Activer la journalisation du proxy HA

Contenu

Introduction

Cet article décrit la procédure d'activation de la journalisation High Available-Proxy (HA-Proxy) dans Cisco Policy Suite (CPS). HA-Proxy est utilisé pour l'équilibrage de charge disponible élevé. Par défaut, pour des raisons de performances, HA-Proxy ne consigne pas les messages.

> **Note**: Vous ne devez activer les journaux du proxy HA que si un problème lié au proxy HA apparaît.

Informations générales

La journalisation HA-Proxy doit être activée uniquement lorsqu'un problème potentiel lié au proxy HA, qui ne peut pas être identifié par d'autres journaux de débogage dans le système CPS, est détecté.

Procédure d'activation des journaux de proxy HA

Toutes les étapes doivent être effectuées sur la machine virtuelle (VM) de l'équilibreur de charge actif et doivent être répétées dans l'équilibreur de charge passif, de sorte que chaque fois que le basculement de l'équilibreur de charge se produit, la journalisation HA-Proxy est prise en charge.

1. Accédez au fichier **haproxy.cfg** (/etc/haproxy/haproxy.cfg) et vérifiez que vous avez la même entrée que celle illustrée dans cette image. Par défaut, dans la plupart des cas, le niveau du journal est défini sur **debug.** Modifiez-le en **erreur,** sinon des journaux 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 effectuer la journalisation, il existe de nombreuses configurations de proxy dans le fichier de configuration HA-Proxy, telles que svn_proxy, pb_proxy, Portal_admin_proxy. L'activation de la journalisation HA-Proxy pour 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. Modifiez le fichier **/etc/syslog.conf** et ajoutez l'entrée comme indiqué dans cette image. Assurez-vous que **local1** porte le même nom que l'étape 1.

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

4. Modifiez le fichier **/etc/sysconfig/syslog** et modifiez-le comme indiqué dans cette image. Vous ajoutez simplement **r**. Cela garantit la connexion aux machines distantes.

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

5. Modifiez le fichier **/etc/logroate.d/syslog** et assurez-vous d'ajouter une entrée pour **/var/log/haproxy.log** comme indiqué dans 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 processus syslogd et HA-Proxy à l'aide des commandes **service syslog restart** et **service haproxy restart**.