Dépannage du problème de connectivité Splunk dans PCF

Table des matières

Introduction

Ce document décrit la procédure de dépannage du problème Splunk détecté dans le PCF de la plate-forme de déploiement natif cloud (CNDP).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :
· Fonction de contrôle des politiques (PCF)
· CNDP 5G
· Dockers et Kubernetes

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :
· PCF REL_2023.01.2
· Kubernetes v1.24.6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

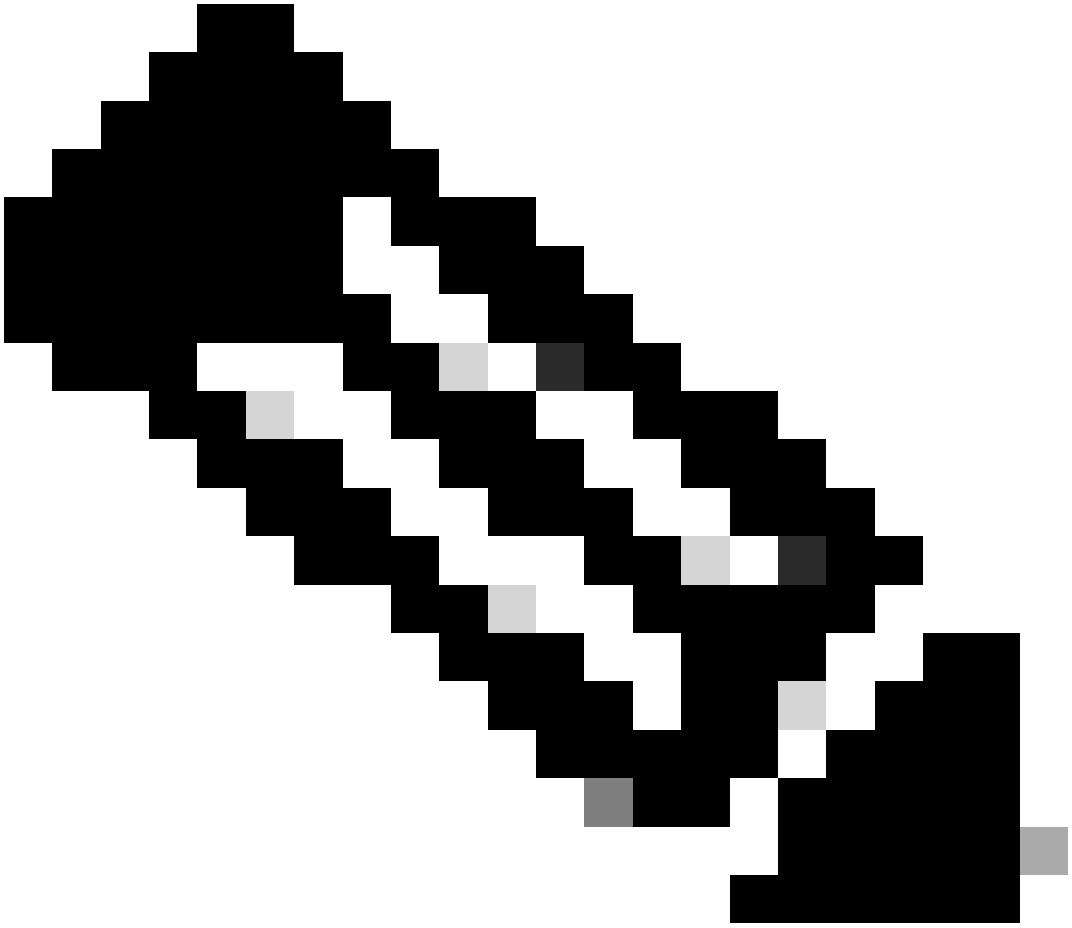
Dans cette configuration, le protocole CNDP héberge un PCF.

Splunk Server est le composant principal de la plate-forme logicielle Splunk. Il s'agit d'une solution évolutive et puissante pour la collecte, l'indexation, la recherche, l'analyse et la visualisation des données générées par la machine.

Le serveur Splunk fonctionne comme un système distribué capable de gérer des données provenant de diverses sources, notamment des journaux, des événements, des mesures et d'autres données machine. Elle fournit l'infrastructure nécessaire pour collecter et stocker des données, effectuer des recherches et des indexations en temps réel et fournir des informations via son interface utilisateur Web.

Règle d'alerte présente dans PCF Ops-Center pour Splunk Connection Down

```
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"
```



Remarque : vous devez vérifier que cette règle est présente dans le centre d'opérations PCF pour une alerte efficace des problèmes de connectivité Splunk.

Problème

Des alertes s'affichent sur le centre d'opérations de l'environnement d'exécution commun (CEE) pour la défaillance du transfert de Splunk.

```
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
```

Dépannage

Étape 1. Connectez-vous au noeud maître et vérifiez l'état du consolidated-logging-0 pod.

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:~$

Étape 2. Vérifiez la connexion Splunk en vous connectant au pod consolidé à l'aide de ces commandes.

Afin de vérifier si une connexion est établie sur le port 8088, vous pouvez utiliser cette commande :

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:/$

Étape 3. S'il n'y a aucune connexion à Splunk, vérifiez la configuration sur le 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#

Étape 4. Si la connexion n'est pas établie, recréez le consolidated-logging-0 pod.

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

Étape 5. Vérifiez le podconsolidated-logging-0 après la suppression.

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

Étape 6. Connectez-vous au podconsolidated-logging et effectuez la connexionnetstat au port 8088 et vérifiez la connexion Splunk établie.

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.