

Le redirecteur de liaison n'envoie pas d'événements au nuage de liaison

Applicabilité

Cloud Splunk

Description

Un redirecteur Splunk n'envoie plus d'événements au cloud Splunk. Cela peut affecter un redirecteur universel, un redirecteur lourd ou un niveau de transfert intermédiaire.

L'erreur suivante apparaît dans `splunkd.log` :

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

Le message `sock_error = 104` indique que la connexion TCP a été réinitialisée alors que le redirecteur tentait de communiquer avec le point d'extrémité de réception du nuage Splunk.

Enquête

Vérifiez la connectivité réseau de base entre le redirecteur affecté et le point d'extrémité d'entrée du cloud Splunk :

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

Une connexion `Telnet` réussie confirme que le port est accessible. Cependant, il ne valide pas complètement la connexion SSL/TLS ou ne confirme pas que le trafic n'est pas réinitialisé par un

périphérique réseau intermédiaire.

Pour valider davantage la connexion, exécutez l'une des commandes suivantes à partir du redirecteur concerné :

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

OU

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

Si le résultat suivant est renvoyé, la connexion est en cours de réinitialisation :

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

Cela confirme que le redirecteur peut établir initialement une connexion TCP, mais que la connexion est fermée de force avant la fin de la session SSL/TLS.

Examinez également la configuration de transfert sur le redirecteur affecté, y compris `output.conf`, pour confirmer que le redirecteur utilise le point d'extrémité et le port de réception du nuage Splunk corrects.

Résolution

L'erreur 104 est `ECONNRESET`, ce qui signifie « Connection reset by peer ». Cela indique que la connexion a été fermée de force avec un paquet de réinitialisation TCP. La réinitialisation peut être envoyée par le point d'extrémité de destination ou par un périphérique réseau intermédiaire, tel qu'un pare-feu, un proxy, un équilibreur de charge, un système IDS/IPS, un périphérique d'inspection SSL ou un appareil réseau.

Examinez le chemin réseau complet entre le redirecteur affecté et le nuage Splunk. Confirmez que :

- Le trafic sortant vers le point d'extrémité d'entrée du nuage de blocs est autorisé sur le port 9997.
- Les pare-feu, les proxys ou les appliances réseau ne réinitialisent pas les sessions TCP.
- L'inspection SSL n'interfère pas avec la connexion de transfert Splunk.
- Toute modification récente du réseau, du pare-feu, du proxy, du routage ou du certificat est examinée.
- L'application Splunk Cloud Forwarder et les certificats sont à jour et correctement déployés.
- Les redirecteurs intermédiaires peuvent communiquer avec le nuage Splunk et n'abandonnent ni ne bloquent le trafic transféré.

Après avoir corrigé la configuration du réseau, du pare-feu ou du certificat, redémarrez le redirecteur affecté si nécessaire, ou autorisez-le à se reconnecter automatiquement. Confirmez ensuite que les événements sont correctement indexés dans le cloud Splunk.

Liens connexes

[Problèmes de connexion avec Universal Forwarder pour Linux ARM et Splunk Cloud \(erreur SSL\)](#)

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.