



Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Installatiehandleiding BRP Bijhouding en Bevraging Services

Versie 0.5.0

Datum	oktober 2013
Status	concept

Documentinformatie

Titel	Installatiehandleiding BRP Bijhouding en Bevraging Services
Datum	Juni 2015
Versie	0.5.4
Status	concept
Documentlocatie	https://www.modernodam.nl/svn/brp-code/brp-distributie/trunk/src/main/doc/

Versiehistorie

Versie	Datum	Omschrijving
0.0.1	Maart 2012	Eerste versie concept
0.0.2	Maart 2012	Commentaar Eelco verwerkt
0.2.0	April 2012	Configuratie voor WS-Security toegevoegd
0.2.1	April 2012	Kleine aanpassing in verband met toevoeging property
0.2.2	Mei 2012	Stap uitvoeren testdata.sql verwijderd.
0.2.3	Augustus 2012	Aanpassingen ten behoeve van nieuwe database scripts
0.2.4	November 2012	Extra informatie en settings toegevoegd voor server 0.2.4 (Ovelijden basaal).
0.3.0	Maart 2013	Aanpassingen t.b.v. nieuwe "Big Bang" release.
0.3.1	Maart 2013	Aanpassingen m.b.t. het opzetten en configureren van certificaten
0.3.2	April 2013	Toevoeging van JMS properties tbv dashboard en leveringen
0.3.3	Augustus 2013	Aanpassing JMS properties vanweg introductie routing-centrale
0.3.4	Augustus 2013	Paragraaf 2.1.3 opmerking toegevoegd omtrent terugzetten authenticatiemiddel en certificaat informatie.
0.4.0	Augustus 2013	Hoofdstuk 2 aangepast met nieuwe scripts en nieuwe folder structuur database scripts.
0.5.0	Oktober 2013	Bijhouding en Bevraging zijn aparte services geworden, dit is in de handleiding opgenomen.
0.5.1	November 2013	Wijziging van SYSLOG server naar Graylog server configuratie in log4j.xml.
0.5.2	Maart 2014	Wijzigingen i.v.m. BRP Webservice landschap.

0.5.3	September 2014	Verwijzingen naar Whitebox-database verwijderd, archivering properties aangepast en log4j2 verwijzing.
0.5.4	Juni 2015	Wijzigingen naar aanleiding van review door Integratie & Test

INHOUDSOPGAVE

DOCUMENTINFORMATIE	2
1 INLEIDING.....	5
1.1 DOEL.....	5
1.2 ACHTERGROND.....	5
1.3 SCOPE.....	5
1.4 AANNAMES.....	5
1.5 LEESWIJZER.....	5
2 EENMALIGE (INITIËLE) CONFIGURATIE	6
2.1 POSTGRESQL DATABASE	6
2.2 TOMCAT	6
3 DEPLOYMENT	9
4 BEHEER CLIENTCERTIFICATEN	10

1 Inleiding

1.1 Doel

Handleiding voor het initieel installeren van de BRP Bijhouding en Bevraging Services op een nieuwe omgeving en/of het installeren van een nieuwe versie van de services op een bestaande omgeving.

1.2 Achtergrond

Informatieoverdracht vanuit applicatie ontwikkeling naar operationeel beheer.

1.3 Scope

Dit document is bedoeld voor operationeel beheerders van de BRP Bijhouding en Bevraging applicaties/services en beschrijft hoe de services geïnstalleerd/gedeployed dienen te worden.

1.4 Aannames

Kennis van PostgreSQL, Apache Tomcat is vereist.

Op de omgeving zijn PostgreSQL en Apache Tomcat reeds geïnstalleerd en er wordt in deze handleiding van uitgegaan dat de standaardconfiguratie van deze producten gebruikt worden. Als hiervan afgeweken is, dan dient hier door de gebruiker zelf rekening mee worden gehouden bij de stappen die gevolgd dienen te worden in deze installatiehandleiding.

1.5 Leeswijzer

Operationeel beheerders die de Bijhouding en Bevraging Services voor het eerst moeten installeren, dus op een omgeving waar dit nog niet eerder is gebeurd, wordt aangeraden te beginnen bij hoofdstuk 2. Dit hoofdstuk gaat in op de installatie en configuratie van het systeem (zowel PostgreSQL database als Tomcat applicatie server). Indien het systeem reeds draait en is geconfigureerd en er slechts een nieuwe versie van de service dient te worden geïnstalleerd, wordt de operationeel beheerder verwezen naar hoofdstuk 3, het hoofdstuk dat ingaat op de (her)installatie van de service.

Voor het operationeel beheer rond partijen en certificaten ten behoeve van authenticatie kan de lezer hoofdstuk 4 doornemen, waarin beschreven wordt hoe een nieuwe partij kan worden toegevoegd, inclusief bijbehorende authenticatie certificaten.

2 Eenmalige (initiële) configuratie

Dit hoofdstuk beschrijft de initiële installatie van de BRP Bijhouding en Bevraging Services. Hiervoor moet eerst de database worden aangemaakt en gevuld, waarna de applicatie op Tomcat kan worden geïnstalleerd. Het inlezen van de database valt buiten de scope van dit document, zie hiervoor de andere documentatie.

2.1 PostgreSQL database

2.1.1 Aanmaken database

Het is nodig om een database aan te maken, bijvoorbeeld een database met de naam 'brp'.

2.1.2 Vullen database

Er zijn verschillende mogelijkheden waarop de (initiële) vulling voor de database wordt aangeleverd. Veelal zal dit via SQL-bestanden plaatsvinden die achtereenvolgens in een bepaalde volgorde dienen te worden uitgevoerd.

2.1.3 Aanmaken database gebruiker

Voor de applicatie is het nodig dat er een database gebruiker wordt aangemaakt. Deze gebruiker zal dan tenminste de "BRP bijhouder"-rol moeten krijgen die bij de inhoud van de database wordt meegeleverd is. Voor testdoeleinden kan de gebruiker ook functioneren als zogenaamde superuser. Let op: de superuser-rol is niet wenselijk in een productieomgeving.

2.2 Tomcat

2.2.1 Aanmaken private keystore voor het tekenen van antwoordberichten

De applicatie heeft een keystore nodig met daarin de private server key en het bijbehorende certificaat. Het is de bedoeling dat hiervoor andere keys worden gebruikt dan voor SSL, maar dit is technisch niet noodzakelijk. De keys en de keystore zijn geen onderdeel van de release. Voor het aanmaken en vullen van de keystore wordt verwezen naar de opgeleverde scripts en instructies rond certificaten. Hierin is te vinden hoe eventueel een eigen CA kan worden aangemaakt en het server certificaten materiaal (met o.a. de genoemde privatestore keystore).

2.2.2 Applicatiedatabase configuratie

Voor de BRP Bijhouding en Bevraging Services moeten enkele properties m.b.t. de database buiten de applicatie om worden geconfigureerd. Deze moeten daarom staan in een properties bestand op het classpath. Voor Tomcat is dit de [TOMCAT_HOME]/lib/ directory.

Maak voor de applicatie database configuratie daarom een bestand aan in bovengenoemde directory met de naam "brp.properties" met de volgende inhoud:

```
jdbc.driverClassName=org.postgresql.Driver
jdbc.url=jdbc:postgresql://<host>/<database naam>
jdbc.username=brp
jdbc.password=<password>

brp.database.timeout.seconds=10
```

```
#Speciale connectie voor Archivering, Logging en Protocollering
jdbc.archivering.driverClassName=org.postgresql.Driver
jdbc.archivering.url=jdbc:postgresql://<host>/<database naam>
jdbc.archivering.username=brp
jdbc.archivering.password=<password>
```

Vul bij <host>, <database naam>, <username> en <password> de juiste waarden in voor de database, zoals die in paragraaf 2.1 gecreëerd is.

Zowel de Bijhouding als Bevraging service maken gebruik van deze set properties. Mochten de services onder aparte Tomcat servers geïnstalleerd worden moet voor beide services dit brp.properties bestand aanwezig zijn.

2.2.3 Applicatie WS-Security configuratie t.b.v. signing

Op het classpath van Tomcat ([TOMCAT_HOME]/lib/ directory) dienen t.b.v. signing 2 keystores (.jks) aanwezig te zijn:

- publicstore.jks: Bevat certificaten van clients om de handtekening in inkomende berichten te kunnen verifiëren. Zie hoofdstuk 4 voor het aanmaken en beheren van deze keystore.
- privatestore.jks: Bevat een private key waarmee de server uitgaande berichten ondertekent. Zie paragraaf 2.2.1 voor het aanmaken van deze keystore.

Daarnaast moeten extra configuratie parameters worden toegevoegd aan het brp.properties bestand van paragraaf 2.2.2:

```
security.keystore.public.password=<publicstore password>
security.keystore.public.file=publicstore.jks

security.keystore.private.password=<privatestore password>
security.keystore.private.file=privatestore.jks

security.privatekey.alias=1
security.privatekey.password=<private key password>
```

Zowel de Bijhouding als Bevraging service maken gebruik van deze keystores en properties. Mochten de services onder aparte Tomcat servers geïnstalleerd worden, dan moeten deze keystores en properties in beide instanties beschikbaar zijn.

2.2.4 Applicatie logging configuratie

Maak voor de applicatie logging configuratie een bestand aan met de naam "log4j2.xml". Een voorbeeldbestand is opgenomen in de config directory van deze zip.

Zorg ervoor dat dit bestand in de classpath [TOMCAT_HOME]/lib/ wordt gezet.

2.2.5 Applicatie JMS configuratie

Let op

Deze properties zijn alleen van toepassing voor de Bijhouding service. Overigens is het geen probleem als ze ook op de Bevraging service beschikbaar zijn.

Voor bijhoudingen worden berichten op een JMS queue gezet, zodat deze door het dashboard en de leveringen module opgepakt kunnen worden. Hiervoor dient een tweetal properties te worden opgenomen in het brp.properties bestand van paragraaf 2.2.2:

```
jms.administratieve.handeling.url=tcp://<brp-routing-centrale-  
host>:<brp-routing-centrale-poort>  
jms.administratieve.handeling.queue=AdministratieveHandelingen
```

De url is de url waarop de BRP Routing Centrale (met ActiveMQ) draait welke gestart wordt door het brp-routing-centrale project (brp-routing-centrale.war). De queue bevat de naam van de queue waarop de berichten geplaatst moeten worden. De url zal per omgeving verschillen, de queue zal in principe niet wijzigen.

Let op

Als deze properties niet zijn opgenomen in het brp.properties bestand, of niet ingevuld zijn, dan zal er geen bericht op de queue geplaatst worden en zal een bijhouding niet in het dashboard verschijnen en ook niet door de leveringen module opgepakt worden. Bij een bijhouding zal hierover een WARN in de logs verschijnen:

```
"[WARN ] nl.bzk.brp.business.stappen.administratievehandeling.  
PubliceerAdministratieveHandelingStap: Er is geen configuratie ingesteld voor de  
BijhoudingNotificator, daarom wordt er geen Administratieve Handeling Id  
gepubliceerd op de levering JMS queue."
```


3 Deployment

De BRP Bijhouding en Bevraging Services bestaan uit de volgende installeerbare eenheden:

bijhouding.war (bijhouding)
bevraging.war (bevraging)

Een deployment houdt het volgende in:

- Stop de Tomcat server.
- Verwijder de deployables die vervangen gaan worden in [TOMCAT_HOME/webapps/.
- Verwijder de uitgekakte deployables die vervangen gaan worden (directories) in [TOMCAT_HOME/webapps/.
- Plaats de nieuwe of gewijzigde properties-bestanden in [TOMCAT_HOME/lib/.
Let op dat je het 'brp.properties'-bestand hier dus neerzet.
- Plaats de nieuwe deployables in [TOMCAT_HOME/webapps/.
- Start de Tomcat server.

Als de deployment is gelukt dan moeten de volgende webpagina's benaderbaar zijn met een webbrowser¹:

Bijhouding:

<host>/bijhouding/BijhoudingService/

Bevraging:

<host>/bevraging/BijhoudingBevragingService/

Deze webpagina's geven een overzicht van alle beschikbare webservices van deze deployables. Bovendien controleert men hier of de URL's kloppen met het BRP Webservice landschap.

De versie van de bijhouding service kan worden gecontroleerd door met een webbrowser te gaan naar de URL<host>/bijhouding/BijhoudingService/version.html. Voor de bevraging service kan dan dat op de volgende url:
<host>/bevraging/BijhoudingBevragingService/version.html.

¹ Als de SSL offloader is geïnstalleerd dan is deze pagina alleen maar bereikbaar indien de client zich correct authenticceert middels een geldig client certificaat. Hiervoor zal de browser geconfigureerd moeten worden om zich met een geldig client certificaat te authenticeren. Hoe dit gedaan wordt is afhankelijk van de browser versie en valt buiten de scope van dit document.

4 Beheer clientcertificaten

Ten behoeve van de authenticatie (en autorisatie) van de verschillende partijen en afnemers van de BRP Bijhouding en Bevraging services, wordt gebruik gemaakt van client certificaten, waarbij elke partij/afnemer één of meerdere door een door de BRP Bijhouding en Bevraging services erkende Certificate Authority (CA) ondertekend certificaat dient te hebben. De handleidingen om zowel een nieuwe BRP CA certificaat als client certificaten aan te maken zijn te vinden in de "scripts" folder van de oplevering. Hieronder volgt een overzicht hiervan.

Bestand	Omschrijving
scripts/certificaten/LEESMIJ	Algemene informatie over de meegeleverde scripts voor certificaten beheer. Dit dient als eerste gelezen te worden.
scripts/certificaten/INSTRUCTIES_NIEUWE_CA_OF_SERVER	Dit is de handleiding voor het aanmaken van een server root CA certificaat, en een server certificaat met bijbehorende private key. Dit zal enkel nodig zijn bij het installeren van een nieuwe omgeving.
scripts/certificaten/INSTRUCTIES_NIEUWE_CLIENT	Dit is de handleiding voor het aanmaken van een client certificaat inclusief private key. Tevens wordt uitgelegd hoe je dit certificaat importeert in de public keystore van de server, en hoe je het certificaat samen met authenticatiemiddel toevoegt aan de BRP database t.b.v. white listing. Deze handleiding dient voor iedere nieuwe client opnieuw doorlopen te worden.