

Module complémentaire Splunk pour AWS - Echec du déchiffrement

Applicabilité

Modules complémentaires des applications Splunk

Description

Environnement :

Utilisation d'un serveur de déploiement de la liaison commutée (Splunk Deployment Server, DS) pour pousser le module complémentaire de la liaison commutée pour AWS vers le Splunk Heavy Forwarder (HF), qui est configuré pour collecter les fichiers journaux AWS.

Problème :

Les journaux AWS étaient toujours en train d'être ingérés.

Enquête

Le message d'erreur suivant a été trouvé dans les fichiers journaux de l'instance HF.

splunkd.log :

```
07-03-2019 13:28:35.327 -0600 ERROR Crypto - Decryption operation failed: AES-GCM Decryp
07-03-2019 13:28:35.327 -0600 WARN ConfigEncryptor - Decryption operation failed: AES-GC
```

D'après le message d'erreur, ceci est très similaire au problème abordé dans l'article suivant de Splunk Answers :

Installez Splunk Enterprise 7.2.1 et promouvez-le en tant que maître de cluster. Impossible de charger le site Web de spam.

<https://answers.splunk.com/answers/723728/installed-splunk-enterprise-721-and-promoted-it->

Résolution

Sur le serveur de déploiement :

1. Effectuez une copie de sauvegarde de splunk.secret dans le répertoire \$SPLUNK_HOME/etc/auth.
2. Supprimé splunk.secret
3. Clé splunk.secret copiée du redirecteur lourd (HF) vers le serveur de déploiement (DS).
4. Effectuez une copie de sauvegarde du fichier /opt/splunk/etc/system/local/server.conf.
5. Commentée dans pass4SymmKey dans le fichier server.conf
6. Entrez à nouveau sslPassword sous [sslConfig] stanza dans le fichier server.conf.
7. Splunk redémarré
8. Le nouveau fichier Splunk_TA_aws/local/passwords.conf a été envoyé au routeur HF.

Recommandations futures :

1. L'approche actuelle consistant à copier la clé splunk.secret du matériel vers l'instance DS est une solution réalisable, mais les opérations suivantes peuvent être nécessaires à prendre en considération à l'avenir.

Pour que le service d'annuaire fonctionne avec d'autres redirecteurs/clients de déploiement, la même clé splunk.secret doit être distribuée à tous les redirecteurs/clients. Cela évitera d'obtenir des erreurs de déchiffrement échouées.

2. Une autre approche consiste à définir des mots de passe au format texte clair dans le fichier passwords.conf sur l'instance DS.

Laissez ensuite le client de déploiement (HF) chiffrer les mots de passe une fois que les fichiers sont envoyés à partir de DS. Le matériel déchiffrera les mots de passe immédiatement après son redémarrage.

Liens connexes

Réponses Splunk

Installez Splunk Enterprise 7.2.1 et promouvez-le en tant que maître de cluster. Impossible de charger le site Web de spam. <https://answers.splunk.com/answers/723728/installed-splunk-enterprise-721-and-promoted-it-as.html>

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.