

Habilitar registro HA-Proxy

Contents

[Introduction](#)

[Informações de Apoio](#)

[Procedimento para ativar registros HA-Proxy](#)

[Discussões relacionadas da comunidade de suporte da Cisco](#)

Introduction

Este artigo descreve o procedimento para ativar o registro de alto proxy disponível (HA-Proxy) no Cisco Policy Suite (CPS). O HA-Proxy é usado para balanceamento de carga de alta disponibilidade. Por padrão, por motivos de desempenho, o HA-Proxy não registra as mensagens.

Note: Você deve habilitar os registros HA-Proxy somente quando vir um problema relacionado ao HA-Proxy.

Informações de Apoio

O registro HA-Proxy precisa ser ativado somente quando um possível problema relacionado ao proxy HA, que não pode ser identificado por nenhum outro log de depuração no sistema CPS, é visto.

Procedimento para ativar registros HA-Proxy

Todas as etapas precisam ser executadas na máquina virtual (VM) do balanceador de carga ativa e devem ser repetidas novamente no balanceador de carga passivo, de modo que sempre que ocorre failover do balanceador de carga, o registro de HA-Proxy é realizado.

1. Navegue até o arquivo `haproxy.cfg` (`/etc/haproxy/haproxy.cfg`) e verifique se você tem a mesma entrada mostrada nesta imagem. Por padrão, na maioria dos casos, o nível de log é definido como `debug`. Altere-o para `erro`, caso contrário os registros desnecessários serão gravados.

```
stats auth      admin:broadhop # force HTTP Auth to view stats
stats refresh   60s          # refresh rate of stats page
log             127.0.0.1      local1 err
```

2. Selecione o proxy para o qual deseja executar o registro. Há muitas configurações de proxy no arquivo de configuração HA-Proxy, como `svn_proxy`, `pb_proxy`, `Portal_admin_proxy`. A ativação do registro HA-Proxy para `svn_proxy` é mostrada nesta imagem.

```
listen svn_proxy lbvip02:80
    mode http
    log global
    balance roundrobin
    option httpchk
    option httpclose
    option abortonclose
    server pcrfclient01 pcrfclient01:80 check inter 30s
    server pcrfclient02 pcrfclient02:80 check inter 30s backup
```

3. Edite o arquivo `/etc/syslog.conf` e adicione a entrada como mostrado nesta imagem. Certifique-se de que `local1` tenha o mesmo nome que na Etapa 1.

```
# SNMP Trap Logs
local2.* /var/log/snmp/trap
# HA Proxy Logging
local1.* /var/log/haproxy.log
~
```

4. Edite o arquivo `/etc/sysconfig/syslog` e altere-o conforme mostrado nesta imagem. Você apenas adiciona `r`. Isso garante o login em máquinas remotas.

```
# See syslogd(8) for more details
SYSLOGD_OPTIONS="-rm 0"
# Options to klogd
```

5. Edite o arquivo `/etc/logrotate.d/syslog` e certifique-se de adicionar uma entrada para `/var/log/haproxy.log`, como mostrado nesta imagem.

```
/var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boot.log /var/log/cron /var/log/snmp/trap /var/log/haproxy.log |
sharedscripts
postrotate
    /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null || true
    /bin/kill -HUP `cat /var/run/rsyslogd.pid 2> /dev/null` 2> /dev/null || true
endscript
```

7. Reinicie o processo `syslogd` e `HA-Proxy` usando os comandos `service syslog restart` e `service haproxy restart`.