PCFでのSplunk接続の問題のトラブルシューティング

内容

はじめに

このドキュメントでは、クラウドネイティブ導入プラットフォーム(CNDP)のPCFで発生するSplunkの問題をトラブルシューティングする手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。
- ポリシー制御機能(PCF)
- 5G CNDP
- ドッキングとKubernetes

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。
- PCF REL_2023.01.2
- Kubernetes v1.24.6

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

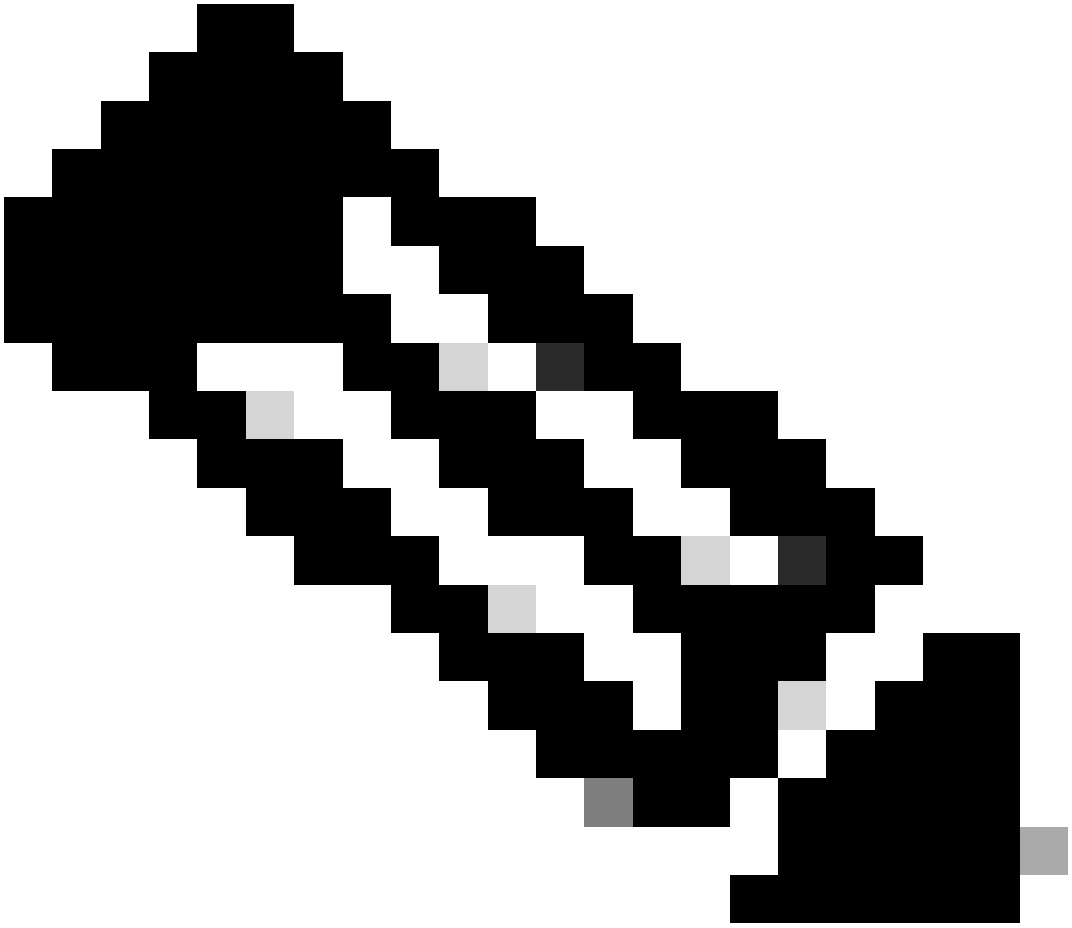
この設定では、CNDPはPCFをホストします。

Splunkサーバは、Splunkソフトウェアプラットフォームのコアコンポーネントです。これは、マシンで生成されたデータの収集、インデックス作成、検索、分析、視覚化を行うスケーラブルで強力なソリューションです。

Splunk Serverは、ログ、イベント、メトリック、その他のマシンデータなど、さまざまなソースからのデータを処理できる分散システムとして動作します。データの収集と保存、リアルタイムのインデックス作成と検索の実行、Webベースのユーザインターフェイスを介した洞察の提供を行うインフラストラクチャを提供します。

PCF Ops-Center for Splunk接続ダウンに含まれるアラートルール

```
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"
```



注:Splunk接続の問題に関する効果的なアラートを生成するには、このルールがPCFオペレーションセンターにあることを確認する必要があります。

問題

Common Execution Environment(CEE)Ops-Center for Splunk転送障害のアラートが表示されます。

```
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
```

トラブルシュート

ステップ 1：マスターノードに接続し、consolidated-logging-0 ポッドステータスを確認します。

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:~$

ステップ 2：次のコマンドを使用して統合ポッドにログインし、Splunk接続を確認します。
ポート8088で接続が確立されているかどうかを確認するには、次のコマンドを使用できます。

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:/$

ステップ 3：Splunkへの接続がない場合は、PDF Ops-Centerで設定を確認します。

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#

ステップ 4：接続が確立されない場合は、consolidated-logging-0 ポッドを再作成します。

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

ステップ 5：削除後にconsolidated-logging-0 podを確認します。

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

手順 6：consolidated-loggingポッドに接続してポート8088へのnetstatを実行し、Splunk接続が確立されたことを確認します。

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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。