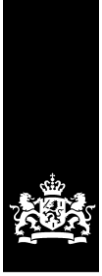


Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Installatie handleiding SSL Offloading via Apache HTTP server

Versie 0.2.1

Datum april 2012
Status Concept

Documentinformatie

Titel	Installatie handleiding SSL Offloading via Apache HTTP server
Datum	maart 2013
Versie	0.3.0
Status	Concept
Documentlocatie	https://www.modernodam.nl/svn/ontwerp/Trunk/06 Deployment/BRP/

Versiehistorie

Versie	Datum	Omschrijving
0.0.1	Maart 2012	Concept
0.1.0	Maart 2012	Gereviewde versie van 0.0.1.
0.2.0	April 2012	Aanpassingen op basis van review, test en ten behoeve van nieuwe BRP service. Met name wijzigingen aan configuratie deel doorgevoerd en stuk over configuratie van Tomcat en de proxy toegevoegd.
0.2.1	Maart 2013	Aanpassingen connector tussen Apache en Tomcat.
0.3.0	Maart 2014	Aanpassingen i.v.m. BRP Webservice landschap.

Reviewhistorie

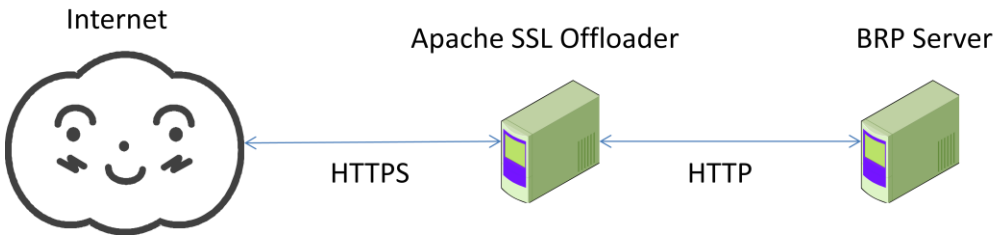
Versie	Datum	Omschrijving
0.0.1	Maart 2012	Review Bas Huisman en Tim Blommerde
0.1.0	April 2012	Review Oussama Chougna en Tim Blommerde

Inhoudsopgave

1 Inleiding

1.1 Doel

Alle communicatie met de BRP dient standaard te verlopen via een beveiligde SSL verbinding. Om de applicatieserver(s) waarop de BRP applicaties draaien in staat te stellen om informatie te lezen dient de beveiliging (encryptie) van de informatie er afgehaald te worden. Dit heet SSL Offloading en wordt voor de BRP Service gerealiseerd door een Apache HTTP server als SSL Offloader voor de BRP applicatie server(s) te configureren.



Deze handleiding beschrijft hoe een Apache HTTP server geconfigureerd kan worden voor de SSL Offloading taak.

1.2 Achtergrond

Informatieoverdracht vanuit applicatie ontwikkeling naar operationeel beheer.

1.3 Scope

Dit document is bedoeld voor operationeel beheerders van de BRP applicaties en beschrijft hoe de Apache HTTP server geconfigureerd moet worden t.b.v. SSL Offloading.

1.4 Aannames

Kennis van Apache HTTP server en Linux (bijv. Debian/Ubuntu) is vereist.
Op de omgeving is Apache HTTP server 2.2.x reeds geïnstalleerd.

1.5 Leeswijzer

Operationeel beheerders die de SSL offloader ten behoeve van de BRP applicaties moeten installeren en/of configureren dienen hoofdstuk 2 geheel te doorlopen, daar dit hoofdstuk beschrijft hoe een Apache HTTP server geconfigureerd moet worden als SSL offloader ten behoeve van een BRP applicatie. Bovendien moeten beheerders kennis hebben genomen van het BRP Webservice landschap, deze staat op de Wiki en beschrijft de URL's waarop de BRP applicaties te benaderen moeten zijn.
Verder kan als inleiding eventueel dit hoofdstuk, hoofdstuk 1, worden doorgenomen.
Voor verdere documentatie aangaande de installatie en configuratie van de BRP applicaties wordt de lezer verwezen naar de "Installatie handleiding BRP", waar de installatie van de BRP applicatie zelf in wordt beschreven.

2 Configuratie

2.1 Benodigde certificaat gerelateerde artifacten

Voor de SSL-offloading dienen er een aantal certificaat gerelateerde artifacten beschikbaar te zijn (of aangemaakt te worden[1]). Zo dienen er een server certificaat en bijbehorende key beschikbaar te zijn (bijvoorbeeld in `/etc/brp/brp_server.crt` en `/etc/brp/brp_server.key`) ten behoeve van de server identificatie. Tevens dient er een bestand aanwezig te zijn (bijvoorbeeld `/etc/brp/ca.crt`) waar alle PEM-encoded Certification Authorities (CA) certificaten in zijn verzameld die certificaten uit mogen geven die door de BRP geaccepteerd worden, dit ten behoeve van de client authenticatie.

2.2 Activeer Modules

Eerst moet er gezorgd worden dat de Apache HTTP server via SSL kan communiceren. Hiervoor moet de SSL module in apache worden geactiveerd. Gebruik hiervoor het "a2enmod" command.

```
#a2enmod ssl
```

Tevens zal Apache moeten fungeren als proxy voor de Tomcat server. Hiervoor moet de "jk" module (mod_jk) in apache worden geactiveerd.

Bij een 'default' installatie van apache2 op linux, wordt mod_jk meestal niet meegeleverd. Als apt-get gebruikt wordt is deze module te installeren (en meteen te activeren), door:

```
#apt-get install libapache2-mod-jk
```

Het activeren van de module gebeurt door een symlink aan te leggen tussen de mods-enabled en mods-available mappen. Het commando is (uitgaande van de local directory mods-enabled):

```
#ln –s ../mods-available/jk.load
```

(NB: Als je hiervoor het a2enmod commando gebruikt, zou het kunnen dat er een default configuratie jk.conf wordt meegenomen. Dat is ongewenst en die link moet dus weer verwijderd worden.)

2.3 Configureer een virtual host voor de BRP

Voor de BRP service kan of een aparte virtual host worden geconfigureerd of de default virtual host configuratie worden gebruikt. De configuratie file hiervoor hoort thuis in:

/etc/apache2/sites-available/

Voorbeeld: `/etc/apache2/sites-available/brp` of

1 Het valt buiten de scope van dit document om te beschrijven hoe certificaten werken en/of hoe deze aangemaakt dienen te worden. Het document gaat er van uit dat deze kennis aanwezig is bij de operationeel beheerders (of eventueel buiten dit document om opgedaan kan worden) en het daarom overbodig is dit hier nog expliciet in op te nemen.

```
/etc/apache2/sites-available/default-ssl
```

Voor de configuratie van mod_jk moeten de volgende directives worden toegevoegd:

```
# Configuration file for the workers
JkWorkersFile /etc/apache2/worker.properties
# Where to put jk logs
JkLogFile /var/log/apache2/mod_jk.log
# Set the jk log level [debug/error/info]
JkLogLevel info
# Select the log format
JkLogStampFormat "[%a %b %d %H:%M:%S %Y] "
# JkOptions indicate to send SSL KEY SIZE,
JkOptions +ForwardKeySize -ForwardDirectories
# JkRequestLogFormat set the request format
JkRequestLogFormat "%w %V %T"
```

De configuratie van de virtual host moet de volgende directives bevatten:

```
<VirtualHost _default_:443>
ServerAdmin beheerder@modernodam.nl

ServerName oapXX.modernodam.nl
ErrorLog /var/log/apache2/ssl_error.log
LogLevel info
CustomLog /var/log/apache2/ssl_access.log combined

SSLEngine on

#voor server identificatie
SSLCertificateFile /etc/brp/brp-server.crt
SSLCertificateKeyFile /etc/brp/brp-server.key

#voor client authenticatie
SSLCACertificateFile /etc/brp/brp-ca.crt
SSLVerifyClient require
SSLVerifyDepth 10

#alleen deze ciphers (conform digikoppeling 2.0)

SSLProxyCipherSuite TLS_DHE_RSA_WITH_AES_128_CBC_SHA:
TLS_RSA_WITH_AES_128_CBC_SHA: TLS_RSA_WITH_AES_256_CBC_SHA:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA: SSL_RSA_WITH_AES_128_CBC_SHA:
TLS_RSA_WITH_3DES_EDE_CBC_SHA

#alleen SSLv3 en TLSv1 (conform digikoppeling 2.0)
SSLProtocol +SSLv3 +TLSv1


JkMount /brp* worker1


</VirtualHost>
```

Zorg ervoor dat alle benodigde certificaat bestanden in het juiste pad staan, zoals aangegeven in bovenstaande configuratie, of pas bovenstaande configuratie aan indien bestanden of bijvoorbeeld de BRP applicatie op een andere locatie zijn te vinden. Let ook op dat URL's kloppen met het BRP Webservice landschap.

Zorg er ook voor dat alle URL's naar de applcaties die in Tomcat draaien worden gekoppeld aan de worker middels de "JkMount" directive. (Bijhouding én Bevraging) Zie hiervoor ook de BRP Webservice landschap welke URL's dit moeten zijn.

Zodra de configuratie aangemaakt is kan de virtual host geactiveerd worden voor de buitenwereld. Gebruik hiervoor het `a2ensite` command.

```
#a2ensite default-ssl
```

Of

```
#a2ensite brp
```

NB: In sommige distributies in het a2ensite commando niet beschikbaar. Gebruik dan het directe symlinken (uitgaande van de sites-enabled directory):

```
#ln –s ../sites-available/default-ssl
```

2.4 Configureer een worker

De communicatie tussen apache en tomcat vindt plaats via zogenaamde workers. Deze workers sturen berichten door volgens een bepaald protocol, genaamd ajp (Apache JServ Protocol, versie 1.3). Er zijn veel mogelijkheden voor specifieke configuratie, zie daarvoor:
http://tomcat.apache.org/connectors-doc/reference/workers.html

In paragraaf 2.3 is een directive opgenomen "*JkWorkersFile*", maak dit bestand aan (worker.properties) en voeg de volgende properties toe:

```
workers.tomcat_home=<pad naar tomcat installatie>
worker.list=worker1
worker.worker1.port=8009
worker.worker1.host=<host van applicatie server>
worker.worker1.type=ajp13
```

N.B. We geven hier de minimale properties die nodig zijn voor het functioneren van de connectie.

2.5 Configureer Tomcat

Ook de Tomcat server dient geconfigureerd te worden voor het correct functioneren van de Apache Proxy server. Hiervoor dient de connector waar de workers naar toe verbinden geactiveerd te worden.
In de tomcat server.xml configuratie file (TOMCAT_HOME/conf) staat al een dergelijke connector, maar die staat mogelijk in commentaar. Haal de definitie uit commentaar of voeg deze zelf toe. Dit is de connector definitie:

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

De default connector (op poort 8080) kan, indien deze niet meer nodig is voor testen etc, uitgeschakeld worden.

2.6 Herstart Services

Herstart nu **eerst** de Tomcat applicatie server en dan de Apache http server om alle configuratie wijzigingen te activeren.