Configurer le splunk avec un compartiment S3 autogéré

Table des matières

Introduction

Ce document décrit comment configurer Splunk avec un bucket S3 autogéré.

Aperçu

Splunk est un outil courant pour l'analyse des journaux. Il fournit une interface puissante pour analyser de grandes quantités de données, telles que les journaux fournis par Cisco Umbrella pour le trafic DNS de votre entreprise.

Cet article présente les bases de la mise en place et de l'exécution de Splunk afin qu'il puisse extraire les journaux de votre seau S3 et les consommer. Il y a deux étapes principales : la première consiste à configurer vos informations d'identification de sécurité AWS S3 pour autoriser l'accès du Splunk aux journaux, et la seconde consiste à configurer le Splunk lui-même pour qu'il pointe vers votre bucket.

La documentation du module complémentaire Splunk pour AWS S3 est disponible ici. Certaines ont été copiées textuellement dans ce document. Pour des questions spécifiques concernant la configuration de Splunk, veuillez vous reporter à http://docs.splunk.com/Documentation/AddOns/latest/AWS/Description

Cet article comporte les sections suivantes :

Conditions préalables

Le module complémentaire Splunk pour Amazon Web Services prend en charge ces plates-formes.

- Linux AWS
- RedHat
- Windows 2008R2, 2012R2

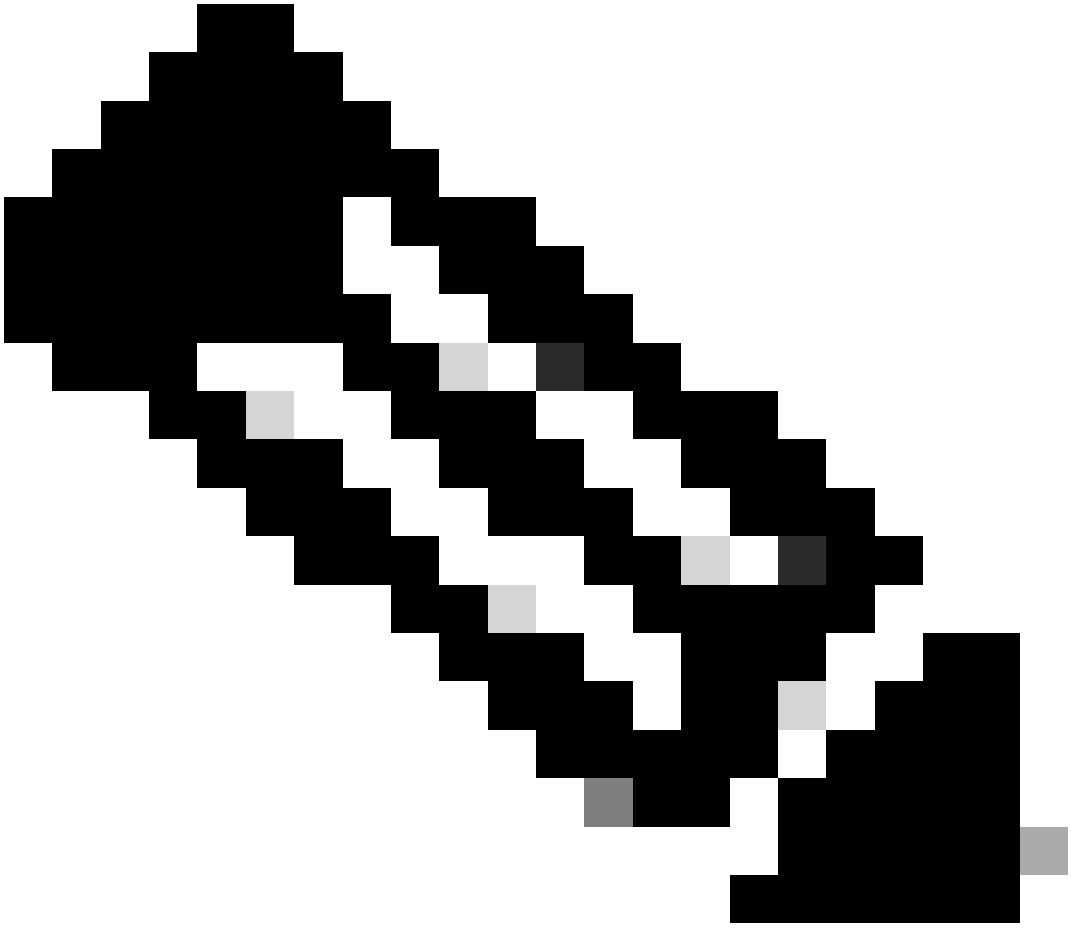
Configuration système requise pour Splunk Enterprise

Étant donné que ce module complémentaire s'exécute sur Splunk Enterprise, toutes les exigences du système Splunk Enterprise s'appliquent. Reportez-vous au manuel d'installation "System Requirements" dans la documentation de Splunk Enterprise. Ces instructions concernent la version 6.2.1 de Splunk Enterprise.

Exigences générales

Ce document suppose que votre bucket Amazon AWS S3 a été configuré dans le tableau de bord Umbrella (Admin> Log Management) et s'affiche en vert avec les journaux récents ayant été téléchargés. Pour plus d'informations sur la gestion des journaux, consultez Gestion des journaux Cisco Umbrella dans Amazon S3.

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



Remarque : Ces étapes sont les mêmes que celles décrites dans l'article décrivant comment configurer un outil pour télécharger les journaux à partir de votre bucket (Comment : Téléchargement des journaux à partir de Cisco Umbrella Log Management dans AWS S3). Si vous avez déjà effectué ces étapes, vous pouvez simplement passer à l'étape 2, bien que vous ayez besoin des informations de sécurité de votre utilisateur IAM pour authentifier le plug-in Splunk dans votre bucket.

Étape 1

1. Ajoutez une clé d'accès à votre compte Amazon Web Services pour permettre l'accès à distance à votre outil local et donner la possibilité de télécharger, télécharger et modifier des fichiers dans S3. Connectez-vous à AWS et cliquez sur le nom de votre compte dans le coin supérieur droit. Dans la liste déroulante, sélectionnez Security Credentials.
2. Vous êtes invité à utiliser les Méthodes Recommandées d'Amazon et à 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 le site : https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Étape 2

1. Créez un utilisateur IAM pour accéder à votre compartiment S3 en cliquant sur Get Started with IAM Users. Vous êtes redirigé vers un écran où vous pouvez créer un utilisateur IAM.
2. Cliquez sur Create New Users, puis continuez et remplissez les champs. Notez que le compte d'utilisateur ne peut pas contenir d'espaces.
3. Après avoir créé le compte d'utilisateur, vous n'avez qu'une seule occasion de récupérer deux informations critiques contenant vos informations d'identification de sécurité utilisateur Amazon. Nous vous recommandons vivement de les télécharger à l'aide du bouton situé en bas à droite pour les sauvegarder. Ils ne sont plus disponibles après cette étape de la configuration. Assurez-vous de noter votre ID de clé d'accès et votre clé d'accès secrète, car nous en aurons besoin plus tard lors de la configuration de Splunk.

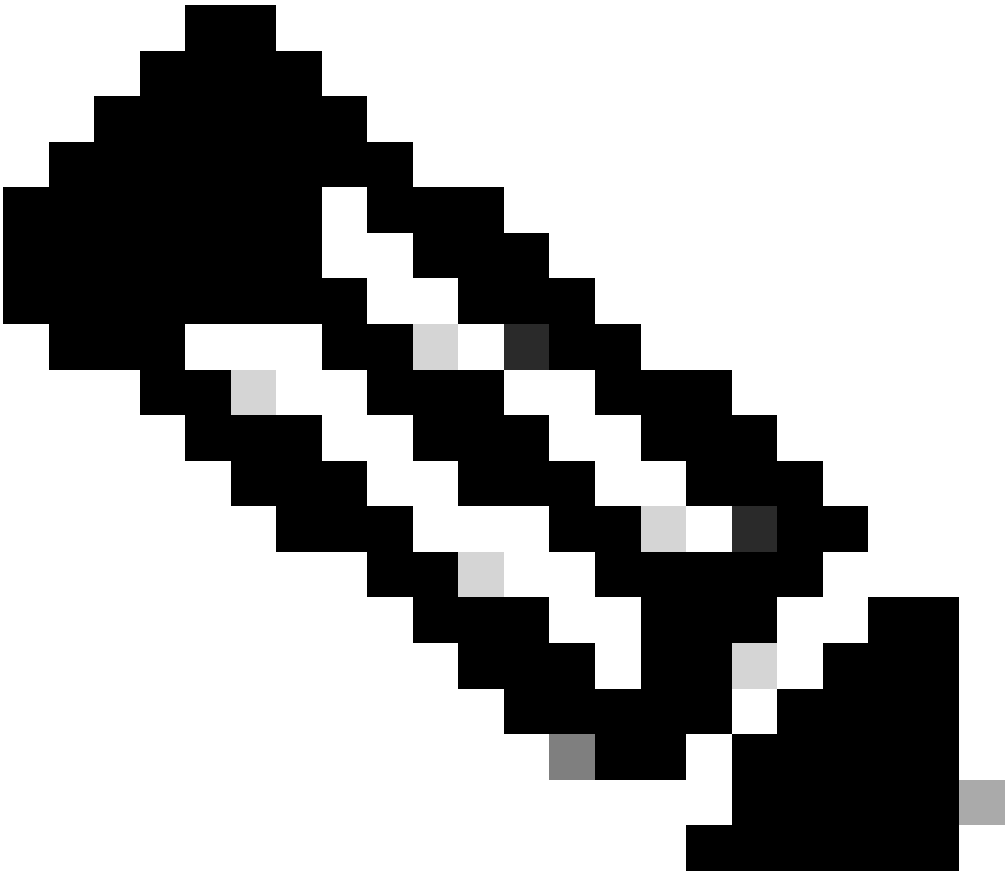
Étape 3

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. Ceci montre deux résultats : "AmazonS3FullAccess" et "AmazonS3ReadOnlyAccess".
3. Sélectionnez AmazonS3FullAccess, puis cliquez sur Attacher une stratégie.

Étape 2 : Configuration du Splunk pour extraire les données de journal DNS de votre compartiment S3

Étape 1 : Configuration du Splunk pour extraire les données du journal DNS du compartiment S3 autogéré

1. Commencez par installer le module complémentaire Splunk pour Amazon Web Services sur votre instance Splunk. Ouvrez votre tableau de bord Splunk et cliquez sur Apps, ou cliquez sur Splunk Apps s'il apparaît sur votre tableau de bord. Une fois dans la section Applications, tapez "s3" dans la fenêtre de recherche pour trouver "Splunk Add-on for Amazon Web Services", et installez l'application.



Remarque : Vous devrez probablement redémarrer Splunk pendant l'installation. Une fois installé, vous voyez Splunk Add-on for AWS avec le nom de dossier 'Splunk_TA_aws' maintenant répertorié sous Apps.

2. Cliquez sur Configurer pour configurer l'application. C'est à ce stade que vous avez besoin des informations d'identification de sécurité de l'étape 1 de cette documentation.
   La configuration nécessite la saisie des champs suivants :

   - Un nom convivial : le nom que vous utilisez pour faire référence à cette intégration
   - Votre ID de clé de compte AWS (à partir de l'étape 1)
   - Votre mot de passe (votre clé secrète de compte AWS, également depuis l'étape 1)

Vous pouvez également définir des informations de proxy local si cela est nécessaire pour que le Splunk atteigne AWS, ainsi que régler la journalisation. L'écran de configuration ressemble à ceci :
3. Une fois que vous avez ajouté des informations pertinentes, cliquez sur Enregistrer et le module complémentaire Splunk pour Amazon Web Services sont entièrement configurés.

Étape 3 : Configuration des entrées de données pour le Splunk

1. Ensuite, vous voulez configurer l'entrée de données pour Amazon Web Services S3. Naviguez à Paramètres > Données > Entrées de données et sous Entrées locales, vous voyez maintenant une liste de diverses entrées Amazon, y compris S3 au bas de la liste.
2. Cliquez sur AWS S3 pour configurer l'entrée.
3. Cliquez sur New.
4. Vous devez fournir les informations suivantes :

    - Entrez un nom convivial pour votre intégration S3.
    - Sélectionnez votre Compte AWS dans la liste déroulante. Il s'agit du nom convivial que vous avez fourni à l'étape 1.
    - Sélectionnez votre compartiment S3 dans la liste déroulante. Il s'agit du nom de compartiment tel qu'il est spécifié dans votre tableau de bord Umbrella (Paramètres > Gestion des journaux).
    - Sélectionnez le nom de la clé S3 dans la liste déroulante. Chaque élément de votre bucket est répertorié, nous vous recommandons de choisir le répertoire de niveau supérieur \dns-logs\ , qui inclut tous les fichiers et répertoires qu'il contient.
    - Il existe plusieurs options sous "Configuration du système de messagerie", nous vous recommandons de les conserver telles quelles : les paramètres par défaut.
    - D'autres options sont disponibles sous « Autres paramètres ». Il est à noter que le « type de source » est aws : s3 par défaut. Nous vous recommandons de laisser ce fichier tel quel, mais si vous le modifiez, le filtre de vos journaux dans la recherche change de ce qui est décrit à l'étape 3 de ces instructions.

Complétez les détails et votre saisie de données ressemble à ceci :

4. Cliquez sur Next pour finaliser vos informations.
   Vous êtes redirigé vers un écran qui indique que l'entrée a été créée avec succès

Étape 3

Effectuez une recherche rapide pour voir si vos données sont importées correctement. Il vous suffit de coller sourcetype="aws:s3" dans la fenêtre de recherche en haut à droite, puis de sélectionner "Ouvrir sourcetype="aws:s3" dans la recherche

Vous accédez ainsi à un écran similaire à celui dans lequel vous voyez les événements des journaux DNS de votre organisation. Ici, le service mobile Cisco Umbrella bloque les médias sociaux sur un iPhone. Vous pouvez également utiliser la source du nom de fichier pour filtrer par rapport à un lot particulier de journaux.

Après cela, la tâche cron en arrière-plan continue à s'exécuter et à extraire les derniers jeux des informations de journal de votre bucket.

Il y a beaucoup plus que vous pouvez faire avec Splunk au-delà de ce qui a été décrit dans cet article, et si vous avez eu la chance d'expérimenter avec l'utilisation de ces données dans votre procédure de réponse de sécurité, nous aimerions avoir de vos nouvelles. Envoyez vos commentaires, questions ou préoccupations à umbrella-support@cisco.com et faites référence à

cet article.

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.