

Splunk Http Event Collector (HEC) tramite SSL

Applicabilità

Splunk Enterprise

Descrizione

Quando un'applicazione invia dati tramite https, si verifica il seguente errore:

```
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
```

Indagine

Risoluzione

Dopo alcune ricerche sull'utilizzo di SSL su HEC, siamo stati in grado di risolvere il problema impostando nuovamente i certificati ma sull'indicizzatore.

NOTA: utilizzare il collegamento seguente per impostare nuovi certificati:

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

Collegamenti correlati

Documentazione relativa a Splunk

Configurare l'inoltro Splunk per l'utilizzo di certificati personalizzati:

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).