PCF에서 Splunk 연결 문제 해결

목차

소개

이 문서에서는 CNDP(Cloud Native Deployment Platform) PCF에 있는 Splunk 문제를 해결하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.
· 정책 제어 기능(PCF)
· 5G CNDP
· 도커와 쿠베르네테

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.
· PCF REL_2023.01.2
· Kubernetes v1.24.6

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

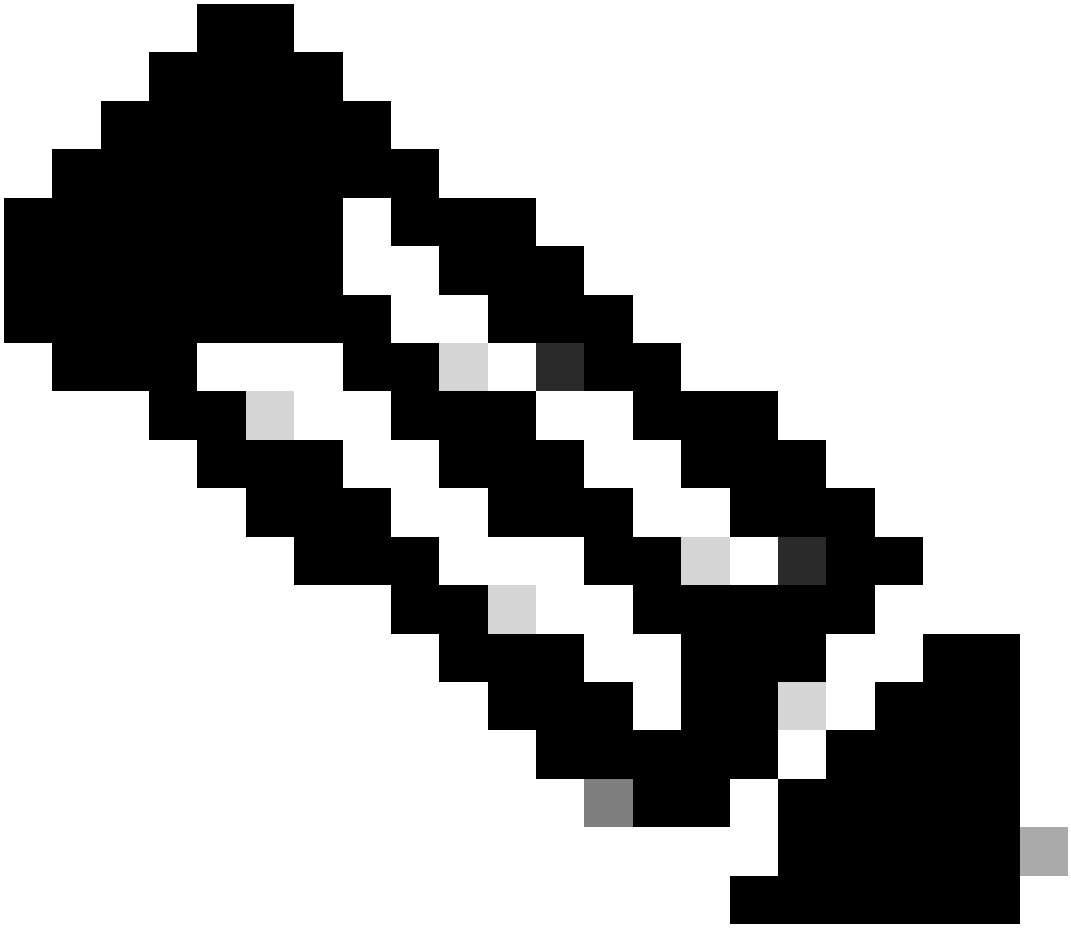
이 설정에서 CNDP는 PCF를 호스팅합니다.

Splunk Server는 Splunk 소프트웨어 플랫폼의 핵심 구성 요소입니다. 이 솔루션은 시스템에서 생성된 데이터를 수집, 인덱싱, 검색, 분석, 시각화하기 위한 확장 가능하고 강력한 솔루션입니다.

Splunk Server는 로그, 이벤트, 메트릭, 기타 시스템 데이터를 비롯한 다양한 소스의 데이터를 처리할 수 있는 분산 시스템으로 작동합니다. 데이터를 수집 및 저장하고, 실시간 인덱싱 및 검색을 수행하며, 웹 기반 사용자 인터페이스를 통해 통찰력을 제공할 수 있는 인프라를 제공합니다.

Splunk Connection Down의 PCF 운영 센터에 경고 규칙 존재

```
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"
```



참고: Splunk 연결 문제를 효과적으로 경고하려면 PCF 운영 센터에 이 규칙이 있는지 확인

해야 합니다.

문제

CEE(Common Execution Environment) Ops-Center에서 Splunk 전달 실패에 대한 경고가 표시됩니다.

```
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
```

문제 해결

1단계. 마스터 노드에 연결하고 consolidated-logging-0 포드 상태를 확인합니다.

```
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:~$
```

2단계. 이 명령을 사용하여 통합 Pod에 로그인하여 Splunk 연결을 확인합니다.

포트 8088에서 연결이 설정되었는지 확인하려면 다음 명령을 사용할 수 있습니다.

```
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:/$
```

3단계. Splunk에 대한 연결이 없는 경우 PDF Ops-Center의 컨피그레이션을 확인합니다.

```
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#
```

4단계. 연결이 설정되지 않은 경우 Pod를 다시 consolidated-logging-0 생성합니다.

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

5단계. 삭제 후 Pod를consolidated-logging-0 확인합니다.

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

6단계. Pod에 consolidated-logging 연결하여 포트 8088에netstat 연결하고 Splunk 연결이 설정되었는지 확인합니다.

```
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
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.