

FOUT: Kan geen zoekpeers toevoegen: verbinding opnieuw instellen op peer

toepasbaarheid

Splunk Enterprise

Beschrijving

Proberen om nieuwe indexers en nieuwe zoekkoppen toe te voegen in de omgeving, de indexers zijn onderdeel van het cluster, maar de zoekkoppen zijn niet geconfigureerd als een cluster.

Andere indexeerders zijn al ingesteld als peers voor de zoekkoppen in vragen, maar de zoekkoppen hebben andere indexeerders als zoekpeers.

onderzoek

- Controleer of de SSL-instelling juist is en er geen problemen zijn met betrekking tot de connectiviteit.
- Fouten in splunkd.log tonen aan: SSL-verbinding kon niet tot stand worden gebracht, verbinding gereset door peer voor IP-adres indexeerder.
- Handmatige configuratie met zowel configuratiebestanden als GUI-instellingen mislukt hetzelfde.
- Bevestig dat https wordt gebruikt voor de URI van de indexeerders omdat SSL in gebruik is.
- Bevestig dat de betreffende indexeerders in clustermodus zijn ingesteld.
- Zoekkoppen zijn niet geclusterd

resolutie

Aangezien indexeerders zijn geclusterd, moet de zoekkop de zoekkopmodus hebben ingeschakeld in server.conf, anders herkent het indexercluster de instantie niet goed en weigert het peer-verzoek.

Houd er rekening mee dat het zoekhoofd een clusterstanza nodig heeft, hoewel de zoekkoppen niet zijn geclusterd.

1. Configureer het bestand server.conf als volgt

```
[clustering]
master_uri = https://x.x.x.x:xxxx (https://x.x.x.xxxxx)
mode = searchhead
pass4SymmKey= yourPass4SymmKey
```

master_uri = de clustermaster-URI voor het ****Indexeerdercluster****, zoekkoppen worden niet geclusterd voor dit geval.

Modus = Dit is vereist om de server in de zoekkopmodus in te stellen voor clustercommunicatie

pass4SymmKey = sleutel voor het cluster, de gebruikers moeten zijn / haar eigen sleutel voor een dergelijk kenmerk toevoegen

2. Start de service opnieuw op en probeer de zoekcollega's opnieuw toe te voegen, het proces moet slagen.

Gerelateerde links

Splunk-documentatie

Voeg zoekpeers toe aan de zoekkop:

<https://docs.splunk.com/Documentation/Splunk/7.3.0/DistSearch/Configuredistributedsearch>

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.