Configuration de QRadar Integration avec Umbrella Log Management et S3

Table des matières

Introduction

Ce document décrit comment configurer QRadar pour ingérer les journaux d'un compartiment AWS S3 pour la gestion des journaux Umbrella.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Ce document suppose que votre godet Amazon AWS S3 a été configuré dans Umbrella (Paramètres > Gestion des journaux) et s'affiche en vert avec les journaux récents ayant été téléchargés. Pour plus d'informations sur la façon de configurer cette fonctionnalité, lisez cet article : Télécharger les journaux à partir de la gestion des journaux Umbrella dans AWS S3
- Outre les droits d'administration sur le ou les appareils QRadar, la configuration d'Amazon S3 et le tableau de bord Umbrella, ces instructions supposent que l'administrateur QRadar est familiarisé avec la création de fichiers LSX (Log source Extension).

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Aperçu

Remarque : La meilleure méthode de configuration de QRadar pour une utilisation avec Cisco Umbrella est via l'application Cisco Cloud Security. N'utilisez cette méthode que si l'application ne peut pas être configurée.

QRadar d'IBM est un SIEM populaire 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 explique comment installer et exécuter QRadar pour qu'il puisse extraire les journaux de votre godet S3 et les consommer. Il y a deux étapes principales :

- Configurez vos informations d'identification de sécurité AWS S3 pour autoriser QRadar à accéder aux journaux.
- Configurez QRadar pour qu'il pointe vers votre bucket.

Si vous utilisez le compartiment S3 géré par Cisco, veuillez utiliser ces instructions dans l'article Download Logs from Umbrella Log Management Using the AWS CLI.

Remarque : Cette intégration a été testée avec des compartiments S3 gérés par le client et des compartiments S3 gérés par Cisco. Les informations traitées dans cet article sont à jour au moment de la rédaction de cet article (octobre 2019). Elles peuvent changer en fonction de la façon dont QRadar et AWS Services s'interfacent. Ce document est un document vivant. Si vous avez des commentaires ou si vous avez trouvé des astuces ou des conseils susceptibles d'aider d'autres clients, veuillez contacter l'assistance Cisco Umbrella.

La prise en charge de QRadar doit provenir d'IBM, car Cisco n'est pas en mesure de prendre directement en charge le matériel ou les logiciels tiers. Pour tout problème de connexion de votre tableau de bord Umbrella à votre compartiment S3, Cisco Umbrella peut vous fournir une assistance. La plupart des informations contenues dans cet article se trouvent également sur le site Web d'IBM.

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 (Download Logs from Umbrella Log Management in AWS S3). Si vous avez déjà effectué ces étapes, vous pouvez passer à l'étape 2, bien que vous ayez besoin par la suite des informations d'identification de sécurité de votre utilisateur IAM pour authentifier QRadar 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 :

1. Connectez-vous à AWS.
2. Sélectionnez le nom de votre compte dans l'angle supérieur droit.
3. Dans la liste déroulante, sélectionnez Security Credentials.

2. Vous êtes ensuite invité à utiliser les Méthodes Recommandées d'Amazon et à créer un utilisateur AWS Identity and Access Management (IAM). 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, lisez la documentation AWS.

Étape 2

1. Sélectionnez Get Started with IAM Users pour créer un utilisateur IAM afin d'accéder à votre compartiment S3. Vous accédez ensuite à un écran dans lequel vous pouvez créer un utilisateur IAM.
2. Sélectionnez Nouveaux utilisateurs, puis renseignez les champs.

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

3. Après avoir créé le compte d'utilisateur, vous n'avez plus qu'une seule occasion de récupérer

deux informations critiques contenant vos informations d'identification et de connexion Amazon User Security. Umbrella vous suggère fortement de les télécharger à l'aide du bouton situé en bas à droite pour les sauvegarder. Ils ne sont pas disponibles après cette étape de la configuration. Assurez-vous de noter à la fois votre ID de clé d'accès et votre clé d'accès secrète car ils sont requis dans une étape ultérieure.

Étape 3

Ajoutez ensuite une stratégie pour votre utilisateur IAM afin qu'il ait accès à votre compartiment S3 :

1. Sélectionnez l'utilisateur que vous venez de créer, puis faites défiler les propriétés des utilisateurs vers le bas jusqu'à ce que vous voyiez le bouton Attacher une stratégie.

2. Sélectionnez Attacher une stratégie, puis entrez « s3 » dans le filtre de type de stratégie. Ceci montre deux résultats :

- AmazonS3AccèsComplet
- AmazonS3ReadOnlyAccess

3. Sélectionnez AmazonS3FullAccess, puis sélectionnez Attacher une stratégie dans l'angle inférieur droit.

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

QRadar utilise le service AWS CloudTrail, qui est un service Web qui enregistre les appels de l'API AWS pour votre compte et vous fournit des fichiers journaux.

Avant d'accéder à Amazon S3 via QRadar, suivez cette procédure depuis IBM pour obtenir le certificat du serveur Amazon. Cette partie est difficile, donc assurez-vous que vous remplissez les instructions exactement.

Remarque : Lors des tests, vous devez utiliser le navigateur Firefox pour que cela fonctionne comme prévu.

Pour obtenir le certificat du serveur Amazon, vous devez déplacer le certificat au format DER vers l'appareil QRadar approprié. L'appliance QRadar qui nécessite le certificat est l'appliance assignée dans le champ Target Event Collector dans la source de journal Amazon AWS CloudTrail.

Avant de commencer

- Le certificat doit être au format .DER.
- L'extension .DER est sensible à la casse et doit être en majuscules.
- Si le certificat est exporté en minuscules, la source du journal peut rencontrer des problèmes de collecte d'événements.

Étapes initiales

1. Accédez à votre compartiment AWS CloudTrail S3 : `https://<bucketname>.s3.amazonaws.com`

2. Utilisez Firefox pour exporter le certificat SSL d'AWS en tant que certificat (.DER). Firefox peut créer le certificat requis avec l'extension .DER :

1. Sélectionnez l'icône Identité du site (l'icône de verrouillage dans la barre d'adresse).
2. Sélectionnez Plus d'informations > Afficher le certificat et sélectionnez l'onglet Détails.
3. Sélectionnez Export pour exporter au format .DER du certificat.

Remarque : L'extension .DER est sensible à la casse et doit être en majuscules.

---

3. Copiez le certificat .DER dans le répertoire /opt/QRadar/conf/trusted_certificates de l'appliance QRadar qui gère la source du journal Amazon AWS CloudTrail. Vous pouvez utiliser WinSCP pour le copier.

Remarque : L'appliance QRadar qui gère la source de journal est identifiée par le champ Target Event Collect dans la source de journal Amazon AWS CloudTrail. L'appliance QRadar qui gère la source du journal Amazon AWS CloudTrail doit disposer d'une copie du certificat .DER dans /opt/QRadar/conf/trusted_certificates.

---

4. Connectez-vous à l'interface utilisateur de QRadar en tant qu'administrateur.

5. Sélectionnez l'onglet Admin.

6. Cliquez sur l'icône Sources de journal.

7. Sélectionnez la source du journal Amazon AWS CloudTrail.

8. Dans le menu de navigation, sélectionnez Enable/Disable pour désactiver puis réactiver la source du journal Amazon AWS CloudTrail.

Remarque : Lorsqu'un administrateur force la désactivation de la source de journal à l'activation, cela permet au protocole de se connecter au compartiment Amazon AWS tel que défini dans la source de journal. Une vérification de certificat est alors effectuée dans

---

le cadre de la première communication.

9. Si vous continuez à rencontrer des problèmes, vérifiez que le champ Log Source Identifier contient le nom de compartiment Amazon AWS correct et que le chemin d'accès au répertoire distant est correct dans la configuration de la source du journal.

Finalisation de la configuration QRadar

1. Dans QRadar, assurez-vous que tous vos protocoles, DSM et autres informations sont à jour. Sélectionnez le LogFileProtocol avec ces configurations (votre fréquence, heure de début, périodicité et d'autres informations peuvent être différentes).

2. Dans l'onglet Origines du journal, entrez un nom d'origine du journal et une description d'origine du journal. Ça peut être ce que tu veux.

3. Entrez votre nom de compartiment S3, votre clé d'accès AWS, votre clé secrète AWS et le répertoire distant (les dnslogs sont probablement en fonction de votre configuration). L'ajout d'un identifiant de source de journal comme l'année peut aider à filtrer de sorte que seuls les journaux contenant « 2019 » sont extraits.

4. Créez un LSX (Log Source Extension) qui peut analyser les événements Cisco Umbrella. (Voici à quoi cela ressemble après l'importation dans QRadar.) Plus d'informations sur la façon exacte de créer LSX peuvent être trouvées sur le site Web d'IBM. Ce n'est qu'un exemple. Les données que vous souhaitez extraire des journaux varient selon le cas d'utilisation.

5. Vérifiez à nouveau que votre clé d'accès AWS et votre clé secrète AWS ont été copiées et collées dans la configuration de la source du journal.

6. Sélectionnez le processeur GZIP et un générateur d'événements RegEx Based Multiline. Le moyen le plus simple d'obtenir un événement par ligne est d'utiliser un modèle de départ RegEx de :

```
("\d{4}-\d{2}-\d{2}\s\d{2}:\d{2}:\d{2}","")
```

Veillez à sélectionner l'extension et la condition d'utilisation de la source du journal, puis enregistrez la source du journal.

7. Effectuez un déploiement complet dans QRadar.

Votre source de journal utilise ensuite RestAPI pour vous connecter à votre bucket avec les informations d'identification et les clés que vous avez fournies et commencer à extraire des événements.

Additional Information

Activer la consignation des compartiments

Pour activer la journalisation du bucket, lisez la documentation AWS et complétez les procédures décrites. Par défaut, la journalisation est désactivée. Une fois activé, un nouveau dossier appelé /logs se trouve dans votre racine de bucket pour vous montrer les informations de GETS, PUTS et DELETES.

Gestion du cycle de consignation

Lorsque vous utilisez S3, vous pouvez gérer le cycle de vie des données dans le compartiment pour prolonger la durée pendant laquelle vous souhaitez conserver les journaux. Selon l'objectif de la gestion des journaux externes, la durée peut être très courte ou très longue. Par exemple, vous pouvez simplement télécharger les journaux à partir du compartiment S3 après 24 heures et les stocker hors ligne, ou les conserver indéfiniment dans le cloud.

Par défaut, Amazon stocke les données dans un compartiment indéfiniment, mais le stockage illimité augmente le coût de maintenance du compartiment. Pour plus d'informations sur les cycles de vie de S3, veuillez lire la documentation AWS.

Pour configurer le cycle de vie de votre compartiment :

1. Sélectionnez Propriétés > Cycle de vie.

2. Sélectionnez Ajouter une règle, puis Appliquer la règle à l'ensemble du compartiment (ou à un sous-dossier si vous l'avez configuré comme tel).

3. Sélectionnez une action sur les objets, telle que Supprimer ou Archiver, puis sélectionnez la période et si vous souhaitez utiliser le stockage Glacier pour aider à réduire vos coûts Amazon. (Glacier est un stockage hors ligne « froid », qui, bien que plus lent à accéder, est beaucoup moins cher.)

Si vous préférez gérer les journaux selon une autre méthode (par exemple, sur votre solution de sauvegarde interne), vous pouvez simplement télécharger les journaux à partir de S3 et les conserver d'une autre manière.

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.