

El reenviador universal no puede enviar datos a Splunk Cloud debido a un paquete de credenciales duplicadas

Aplicabilidad

Nube Splunk de Universal Forwarder

Descripción

El siguiente mensaje de error está disponible en los registros del indizador bajo el 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
```

En los reenviadores universales, los siguientes mensajes se encuentran en splunkd.log, lo que confirma que se puede establecer la conectividad TCP entre instancias:

```
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"
```

Investigación

Así es como output.conf se ve después de usar el paquete de credenciales, que parece estar correctamente configurado:

```
[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
```

Los siguientes mensajes también están en splunkd.log tratando de autenticar la aplicación (100_<SplunkDeployment>_splunkcloud), incluso sabiendo que la ruta al server.pem era correcta.

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

Resolución

Los errores en el reenviador universal que no puede conectarse a Splunk Cloud parecen deberse a que el paquete de credenciales no se ha configurado correctamente.

Para resolverlo, el paquete de credenciales debe enviarse a las instancias. Coloque el nuevo paquete en el servidor de implementación para enviarlo a las instancias, no instale los paquetes de credenciales en el servidor de implementación.

El paquete de credenciales también se puede instalar de forma individual siguiendo estos pasos:

- 1) Inicie sesión en su implementación de Splunk Cloud
- 2) Descargue Splunk Universal Forwarder para Linux.
- 3) Instale el Splunk Universal Forwarder para Linux.
- 4) Descargue e instale las credenciales del reenviador universal.

[Instalar y configurar el paquete de credenciales de reenviador universal de la plataforma de nube Splunk](#)

El puerto 9997 no se abrirá debido a una contraseña de certificado no válida, por lo tanto, se concluye que el paquete de credenciales SPL fue reutilizado en otro reenviador con hash de la contraseña dos veces y ahora los indexadores no pueden reconocer el nuevo reenviador.

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).