Intégration de Splunk à la gestion des journaux Umbrella avec S3 et synchronisation locale

Table des matières

Introduction

Ce document décrit comment configurer Splunk pour analyser les journaux de trafic DNS à partir d'un compartiment S3 géré par Cisco.

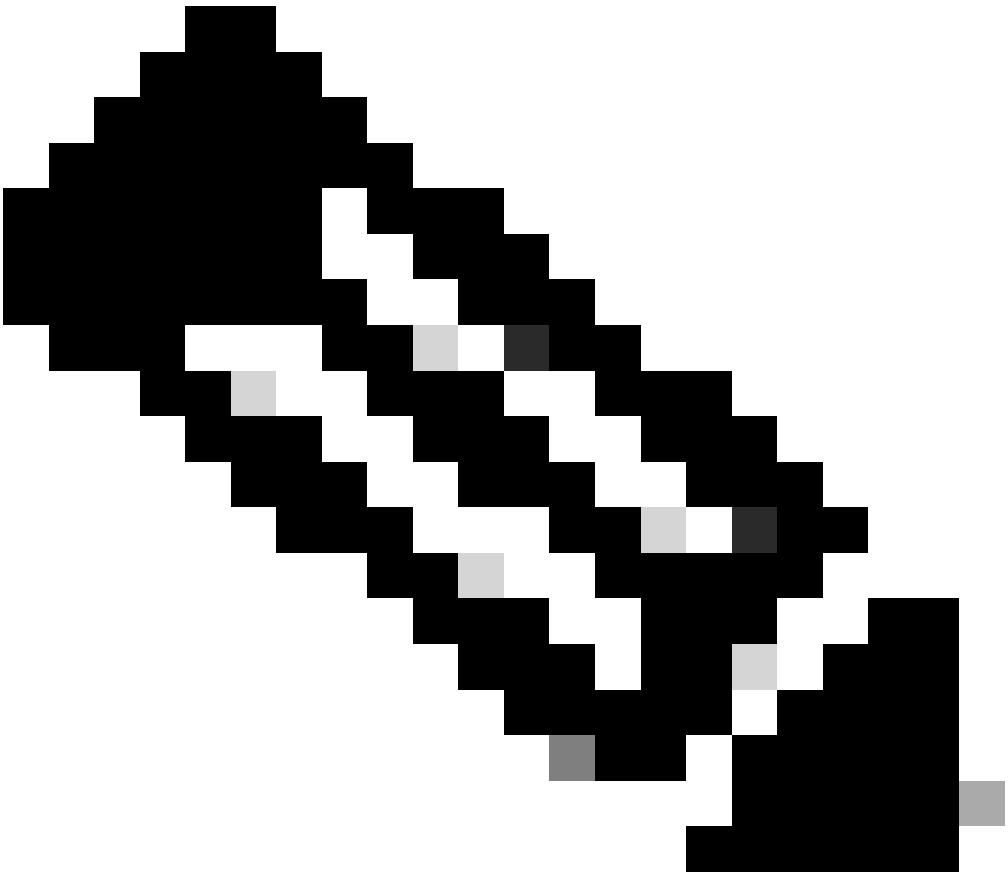
Aperçu

Splunk est un outil d'analyse de journaux. Il fournit une interface puissante pour analyser de grandes quantités de données, telles que les journaux fournis par Cisco Umbrella pour votre trafic DNS. Cet article décrit comment :

- Configurez votre compartiment S3 géré par Cisco dans votre tableau de bord.
- Vérifiez que les conditions requises pour l'interface de ligne de commande AWS (AWS CLI) sont remplies.
- Créez une tâche cron pour récupérer des fichiers du bucket et les stocker localement sur votre serveur.
- Configurez le Splunk pour lire à partir d'un répertoire local.

Conditions préalables

- Téléchargez et installez l'interface de ligne de commande AWS (AWS CLI).
- Créez votre compartiment S3 géré par Cisco.



Remarque : Les clients existants d'Umbrella Insights et d'Umbrella Platform peuvent accéder à Log Management avec Amazon S3 via le tableau de bord. La gestion des journaux n'est pas disponible dans tous les packages. Contactez votre gestionnaire de compte si cette fonctionnalité vous intéresse.

Créer une tâche Cron sur le serveur Splunk

1. Créez un script shell nommé **pull-umbrella-logs.sh** avec le contenu fourni, qui s'exécute sur une tâche cron planifiée :

```
#!/bin/sh
cd <local data dir>
AWS_ACCESS_KEY_ID=<accesskey> AWS_SECRET_ACCESS_KEY=<secretkey> aws s3 sync <data path> .
```

Remplacez les espaces réservés par vos valeurs réelles :

-

: Répertoire sur le disque pour stocker les fichiers journaux téléchargés.

- : Clé d'accès du tableau de bord Umbrella.
- : Clé secrète du tableau de bord Umbrella.
- : Chemin de données de l'interface utilisateur de gestion des journaux (par exemple, s3://cisco-managed-

/1_2xxxxxxxxxxxxxxxxxa120c73a7c51fa6c61a4b6/dnslogs/
).

2. Enregistrez le script shell et définissez l'autorisation d'exécution. Le script doit appartenir à la racine.

```
$ chmod u+x pull-umbrella-logs.sh
```

3. Exécutez le **pull-umbrella-logs.sh** script manuellement pour confirmer que le processus de synchronisation fonctionne. Il n'est pas nécessaire de remplir complètement le formulaire; cette étape confirme que les informations d'identification et la logique de script sont correctes.

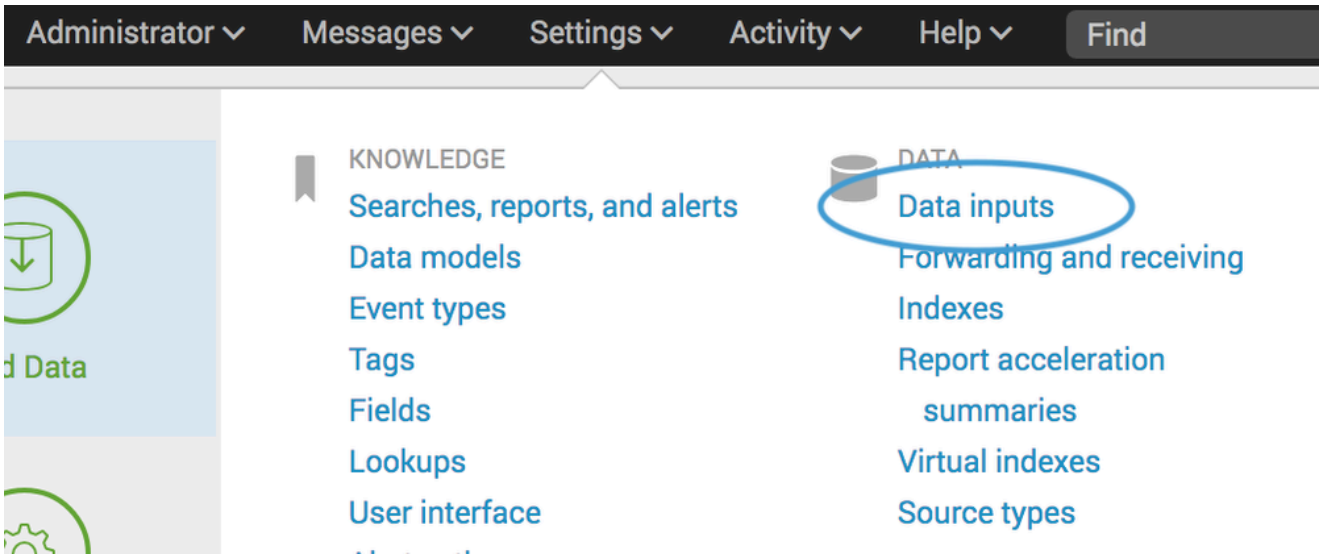
4. Ajoutez cette ligne à votre crontab de serveur Splunk :

```
*/5 * * * * root root /path/to/pull-umbrella-logs.sh &2>1 >/var/log/pull-umbrella-logs.txt
```

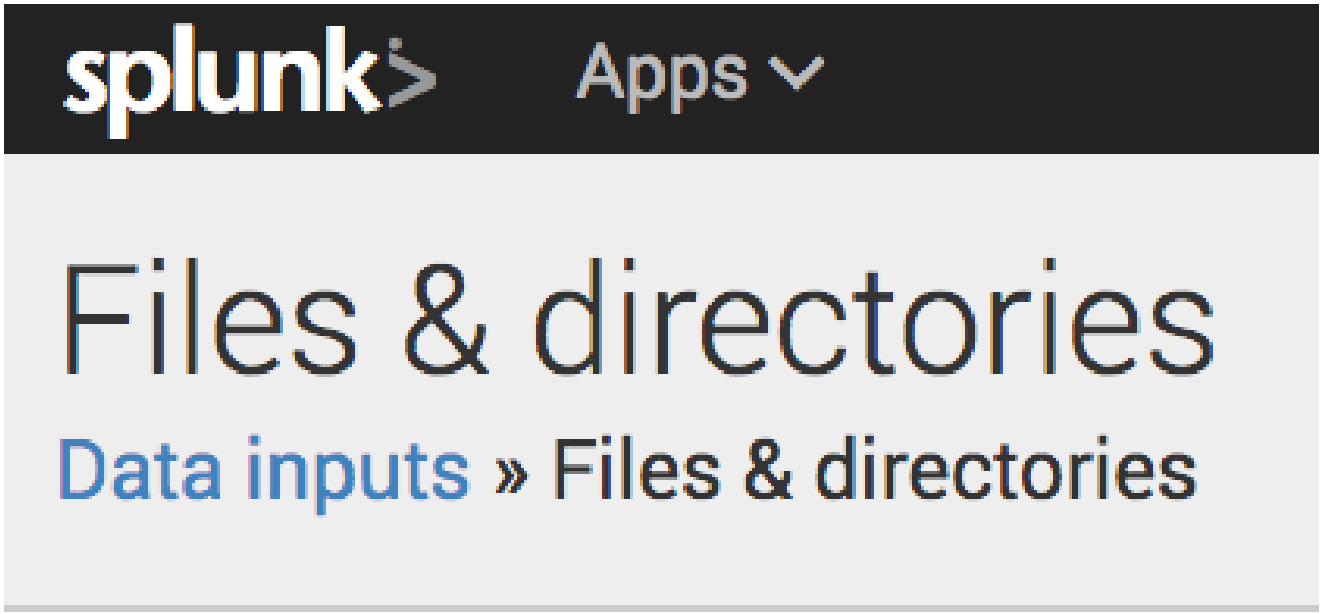
Veillez à modifier la ligne pour utiliser le chemin correct vers le script. Cette opération exécute une synchronisation toutes les cinq minutes. Le répertoire de stockage S3 est mis à jour toutes les 10 minutes et les données restent sur le stockage S3 pendant 30 jours. Cela permet de maintenir les deux en synchronisation.

Configurer le Splunk pour la lecture à partir d'un répertoire local

1. Dans Splunk, accédez à Settings > Data Inputs > Files & Directories et sélectionnez New.

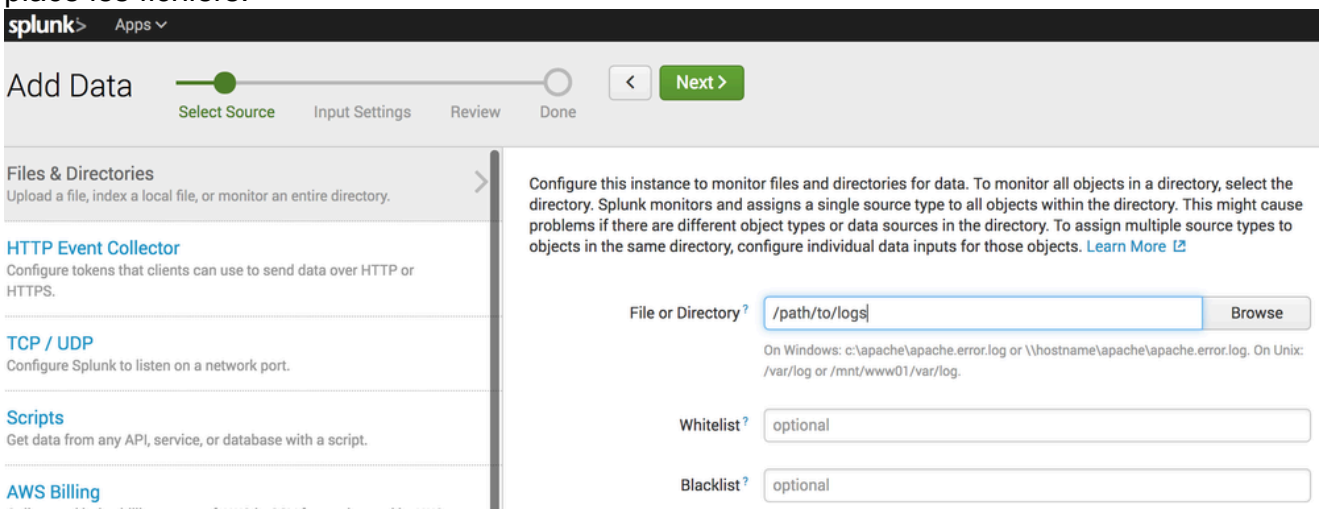


360002731126



360002731146

2. Dans le champ Fichier ou Répertoire, spécifiez le répertoire local où la synchronisation S3 place les fichiers.



360002731106

3. Cliquez sur Next et terminez l'Assistant en utilisant les paramètres par défaut.

Une fois que le répertoire local contient des données et que le Splunk est configuré, les données peuvent être disponibles pour la requête et le rapport dans le Splunk.

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.