région par défaut [US] :

Le mot de passe de chiffrement est utilisé pour protéger vos fichiers contre la lecture par des personnes non autorisées lors du transfert vers S3

Mot de passe de chiffrement :

Chemin vers le programme GPG [Aucun] :

Lors de l'utilisation du protocole HTTPS sécurisé, toutes les communications avec les serveurs Amazon S3 sont protégées contre l'écoute électronique tierce. Cette méthode est

plus lent que le HTTP simple, et ne peut être mis en proxy qu'avec Python 2.7 ou plus récent

Utiliser le protocole HTTPS [Non] :

Sur certains réseaux, tous les accès Internet doivent passer par un proxy HTTP.

Essayez de le définir ici si vous ne pouvez pas vous connecter directement à S3

Nom du serveur proxy HTTP :

Après avoir saisi des paramètres spécifiques au réseau ou un cryptage, vous avez la possibilité de consulter les éléments suivants :

Nouveaux paramètres :

Clé d'accès : VOTRE CLÉ

Clé secrète : VOTRE CLÉ SECRÈTE

Région par défaut : US

Mot de passe de chiffrement :

Chemin vers le programme GPG : Aucune

Utiliser le protocole HTTPS : Faux

Nom du serveur proxy HTTP :

Port du serveur proxy HTTP : 0

Enfin, vous êtes invité à tester et, si vous réussissez, enregistrez les paramètres :

Tester l'accès avec les informations d'identification fournies ? [O/n] o

Veuillez patienter pendant la tentative de mise en vente de tous les compartiments...

Succès. Votre clé d'accès et votre clé secrète ont bien fonctionné ��

Vérification du fonctionnement du cryptage...

Non configuré. Peu importe.

Enregistrer les paramètres ? [o/N]

Exécutable de la ligne de commande Windows (s3.exe)

Après avoir téléchargé l'outil (https://s3.codeplex.com/releases/view/47595), copiez le fichier .exe dans votre dossier de travail préféré et, à partir de l'invite de commandes, tapez ceci, en remplaçant votre clé d'accès et votre mot de passe secret :

<#root>

```
s3 auth [
```

```
]
```

Pour plus d'informations sur la syntaxe d'authentification, lisez ici.

Étape 3 : Test du téléchargement de fichiers à partir de votre compartiment

Étape 1 : Tester le téléchargement

s3cmd pour OS/X et Linux

À partir du terminal, exécutez cette commande où « my-organization-name-log-bucket » est le nom de votre bucket déjà configuré dans la partie Gestion des journaux du tableau de bord Umbrella. Dans cet exemple, ceci est exécuté à partir du dossier qui contient l'exécutable s3cmd et les fichiers sont livrés au même chemin, mais ceux-ci peuvent être modifiés :

<#root>

```
./s3cmd sync s3://my-organization-name-log-bucket ./
```

S'il existe une différence entre les fichiers de votre bucket et les fichiers du chemin de destination sur le disque, la synchronisation doit télécharger les fichiers manquants ou mis à jour. Le premier fichier récupéré doit être le fichier README généralement chargé :

./s3cmd sync s3://nom-mon-organisation-log-bucket ./

s3://my-organization-name-log-bucket/README_FROM_UMBRELLA.txt -> <fdopen> [1 sur 1]

1800 sur 1800 100 % en 0 15,00 kB/s effectués

Terminé. Téléchargement de 1 800 octets en 1 seconde, 1 800 bits/s

Tous les fichiers journaux présents sont également téléchargés. C'est à vous de définir une tâche cron pour programmer cette fonction régulièrement, mais vous devriez maintenant pouvoir télécharger automatiquement tous les fichiers journaux nouveaux ou modifiés dans votre bucket vers un chemin local pour une rétention à long terme.

Exécutable de la ligne de commande Windows (s3.exe)

À partir de l'invite de commandes, exécutez cette commande où « my-organization-name-log-bucket » est le nom de votre bucket déjà configuré dans la partie Gestion des journaux du tableau de bord Umbrella. Dans cet exemple, tous les fichiers du bucket (défini avec le caractère générique astérisque) sont téléchargés dans le dossier \dnslogbackups\.

<#root>

```
s3 get my-organization-name-log-bucket/* c:\dnslogbackups\
```

Pour plus d'informations sur la syntaxe de cette commande, lisez ici.

Étape 2 : Automatiser le téléchargement

Une fois que la syntaxe a été testée et fonctionne comme prévu, copiez les instructions dans un script de configuration d'une tâche cron (OS X / Linux) ou d'une tâche planifiée (Windows) ou utilisez tout autre outil d'automatisation des tâches que vous pourriez avoir à votre disposition. Il est également possible d'utiliser les outils pour supprimer des fichiers de votre bucket après les avoir téléchargés pour libérer de l'espace dans votre instance S3. Nous vous encourageons à consulter la documentation de l'outil que vous utilisez pour voir ce qui pourrait fonctionner le mieux pour votre politique de rétention des données.

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.