

Universal Forwarder kann aufgrund doppelter Anmeldeinformationen keine Daten an Splunk Cloud senden

Geltungsbereich

Universal Forwarder Splunk Cloud

Beschreibung

Die folgende Fehlermeldung steht in Indexerprotokollen unter der TcpInputProc-Komponente zur Verfügung:

```
ERROR TcpInputProc - Error encountered for connection from  
src=xxx.xxx.xxx.xxx:99999. error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version num
```

In den universellen Weiterleitungen befinden sich die folgenden Meldungen auf splunkd.log, die bestätigen, dass TCP-Verbindungen zwischen Instanzen hergestellt werden können:

```
INFO TcpOutputProc - Removing quarantine from idx=xxx.xxx.xxx.xxx:9997ERROR TcpOutputFd  
group splunkcloud has been blocked for 82150 seconds. This will probably stall the data  
for host="inputsN.<SplunkDeployment>.splunkcloud.com"
```

Untersuchung

So kümmert sich die Datei output.conf um die Verwendung des Credentials-Pakets, das korrekt konfiguriert zu sein scheint:

```
[tcpout:splunkcloud]  
compressed = false  
server = inputs1.<SplunkDeployment>.splunkcloud.com:9997, inputs2.<SplunkDeployment>.spl
```

```
inputs3.<SplunkDeployment>.splunkcloud.com:9997, inputs4.<SplunkDeployment>.splunkcloud.  
inputs5.<SplunkDeployment>.splunkcloud.com:9997, inputs6.<SplunkDeployment>.splunkcloud.  
inputs7.<SplunkDeployment>.splunkcloud.com:9997, inputs8.<SplunkDeployment>.splunkcloud.  
sslCertPath = $SPLUNK_HOME/etc/apps/100_splunk_splunkcloud/default/splunk_server.pem  
sslCommonNameToCheck = *.<SplunkDeployment>.splunkcloud.com  
sslPassword = DIAG_REDACTED_ENCRYPTED_PASSWORD  
sslRootCAPath = $SPLUNK_HOME/etc/apps/100_splunk_splunkcloud/default/splunk_cacert.pem  
sslVerifyServerCert = true etc/apps/100_splunk_splunkcloud/default/outputs.conf  
useClientSSLCompression = true
```

Die folgenden Nachrichten befinden sich ebenfalls auf splunkd.log und versuchen, die (100_<SplunkDeployment>_splunkcloud-App) zu authentifizieren, obwohl sie wissen, dass der Pfad zu server.pem richtig war.

```
ERROR SSLCommon - Can't read key file /opt/splunk/etc/apps/100_splunk_splunkcloud/default
```

Auflösung

Die Fehler auf dem Universal Forwarder, der keine Verbindung mit Splunk Cloud herstellen kann, scheinen darauf zurückzuführen zu sein, dass das Anmeldeinformationspaket nicht richtig konfiguriert wurde.

Um es aufzulösen, sollte das Paket mit den Anmeldeinformationen an Instanzen weitergeleitet werden. Platzieren Sie das neue Paket auf dem Bereitstellungsserver, um es an die Instanzen weiterzuleiten. Installieren Sie die Anmeldeinformationspakete nicht auf dem Bereitstellungsserver.

Das Paket mit den Anmeldeinformationen kann auch einzeln installiert werden, indem Sie die folgenden Schritte ausführen:

- 1) Melden Sie sich bei Ihrer Splunk Cloud-Bereitstellung an.
- 2) Laden Sie den Splunk Universal Forwarder für Linux herunter.
- 3) Installation des Splunk Universal Forwarder für Linux.
- 4) Laden Sie die Universellen Forwarder-Anmeldeinformationen herunter, und installieren Sie sie.

[Installation und Konfiguration des Pakets mit den Anmeldeinformationen für die universelle Weiterleitung der Splunk Cloud-Plattform](#)

Port 9997 lässt sich aufgrund eines ungültigen Zertifikatskennworts nicht öffnen. Daher wird der Schluss gezogen, dass das Anmeldeinformationspaket SPL in einem anderen Forwarder wiederverwendet wurde, der das Kennwort zweimal hasht, und jetzt können die Indexer den

neuen Forwarder nicht erkennen.

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.