"ERREUR TcpInputProc - A rencontré un S2S en continu" dans splunkd.log lors de l'envoi de données de Splunk vers Splunk

Applicabilité

Splunk Enterprise

Description

Le module Splunk rencontre des erreurs S2S en raison de champs manquants ou incohérents.

```
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.
```

Enquête

La communication S2S peut ne pas être directement liée à l'ingestion de nmon et IIS, qui sont des composants tels que TcpInputProc qui sont l'un des canaux de journalisation qui rapportent des informations réseau, tels que les messages du protocole S2S.

Plusieurs événements signalent que le TcpOutputProc (TCP Output Processor et FD) de l'interface HF connaît des délais d'expiration de connexion à l'indexeur x.x.x.x, lors de l'envoi des données cuites.

Il a commencé à signaler des avertissements avec Connection Refused et, finalement, une connexion a échoué.

<#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
```

Résolution

Ce message d'erreur peut être déclenché lorsque le Splunk attend un certain nombre de champs et qu'il reçoit le mauvais numéro. Dans ce cas particulier, il était 0. Cela peut être dû à un manque de communication, à un réseau ou à des ressources occupées.

Comme TCPOuputProc et TcpOutputFd les composants sont les processeurs de sortie qui gèrent le transfert des données vers les serveurs configurés : port, principalement utilisé par UF et HF. Ils gèrent le descripteur de fichier sur les ports TCP et effectuent des opérations telles que la lecture/écriture.

Les messages d'erreur S2S (splunk to splunk) peuvent être déclenchés lorsque Splunk attend un certain nombre de champs et reçoit le mauvais numéro, dans ce cas particulier, il était 0. Cela peut être dû à un manque de communication causé par des ressources occupées, un manque d'espace d'E/S pour écrire des données ou une fluctuation réseau courante.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.