

クレデンシャルパッケージが重複しているため、ユニバーサルフォワーダがSplunk Cloudにデータを送信できない

適用性

Universal Forwarder Splunkクラウド

説明

TcpInputProcコンポーネントの下にあるインデクサログには、次のエラーメッセージが表示されます。

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

ユニバーサルフォワーダでは、インスタンス間のTCP接続が確立できることを確認する次のメッセージがsplunkd.logにあります。

```
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"
```

調査

正しく設定されているように見えるクレデンシャルパッケージの使用後のoutputs.confの表示を次に示します。

```
[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
```

また、server.pemへのパスが正しいことがわかっていても、
(100_<SplunkDeployment>_splunkcloudアプリケーション) の認証を試行するsplunkd.logに次の
メッセージが記録されます。

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

解決方法

Splunk Cloudに接続できないユニバーサルフォワーダのエラーは、クレデンシャルパッケージが
正しく設定されていないことが原因と考えられます。

これを解決するには、クレデンシャルパッケージをインスタンスにプッシュする必要があります。
インスタンスにプッシュする新しいパッケージを配置サーバーに配置します。配置サーバーに
資格情報パッケージをインストールしないでください。

クレデンシャルパッケージは、次の手順で個別にインストールすることもできます。

- 1) Splunk Cloud環境にログインします。
- 2) Linux用Splunk Universal Forwarderをダウンロードします。
- 3) Linux用Splunk Universal Forwarderをインストールします。
- 4) ユニバーサルフォワーダのクレデンシャルをダウンロードしてインストールします。

[Splunk Cloud Platformユニバーサルフォワーダ資格情報パッケージのインストールと設定](#)

証明書パスワードが無効なため、ポート9997が開きません。そのため、資格情報パッケージ
SPLは、パスワードを2回ハッシュした別のフォワーダで再利用されたと判断され、インデクサは
新しいフォワーダを認識できません。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。