

Splunk Http Event Collector (HEC) met SSL

toepasbaarheid

Splunk Enterprise

Beschrijving

Wanneer een applicatie gegevens via https verzendt, treedt de volgende fout op:

```
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
```

onderzoek

resolutie

Na wat onderzoek over het gebruik van SSL op HEC, konden we het probleem oplossen door de certificaten opnieuw in te stellen, maar op de indexeerder.

OPMERKING: Gebruik de volgende koppeling om nieuwe certificaten in te stellen:

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

Gerelateerde links

Splunk-documentatie

Configureer Splunk forwarding om je eigen certificaten te gebruiken:

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.