Fehlerbehebung bei Splunk-Verbindungsproblemen in PCF

Inhalt

Einleitung

In diesem Dokument wird das Verfahren zur Behebung des Splunk-Problems in der Cloud Native Deployment Platform (CNDP) PCF beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:
- Policy Control Function (PCF)
- 5G CNDP
- Dockers und Kubernetes

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:
- PCF REL_2023.01.2
- Kubernetes v1.24.6

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

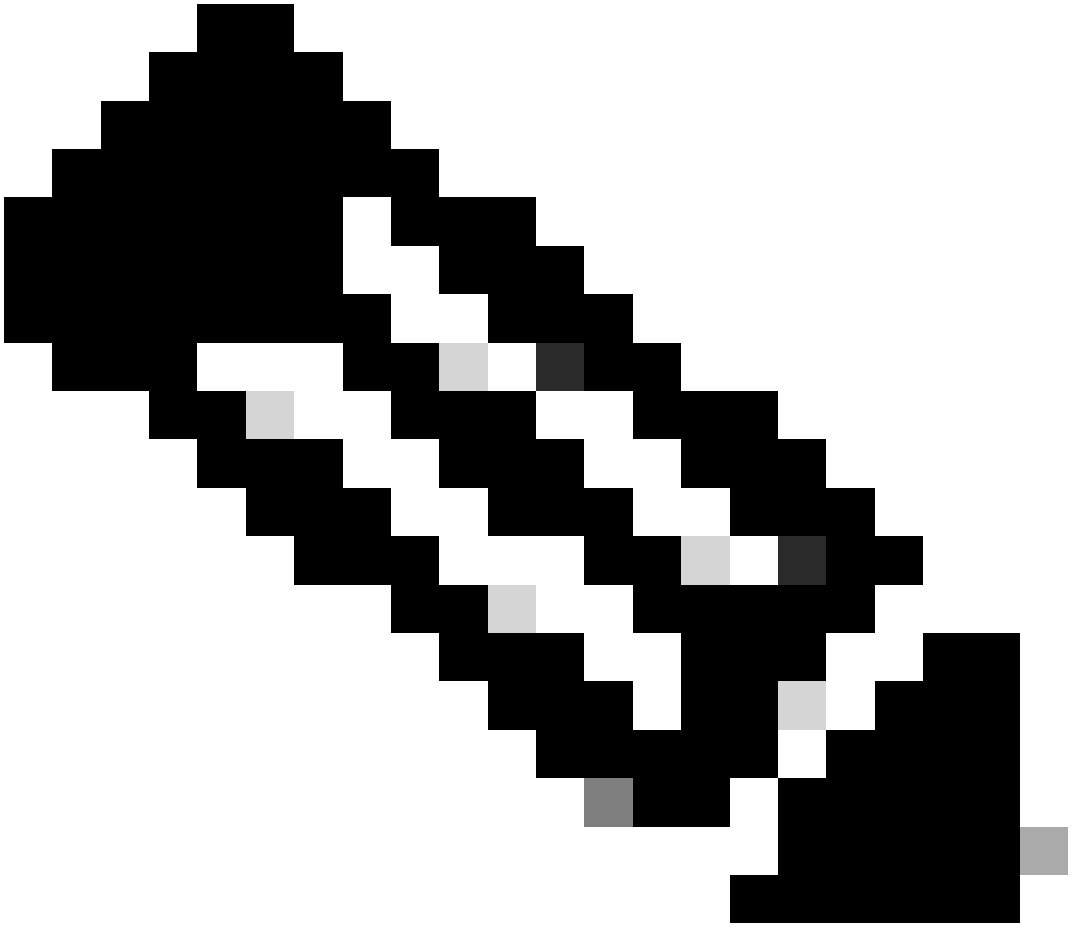
In dieser Konfiguration hostet der CNDP eine PCF.

Splunk Server ist die Kernkomponente der Splunk Softwareplattform. Es ist eine skalierbare und leistungsstarke Lösung für das Sammeln, Indizieren, Suchen, Analysieren und Visualisieren von maschinell generierten Daten.

Der Splunk-Server agiert als verteiltes System, das Daten aus einer Vielzahl von Quellen verarbeiten kann, darunter Protokolle, Ereignisse, Metriken und andere Maschinendaten. Die Lösung bietet die Infrastruktur zum Sammeln und Speichern von Daten, zur Durchführung von Indizierungen und Suchvorgängen in Echtzeit und zur Bereitstellung von Informationen über die webbasierte Benutzeroberfläche.

Warnungsregel in PCF-Betriebszentrum für ausgefallene Splunk-Verbindung vorhanden

```
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"
```



Hinweis: Sie müssen sicherstellen, dass diese Regel im PCF-Betriebszentrum vorhanden ist, um bei Splunk-Verbindungsproblemen effektiv gewarnt zu werden.

Problem

Es werden Warnmeldungen zum Common Execution Environment (CEE) Ops-Center bei Splunk-Weiterleitungsfehlern angezeigt.

```
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
```

Fehlerbehebung

Schritt 1: Stellen Sie eine Verbindung zum Master-Knoten her, und überprüfen Sie den 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:~$

Schritt 2: Überprüfen Sie die Splunk-Verbindung, indem Sie sich mit diesen Befehlen beim konsolidierten POD anmelden.

Mit dem folgenden Befehl können Sie überprüfen, ob eine Verbindung mit Port 8088 hergestellt wurde:

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:/$

Schritt 3: Wenn keine Verbindungen zu Splunk bestehen, überprüfen Sie die Konfiguration im 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#

Schritt 4: Wenn die Verbindung nicht hergestellt ist, erstellen Sie den consolidated-logging-0 Pod neu.

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

Schritt 5: Überprüfen Sie den consolidated-logging-0 PoD nach dem Löschen.

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

Schritt 6: Stellen Sie eine Verbindung zum consolidated-logging PoD her, schließen Sie den netstat Anschluss an Port 8088 an, und überprüfen Sie, ob die Splunk-Verbindung hergestellt wurde.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.