# Risoluzione dei problemi di connettività dello splunk in PCF

## Sommario



## Introduzione

In questo documento viene descritta la procedura per risolvere il problema dello Splunk rilevato nel PCF Cloud Native Deployment Platform (CNDP).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:
· Funzione di controllo delle policy (PCF)
· CNDP 5G
· Docker e Kubernetes

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:
· PCF REL_2023.01.2
· Kubernetes v1.24.6

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

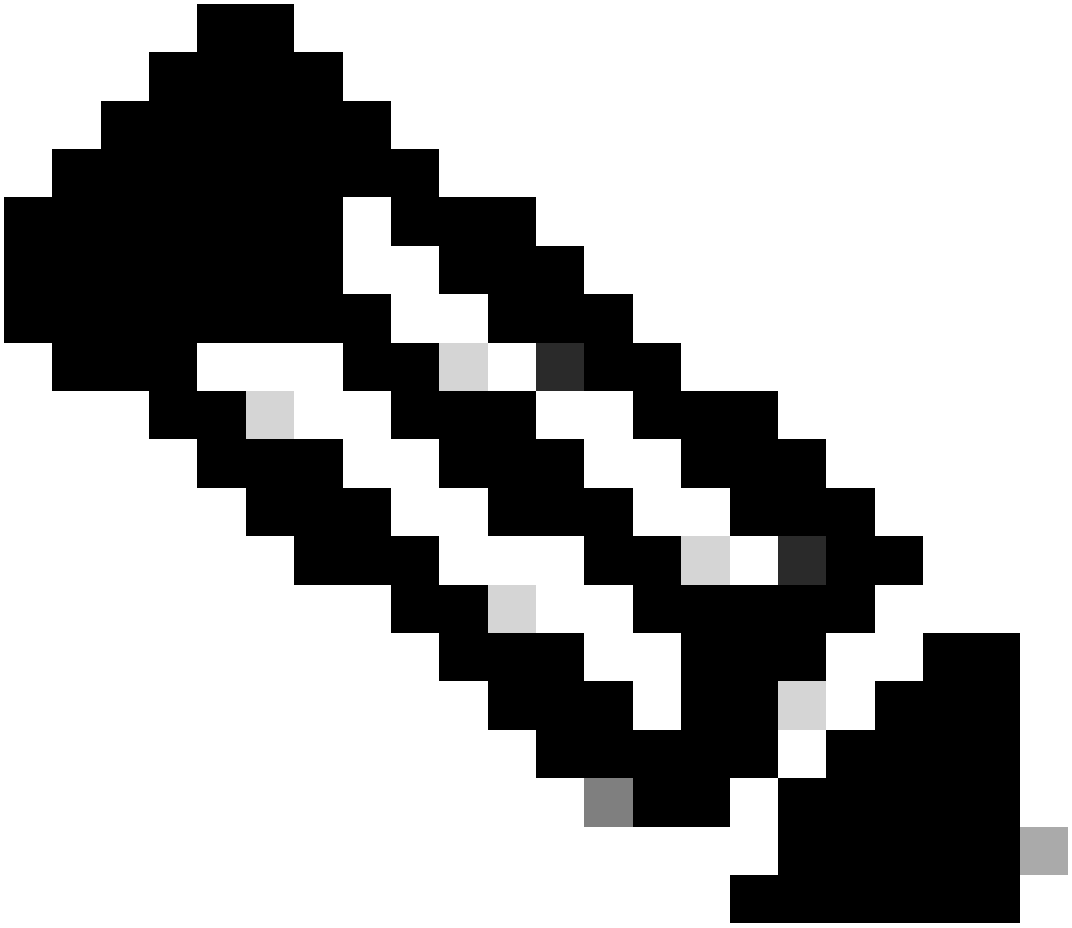
In questa configurazione, il CNDP ospita un PCF.

Splunk Server è il componente principale della piattaforma software Splunk. Si tratta di una soluzione scalabile e potente per la raccolta, l'indicizzazione, la ricerca, l'analisi e la visualizzazione di dati generati automaticamente.

Splunk Server funziona come un sistema distribuito in grado di gestire i dati provenienti da diverse origini, tra cui registri, eventi, metriche e altri dati del computer. Fornisce l'infrastruttura necessaria per raccogliere e memorizzare i dati, eseguire ricerche e indicizzazioni in tempo reale e fornire informazioni dettagliate attraverso l'interfaccia utente basata sul Web.

# Regola di avviso presente in PCF Ops-Center per la connessione a splunk inattiva

```
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: è necessario verificare che questa regola sia presente nel centro operativo PCF per poter inviare un avviso sui problemi di connettività Splunk.

## Problema

Vengono visualizzati avvisi sul centro operativo Common Execution Environment (CEE) per l'errore di inoltro 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
```

# Risoluzione dei problemi

## Passaggio 1. Connettersi al nodo master e verificare lo stato del 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:~$

Passaggio 2. Verificare la connessione Splunk accedendo al pod consolidato con questi comandi.

Per verificare se è stata stabilita una connessione sulla porta 8088, è possibile utilizzare questo 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:/$

Passaggio 3. Se non sono presenti connessioni a Splunk, verificare la configurazione nel centro operativo PDF.

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#

Passaggio 4. Se la connessione non viene stabilita, ricreare il consolidated-logging-0 pod.

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

Passaggio 5. Verificare il pod dopo l'consolidated-logging-0eliminazione.

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

Passaggio 6. Connettersi al consolidated-logging pod e completare la procedura allanetstat porta 8088 e verificare la connessione Splunk stabilita.

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).