HA-Proxy-Protokollierung aktivieren

Inhalt

Einführung

In diesem Artikel wird das Verfahren zur Aktivierung der HA-Proxy-Protokollierung (High Available-Proxy) in der Cisco Policy Suite (CPS) beschrieben. HA-Proxy wird für den hochverfügbaren Lastenausgleich verwendet. In der Standardeinstellung werden die Meldungen aus Leistungsgründen nicht vom HA-Proxy protokolliert.

> **Hinweis**: Sie müssen die HA-Proxy-Protokolle nur aktivieren, wenn Sie ein Problem im Zusammenhang mit HA-Proxy sehen.

Hintergrundinformationen

HA-Proxy-Protokollierung muss nur aktiviert werden, wenn ein potenzielles Problem im Zusammenhang mit HA-Proxy, das nicht durch andere Debug-Protokolle im CPS-System identifiziert werden kann, erkannt wird.

Verfahren zum Aktivieren von HA-Proxy-Protokollen

Alle Schritte müssen auf dem aktiven Load Balancer Virtual Machine (VM) ausgeführt und im passiven Load Balancer wiederholt werden, sodass HA-Proxy-Protokollierung bei jedem Failover des Load Balancers gewährleistet ist.

1. Navigieren Sie zur Datei **haproxy.cfg** (/etc/haproxy/haproxy.cfg), und stellen Sie sicher, dass Sie den gleichen Eintrag wie in diesem Bild haben. Standardmäßig ist die Protokollebene in den meisten Fällen auf **debug** festgelegt. Ändern Sie sie auf **Fehler,** andernfalls werden unnötige Protokolle aufgezeichnet.

```
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. Wählen Sie den Proxy aus, für den Sie die Protokollierung durchführen möchten. Es gibt viele Proxykonfigurationen in der HA-Proxy-Konfigurationsdatei wie svn_proxy, pb_proxy, Portal_admin_proxy. Das Aktivieren der HA-Proxy-Protokollierung für svn_proxy wird in diesem Bild angezeigt.

```
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. Bearbeiten Sie die **/etc/syslog.conf**-Datei, und fügen Sie den Eintrag wie in diesem Bild gezeigt hinzu. Stellen Sie sicher, dass **local1** denselben Namen wie in Schritt 1 hat.

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

4. Bearbeiten Sie die Datei **/etc/sysconfig/syslog**, und ändern Sie sie, wie in diesem Bild gezeigt. Sie fügen einfach **r hinzu**. Dadurch wird die Anmeldung an Remote-Computern sichergestellt.

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

5. Bearbeiten Sie die Datei **/etc/logroate.d/syslog**, und stellen Sie sicher, dass Sie einen Eintrag für **/var/log/haproxy.log** hinzufügen, wie in diesem Bild gezeigt.

```
/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. Starten Sie den Syslog- und HA-Proxy-Prozess mithilfe der **Service Syslog Restart** und der Befehle **Service-Syslog-Neustart** neu.