

Il server di inoltro di Splunk non invia eventi a Splunk Cloud

Applicabilità

Splunk Cloud

Descrizione

Un server d'inoltro Splunk non invia più eventi a Splunk Cloud. Ciò può influire su un server di inoltro universale, un server di inoltro pesante o un livello di inoltro intermedio.

In `splunkd.log` viene visualizzato il seguente errore:

```
ERROR TcpOutputFd - Connection to host=1.22.122.222:9997 failed. sock_error = 104. SSL  
Error = No error
```

Il messaggio `sock_error = 104` indica che la connessione TCP è stata reimpostata mentre il server d'inoltro stava tentando di comunicare con l'endpoint di ricezione di Splunk Cloud.

Indagine

Verificare la connettività di rete di base dal server di inoltro interessato all'endpoint di input di Splunk Cloud:

```
telnet inputs1.<stack_id>.splunkcloud.com 9997
```

Se la connessione `telnet` riesce, la porta è raggiungibile. Tuttavia, non convalida completamente la connessione SSL/TLS o conferma che il traffico non viene reimpostato da un dispositivo di rete

intermedio.

Per convalidare ulteriormente la connessione, eseguire uno dei comandi seguenti dal server di inoltro interessato:

```
openssl s_client -connect inputs1.<stack_id>.splunkcloud.com:9997
```

O

```
$SPLUNK_HOME/bin/splunk cmd openssl s_client -connect inputs1.<stack_id>.splunkcloud.com
```

Se viene restituito il seguente output, la connessione verrà reimpostata:

```
CONNECTED(00000003)  
write:errno=104
```

Ciò conferma che il server d'inoltro può inizialmente stabilire una connessione TCP, ma che la connessione viene chiusa forzatamente prima del completamento della sessione SSL/TLS.

Esaminare inoltre la configurazione di inoltro nel server di inoltro interessato, incluso `outputs.conf`, per verificare che il server di inoltro stia utilizzando l'endpoint di ricezione e la porta Splunk Cloud corretti.

Risoluzione

L'errore 104 è `ECONNRESET`, che significa "Connessione reimpostata dal peer". Ciò indica che la connessione è stata chiusa forzatamente con un pacchetto di ripristino TCP. Il ripristino può essere inviato dall'endpoint di destinazione o da un dispositivo di rete intermedio, ad esempio un firewall, un proxy, un servizio di bilanciamento del carico, IDS/IPS, un dispositivo di ispezione SSL o un accessorio di rete.

Esaminare il percorso di rete completo tra il server d'inoltro interessato e Splunk Cloud.
Confermare che:

- Il traffico in uscita verso l'endpoint di input di Splunk Cloud è consentito sulla porta 9997.
- Firewall, proxy o dispositivi di rete non reimpostano le sessioni TCP.
- L'ispezione SSL non interferisce con la connessione di inoltro Splunk.
- Qualsiasi modifica recente relativa alla rete, al firewall, al proxy, al routing o al certificato viene esaminata.
- L'app e i certificati del server di inoltro di Splunk Cloud sono aggiornati e distribuiti correttamente.
- I server di inoltro intermedi possono comunicare con Splunk Cloud e non eliminano o bloccano il traffico inoltrato.

Dopo aver corretto la configurazione della rete, del firewall o del certificato, riavviare il server d'inoltro interessato, se necessario, oppure consentire la riconnessione automatica. Verificare quindi che gli eventi vengano indicizzati correttamente in Splunk Cloud.

Collegamenti correlati

[Problemi di connessione con Universal Forwarder per Linux ARM e Splunk Cloud \(errore SSL\)](#)

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).