

CPS에서 Consolidated-engine.log 생성 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[문제](#)

[솔루션](#)

소개

이 문서에서는 Cisco CPS(Policy Suite)에서 통합된 engine.log 생성 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 리눅스
- CPS

Cisco에서는 CPS CLI에 대한 루트 액세스에 대한 권한 액세스 권한이 있어야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CPS 20.2
- UCS-B

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

배경 정보

CPS에서 정책 엔진 로그는 모든 QNS(Quantum Network Suite) VM(Virtual Machine)에서 수집되고 pcrfclient VM에서 분리됩니다.

Logback 프레임워크는 정책 엔진 관련 로그를 수집하는 데 사용되며 활성 pcrfclient VM에서 저장/분리됩니다.

Logback은 널리 사용되는 log4j 프로젝트의 후속 작업으로 생성된 Java 응용 프로그램의 로깅 프레임워크입니다.

다음은 엔진 로그 생성 및 수집을 위한 `/etc/broadhop/logback.xml` 파일의 관련 컨피그레이션입니다

1. 정책 엔진 로그는 SOCKET Appender로 전송됩니다.

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

2. SOCKET Appender는 SOCKET-BASE Appender에서 참조됩니다.

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

3. SOCKET-BASE에는 원격 호스트로 로그를 전송하는 구성이 있습니다. 포트.

```
<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>
```

문제

CPS 환경 설정 내에 네트워크 플랩 또는 TCP 관련 오류가 있으면 pcrfclient VM이 중지되어 개별 VM에서 SOCKET Appender 유형 로그를 수신합니다.

SOCKET-BASE에서 구성된 포트 5644는 TIMEWAIT를 표시합니다.

```
[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 ~]#
```

몇 분 후에 동일한 상태를 확인하면 포트 5644와 관련된 항목이 없습니다.

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

솔루션

SOCKET 연결을 복원하는 절차는 활성 pcrfclient에서 qns-1 프로세스를 다시 시작하는 것입니다.

```
[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
```