HB plus

Hewlett Packard Enterprise
Proximus
Deelgenoten THV

Vlaamse overheid

PaaS – Tomcat 8 – Setup

Vlaamse overheid

Versie 1.00
10/29/2015

Inhoud

1. Over dit document

1.1. Doel van het document

Dit document is bedoeld om bijkomende informatie te voorzien over de Platform dienst Tomcat 8 die worden aangeboden door HB-plus binnen de Vlaamse overheid Virtual Private Cloud (VPC) en dan meer specifiek hoe het product werd geinstalleerd.
Dit document is niet bedoeld als handleiding van Tomcat 8 zelf. Een basiskennis van Tomcat 8 wordt verondersteld aanwezig te zijn.

1.2. Gebruikte “rollen” en hun betekenis

Binnen dit document wordt de dienst vanuit verschillende perspectieven toegelicht. Hieronder beschrijven we de verschillende “rollen” die gebruikt worden in dit document en de betekenis die in dit document gehanteerd wordt:

- **Afnemer (klant):** is de partij die de dienst afneemt bij HB-plus, ook wel “Technical owner” genoemd
- **Gebruiker:** is de partij die de toepassing - gehost op de PaaS dienst – gebruikt
- **Beheerder (HB-plus):** is een persoon binnen de HB-plus vennootschap die beheer uitvoert op de datacenter diensten

2. Inleiding

Apache Tomcat is een open-source webserver en java servlet container ontwikkeld onder toezicht van de Apache Software Foundation (ASF). Tomcat implementeert verschillende Java EE specificaties, waaronder Java Servlet, JavaServer Pages (JSP), Java EL en WebSocket. Apache Tomcat voorziet een "pure Java" HTTP webserver omgeving waarin Java code gebruikt kan worden voor dynamische inhoud.
Apache wordt beschikbaar gesteld onder de Apache License 2.0 licentie. Het betreft dan ook open-souce software.
Apache Tomcat server kan gebruikt worden als platform voor zowel aangekochte (of-the-shelf) als eigen ontwikkelde toepassingen.

3. Opzet van de Tomcat 8

De tomcat software wordt in verschillende stappen geïnstalleerd en geconfigureerd:

- Basisinstallatie: installatie van de software zelf
- Aanpassingen specifiek voor ontwikkeling of productie

3.1. Gebruikte software versies

Onderstaande geeft weer welke software versies gebruikt zijn in de PaaS Tomcat 8.

Software	Versie
Apache Tomcat	8.0.22

3.2. Licentie

Binnen de PaaS-omgeving, voorziet HB-plus de licenties. Voor Tomcat 8 is er geen aparte licentie nodig.
U bent als klant wel verantwoordelijk voor eventuele bijkomende licenties die nodig zijn voor andere opties of voor software die draait bovenop de Tomcat middleware laag.

3.3. Basisinstallatie

Vooreerst wordt de Tomcat 8 software geïnstalleerd.
Hierbij worden geen aanpassingen gedaan. De software wordt opgezet door het standaard uitpakken van het pakket zoals voorzien door Apache.
Er worden wel een aantal kleinere aanpassingen gedaan zoals zorgen dat Tomcat automatisch opstart bij het opstarten van de server.

3.4. Aanpassingen productie/ontwikkeling

Als volgende stap worden een aantal zaken aangepast afhankelijk van de functie van het systeem. Het is vanzelfsprekend dat een ontwikkelingssysteem meer mogelijkheden moet hebben dan een productie-systeem dat toegankelijk is vanaf het internet.

Volgende tabel geeft in het kort de verschillen weer:

Functie beschikbaar	Productie	Ontwikkeling
Automatisch logbeheer	Ja	Nee
Host-manager	Nee	Ja
Manager	Nee	Ja
Voorbeeld apps (examples)	Nee	Ja
Documentatie	Nee	Ja
ROOT-webapp	Nee	Ja

User-roles aangemaakt	Nee	Ja
Shutdown-poort	Nee	Ja
Nginx aanpassing	Ja	Nee

In de volgende paragrafen wordt ieder van deze verder besproken.

Waarschuwing

U kan een aantal van deze instellingen handmatig veranderen (zowel op ontwikkelings- als productie-systemen.
Hou er rekening mee dat dit de veiligheid van uw systeem kan beinvloeden, dus de nodige waakzaamheid bij aanpassingen blijft nodig.

3.4.1. Automatisch logbeheer

Voor productie-systemen wordt automatische logrotatie opgezet. NIET voor ontwikkelings-systemen, daar blijft de beheerder verantwoordelijk voor het opschonen van de logs.

Dit onderscheid wordt gemaakt omdat voor ontwikkelings-systemen men mogelijk verder terug in de tijd moet kunnen in de logs om bepaalde items uit te zoeken. Voor productie-systemen mag er geen onderbreking komen van het systeem ingeval de schijf volloopt wegens logs die niet tijdig opgeschoond worden.

De logs worden verder ook ge-backuped, dus indien nodig kan er tot 30 dagen terug gekeken worden.

Enkel de catalina.out wordt opgenomen in de logrotatie. Mocht u voor uw applicatie die op Tomcat draait een andere logfile gebruiken, dan moet u deze manueel opschonen.

U kan deze instellingen niet zelf wijzigen. Mocht u een ander logrotatie-patroon nodig hebben, gelieve dan een niet voorgedefinieerde eenvoudige werkaanvraag in te dienen.

3.4.2. Host-manager applicatie

Voor productie-systemen wordt de host-manager applicatie NIET opgezet. Wel voor ontwikkelings-systemen

Dit wordt gedaan omdat de host-manager applicatie verschillende security-problemen heeft:

1. De Tomcat-versie wordt zichtbaar, wat aanvallers duidelijk maakt welke versie van Tomcat beschikbaar is.
2. Als de server naar internet ontsloten is, is ook de host-manager applicatie via internet beschikbaar.

3.4.3. Manager applicatie

Voor productie-systemen wordt de manager applicatie NIET opgezet. Wel voor ontwikkelings-systemen

Dit wordt gedaan omdat de manager applicatie verschillende security-problemen heeft:

1. De Tomcat-versie wordt zichtbaar, wat aanvallers duidelijk maakt welke versie van Tomcat beschikbaar is.
2. Als de server naar internet ontsloten is, is ook de manager applicatie via internet beschikbaar.

Dit heeft implicaties naar het uitrollen van applicaties (war-files of andere types). Deze moeten op productie-systemen manueel worden geïmplementeerd en kunnen niet via de manager-applicatie uitgerold worden.

3.4.4. Voorbeeld-applicaties (examples)

Voor productie-systemen worden de voorbeeld-applicaties NIET opgezet. Wel voor ontwikkelings-systemen.

Dit wordt gedaan omdat de voorbeeld-applicaties verschillende security-problemen hebben:

1. De Tomcat-versie wordt in bepaalde gevallen zichtbaar, wat aanvallers duidelijk maakt welke versie van Tomcat beschikbaar is.
2. De veiligheid op deze applicaties is bijna altijd lager dan in ontwikkelde applicaties
3. Als de server naar internet ontsloten is, zijn ook de voorbeeld-applicaties via internet beschikbaar.

3.4.5. Documentatie

Voor productie-systemen wordt de documentatie NIET opgezet. Wel voor ontwikkelings-systemen.

Dit wordt gedaan vanwege verschillende redenen:

1. Documentatie is op een productie-machine niet onmiddellijk nodig. Op ontwikkelingssystemen is ze echter onontbeerlijk.
2. De Tomcat-versie wordt in bepaalde gevallen zichtbaar, wat aanvallers duidelijk maakt welke versie van Tomcat beschikbaar is.
3. Er is geen veiligheid voorzien op deze documentatie.
4. Als de server naar internet ontsloten is, is ook de documentatie via internet beschikbaar.

3.4.6. ROOT-webapp

Voor productie-systemen wordt de ROOT-webapp NIET opgezet. Wel voor ontwikkelings-systemen.

Dit wordt gedaan vanwege verschillende redenen:

1. Dit is op een productie-machine niet onmiddellijk nodig. Het is toch de bedoeling dat de eigen applicatie hier terechtkomt. Op ontwikkelingssystemen is dit niet noodzakelijk het geval.
2. De Tomcat-versie is hierop zichtbaar, wat aanvallers duidelijk maakt welke versie van Tomcat beschikbaar is.
3. Er is geen veiligheid voorzien op deze applicatie.
4. Als de server naar internet ontsloten is, is ook deze applicatie via internet beschikbaar.

U kan deze zelf wijzigen door de file server.xml aan te passen.

3.4.7. Gebruikers/rollen (tomcat-users.xml)

Voor productie-systemen worden er geen gebruikers noch rollen gedefinieerd. Wel voor ontwikkelings-systemen.

Dit wordt gedaan vanwege veiligheidsredenen op de productie-systemen:

1. Op een productie-systeem moeten enkel de gebruikers/rollen gedefinieerd worden die nodig zijn voor de applicatie. Als er geen “standaard” gebruikers zijn gedefinieerd, worden deze ook niet vergeten.
2. De host-manager en manager-applicaties zijn niet opgezet, dus zijn deze gebruikers ook niet nodig.

Op ontwikkelings-systemen worden de volgende gebruikers gedefinieerd met bijpassende rollen:

Gebruikersnaam	**rollen**
admin	admin-script, manager-script
manager	admin-gui, manager-gui

De paswoorden van deze gebruikers worden u meegedeeld na de opzet van het systeem.

U kan deze zelf wijzigen door de file tomcat-users.xml aan te passen.

3.4.8. Shutdown-poort (8005)

Voor productie-systemen wordt deze poort gedeactiveerd. Voor ontwikkelings-systemen blijft deze behouden.

Dit wordt gedaan vanwege veiligheidsredenen op de productie-systemen.
Op ontwikkelings-systemen heeft dit weinig invloed.

U kan deze zelf wijzigen door de file server.xml aan te passen.

3.4.9. Nginx aanpassing

Voor productie-systemen gaat de nginx alle verbindingen op het externe IP-adres via poort 80 en 443 verbinden met poort 8080 (van de Tomcat-software). Voor ontwikkelings-systemen gebeurt dit op het interne IP-adres.

3.5. Niet toegestaan

Vanwege de monitoring die op de systemen draait, mogen bepaalde configuratie-onderdelen niet veranderd worden, aangezien dit de monitoring zou blokkeren.

3.5.1. setenv.sh/JMX

Volgende lijnen mogen NIET aangepast worden.

```
JMX_OPTS=”-Dcom.sun.management.jmxremote
  -Dcom.sun.management.jmxremote.port=1099
  -Dcom.sun.management.jmxremote.ssl=false
  -Dcom.sun.management.jmxremote.authenticate=false”
```

Opgepast: volgende lijn mag aangepast worden, maar MOET het gedeelte met de JMX_OPTS behouden.

```
Export CATALINA_OPTS=”${USER_OPTS} ${JMX_OPTS}”
```

4. Extra ondersteuning door HB-plus

In het aanbod van de PaaS dienst voorziet HB-plus in een stabiel en veilig platform dat u als klant kan gebruiken om uw toepassing en gegevens te hosten. Uiteraard zijn er tal van mogelijkheden waarop u dit platform kan gebruiken. In sommige gevallen kan het dan ook voorkomen dat de geboden 'standaard' niet volstaat voor uw oplossing. In dat geval kan u een niet voorgedefinieerde eenvoudige werkaanvraag richten tot HB-plus voor het inrichten van extra componenten die u nodig heeft.
Enkele voorbeelden hiervan zijn:

- Aanpassing op automatisch comprimeren en opschonen van logbestanden
- Automatische bestanden overbrengen via een sFTP dropserver
- ...

Belangrijk

Voor complexe oplossingen raden we aan om vooraf contact te nemen met HB-plus om samen de oplossing te bespreken.

5. Online documentatie

Indien u vragen heeft over specifieke zaken in Apache Tomcat 8.0, kan onderstaande online documentatie mogelijks van pas komen:

- Tomcat 8.0 documentatie: http://tomcat.apache.org/tomcat-8.0-doc/
- Tomcat 8.0 configuratie: http://tomcat.apache.org/tomcat-8.0-doc/config/index.html
- Tomcat Wiki: http://wiki.apache.org/tomcat/FAQ