

O encaminhador universal não pode enviar dados para a Nuvem de Splunk devido a um pacote de credenciais duplicado

Aplicabilidade

Nuvem Splunk de Encaminhador Universal

Descrição

A seguinte mensagem de erro está disponível nos logs do indexador no 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
```

Nos encaminhadores universais, as seguintes mensagens estão em splunkd.log, confirmando que a conectividade TCP entre instâncias pode ser estabelecida:

```
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"
```

Investigação

Esta é a aparência do outputs.conf após o uso do pacote de credenciais, que parece estar configurado corretamente:

```
[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
```

As mensagens a seguir também estão no splunkd.log tentando autenticar o aplicativo (100_<SplunkDeployment>_splunkcloud), mesmo sabendo que o caminho para o server.pem estava correto.

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

Resolução

Os erros no encaminhador Universal que não podem se conectar ao Splunk Cloud parecem ser causados pelo pacote de credenciais não estar configurado corretamente.

Para resolvê-lo, o pacote de credenciais deve ser enviado para instâncias. Coloque o novo pacote no Servidor de Implantação a ser enviado para as instâncias, não instale os pacotes de credenciais no Servidor de Implantação.

O pacote de credenciais também pode ser instalado individualmente seguindo as etapas:

- 1) Faça login na implantação do Splunk Cloud
- 2) Faça o download do Splunk Universal Forwarder para Linux.
- 3) Instale o Splunk Universal Forwarder para Linux.
- 4) Baixe e instale as credenciais do encaminhador universal.

[Instalar e configurar o pacote de credenciais de encaminhador universal do Splunk Cloud Platform](#)

A porta 9997 não será aberta devido a uma senha de certificado inválida. Portanto, conclui-se que o SPL do pacote de credenciais foi reutilizado em outro encaminhador que hash a senha duas vezes e agora os indexadores não podem reconhecer o novo encaminhador.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.