

# Solucionar problemas de alerta de alta carga e soluções recomendadas em CPS

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problema](#)

[Solucionar problemas de alta carga](#)

[Solução](#)

## Introduction

Este documento descreve a investigação de alerta de alta carga e as soluções alternativas recomendadas no Cisco Policy Suite (CPS).

## Prerequisites

## Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Linux
- CPS

A Cisco também recomenda que você tenha acesso de raiz privilegiado à CLI do CPS.

## Componentes Utilizados

As informações neste documento são baseadas no CPS 19.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

A média de carga é a carga média do sistema em um servidor Linux por um período definido. Em outras palavras, é a demanda da CPU de um servidor que inclui a soma dos segmentos ativos e ociosos.

A medição da média de carga é essencial para entender o desempenho dos servidores; se

sobrecarregado, você deve eliminar ou otimizar os processos que consomem grandes quantidades de recursos ou fornecer mais recursos para equilibrar a carga de trabalho.

Normalmente, o **topo** ou o comando **uptime** fornece a média de carga do servidor com saída que se parece com:

```
[root@cps-194-aio-mob ~]# uptime
11:41:08 up 6 days, 5:20, 2 users, load average: 0.71, 0.35, 0.24
[root@cps-194-aio-mob ~]#
```

```
[root@cps-194-aio-mob ~]# top
top - 12:17:26 up 6 days, 5:56, 2 users, load average: 0.09, 0.12, 0.13
Tasks: 185 total, 1 running, 183 sleeping, 0 stopped, 1 zombie
%Cpu(s): 0.8 us, 0.8 sy, 0.0 ni, 98.4 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 12137348 total, 4128956 free, 5219860 used, 2788532 buff/cache
KiB Swap: 4194300 total, 4194300 free, 0 used. 6586848 avail Mem
```

```
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
7070 root 5 -15 8263680 1.3g 21728 S 12.5 11.6 561:38.74 java
1 root 20 0 191384 4320 2620 S 0.0 0.0 3:11.17 systemd
```

Esses números são as médias da carga do sistema durante um período de um, cinco e 15 minutos.

Antes de prosseguir, vamos entender essas duas frases importantes em todos os sistemas Unix:

Carga do sistema/Carga da CPU - é uma medida da CPU sobre ou subutilização em um sistema Linux; o número de processos executados pela CPU ou no estado ocioso.

Carga média - é a carga média do sistema calculada durante um determinado período de 1, 5 e 15 minutos.

## Problema

Sempre que a média de carga de uma VM CPS exceder o limite definido, o HighLoadAlert será gerado. O valor limite do alerta HighLoad é definido como  $1,5 * \text{No Of CPUs}$  na VM. Esta configuração é fornecida em `/etc/snmp/snmpd.conf`:

```
load 12 12 12
```

```
# 1, 5 and 15 Minute Load Averages (UCD-SNMP-MIB la)
proxy -v 2c -c broadhop localhost .1.3.6.1.4.1.26878.200.3.2.70.1.4 .1.3.6.1.4.1.2021.10.1.5.1
proxy -v 2c -c broadhop localhost .1.3.6.1.4.1.26878.200.3.2.70.1.5 .1.3.6.1.4.1.2021.10.1.5.2
proxy -v 2c -c broadhop localhost .1.3.6.1.4.1.26878.200.3.2.70.1.6 .1.3.6.1.4.1.2021.10.1.5.3
proxy -v 2c -c broadhop localhost .1.3.6.1.4.1.26878.200.3.2.70.1.4.0 .1.3.6.1.4.1.2021.10.1.5.1
proxy -v 2c -c broadhop localhost .1.3.6.1.4.1.26878.200.3.2.70.1.5.0 .1.3.6.1.4.1.2021.10.1.5.2
proxy -v 2c -c broadhop localhost .1.3.6.1.4.1.26878.200.3.2.70.1.6.0 .1.3.6.1.4.1.2021.10.1.5.3
```

Exemplo de alerta de alta carga:

```
2021-10-31T14:25:36.572711+05:30 XXXXX-lb01 snmptrapd[5717]: 2021-10-31 14:25:36 pcrfclient01
[UDP: [XX.XX.XX.XX]:46046->[XX.XX.XX.XX]:162]:#012DISMAN-EVENT-MIB::sysUpTimeInstance =
99307800#011SNMPv2-MIB::snmpTrapOID.0 = OID: DISMAN-EVENT-MIB::mteTriggerFired#011DISMAN-EVENT-
MIB::mteHotTrigger.0 = STRING: HighLoadAlert#011DISMAN-EVENT-MIB::mteHotTargetName.0 = STRING:
#011DISMAN-EVENT-MIB::mteHotContextName.0 = STRING: #011DISMAN-EVENT-MIB::mteHotOID.0 = OID:
UCD-SNMP-MIB::laErrorFlag.1#011DISMAN-EVENT-MIB::mteHotValue.0 = INTEGER: 1#011UCD-SNMP-
```

MIB::laNames.1 = STRING: Load-1#011UCD-SNMP-MIB::laErrorMessage.1 = STRING: 1 min Load Average too high (= 64.84)

## Solucionar problemas de alta carga

Antes de investigar mais, verifique se a VM afetada tem a contagem de CPU conforme padrão. Isso pode ser feito com o respectivo guia de instalação do CPS, no qual ele menciona a contagem de CPU necessária para cada VM.

O único comando Linux que combinado fornece média de carga e utilização da CPU por processos é o **principal** comando. Para identificar o processo que causa o HighLoad, o comando **top** deve ser executado na VM afetada em intervalos regulares por um determinado período que cubra a instância do HighLoad. Este comando fornece saída **superior** para cada 3 segundos, para um número de 15000 vezes (você pode alterar o número de acordo com o seu cenário):

```
#top -b -n15000 >> top.txt &
```

```
[root@cps-194-aio-mob ~]# top
top - 09:32:11 up 7 days, 3:11, 3 users, load average: 0.13, 0.16, 0.15
Tasks: 184 total, 1 running, 182 sleeping, 0 stopped, 1 zombie
%Cpu(s): 0.8 us, 0.8 sy, 0.0 ni, 98.4 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 12137348 total, 3911352 free, 5262096 used, 2963900 buff/cache
KiB Swap: 4194300 total, 4194300 free, 0 used. 6520076 avail Mem
```

```
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
7014 redis 20 0 147356 2372 1184 S 6.7 0.0 48:15.15 redis-server
7070 root 5 -15 8263688 1.4g 21744 S 6.7 11.8 645:12.88 java
1 root 20 0 191384 4320 2620 S 0.0 0.0 3:38.65 systemd
2 root 20 0 0 0 0 S 0.0 0.0 0:00.12 kthreadd
3 root 20 0 0 0 0 S 0.0 0.0 0:04.51 ksoftirqd/0
5 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/0:0H
7 root rt 0 0 0 0 S 0.0 0.0 0:01.76 migration/0
8 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcu_bh
9 root 20 0 0 0 0 S 0.0 0.0 11:53.47 rcu_sched
```

Relacione e compare estreitamente a instância do HighLoadAlert com a saída do comando **top**, identifique o processo que é a CPU altamente utilizada no momento do alerta.

Em seguida, para coletar mais informações sobre esse processo, execute este comando:

```
Command Template:
#ps -ef | grep {PID}
```

```
Sample command:
[root@cps-194-aio-mob ~]# ps -ef | grep 7070
root 7070 1 6 Dec02 ? 12:17:06 /usr/bin/java -server -XX:+UnlockDiagnosticVMOptions -
XX:+UnsyncloadClass -Xms2048m -Xmx2048m -javaagent:/opt/broadhop/qns-1/bin/jmxagent.jar -
Dqns.config.dir=/etc/broadhop/pcrf -Dqns.instancenum=1 -
Dlogback.configurationFile=/etc/broadhop/logback.xml -Djmx.port=9045 -
Dorg.osgi.service.http.port=8080 -Dsnmp.port=1161 -Dcom.broadhop.run.systemId=lab -
Dcom.broadhop.run.clusterId=cluster-1 -Dcom.broadhop.run.instanceId=cps-194-aio-mob-1 -
Dcom.broadhop.config.url=http://pcrfclient01/repos/run/ -
Dcom.broadhop.repository.credentials.isEncrypted=true -Dcom.broadhop.repository.credentials=qns-
svn/3300901EA069E81CE29D4F77DE3C85FA@pcrfclient01 -
Dcom.broadhop.referencedata.local.location=/var/broadhop/checkout -DdisableJms -
DrefreshOnChange=true -DenableRuntimePolling=true -DdefaultNasIp=127.0.0.1 -Xdebug -
Xrunjdpw:transport=dt_socket,server=y,suspend=n,address=1044 -Dua.version.2.0.compatible=true -
Denable.compression=true -Denable.dictionary.compression=true -DuseZlibCompression=true -
```

```
DenableBestCompression=true -DenableQueueSystem=false -
Dredis.keystore.connection.string=lb01:lb01:6379:6379 -
DbrokerUrl=failover:(tcp://lb01:61616,tcp://lb02:61616)?randomize=false -
DjmsFlowControlHost=lb02 -DjmsFlowControlPort=9045 -Dosgi.framework.activeThreadType=normal -jar
/opt/broadhop/qns-1/plugins/org.eclipse.equinox.launcher_1.1.0.v20100507.jar -console cps-194-
aio-mob:9091 -clean -os linux -ws gtk -arch x86_64
root 7846 7587 0 11:00 pts/0 00:00:00 grep --color=auto 7070
[root@cps-194-aio-mob ~]#
```

## Solução

Uma vez identificado o processo que causa o HighLoadAlert, essas soluções podem ser consideradas:

Etapa 1. Reinicie o processo.

```
#monit stop {Process Name}
wait for 10 secs
#monit start {Process Name}
```

Etapa 2. Se o processo incluir logback, verifique qualquer logger com nível de log de depuração e altere o nível de log dos loggers de debug para warn/error.

Etapa 3. Se a Etapa 1. e Etapa 2. não funcionar, ajuste o respectivo arquivo de configuração, com a ajuda da equipe de desenvolvimento, se necessário.