

# Configuring Apache as a Load Balancer

## 1. Introduction

This guide is for administrators who want to use Apache as a load balancer for a DoubleClue cluster.

Tested with Apache2 server under Ubuntu.

## 2. Installation of Apache2

Open the prompt or Shell and enter the command **"sudo apt-get install apache2"**. Confirm the change with **"Y"**.

## 3. Configuration of the Load Balancers

Activate the SSL main menu in the prompt or Shell with the command **"sudo a2enmod ssl"**.

By installing the Load Balancer, the following file is created: **"/etc/apache2/apache2.conf"**.

In order to load the necessary Modules for the Load Balancer, add the following lines to the configuration file. For this you need administrator / root rights:

```
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. Create an SSL-Zertifikat

Create a self-signed certificate by entering the following command in the prompt or 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
```

Complete the necessary specifications.

## 5. Opening Ports

By installing the Apache server, the following file is created: **“/etc/apache2/ports.conf”**.

In order to open the port/s, change the desired port/s in the configuration file.

Example:

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

## 6. Configuration of a Load Balancer Secured with SSL/TLS

In order that the Apache server uses the secure SSL/TLS connection, some changes have to be made in the following file: **“/etc/apache2/sites-enabled/default-ssl.conf”**.

Example: This configuration was used during development.

Replace the content of the existing file by the following programming and adapt the data printed in bold to your requirements:

```

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

```

## 7. Testing the Configuration of the Load Balancer Secured with SSL/TLS

Test if the configuration was successful by entering the command “**sudo apachectl configtest**” in the prompt or Shell. If “Syntax OK” appears at the end of the execution, the configuration has been completed successfully.

If the configuration has not been successful, check the data entered in chapter [13.5 Configuration of a Load Balancer Secured with SSL/TLS](#).

## 8. Rebooting the Server

Reboot the server by entering the command “**sudo /etc/init.d/apache2 restart**” in the prompt or Shell.