

Universele expediteur kan geen gegevens naar Splunk Cloud verzenden vanwege dubbele aanmeldgegevens

toepasbaarheid

Universal Forwarder Splunk Cloud

Beschrijving

De volgende foutmelding is beschikbaar in indexeringslogboeken onder de component TcpInputProc:

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

In de Universal-forwarders staan de volgende berichten op splunkd.log, waarmee wordt bevestigd dat TCP-connectiviteit tussen instanties kan worden ingesteld:

```
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"
```

onderzoek

Dit is hoe de outputs.conf er uitziet na het gebruik van het credentials-pakket, dat correct lijkt te zijn geconfigureerd:

```
[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
```

De volgende berichten staan ook op splunkd.log en proberen de (100_<SplunkDeployment>_splunkcloud-app) te verifiëren, zelfs wetende dat het pad naar de server.pem correct was.

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

resolutie

De fouten op de Universal-forwarder die geen verbinding kunnen maken met Splunk Cloud lijken te worden veroorzaakt door het inlogpakket dat niet correct is geconfigureerd.

Om dit op te lossen, moet het pakket met referenties naar instanties worden geduwd. Plaats het nieuwe pakket in de implementatieserver dat naar de instanties moet worden geduwd. Installeer de referentiepakketten niet in de implementatieserver.

Het aanmeldpakket kan ook afzonderlijk worden geïnstalleerd door de volgende stappen te volgen:

- 1) Log in op uw Splunk Cloud-implementatie
- 2) Download de Splunk Universal Forwarder voor Linux.
- 3) Installeer de Splunk Universal Forwarder voor Linux.
- 4) Download en installeer de universele forwarder referenties.

[Installeer en configureer het Splunk Cloud Platform Universal Forwarder Credentials pakket](#)

Poort 9997 wordt niet geopend vanwege een ongeldig cert-wachtwoord, daarom wordt geconcludeerd dat het credentials-pakket SPL opnieuw is gebruikt in een andere expediteur die het wachtwoord twee keer heeft gehasht en nu kunnen de indexeers de nieuwe expediteur niet herkennen.

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.