

Permita o registro do HA-proxy

Índice

[Introdução](#)

[Informações de Apoio](#)

[Procedimento para permitir logs do HA-proxy](#)

[Cisco relacionado apoia discussões da comunidade](#)

Introdução

Este artigo descreve o procedimento para permitir a série de abertura alta da política de Cisco do Disponível-proxy (HA-proxy) (CP). O HA-proxy é usado para o Balanceamento de carga disponível alto. À revelia, para razões de desempenho, o HA-proxy não registra as mensagens.

Note: Você deve permitir os logs do HA-proxy somente quando você vê um problema relativo ao HA-proxy.

Informações de Apoio

O HA-proxy que registra necessidades de ser permitido somente quando um problema potencial se relacionou ao HA-proxy, que não podem ser identificados por qualquer outro debugam entram o sistema CP, é visto.

Procedimento para permitir logs do HA-proxy

Todas as etapas precisam de ser executadas na máquina virtual do equilibrador ativo da carga (VM) e devem ser repetidas outra vez no equilibrador passivo da carga, de modo que sempre que o Failover do equilibrador da carga acontece, o registro do HA-proxy seja tomado de.

1. Navegue ao **arquivo haproxy.cfg** (/etc/haproxy/haproxy.cfg) e assegure-se de que você tenha a mesma entrada segundo as indicações desta imagem. À revelia, o nível do log é ajustado na maioria dos casos para debugar. Mude-o **por favor** para errar, **se não os** logs desnecessários são 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 que você quer executar o registro, lá são muitas configurações de proxy no arquivo de configuração do HA-proxy tal como o svn_proxy, pb_proxy, Portal_admin_proxy. Permitir o HA-proxy que registra para o 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 de `/etc/syslog.conf` e adicionar a entrada segundo as indicações desta imagem. Assegure-se de que o `local1` tenha mesmo nome que em etapa 1.

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

4. Edite o arquivo de `/etc/sysconfig/syslog` e mude-o segundo as indicações desta imagem. Você apenas adiciona o `R`. Isto assegura máquinas remotas de abertura.

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

5. Edite o arquivo de `/etc/logrotate.d/syslog` e assegure-se de que você adicione uma entrada para `/var/log/haproxy.log` segundo as indicações desta 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 `syslogd` e o processo do HA-proxy usando o reinício do Syslog do serviço e preste serviços de manutenção a comandos do reinício do haproxy.