Problemen met Splunk-connectiviteit in PCF-oplossing

Inhoud

Inleiding

Dit document beschrijft de procedure voor probleemoplossing voor de Splunk-kwestie die wordt gezien in de CNDP-PCF (Cloud Native Implementation Platform).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:
· Beleidscontrolefunctie (PCF)
· 5G CNDP
Dockers en Kubernetes

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:
· PCF REL_2023.01.2
· Kubernetes v1.24.6

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

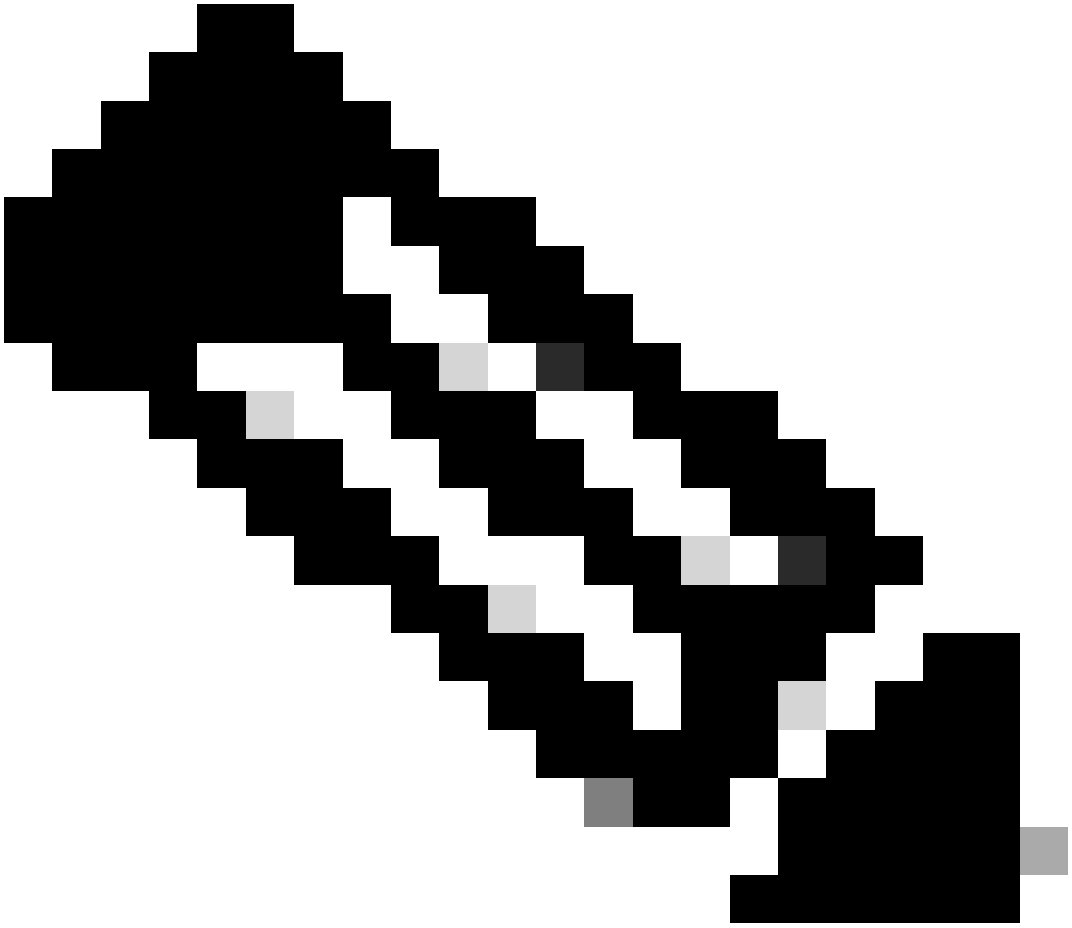
In deze installatie wordt op de CNDP een PCF gehost.

Splunk Server is de kerncomponent van het Splunk-softwareplatform. Het is een schaalbare en krachtige oplossing voor het verzamelen, indexeren, doorzoeken, analyseren en visualiseren van door machines gegenereerde gegevens.

Splunk Server werkt als een gedistribueerd systeem dat gegevens kan verwerken uit verschillende bronnen, waaronder logbestanden, gebeurtenissen, metriek en andere machinedata. Het biedt de infrastructuur om gegevens te verzamelen en op te slaan, real-time indexering en zoeken uit te voeren en inzichten te leveren via zijn web-based gebruikersinterface.

Waarschuwingsregel aanwezig in PCF-datacenter voor Splunk-verbinding omlaag

```
alerts rules group splunk-forwarding-status-change
rule splunk-forwarding-status-change
expression "splunk_log_forwarding_status== 1"
duration 1m
severity major
type "Equipment Alarm"
annotation description
value "splunk-forward-log Down"
```



Opmerking: U moet controleren of deze regel aanwezig is in het PCF-operatiecentrum voor het effectief waarschuwen van problemen met Splunk-connectiviteit.

Probleem

Je ziet waarschuwingen op de Common Execution Environment (CEE) Ops-Center voor Splunk voorwaartse fout.

```
Command:
cee# show alerts active summary summary
Example:
[pcf01/pcfapp] cee# show alerts active summary
NAME UID SEVERITY STARTS AT DURATION SOURCE SUMMARY
-----------------------------------------------------------------------------------------------------
splunk-forwarding-sta 23df441759f5 major 05-12T22:47:21 43h33m50s pcf-master-3 Unknown
splunk-forwarding-sta 0bf8ad5f91f1 major 05-12T19:07:51 3h20m20s pcf-master-2 Unknown
splunk-forwarding-sta 612f428fa42e major 05-09T06:43:01 70h32m40s pcf-master-2 Unknown
splunk-forwarding-sta 23df441759f5 major 05-12T22:47:21 43h33m50s pcf-master-3 Unknown
```

Problemen oplossen

Stap 1. Maak verbinding met de master node en controleer de consolidated-logging-0 pod status.

Command:
cloud-user@pcf01-master-1$ kubectl get pods -A |grep consolidated-logging-0
Example:
cloud-user@pcf01-master-1:~$ kubectl get pods -A -o wide | grep consolidated-logging-0
NAMESPACE NAME READY STATUS RESTARTS AGE
pcf-pcf01 consolidated-logging-0 1/1 Running 0 2d22h xxx.xxx.x.xxx pcf01-primary-1 <none> <none>
cloud-user@pcf01-master-1:~$

Stap 2. Controleer de Splunk-verbinding door in te loggen op de geconsolideerde peul met deze opdrachten.

Om te controleren of een verbinding tot stand is gebracht op poort 8088 kunt u deze opdracht gebruiken:

cloud-user@pcf01-master-1:~$ kubectl exec -it -n pcf-pcf01 consolidated-logging-0 bash
kubectl exec [POD] [COMMAND] is DEPRECATED and will be removed in a future version. Use kubectl exec [POD] -- [COMMAND] instead.
groups: cannot find name for group ID 303
I have no name!@consolidated-logging-0:/$
I have no name!@consolidated-logging-0:/$
I have no name!@consolidated-logging-0:/$ netstat -anp | grep 8088
I have no name!@consolidated-logging-0:/$
I have no name!@consolidated-logging-0:/$

Stap 3. Als er geen verbindingen met Splunk zijn, controleert u de configuratie op het PDF Ops-Center.

cloud-user@pcf01-master-1:~$ ssh -p 2024 admin@$(kubectl get svc -A -o wide |grep 2024 | grep ops-center-pcf | awk '{ print $4}')
[pcf01/pcfapp] pcf#show running-config| include splunk
[pcf01/pcfapp] pcf# debug splunk hec-url https://xx.xxx.xxx.xx:8088
[pcf01/pcfapp] pcf# debug splunk hec-token d3a6e077-d51b-4669-baab-1ddf19aba325
[pcf01/pcfapp] pcf#

Stap 4. Als de verbinding niet tot stand is gebracht, moet u de consolidated-logging-0 peul opnieuw genereren.

cloud-user@pcf01-master-1:~$ kubectl delete pod -n pcf-pcf01 consolidated-logging-0

Stap 5. Controleer de consolidated-logging-0 peul na verwijdering.

cloud-user@pcf01-master-1:~$ kubectl get pods -A | grep consolidated-logging-0

Stap 6. Maak verbinding met de consolidated-logging peul, voer de netstat poort naar 8088 uit en controleer de ingestelde Splunk-verbinding.

cloud-user@pcf01-master-1:$ kubectl exec -it -n pcf-wscbmpcf consolidated-logging-0 bash
I have no name!@consolidated-logging-0:/$ netstat -anp | grep 8088
tcp 0 0 xxx.xxx.xx.xxx:60808 xx.xxx.xxx.xx:8088 ESTABLISHED 1/java
tcp 0 4957 xxx.xxx.xx.xxx:51044 xx.xxx.xxx.xx:8088 ESTABLISHED 1/java
tcp 0 4963 xxx.xxx.xx.xxx:59298 xx.xxx.xxx.xx:8088 ESTABLISHED 1/java
tcp 0 0 xxx.xxx.xx.xxx:34938 xx.xxx.xxx.xx:8088 ESTABLISHED 1/java
tcp 0 0 xxx.xxx.xx.xxx:43964 xx.xxx.xxx.xx:8088 ESTABLISHED 1/java

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.