

Splunk Http Event Collector (HEC) mit SSL

Geltungsbereich

Splunk Enterprise

Beschreibung

Wenn eine Anwendung Daten über HTTPS sendet, tritt der folgende Fehler auf:

```
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
```

Untersuchung

Auflösung

Nach einigen Recherchen über die Verwendung von SSL auf HEC konnten wir das Problem lösen, indem wir die Zertifikate erneut einrichten, aber auf dem Indexer.

HINWEIS: Verwenden Sie den folgenden Link, um neue Zertifikate einzurichten:

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

Verwandte Links

Splunk-Dokumentation

Konfigurieren Sie die Splunk-Weiterleitung zur Verwendung Ihrer eigenen Zertifikate:

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.