排除PCF中的Splunk連線故障

目錄

簡介

本文檔介紹對雲本地部署平台(CNDP) PCF中出現的Splunk問題進行故障排除的過程。

必要條件

需求

思科建議您瞭解以下主題：
· 策略控制功能(PCF)
· 5G CNDP
· 多克和庫貝爾內特

採用元件

本文中的資訊係根據以下軟體和硬體版本：
· PCF REL_2023.01.2
· Kubernetes v1.24.6

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在此設定中，CNDP託管一個PCF。

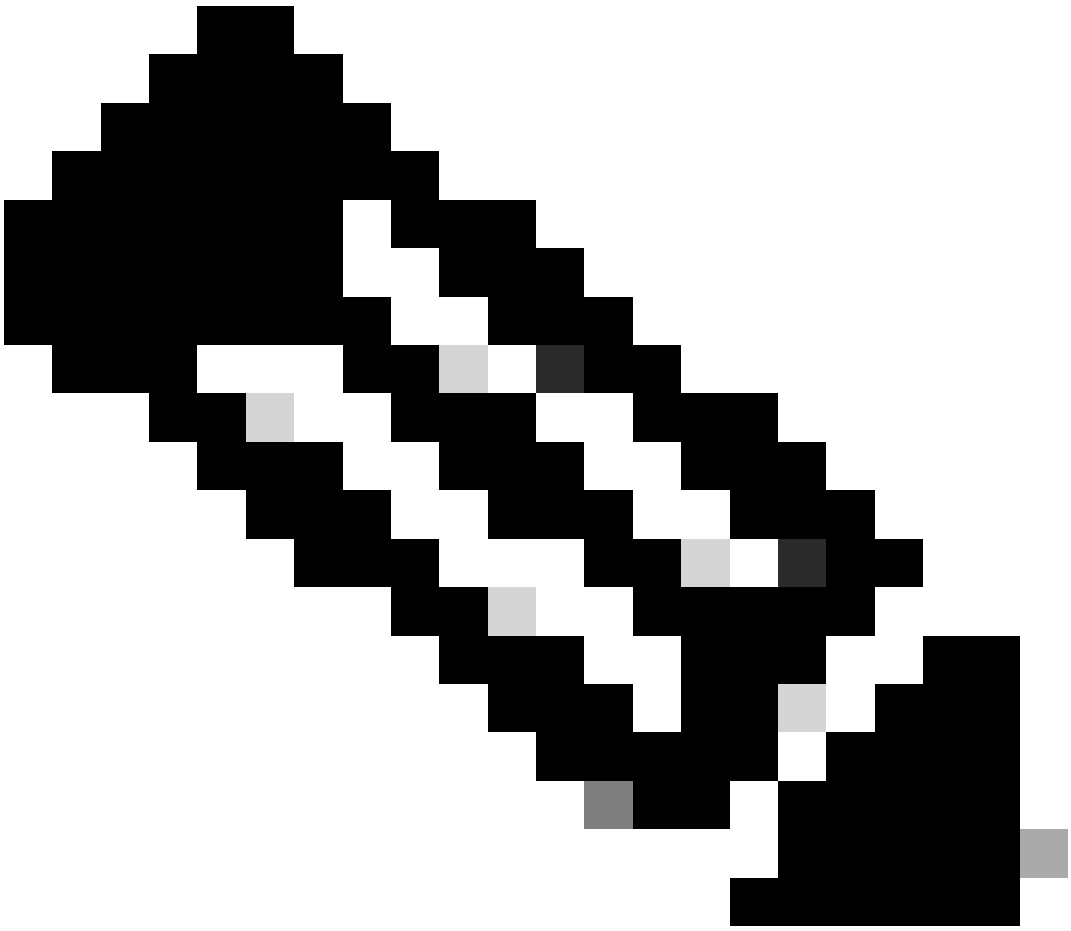
Splunk Server是Splunk軟體平台的核心元件。它是一種可擴展且功能強大的解決方案，可用於收集、索引、搜尋、分析和視覺化機器生成的資料。

Splunk Server作為分散式系統運行，可以處理各種來源的資料，包括日誌、事件、度量和其他電腦資料。它提供收集和儲存資料、執行即時索引和搜尋的基礎設施，並透過其基於Web的使用者介面

提供見解。

PCF Ops-Center for Splunk Connection Down中存在警報規則

```
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"
```



注意：您需要驗證PCF運行中心中是否存在此規則，以便有效地對Splunk連線問題進行警報。

問題

您會看到Splunk轉發失敗的通用執行環境(CEE) Ops-Center警報。

```
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
```

疑難排解

步驟 1.連線到主節點並驗證consolidated-logging-0 Pod狀態。

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:~$

步驟 2.使用以下命令登入統一的Pod，驗證Splunk連線。
為了檢查是否已在埠8088上建立連線，您可以使用此命令：

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:/$

步驟 3.如果沒有與Splunk的連線，請驗證PDF Ops-Center上的配置。

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#

步驟 4.如果未建立連線，則重新建立consolidated-logging-0 Pod。

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

步驟 5.刪除後驗證consolidated-logging-0Pod。

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

步驟 6.連線到consolidated-loggingpod，完成到埠8088的netstat連線，並驗證已建立Splunk連線。

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。