

Splunk Http Event Collector (HEC) utilisant SSL

Applicabilité

Splunk Enterprise

Description

Lorsqu'une application envoie des données via https, l'erreur suivante se produit :

```
org.apache.http.conn.ssl.DefaultHostnameVerifier:07/18/2019 01:14:42:192 PM CEST: Thread
Certificate for <[Hostname SPLUNK-INDEXER]> doesn't match common name of the certificate
javax.net.ssl.SSLException: Certificate for <[Hostname SPLUNK-INDEXER]> doesn't match co
```

Enquête

Résolution

Après quelques recherches sur l'utilisation de SSL sur HEC, nous avons pu résoudre le problème en configurant à nouveau les certificats mais sur l'indexeur.

REMARQUE : utilisez le lien suivant pour configurer de nouveaux certificats :

<https://docs.splunk.com/Documentation/Splunk/7.3.0/Security/ConfigureSplunkforwardingtousesignedcert>

Liens connexes

Documentation Splunk

Configurez le transfert Splunk pour utiliser vos propres certificats :

<https://docs.splunk.com/Documentation/Splunk/7.3.0/Security/ConfigureSplunkforwardingtousesignedcert>

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.