排除CPS中的Consolidated-engine.log生成问题

目录

简介

本文档介绍如何对思科策略套件(CPS)中的consolidated-engine.log生成问题进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- Linux
- CPS

思科建议您必须拥有对CPS CLI的根访问权限。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CPS 20.2
- UCS-B

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

在CPS中，策略引擎日志从所有Quantum Network Suite(QNS)虚拟机(VM)收集，并隔离在pcrfclient VM。

Logback框架用于收集与策略引擎相关的日志，并保存/隔离在活动的pcrfclient VM。

Logback是Java应用程序的日志记录框架，创建为常用log4j项目的后继项。

以下是/etc/broadhop/logback.xml文件中用于生成和收集引擎日志的相关配置。

1.策略引擎日志被发送到SOCKET附加器。

```
<logger name="policy.engine" level="info" additivity="false">
<appender-ref ref="SOCKET" />
</logger>
```

2. SOCKET附加器引用SOCKET-BASE附加器。

```
<appender name="SOCKET" class="com.broadhop.logging.appenders.AsynchAppender">
<appender-ref ref="SOCKET-BASE"/>
```

3. SOCKET-BASE具有将日志发送到远程主机的配置：端口。

```
<appender name="SOCKET-BASE" class="com.broadhop.logging.net.SocketAppender">
<RemoteHost>${logging.controlcenter.host:-lbvip02}</RemoteHost>
<Port>${logging.controlcenter.port:-5644}</Port>
<ReconnectionDelay>10000</ReconnectionDelay>
<IncludeCallerData>false</IncludeCallerData>
</appender>
```

问题

如果CPS环境设置中存在任何类型的网络抖动或TCP相关错误，则pcrfclient VM会停止从单个VM接收套接字附加器类型日志。

在SOCKET-BASE下配置的端口5644显示TIMEWAIT。

```
[root@dc1-pcrfclient01 ~]# netstat -plan|grep 5644
tcp6 0 0 192.168.10.135:5644 192.168.10.137:47876 TIME_WAIT -
tcp6 0 0 192.168.10.135:5644 192.168.10.137:57042 TIME_WAIT -
tcp6 0 0 192.168.10.135:5644 192.168.10.137:60888 TIME_WAIT -
tcp6 0 0 192.168.10.135:5644 192.168.10.137:60570 TIME_WAIT -
tcp6 0 0 192.168.10.135:5644 192.168.10.137:32902 TIME_WAIT -
tcp6 0 0 192.168.10.135:5644 192.168.10.137:57052 TIME_WAIT -
tcp6 0 0 192.168.10.135:5644 192.168.10.137:47640 TIME_WAIT -
tcp6 0 0 192.168.10.135:5644 192.168.10.137:36484 TIME_WAIT -
tcp6 0 0 192.168.10.135:5644 192.168.10.137:57040 TIME_WAIT -
tcp6 0 0 192.168.10.135:5644 192.168.10.137:55788 TIME_WAIT -
[root@dc1-pcrfclient01 ~]#
```

如果您在几分钟后检查相同的状态，则没有与端口5644相关的条目。

```
[root@dc1-pcrfclient01 ~]# netstat -plan|grep 5644
[root@dc1-pcrfclient01 ~]#
```

解决方案

恢复SOCKET连接的步骤是在活动pcrfclient中重新启动qns-1进程。

```
[root@dc1-pcrfclient01 ~]# monit stop qns-1
```

```
[root@dc1-pcrfclient01 ~]# monit status qns-1
Monit 5.26.0 uptime: 4d 22h 43m
Process 'qns-1'
status Not monitored
monitoring status Not monitored
monitoring mode active
on reboot start
data collected Tue, 04 Jan 2022 11:52:38



[root@dc1-pcrfclient01 ~]# monit start qns-1


[root@dc1-pcrfclient01 ~]# monit status qns-1
Monit 5.26.0 uptime: 4d 22h 42m
Process 'qns-1'
status OK
monitoring status Monitored
monitoring mode active
on reboot start
pid 25368
parent pid 1
uid 0
effective uid 0
gid 0
uptime 0m
threads 31
children 0
cpu 0.0%
cpu total 0.0%
memory 1.2% [197.4 MB]
memory total 1.2% [197.4 MB]
security attribute -
disk read 0 B/s [112 kB total]
disk write 0 B/s [60.2 MB total]
port response time -
data collected Tue, 04 Jan 2022 11:51:04
```