"ERROR TcpInputProc - Rilevato Streaming S2S" in splunkd.log durante l'invio dei dati da Splunk a Splunk

Applicabilità

Splunk Enterprise

Descrizione

Splunk rileva errori da sito a sito a causa di campi mancanti o incoerenti.

```
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.
```

Indagine

La comunicazione da sito a sito potrebbe non essere direttamente correlata all'acquisizione di nmon e IIS, che componenti come TcpInputProc sono uno dei canali di registro che segnalano le informazioni di rete, ad esempio i messaggi del protocollo da sito a sito.

Ci sono diversi eventi che segnalano il TcpOutputProc (TCP Output Processor e FD) dall'HF sta riscontrando timeout di connessione all'indicizzatore x.x.x, quando invia i dati elaborati.

È stato avviato il report degli avvisi con la connessione rifiutata e, infine, una connessione non riuscita.

<#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
```

Risoluzione

Questo messaggio di errore può essere generato quando Splunk prevede una quantità di campi e riceve il numero errato, in questo caso specifico il valore è 0. Il problema potrebbe essere dovuto a una mancanza di risorse di comunicazione, di rete o occupate.

Poiché i componenti TCPOuputProc e TcpOutputFd sono i processori di output che gestiscono l'inoltro dei dati ai server configurati:porta, utilizzati principalmente da UF e HF. Gestiscono il descrittore del file sulle porte TCP ed eseguono operazioni come la lettura/scrittura.

I messaggi di errore S2S (splunk to splunk) possono essere attivati quando Splunk prevede una quantità di campi e riceve il numero errato, in questo caso specifico è 0. Ciò può essere causato da una mancanza di comunicazione causata da risorse occupate, mancanza di spazio I/O per la scrittura di dati o da fluttuazioni di rete comuni.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).