Identificar e Solucionar Problemas de Conectividade Splunk no PCF

Contents

Introdução

Este documento descreve o procedimento para solucionar o problema de Splunk visto no PCF do Cloud Native Deployment Platform (CNDP).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:
· Policy Control Function (PCF, Função de Controle de Políticas)
· CNDP 5G
· Dockers e Kubernetes

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:
PCF REL_2023.01.2
Kubernetes v1.24.6

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

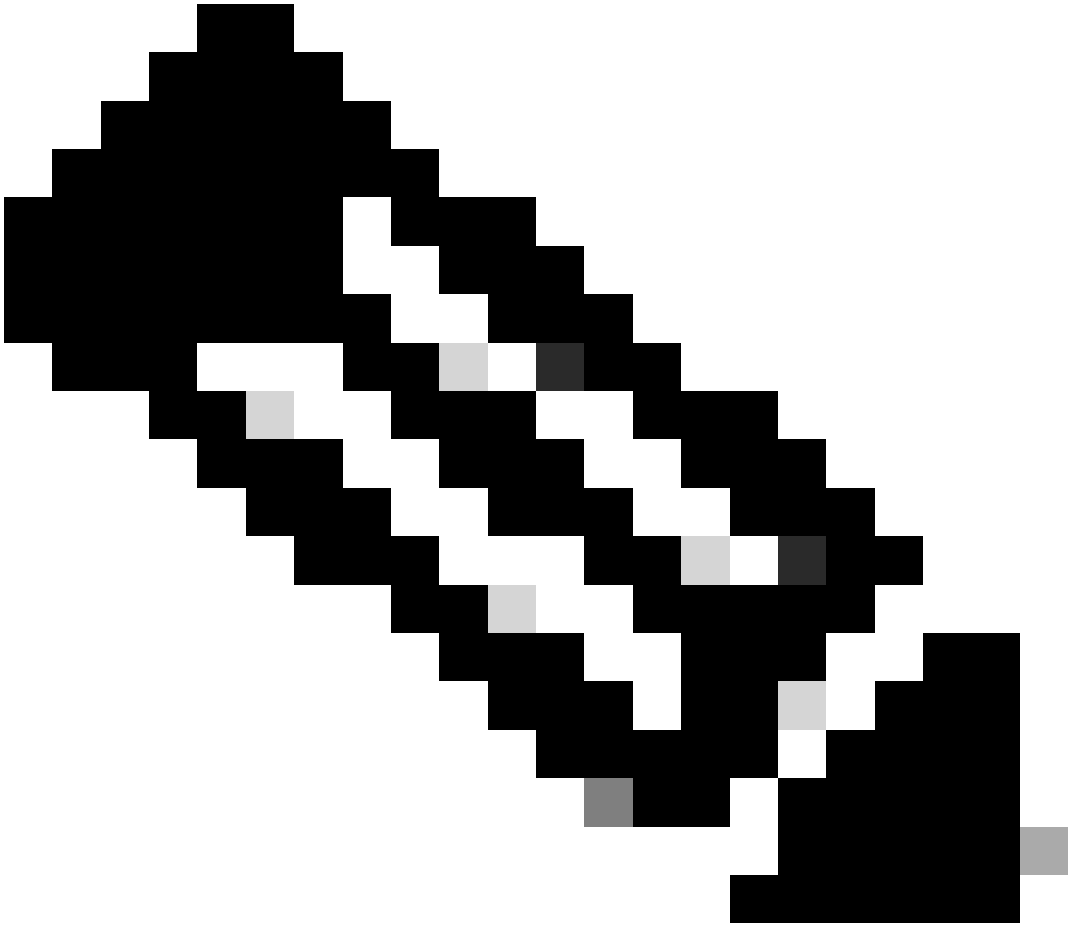
Nesta configuração, o CNDP hospeda um PCF.

O Splunk Server é o componente principal da plataforma do software Splunk. É uma solução escalável e poderosa para coletar, indexar, pesquisar, analisar e visualizar dados gerados por máquinas.

O Splunk Server opera como um sistema distribuído que pode lidar com dados de várias fontes, incluindo logs, eventos, métricas e outros dados da máquina. Ele fornece a infraestrutura para coletar e armazenar dados, executar indexação e pesquisa em tempo real e fornecer insights por meio de sua interface de usuário baseada na Web.

Regra de Alerta Presente no Centro de Operações do PCF para Conexão de Splunk Inativa

```
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"
```



Observação: você precisa verificar se essa regra está presente no PCF Ops-Center para o alerta eficaz de problemas de conectividade de Splunk.

Problema

Você vê alertas sobre a falha do encaminhamento de Splunk no Common Execution Environment (CEE) Ops-Center.

```
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
```

Troubleshooting

Etapa 1. Conecte-se ao nó mestre e verifique o status do 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:~$

Etapa 2. Verifique a conexão Splunk fazendo login no pod consolidado com esses comandos.

Para verificar se uma conexão foi estabelecida na porta 8088, você pode usar 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:/$

Etapa 3. Se não houver conexões ao Splunk, verifique a configuração no 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#

Etapa 4. Se a conexão não for estabelecida, recrie o consolidated-logging-0 pod.

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

Etapa 5. Verificar o podconsolidated-logging-0 após a exclusão.

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

Etapa 6. Conecte-se ao podconsolidated-logging e realize o testenetstat para a porta 8088 e verifique se a conexão Splunk foi estabelecida.

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.