Konfiguration von Apache als Load Balancer

1. Einführung

Diese Anleitung ist für Administratoren, die Apache als Load Balancer für ein DoubleClue-Cluster verwenden wollen.

Getestet wurde mit Apache2-Server unter Ubuntu.

2. Installation des Apache2

Öffnen Sie die Eingabeaufforderung bzw. Shell und geben den Befehl "**sudo apt-get install apache2**" ein. Bestätigen Sie die Änderung mit "**J**" bzw. "**Y**".

3. Konfiguration des Load Balancers

Aktivieren Sie das SSL-Hauptmenü in der Eingabeaufforderung bzw. Shell mit dem Befehl "**sudo a2enmod ssl**".

Durch die Installation des Load Balancers wurde folgende Datei erstellt:
"**/etc/apache2/apache2.conf**".
Um die benötigten Module für den Load Balancer zu laden, ergänzen Sie die Konfigurationsdatei um folgende Zeilen. Hierzu benötigen Sie Administrator- bzw. Root-Rechte:

```
     LoadModules lbmethod_byrequests_Modules
/usr/lib/apache2/Modules/mod_lbmethod_byrequests.so
     LoadModules proxy_Modules /usr/lib/apache2/Modules/mod_proxy.so
     LoadModules proxy_wstunnel_Modules
/usr/lib/apache2/Modules/mod_proxy_wstunnel.so
     LoadModules proxy_balancer_Modules
/usr/lib/apache2/Modules/mod_proxy_balancer.so
     LoadModules slotmem_shm_Modules /usr/lib/apache2/Modules/mod_slotmem_shm.so
     LoadHauptmenüe proxy_http_Hauptmenüe
/usr/lib/apache2/Hauptmenües/mod_proxy_http.so
```

4. SSL-Zertifikat erstellen

Erstellen Sie ein SSL-Zertifikat durch Eingabe des folgenden Befehls in der Eingabeaufforderung bzw. Shell:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.pem
```

Vervollständigen Sie die benötigten Angaben.

5. Ports öffnen

Durch die Installation des Apache-Servers wurde folgende Datei erstellt: "**/etc/apache2/ports.conf**".

Um die Ports zu öffnen, ändern Sie den/die gewünschten Port/s in der Konfigurationsdatei.

Beispiel:

```
<IfModules ssl_Modules>
        Listen 8445
        Listen 8444
        Listen 8443
</IfModules>

<IfModules mod_gnutls.c>
        Listen 8445
        Listen 8444
        Listen 8443
</IfModules>
```

6. Konfiguration eines mit SSL/TLS gesicherten Load Balancers

Damit der Apache-Server die gesicherte SSL/TLS-Verbindung verwendet, müssen in der folgenden Datei Änderungen vorgenommen werden: "**/etc/apache2/sites-enabled/default-ssl.conf**".

Beispiel: Diese Konfiguration wurde bei der Entwicklung verwendet.

Ersetzen Sie den Inhalt der vorhandenen Datei durch die folgende Programmierung und passen Sie die fettgedruckten Daten an Ihre Erfordernisse an:

```
##VirtualHost für WebSocket
<VirtualHost *:8445>
       ServerAdmin xxxxxx.yyyyyy@hws-gruppe.de
       DocumentRoot /var/www/html
       ErrorLog ${APACHE_LOG_DIR}/error.log
       CustomLog ${APACHE_LOG_DIR}/access.log combined
       SSLEngine on
       SSLCertificateFile      /etc/ssl/certs/apache-selfsigned.pem
       SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key

             <Proxy balancer://wsCluster>
                   BalancerMember ws://IP-WS-1:8000
                   BalancerMember ws://IP-WS-2:8000
             </Proxy>
       ProxyPass /dcem/ws/appConnection balancer://wsCluster/dcem/ws/appConnection

       <FilesMatch "\.(cgi|shtml|phtml|php)$">
                               SSLOptions +StdEnvVars
       </FilesMatch>

       <Directory /usr/lib/cgi-bin>
                 SSLOptions +StdEnvVars
       </Directory>
</VirtualHost>
##VirtualHost für Portal
<VirtualHost *:8444>

        SSLEngine on
        ServerName domain.com
        SSLCertificateFile      /etc/ssl/certs/apache-selfsigned.pem
        SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key
        ProxyRequests Off
        <Proxy balancer://portalCluster>
               BalancerMember http://IP-Portal-1:8080 route=server1
               BalancerMember http://IP-Portal-2:8080 route=server2
               ProxySet lbmethod=byrequests
        </Proxy>
ProxyPass "/PortalDemo"  "balancer://portalCluster/PortalDemo"stickysession=JSESSIONID

</VirtualHost>
##VirtualHost für Management
<VirtualHost *:8443>
        SSLEngine on
        SSLProxyEngine on
        ServerName domain.com
        SSLCertificateFile      /etc/ssl/certs/apache-selfsigned.pem
       SSLCertificateKeyFile   /etc/ssl/private/apache-selfsigned.key
        ProxyRequests Off
        SSLProxyVerify none
        SSLProxyCheckPeerCN off
        SSLProxyCheckPeerName off
        SSLProxyCheckPeerExpire off

        <Proxy balancer://dcemCluster>
               BalancerMember https://IP-DCEM-Knoten-1:8443 route=WRS01S0212
               BalancerMember https://IP-DCEM-Knoten-2:8443 route=WRS01S0213
               ProxySet lbmethod=byrequests
        </Proxy>
        ProxyPass "/dcem"  "balancer://dcemCluster/dcem" stickysession=JSESSIONID
</VirtualHost>
```

7. Testen der Konfiguration des Load Balancers gesichert mit SSL/TLS

Testen Sie durch Eingabe des Befehls "**sudo apachectl configtest**" in der Eingabeaufforderung bzw. Shell, ob die Konfiguration erfolgreich war. Erscheint am Ende der Ausführung "Syntax OK" wurde die Konfiguration erfolgreich abgeschlossen.

War die Konfiguration nicht erfolgreich, überprüfen Sie die in Kapiteleingetragenen Daten.

8. Neustart des Servers

Starten Sie den Server durch Eingabe des Befehls "**sudo /etc/init.d/apache2 restart**" in der Eingabeaufforderung bzw. Shell neu.