"ERROR TcpInputProc - Encontrado fluxo S2S" em splunkd.log ao enviar dados de Splunk para Splunk

Aplicabilidade

Empresa Splunk

Descrição

O Splunk encontra erros S2S devido à ausência ou inconsistência de campos.

```
06-21-2019 11:10:31.738 +0200 ERROR TcpInputProc - Encountered Streaming S2S error=Cannot regis
new_channel="source::perfdata|host:: xxxx.xx.xxx.xxx.xx (https://xxxxx.xx.xxxx.xxx.xx/) |source
:nmon_data|145804": desired_field_count=14 conflicts with existing_field_count=0 for data recei
from src=10.121.200.154:50626.
```

Investigação

A comunicação S2S pode não estar diretamente relacionada à inclusão do nmon e do IIS, que componentes como TcpInputProc são um dos canais de log que relatam informações de rede, como mensagens de protocolo S2S.

Há vários eventos relatando que o TcpOutputProc (TCP Output Processor e FD) do HF está experimentando tempos limite de conexão para o indexador x.x.x.x, ao enviar os dados cozidos.

Começou a relatar avisos com Conexão Recusada e, finalmente, uma conexão falhou.

<#root>

```
WARN TcpOutputFd - Connect to x.x.x.x:10101 failed. Connection refused
ERROR TcpOutputFd - Connection to host=x.x.x.x:10101 failed
WARN TcpOutputFd - Connect to x.x.x.x:10101 failed. Connection refused
ERROR TcpOutputFd -
```

Connection to host=x.x.x.x:10101 failed

WARN TcpOutputFd –

Connect to x.x.x.x:10101 failed. Connection refused

WARN TcpOutputProc –

Cooked connection to ip=x.x.x.x:10101 timed out

```
WARN TcpOutputProc - Cooked connection to ip=x.x.x.x:10101 timed out
WARN TcpOutputProc - Cooked connection to ip=x.x.x.x:10101 timed out
```

Resolução

Essa mensagem de erro pode ser disparada quando o Splunk espera uma quantidade de campos e recebe o número incorreto; nesse caso específico, ele era 0. Isso pode ser causado por falta de comunicação, rede ou recursos ocupados.

Como os componentes TCPOuputProc e TcpOutputFd são os processadores de saída que gerenciam o encaminhamento de dados para servidores configurados:porta, usados principalmente por UF e HF. Eles gerenciam o descritor de arquivos nas portas TCP e executam operações como leitura/gravação.

As mensagens de erro S2S (splunk to splunk) podem ser disparadas quando o Splunk espera uma quantidade de campos e recebe o número incorreto; nesse caso específico, ele era 0. Isso pode ser causado por uma falta de comunicação causada por recursos ocupados, falta de espaço de E/S para gravar dados ou flutuação de rede comum.

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.