"ERROR TcpInputProc: se detectó transmisión de S2S" en splunkd.log al enviar datos de Splunk a Splunk

Aplicabilidad

Splunk Enterprise

Descripción

Splunk encuentra errores de S2S debido a la falta o inconsistencia de los 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.
```

Investigación

La comunicación S2S puede no estar directamente relacionada con la ingestión de nmon e IIS, cuyos componentes como TcpInputProc es uno de los canales de registro que notifican información de red, como los mensajes del protocolo S2S.

Hay varios eventos que informan que el TcpOutputProc (procesador de salida TCP y FD) del HF está experimentando tiempos de espera de conexión al indizador x.x.x.x, al enviar los datos cocinados.

Comenzó a notificar advertencias con Connection Refused y, finalmente, se produjo un error en la conexión.

<#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
```

Resolución

Este mensaje de error se puede activar cuando Splunk espera una cierta cantidad de campos y recibe el número incorrecto, en este caso en particular, era 0. Esto puede deberse a una falta de comunicación, red o recursos ocupados.

Los componentes TCPOuputProc y TcpOutputFd son los procesadores de salida que administran el reenvío de datos a los servidores:puerto configurados, utilizados principalmente por UF y HF. Administran el descriptor de archivo en los puertos TCP y realizan operaciones como lectura/escritura.

Los mensajes de error de S2S (splunk a splunk) se pueden activar cuando Splunk espera cierta cantidad de campos y recibe el número incorrecto, en este caso concreto, era 0. Esto puede deberse a una falta de comunicación causada por recursos ocupados, falta de espacio de E/S para escribir datos o fluctuación de red común.

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).