

Se connecter de Ha-proxy d'enable

Contenu

[Introduction](#)

[Informations générales](#)

[Procédure pour activer des logs de Ha-proxy](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

Introduction

Cet article décrit la procédure pour activer la suite ouvrante une session élevée de stratégie de Cisco de Disponible-proxy (Ha-proxy) (CPS). Le Ha-proxy est utilisé pour l'Équilibrage de charge disponible élevé. Par défaut, pour des raisons de représentation, le Ha-proxy ne se connecte pas les messages.

Note: Vous devez activer les logs de Ha-proxy seulement quand vous voyez un problème lié au Ha-proxy.

[Informations générales](#)

Le Ha-proxy se connectant les besoins d'être activé seulement quand un problème potentiel a associé au Ha-proxy, qui ne peut pas être identifié par tout autre met au point des logins le système CPS, est vu.

Procédure pour activer des logs de Ha-proxy

Toutes les étapes doivent être exécutées sur le virtual machine actif d'équilibreur de charge (VM) et doivent être répétées de nouveau dans l'équilibreur de charge passif, de sorte que toutes les fois que le Basculement d'équilibreur de charge se produit, se connecter de Ha-proxy soit géré.

1. Naviguez vers le **fichier haproxy.cfg** (/etc/haproxy/haproxy.cfg) et assurez-vous que vous avez la même entrée suivant les indications de cette image. Par défaut, dans la plupart des cas le niveau de log est placé pour mettre au point. **Veillez le changer pour errer, autrement des logs inutiles sont enregistrés.**

```
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. Sélectionnez le proxy pour lequel vous voulez exécuter se connecter, là sont beaucoup de configurations de proxy dans le fichier de configuration de Ha-proxy tel que le svn_proxy, pb_proxy, Portal_admin_proxy. L'activation du Ha-proxy se connectant pour le svn_proxy est affichée dans cette image.

```
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. Éditez le fichier de `/etc/syslog.conf` et ajoutez l'entrée suivant les indications de cette image. Assurez-vous que `local1` a le même nom que dans l'étape 1.

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

4. Éditez le fichier de `/etc/sysconfig/syslog` et changez suivant les indications de cette image. Vous ajoutez juste le **R**. Ceci assure les ordinateurs distants logging on.

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

5. Éditez le fichier de `/etc/logrotate.d/syslog` et l'assurez que vous ajoutez une entrée pour `/var/log/haproxy.log` suivant les indications de cette image.

```
/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. Redémarrez le `syslogd` et le processus de `Ha-proxy` utilisant la **reprise de Syslog de service** et **entretenez les commandes de reprise de haproxy**.