Setup HAProxy as Loadbalancer for DoubleClue

1. Introduction

This guide is for administrators who want to use HAProxy as a load balancer for a DoubleClue cluster. HAProxy is a free open source load balancer for TCP and HTTP/s based applications published under the GNU General Public License Version 2. It runs on Unix and Unix-like operating systems.

For more information, please visit http://www.haproxy.org/

The clients (browsers, the DoubleClue App, DoubleClue AuthConnectors or DoubleClue Plugins) will connect to HAProxy. HAProxy will then forward the connection to multiple DoubleClue nodes.

2. Requirements

- Linux 64Bit with minimum 4 Gigabyte memory
- Server Certificate with private key in 'pem' format

3. Installing HAProxy on an Ubuntu Machine

You need sudo rights to successfully install and configure HAProxy.

Download HAProxy from http://www.haproxy.org/#down. Execute the command *apt-get -install haproxy* in the prompt or shell.

After executing the command successfully, a folder called ***haproxy*** will be created in the */etc/*. Within this new folder, you will find the ***haproxy.cfg*** configuration file. In order to configure HAProxy, you need to make some changes to this file. You will find more information about the configuration of the haproxy.cfg in chapter 4.2 HAProxy.cfg.

4. Configuring HAProxy

4.1 Configure the SSL Connection

HAProxy will forward the TCP connections from the internet to multiple DoubleClue nodes. Thereby, HAProxy will terminte the client SSL connection and establish its own SSL/TLS connection to the DoubleClue nodes.

To establish this SSL/TLS connection, you need a Server Certificate from a CA whose common name is set to the host name of the HAProxy. If you are using tenants in DoubleClue, you would need a wild card certificate suche as “*.MyDoubleClue.com”.

The format of the certificate is a “pem” format which contains the certificate and the private key. Copy the certificat pem file to /etc/ssl/certs/MyDoubleClue.pem

4.2 HAProxy.cfg

In the sample below, we configured the load balancer to support two DoubleClue nodes.

DoubleClue requires sticky sessions, so we added a cookie statement in the backend configuration. The connection to the backend is also established using SSL/TLS, but we are not verifying the DoubleClue certificates. Optionally, if the DoubleClue Nodes and the HAProxy are on an isolated network, you may disable the SSL/TLS between HAProxy and DoubleClue nodes. This will increase performance.

See the code sample below.

```
global
       log /dev/log  local0
       log /dev/log  local1 notice
       chroot /var/lib/haproxy
       stats socket /run/haproxy/admin.sock mode 660 level admin
       stats timeout 30s
       user haproxy
       group haproxy
       daemon
       # Default SSL material locations
       ca-base /etc/ssl/certs
       crt-base /etc/ssl/private
       # Default ciphers to use on SSL-enabled listening sockets.
       # For more information, see ciphers(1SSL). This list is from:
       #  https://hynek.me/articles/hardening-your-web-servers-ssl-ciphers/
       ssl-default-bind-ciphers
ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:ECDH+3DES:DH+3DES:RSA+A
ESGCM:RSA+AES:RSA+3DES:!aNULL:!MD5:!DSS
       ssl-default-bind-options no-sslv3

defaults
       log    global
       mode   http
       option httplog
       option dontlognull
       retries 3
       option redispatch
       maxconn 2000
      timeout connect 5000
      timeout client  600000

### Attention
### This timer should always be higher than the DoubleClue 'Keep Alive Connection'
### configured in the 'Identity Management' preferences. Which is default 5 minutes.
     timeout server  600000

listen stats
    bind *:8080
    mode http
    stats enable
    stats hide-version
    stats uri /

frontend https_front
       bind *:443 ssl crt /etc/ssl/certs/MyDoublelClue.pem
       default_backend https_back


backend https_back
       cookie dcem insert
       balance roundrobin
       option forwardfor
### configure the health check every 20 seconds
       option httpchk GET /dcem/healthcheck
       default-server inter 10s fall 2
       http-request set-header X-Forwarded-For %[src]
       server dcem210 172.14.32.153:8443 cookie dcem210 check ssl verify none
       server dcem211 172.14.32.154:8443 cookie dcem211 check ssl verify none
```

Please Note:

The options ‘`option forwardfor’ and ‘http-request set-header X-Forwarded-For %[src]’ will transfer the client source IP address to the backend http-header ‘X-Frowarded-For’. This is required if you will use the Network Adaptive Policies in DoubleClue.`

4.3 View HAProxy Statistics

You can also enable the HAProxy statistics by configuring them in the HAProxy.cfg. Simply include the section “listen stats” from the sample. Please note the stats port should be disabled by your firewall. Optionally, you can add authentication for the statistics. For more information see www.haproxy.org.

You can now see the statistics at http://*loadbalancerHostname:8080*. If the statistics report side is displayed correctly, the installation is successfully completed.

Please remember that you will need to restart the HAProxy service after every change to the configuration. You can do so by using the command *Systemctl restart haproxy* or *service HAProxy restart.*