

Splunk Forwarder stuurt geen events naar Splunk Cloud

toepasbaarheid

splunkwolk

Beschrijving

Een Splunk-forwarder stuurt geen evenementen meer naar Splunk Cloud. Dit kan een Universal Forwarder, Heavy Forwarder of een tussenliggende forwarding tier beïnvloeden.

De volgende fout wordt weergegeven in `splunkd.log`:

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

Het bericht `sock_error = 104` geeft aan dat de TCP-verbinding is gereset terwijl de forwarder probeerde te communiceren met het eindpunt van Splunk Cloud-ontvangst.

onderzoek

Verifieer de basisnetwerkconnectiviteit van de betreffende expediteur naar het Splunk Cloud-invoereindpunt:

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

Een succesvolle `telnet`-verbinding bevestigt dat de poort bereikbaar is. De SSL/TLS-verbinding wordt echter niet volledig gevalideerd of er wordt niet bevestigd dat het verkeer wordt gereset door

een tussenliggend netwerkapparaat.

Voer een van de volgende opdrachten uit van de betreffende expediteur om de verbinding verder te valideren:

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

OF

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

Als de volgende uitvoer wordt geretourneerd, wordt de verbinding opnieuw ingesteld:

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

Dit bevestigt dat de forwarder in eerste instantie een TCP-verbinding tot stand kan brengen, maar dat de verbinding met geweld wordt gesloten voordat de SSL/TLS-sessie is voltooid.

Controleer ook de forwarding configuratie op de betrokken forwarder, met inbegrip van `outputs.conf`, om te bevestigen dat de forwarder is met behulp van de juiste Splunk Cloud ontvangen eindpunt en poort.

resolutie

Fout 104 is `ECONNRESET`, wat betekent "Verbinding gereset door peer." Dit geeft aan dat de verbinding met geweld werd afgesloten met een TCP-reset-pakket. De reset kan worden verzonden door het eindpunt van de bestemming of door een tussenliggend netwerkapparaat, zoals een firewall, proxy, load balancer, IDS/IPS, SSL-inspectieapparaat of netwerkapparaat.

Bekijk het volledige netwerkpad tussen de betreffende forwarder en Splunk Cloud. Bevestig dat:

- Uitgaand verkeer naar het Splunk Cloud-invoereindpunt is toegestaan op poort 9997.
- Firewalls, proxy's of netwerkapparaten herstellen geen TCP-sessies.
- SSL-inspectie interfereert niet met de Splunk-forwarding-verbinding.
- Alle recente wijzigingen in het netwerk, de firewall, de proxy, de routing of het certificaat worden beoordeeld.
- De Splunk Cloud forwarder app en certificaten zijn actueel en correct geïmplementeerd.
- Intermediate forwarders kunnen communiceren met Splunk Cloud en laten geen doorgestuurd verkeer vallen of blokkeren.

Nadat u de netwerk-, firewall- of certificaatconfiguratie hebt gecorrigeerd, start u de betreffende expediteur indien nodig opnieuw op of laat u deze automatisch opnieuw verbinding maken. Bevestig vervolgens dat gebeurtenissen met succes worden geïndexeerd in Splunk Cloud.

Gerelateerde links

[Verbindingsproblemen met Universal Forwarder voor Linux ARM en Splunk Cloud \(SSL-fout\)](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.