

Il server d'inoltro universale non è in grado di inviare dati a Splunk Cloud a causa di un pacchetto di credenziali duplicato

Applicabilità

Universal Forwarder Splunk Cloud

Descrizione

Il seguente messaggio di errore è disponibile nei log dell'indicizzatore nel componente TcpInputProc:

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

Nei server d'inoltro universali, il seguente messaggio è disponibile in splunkd.log, per confermare che è possibile stabilire la connettività TCP tra le istanze:

```
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"
```

Indagine

Di seguito viene riportato l'aspetto di outputs.conf dopo l'utilizzo del pacchetto di credenziali, che sembra essere configurato correttamente:

```
[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
```

Anche i messaggi seguenti si trovano su splunkd.log e tentano di autenticare l'app (100_<SplunkDeployment>_splunkcloud), anche se il percorso di server.pem è corretto.

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

Risoluzione

Gli errori nel server d'inoltro universale che non è in grado di connettersi a Splunk Cloud sembrano essere causati dalla configurazione non corretta del pacchetto di credenziali.

Per risolverlo, è necessario eseguire il push del pacchetto di credenziali nelle istanze. Inserire il nuovo pacchetto nel server di distribuzione da inserire nelle istanze. Non installare i pacchetti di credenziali nel server di distribuzione.

È inoltre possibile installare singolarmente il pacchetto di credenziali eseguendo la procedura seguente:

- 1) Accedere alla distribuzione di Splunk Cloud
- 2) Scaricare Splunk Universal Forwarder per Linux.
- 3) Installare Splunk Universal Forwarder per Linux.
- 4) Scaricare e installare le credenziali del server d'inoltro universale.

[Installare e configurare il pacchetto di credenziali del server di inoltro universale della piattaforma Splunk Cloud](#)

La porta 9997 non si aprirà a causa di una password del certificato non valida. Si è pertanto concluso che l'SPL del pacchetto di credenziali è stato riutilizzato in un altro server di inoltro che ha eseguito due volte l'hashing della password e che ora gli indicatori non sono in grado di riconoscere il nuovo server di inoltro.

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).