# Resolución de problemas de conectividad Splunk en PCF

## Contenido



## Introducción

Este documento describe el procedimiento para resolver el problema de Splunk que se observa en la plataforma de implementación nativa en la nube (CNDP) PCF.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:
· Función de control de políticas (PCF)
· 5G CNDP
· Dockers y Kubernetes

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.
PCF REL_2023.01.2
· Kubernetes v1.24.6

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

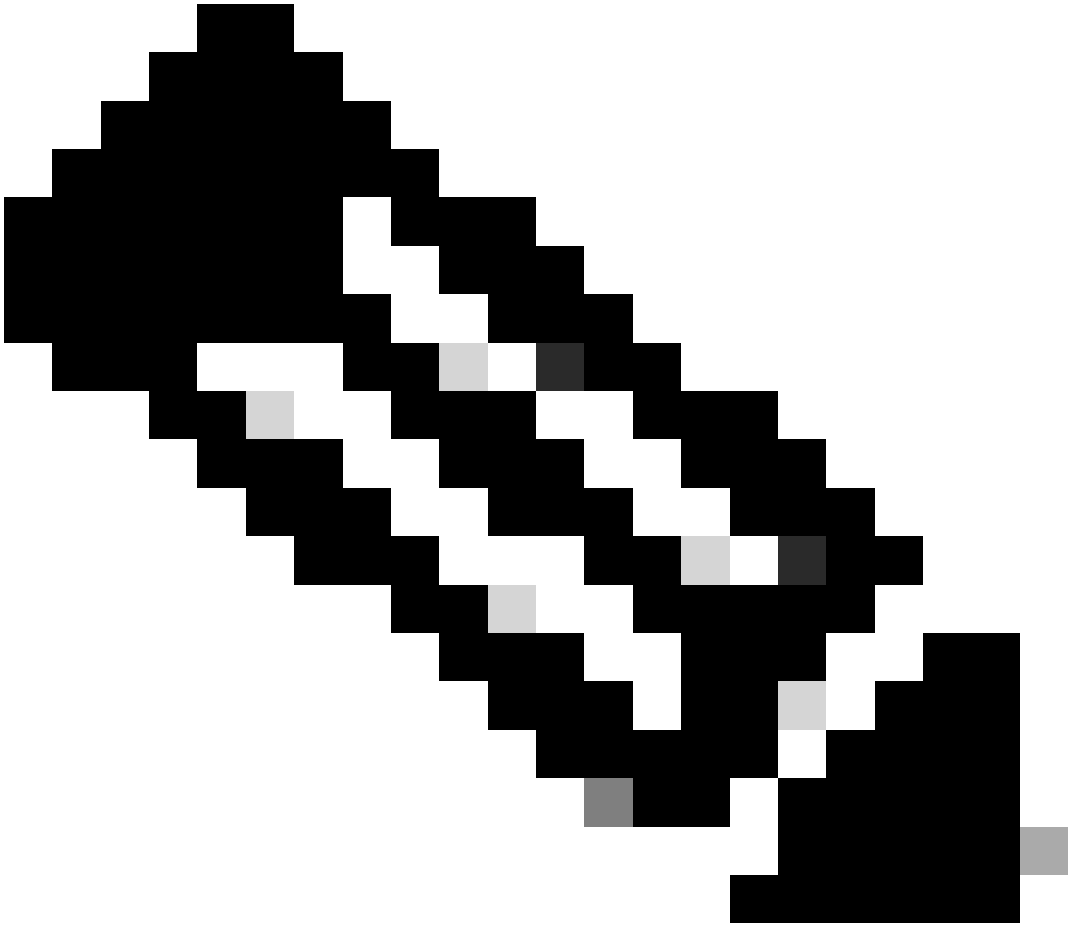
En esta configuración, el CNDP aloja un PCF.

Splunk Server es el componente principal de la plataforma de software Splunk. Se trata de una solución escalable y potente para recopilar, indexar, buscar, analizar y visualizar datos generados por máquinas.

Splunk Server funciona como un sistema distribuido que puede manejar datos de una variedad de orígenes, incluidos registros, eventos, métricas y otros datos de la máquina. Proporciona la infraestructura necesaria para recopilar y almacenar datos, realizar búsquedas e índices en tiempo real y proporcionar información a través de su interfaz de usuario basada en Web.

# Regla de alerta presente en el centro de operaciones de PCF para la conexión de splunk inactiva

```
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"
```



Nota: Debe verificar que esta regla esté presente en el Centro de operaciones de PCF para la alerta efectiva de problemas de conectividad de Splunk.

## Problema

Verá alertas sobre el centro de operaciones de Common Execution Environment (CEE) para fallos de reenvío 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
```

# Troubleshoot

## Paso 1. Conéctese al nodo maestro y verifique el estado del consolidated-logging-0 grupo de dispositivos.

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:~$

Paso 2. Verifique la conexión Splunk iniciando sesión en el grupo de dispositivos consolidado con estos comandos.

Para verificar si se ha establecido una conexión en el puerto 8088, puede utilizar este comando:

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:/$

Paso 3. Si no hay conexiones a Splunk, verifique la configuración en el 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#

Paso 4. Si no se establece la conexión, vuelva a crear el consolidated-logging-0 grupo de dispositivos.

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

Paso 5. Verifique el consolidated-logging-0 pod después de la eliminación.

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

Paso 6. Conéctese a la consolidated-logging vaina y realice la conexión netstat al puerto 8088 y verifique la conexión Splunk establecida.

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).