Configurer les journaux d'événements consolidés pour AWS S3 Push

Contenu

Introduction

Ce document décrit comment configurer les journaux d'événements consolidés pour qu'ils soient envoyés à un compartiment S3 sur un dispositif de sécurité de la messagerie électronique (ESA) ou une sécurité de la messagerie électronique cloud (CES).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ESA exécutant Async OS 13.0 ou supérieur
- Accès administratif à la solution matérielle-logicielle
- Compte Amazon Web Services (AWS) et accès pour créer et gérer le compartiment S3

Components Used

Les informations de ce document sont basées sur tous les modèles matériels ESA et appliances virtuels pris en charge exécutant Async OS 13.0 ou version ultérieure. Afin de vérifier les informations de version de l'appliance à partir de l'interface de ligne de commande, entrez la commande version. Dans l'interface utilisateur graphique, sélectionnez **Monitor > System Status**.

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 actif, assurez-vous de bien comprendre l'impact potentiel de toute configuration.

Informations générales

Depuis Async OS 13.0 et versions ultérieures, ESA permet la configuration de la journalisation basée sur Unified Common Event Format (CEF), connue sous le nom de fichiers de journalisation consolidés, largement utilisée par les fournisseurs SIEM. Reportez-vous aux notes de version ESA 13.0 ici.

Les journaux CEF peuvent également être configurés pour être poussés vers un compartiment AWS S3, à l'exception du téléchargement manuel, SCP et Syslog push.

> **Note**: Les étapes fournies pour la configuration AWS sont basées sur les informations disponibles au moment de la rédaction de cet article.

Configuration

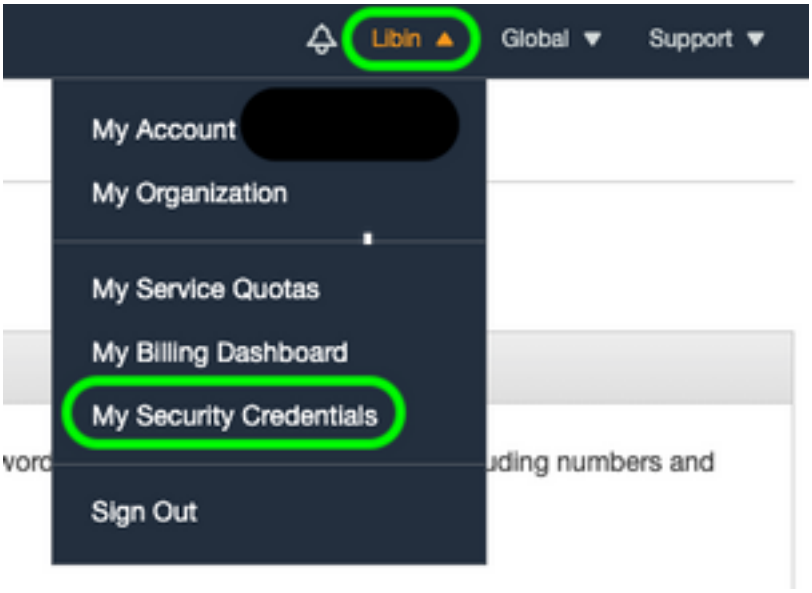
1. Accédez à la console cloud AWS afin de collecter le nom de groupement S3, la clé d'accès S3 et la clé secrète S3.

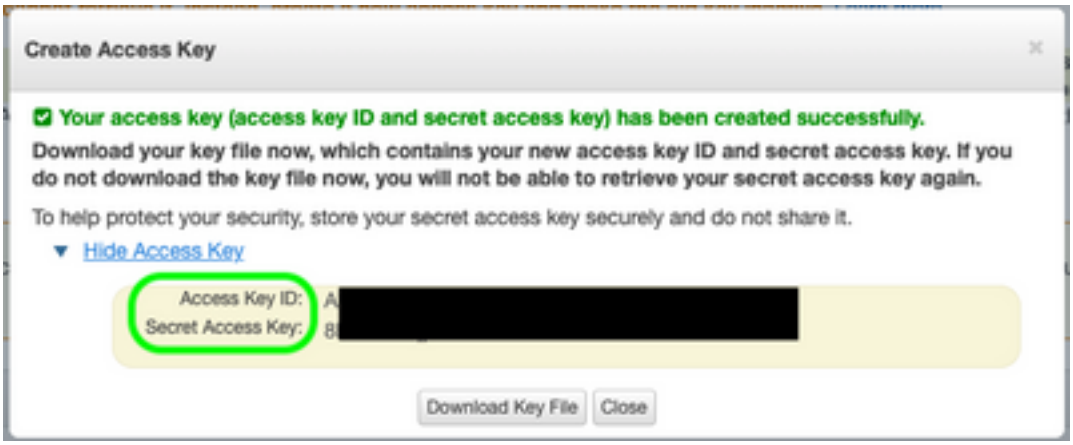
Pour le nom du groupement S3 :

Une fois connecté au cloud AWS, utilisez la liste déroulante Services pour sélectionner S3 ou utilisez la barre de recherche en haut pour rechercher S3. Créez un groupement avec les options par défaut ou le nom de capture pour l'un des compartiments existants à utiliser.

Pour la clé d'accès S3 et la clé secrète S3 :

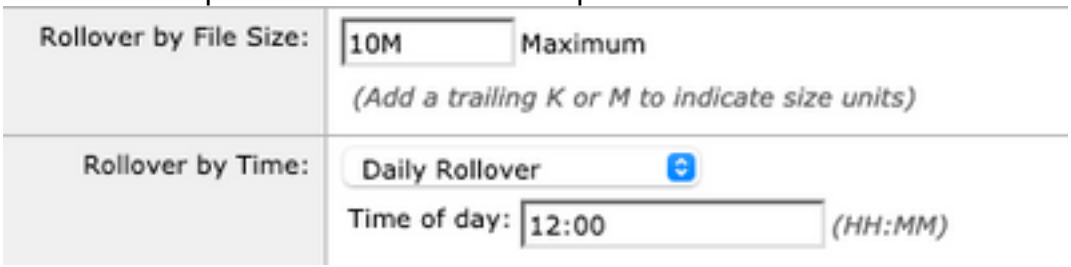
Cliquez sur le nom de votre compte en haut à droite et, dans la liste déroulante, sélectionnez “ Mes informations d'identification de sécurité ”. Sur la page ouverte, cliquez sur “ clés d'accès (ID de clé d'accès et clé d'accès secrète). Créez une nouvelle clé d'accès, affichez ou téléchargez les détails de la clé.



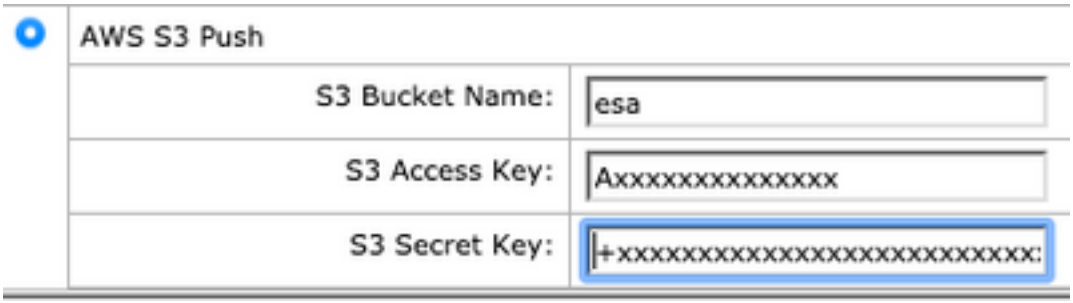


Attention : NE PAS partager les clés d'accès sur les forums publics. Assurez-vous que ces informations sont stockées en toute sécurité.

2. Accédez à ESA avec les journaux CEF configurés sous **Administration système > Abonnements au journal** et cliquez sur le nom du **journal**.
3. Sélectionnez **Rollover par taille de fichier** ou **Rollover par heure** ou les deux et les journaux seront repoussés en fonction de la première condition vraie.



4. Sélectionnez AWS S3 Push, saisissez les informations collectées à l'étape 1.



5. Envoi et validation des modifications.

Si des journaux CEF étaient déjà présents sur la solution matérielle-logicielle, les fichiers journaux existants sont immédiatement poussés et doivent apparaître dans le compartiment S3 configuré. Le prochain programme de retransmission du journal se fera en fonction de la taille et de l'heure de transfert configurées.

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Utilisez les journaux s3_client disponibles sur le périphérique afin de suivre les journaux en cours d'envoi ou toute erreur qui se connecte à celui-ci.

Successful log push

```
Fri Feb 19 11:21:38 2021 Info: S3_CLIENT: Uploaded 3 file(s) to the S3 Bucket esa for the
subscription: cef

Fri Feb 19 12:03:16 2021 Info: S3_CLIENT: Uploading files to S3 Bucket esa for the subscription:
cef
Fri Feb 19 12:03:22 2021 Info: S3_CLIENT: Uploaded 1 file(s) to the S3 Bucket esa for the
subscription: cef
```

Unsuccessful log push

```
Fri Feb 19 12:34:10 2021 Info: S3_CLIENT: Uploading files to S3 Bucket esa for the subscription:
cef
Fri Feb 19 12:34:11 2021 Warning: S3_CLIENT: ERROR: Upload Failed to S3 bucket esa. Reason:
Failed to upload /data/pub/cef/sll.@20210219T120000.s to esa/sll.@20210219T120000.s: An error
occurred (InvalidAccessKeyId) when calling the PutObject operation: The AWS Access Key Id you
provided does not exist in our records.
Fri Feb 19 12:34:11 2021 Warning: S3_CLIENT: Uploading files to S3 Bucket esa encountered one or
more failures for the subscription: cef.
Upload failed for the following:
[u'sll.@20210219T120000.s']

Re-check your configuration.
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Guides de l'utilisateur final du dispositif de sécurité de la messagerie Cisco
- Notes de version de l'appliance de sécurité de la messagerie Cisco et informations générales
- SLL (Single Log Line) CES
- AWS Création du groupement S3
- **Support et documentation techniques - Cisco Systems**