Activar registro de proxy HA

Contenido

Introducción

En este artículo se describe el procedimiento para habilitar el inicio de sesión de Proxy de alta disponibilidad (HA-Proxy) en Cisco Policy Suite (CPS). HA-Proxy se utiliza para el balanceo de carga disponible alto. De forma predeterminada, por razones de rendimiento, HA-Proxy no registra los mensajes.

> **Nota:** Debe habilitar los registros HA-Proxy sólo cuando vea un problema relacionado con HA-Proxy.

Antecedentes

El registro de HA-Proxy debe habilitarse solamente cuando se observa un problema potencial relacionado con HA-proxy, que no puede ser identificado por ningún otro registro de depuración en el sistema CPS.

Procedimiento para Habilitar Registros de Proxy HA

Todos los pasos deben realizarse en la máquina virtual (VM) del equilibrador de carga activa y deben repetirse de nuevo en el equilibrador de carga pasivo, de modo que siempre que se produzca una conmutación por fallo del equilibrador de carga, se cuide el registro de HA-Proxy.

1. Navegue hasta el archivo **haproxy.cfg** (/etc/haproxy/haproxy.cfg) y asegúrese de tener la misma entrada que se muestra en esta imagen. De forma predeterminada, en la mayoría de los casos el nivel de registro se establece en **debug.** Por favor, cámbielo a **err,** si no se registran registros innecesarios.

```
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. Seleccione el proxy para el que desea realizar el registro, hay muchas configuraciones de proxy en el archivo de configuración HA-Proxy como svn_proxy, pb_proxy, Portal_admin_proxy. En esta imagen se muestra cómo habilitar el registro de HA-Proxy para svn_proxy.

```
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 el archivo **/etc/syslog.conf** y agregue la entrada como se muestra en esta imagen. Asegúrese de que **local1** tenga el mismo nombre que en el Paso 1.

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

4. Edite el archivo **/etc/sysconfig/syslog** y cambie como se muestra en esta imagen. Sólo agregas **r**. Esto garantiza el inicio de sesión en equipos remotos.

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

5. Edite el archivo **/etc/logroate.d/syslog** y asegúrese de agregar una entrada para **/var/log/haproxy.log** como se muestra en esta imagen.

```
/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 el proceso syslogd y HA-Proxy usando los comandos **service syslog restart** y **service haproxy restart** .