Troubleshoot Splunk Connectivity Issue in PCF

Contents

Introduction

This document describes the procedure to troubleshoot the Splunk issue seen in the Cloud Native Deployment Platform (CNDP) PCF.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Policy Control Function (PCF)
- 5G CNDP
- Dockers and Kubernetes

Components Used

The information in this document is based on these software and hardware versions:

- 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

In this setup, the CNDP hosts a PCF.

Splunk Server is the core component of the Splunk software platform. It is a scalable and powerful solution for collecting, indexing, searching, analyzing, and visualizing machine-generated data.

Splunk Server operates as a distributed system that can handle data from a variety of sources, including logs, events, metrics, and other machine data. It provides the infrastructure to collect and store data, perform real-time indexing and searching, and deliver insights through its web-based user interface.

Alert Rule Present in PCF Ops-Center for 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"
```

Note: You need to verify that this rule is present in the PCF Ops-Center for the effective alerting of Splunk connectivity issues.

Problem

You see alerts on the Common Execution Environment (CEE) Ops-Center for Splunk forward failure.

```
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

Step 1. Connect to the master node and verify the 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:~$
```

Step 2. Verify the Splunk connection by logging in to the consolidated pod with these commands.
In order to check if a connection is established on port 8088, you can use this command:

```
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 [P
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:/$
```

Step 3. If there are no connections to Splunk, verify the configuration on the PDF Ops-Center.

```
cloud-user@pcf01-master-1:~$ ssh -p 2024 admin@$(kubectl get svc -A -o wide |grep 2024 | grep ops-cente
[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#
```

Step 4. If the connection is not established, then recreate the consolidated-logging-0 pod.

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

Step 5. Verify the consolidated-logging-0 pod after deletion.

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

Step 6. Connect to the consolidated-logging pod and accomplish the netstat to port 8088 and verify the Splunk connection established.

```
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
```