CPSでのConsolidated-engine.log生成の問題のトラブルシューティング

内容

概要

このドキュメントでは、Cisco Policy Suite(CPS)のconsolidated-engine.log生成の問題をトラブルシューティングする方法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。

- Linux
- CPS

シスコでは、CPS CLIへのルートアクセスに対する権限を持っていることが推奨しています。

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。

- CPS 20.2
- UCS-B

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、初期（デフォルト）設定の状態から起動しています。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

CPSでは、ポリシーエンジンログはすべてのQuantum Network Suite(QNS)仮想マシン(VM)から収集され、pcrfclient VMで分離されます。

ログバックフレームワークは、ポリシーエンジン関連のログを収集するために使用され、アクティブなpcrfclient VMで保存/分離されます。

Logbackは、一般的なlog4jプロジェクトの後継として作成されたJavaアプリケーションのロギングフレームワークです。

エンジンログの生成と収集に関して**/etc/broadhop/logback.xml**ファイルの関連する設定を次に示します。

1.ポリシーエンジンのログがSOCKET Appenderに送信されます。

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

2. SOCKET AppenderはSOCKET-BASE Appenderに参照されます。

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

3. SOCKET-BASEの設定では、ログがリモートホストに送信されます。Port.

```
<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>
```

問題

CPS環境セットアップ内にネットワークフラップまたはTCP関連のエラーが発生すると、pcrfclient VMは停止し、個々のVMからSOCKETアペンダータイプのログを受信します。

SOCKET-BASEで設定されたポート5644はTIMEWAITを示します。

```
[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 ~]#
```

数分後に同じステータスを確認すると、ポート5644に関連するエントリはありません。

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

解決方法

SOCKET接続を復元する手順は、アクティブなpcrfclientのqns-1プロセスを再起動することです。

```
[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
```