

Splunk Http Event Collector (HEC) con SSL

Aplicabilidad

Splunk Enterprise

Descripción

Cuando una aplicación envía datos a través de https, se produce el siguiente error:

```
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
```

Investigación

Resolución

Después de algunas investigaciones sobre el uso de SSL en HEC, pudimos resolver el problema configurando de nuevo los certificados, pero en el indizador.

NOTA: Utilice el siguiente enlace para configurar nuevos certificados:

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

Enlaces relacionados

Documentación de Splunk

Configure el reenvío de Splunk para utilizar sus propios certificados:

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).