

Tomcat en production

Préambule

 Ce document est un exemple de ce qui se fait sur des serveurs de production, il n'a pas la prétention d'être **LA référence**. D'ailleurs j'encourage tout personne le souhaitant à enrichir ce document pour apporter son expérience.

Le but de ce document est de :

1. Faciliter les mises à jour ultérieures
2. Supprimer ce qui est inutile et consommateur de ressources
3. Sécuriser nos installations
4. Disposer d'outils de maintenance

Pour l'exemple

Astuce

Pour vous faciliter les mises à jours ultérieures de tomcat ou des versions d'esup-portail, il est conseillé d'utiliser des liens symboliques. Par exemple :

- `/esup/tomcat6` est un lien symbolique vers l'installation binaire de tomcat (`server.home`)
- `/esup/esup-install` est un lien symbolique vers l'installation binaire de tomcat (`esup.root`)
- `/esup/esup-sources` est un lien symbolique vers les sources uPortal (`esup.sources`)
- `/esup/webapps` est un lien symbolique vers le webapps de déploiement esup-portail (`esup.deploy`)

Installation d'un serveur tomcat 6

```
[esup@test]$ mkdir /esup
[esup@test]$ cd /esup
[esup@test]$ wget http://apache.cict.fr/tomcat/tomcat-6/v6.0.24/bin/apache-tomcat-6.0.24.tar.gz
[esup@test]$ tar -zxvf apache-tomcat-6.0.24.tar.gz
[esup@test]$ ln -s apache-tomcat-6.0.24 tomcat6
[esup@test]$ rm apache-tomcat-6.0.24.tar.gz
```

On a donc :

```
/esup/tomcat6 => /esup/apache-tomcat-6.0.24
```

Installation esup-3

```
[esup@test]$ cd /esup
[esup@test]$ wget http://sourcesup.cru.fr/frs/download.php/2875/esup-3.1.2-esup-0.5-RC1.tar.gz
[esup@test]$ tar -zxvf esup-3.1.2-esup-0.5-RC1.tar.gz
[esup@test]$ ln -s esup-3.1.2-esup-0.5-RC1 esup-install
[esup@test]$ rm esup-3.1.2-esup-0.5-RC1.tar.gz
```

On a donc :

```
/esup/esup-install => /esup/esup-3.1.2-esup-0.5-RC1
```

Librairies

Modifier le `/esup/tomcat6/conf/catalina.properties`

```
[esup@test]$ vi /esup/tomcat6/conf/catalina.properties  
  
> shared.loader=${catalina.base}/shared/classes,${catalina.base}/shared/lib/*.jar
```

Créer les dossiers shared/classes et shared/lib

```
[esup@test]$ mkdir -p /esup/tomcat6/shared/classes  
[esup@test]$ mkdir -p /esup/tomcat6/shared/lib
```

Le driver SQL

Placer le driver de base de données dans /esup/tomcat6/lib (Utilisé par le pool de connexion Tomcat)

```
[esup@test]$ cp /esup/esup-install/update/Tomcat/lib/mysql-connector-java-5.1.6.jar /esup/tomcat6/lib
```

Vous trouverez différents drivers dans le package [/esup/esup-install/update/Tomcat/lib]

Les jar du portail (pluto)

```
[esup@test]$ ant init deploy-ear -Dtomcat.update=true
```

Context Tomcat

Modifier le server.xml [/esup/tomcat6/conf/server.xml]

Ajouter les contextes dans le portail (Attention au 2 docBase, username, password, url à adapter)



Pour l'utilisation de portlet, on rajoute le paramètre emptySessionPath dans le Connector (cf. <https://wiki.jasig.org/display/UPM31/01+Tomcat>)

```

<?xml version='1.0' encoding='utf-8'?><Server port="8005" shutdown="SHUTDOWN">
  <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
  <Listener className="org.apache.catalina.core.JasperListener" />
  <Listener className="org.apache.catalina.mbeans.ServerLifecycleListener" />
  <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener" />

  <Service name="Catalina">
    <!-- Define an AJP 1.3 Connector on port 8009 -->
    <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" emptySessionPath="true" />
    <Engine name="Catalina" defaultHost="localhost">
      <Host name="localhost" appBase="webapps"
        unpackWARs="false" autoDeploy="false"
        xmlValidation="false" xmlNamespaceAware="false">

        <Context path=""
          docBase="/esup/webapps/uPortal"
          crossContext="true"
          reloadable="true">
          <Resource name="jdbc/PortalDb"
            auth="Container"
            type="javax.sql.DataSource"
            username="XXXXX" password="XXXXX"
            driverClassName="com.mysql.jdbc.Driver"
            url="jdbc:mysql://XXXX.univ.fr/XXXXX?autoReconnect=true"
            maxActive="50" maxIdle="30" maxWait="10000"
            poolPreparedStatements="true"
            removeAbandoned="true"
            removeAbandonedTimeout="300"
          />
          <Manager pathname="" />
        </Context>

        <Context path="/ResourceServingWebapp"
          docBase="/esup/webapps/ResourceServingWebapp"
          reloadable="false">
          <Manager pathname="" />
        </Context>

        <Context path="/manager"
          docBase="/esup/tomcat6/webapps/manager"
          reloadable="false"
          antiResourceLocking="false"
          privileged="true">
          <Manager pathname="" />
        </Context>

        <!--
        <Context path="/probe"
          docBase="/esup/webapps/probe"
          reloadable="false"
          privileged="true">
          <Manager pathname="" />
        </Context>
        -->
      </Host>
    </Engine>
  </Service>
</Server>

```

Nettoyage

Supprimer les dossiers suivants :

```
[esup@test]$ rm -rf /esup/tomcat6/webapps/docs
[esup@test]$ rm -rf /esup/tomcat6/webapps/examples
[esup@test]$ rm -rf /esup/tomcat6/webapps/host-manager
[esup@test]$ rm -rf /esup/tomcat6/webapps/ROOT
[esup@test]$ rm -rf /esup/tomcat6/conf/Catalina
```

Cassifier le manager Tomcat

Créer un dossier de librairies dans le manager

```
[esup@test]$ mkdir -p /esup/tomcat6/webapps/manager/WEB-INF/lib
```

- Télécharger le cas-client <http://www.ja-sig.org/downloads/cas-clients/>
- En extraire cas-client-core-3.X.X.jar, commons-logging-X.X.jar
- Les placer dans /esup/tomcat6/webapps/manager/WEB-INF/lib

```
[esup@test]$ cd /tmp
[esup@test]$ wget http://www.ja-sig.org/downloads/cas-clients/cas-client-3.1.10-release.tar.gz
[esup@test]$ tar -zxvf cas-client-3.1.10-release.tar.gz
[esup@test]$ cp cas-client-3.1.10/modules/cas-client-core-3.1.10.jar /esup/tomcat6/webapps/manager/WEB-INF/lib
[esup@test]$ cp cas-client-3.1.10/modules/commons-logging-1.1.jar /esup/tomcat6/webapps/manager/WEB-INF/lib
[esup@test]$ rm -rf /tmp/cas-client-3.1.10
```

- Vous devrez aussi vous procurer le xercesImpl.jar <http://www.apache.org/dist/xerces/j/binaries/>
- Mettre le xercesImpl.jar dans /esup/tomcat6/webapps/manager/WEB-INF/lib

```
[esup@test]$ cd /tmp
[esup@test]$ wget http://www.apache.org/dist/xerces/j/binaries/Xerces-J-bin.2.9.1.tar.gz
[esup@test]$ tar -zxvf Xerces-J-bin.2.9.1.tar.gz
[esup@test]$ cp xerces-2_9_1/xercesImpl.jar /esup/tomcat6/webapps/manager/WEB-INF/lib
[esup@test]$ rm -rf /tmp/xerces-2_9_1
```

Filtre d'authentification

Copier la classe java SimpleCASAAuthorizationFilter dans le manager.

Cette classe permet de filtrer les utilisateurs pouvant utiliser le manager

```
[esup@test]$ cp /esup/webapps/uPortal/WEB-INF/classes/org/esupportail/portal/utils/filter
/SimpleCASAAuthorizationFilter.class /esup/tomcat6/webapps/manager/WEB-INF/classes/org/esupportail/portal/utils
/filter/SimpleCASAAuthorizationFilter.class
```

web.xml du manager

```
[esup@test]$ vi /esup/tomcat6/webapps/manager/WEB-INF/web.xml
```

Les filtres CAS

Attention au serverName, casServerLoginUrl, casServerUrlPrefix, LOGIN, LOGIN 2 (personne autorisées)

```

<!-- Server Name -->
<context-param>
  <param-name>serverName</param-name>
  <param-value>XXXXXXXXXX</param-value>
</context-param>

<filter>
  <filter-name>CAS Single Sign Out Filter</filter-name>
  <filter-class>org.jasig.cas.client.session.SingleSignOutFilter</filter-class>
</filter>

<!-- CAS Authentication Filter -->
<filter>
  <filter-name>CASFilter</filter-name>
  <filter-class>
    org.jasig.cas.client.authentication.AuthenticationFilter
  </filter-class>
  <init-param>
    <param-name>casServerLoginUrl</param-name>
    <param-value>https://XXXXX/cas/login</param-value>
  </init-param>
</filter>

<!-- CAS Validation Filter -->
<filter>
  <filter-name>CASValidation</filter-name>
  <filter-class>
    org.jasig.cas.client.validation.Cas20ProxyReceivingTicketValidationFilter
  </filter-class>
  <init-param>
    <param-name>casServerUrlPrefix</param-name>
    <param-value>https://XXXXX/cas</param-value>
  </init-param>
  <init-param>
    <param-name>redirectAfterValidation</param-name>
    <param-value>true</param-value>
  </init-param>
</filter>

<!-- CAS Wrapper Filter -->
<filter>
  <filter-name>CASWrapper</filter-name>
  <filter-class>
    org.jasig.cas.client.util.HttpServletRequestWrapperFilter
  </filter-class>
</filter>

<filter>
  <filter-name>AuthzFilter</filter-name>
  <filter-class>org.esupportail.portal.utils.filter.SimpleCASAutorizationFilter</filter-class>
  <init-param>
    <param-name>org.esupportail.portal.utils.filter.authorizedUsers</param-name>
    <param-value>LOGIN1 LOGIN2 ...</param-value>
  </init-param>
</filter>

```

Les mappings

```

<filter-mapping>
  <filter-name>CAS Single Sign Out Filter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>

<!-- CAS Authentication Filter Mapping -->
<filter-mapping>
  <filter-name>CASFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>

<!-- CAS Validation Filter Mapping -->
<filter-mapping>
  <filter-name>CASValidation</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>

<!-- CAS Wrapper Filter Mapping -->
<filter-mapping>
  <filter-name>CASWrapper</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>

<filter-mapping>
  <filter-name>AuthzFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>

```

Le Listener

```

<listener>
  <listener-class>org.jasig.cas.client.session.SingleSignOutHttpSessionListener</listener-class>
</listener>

```

Nettoyage web.xml

Supprimer les parties :

- <resource-env-ref>...</resource-env-ref>
- <security-constraint>...</security-constraint>
- <login-config>...</login-config>
- <security-role>...</security-role>

Les logs Tomcat

Modifier le fichier logging.properties pour :

- Ne plus logger à la console mais uniquement dans un fichier
- Tourner automatiquement les fichiers quand ils font plus de 10Mo
- Garder seulement 7 fichiers (donc 70Mo)
- Passer le niveau de log en WARNING
- N'avoir qu'un seul fichier

```
[esup@test]$ vi /esup/tomcat6/conf/logging.properties

# see http://tomcat.apache.org/tomcat-6.0-doc/logging.html
handlers = 1catalina.java.util.logging.FileHandler
.handlers = 1catalina.java.util.logging.FileHandler
.level= WARNING

1catalina.java.util.logging.FileHandler.pattern = ${catalina.base}/logs/catalina.%g.log
1catalina.java.util.logging.FileHandler.limit = 10485760
1catalina.java.util.logging.FileHandler.count = 7
1catalina.java.util.logging.FileHandler.append=true
1catalina.java.util.logging.FileHandler.formatter=java.util.logging.SimpleFormatter

# Pour avoir les lignes de démarrage
org.apache.catalina.startup.Catalina.level=INFO
# Pour avoir les lignes d'arrêt
org.apache.catalina.core.StandardService.level=INFO

# Pour avoir les manger de ce qui est fait au niveau manager
org.apache.catalina.core.ContainerBase.[Catalina].[localhost].[/manager].level = INFO
```

Installation de LamdaProbe

LambdaProbe est un outil qui ressemble au manager de Tomcat mais un peu plus évolué.

Il vous permet de :

- Lister vos contextes Tomcat
- Redémarrer les contextes
- Lister vos sessions et leurs contenus
- Monitorer les sources de données
- Voir les logs a chaud
- Analyser les Threads
- Voir l'utilisation de la mémoire
- ...

```
[esup@test]$ cd /tmp
[esup@test]$ wget http://www.lambdaprobe.org/downloads/1.7/probe.1.7b.zip
[esup@test]$ unzip probe.1.7b.zip
[esup@test]$ mkdir /esup/webapps/probe
[esup@test]$ cd /esup/webapps/probe
[esup@test]$ unzip /tmp/probe.war
```

Context tomcat

Modifier le server.xml [/esup/tomcat6/conf/server.xml]

```
<Context path="/probe"
    docBase="/esup/webapps/probe"
    reloadable="false"
    privileged="true">
    <Manager pathname=""/>
</Context>
```

Cassification

Vous pouvez vous reporter à la partie "Cassifier le manager Tomcat" qui s'en rapproche fortement

```
[esup@test]$ cd /tmp
[esup@test]$ wget http://www.ja-sig.org/downloads/cas-clients/cas-client-3.1.10-release.tar.gz
[esup@test]$ tar -zxvf cas-client-3.1.10-release.tar.gz
[esup@test]$ cp cas-client-3.1.10/modules/cas-client-core-3.1.10.jar /esup/webapps/probe/WEB-INF/lib
[esup@test]$ cp cas-client-3.1.10/modules/commons-logging-1.1.jar /esup/webapps/probe/WEB-INF/lib
[esup@test]$ rm -rf /tmp/cas-client-3.1.10

[esup@test]$ cd /tmp
[esup@test]$ wget http://www.apache.org/dist/xerces/j/binaries/Xerces-J-bin.2.9.1.tar.gz
[esup@test]$ tar -zxvf Xerces-J-bin.2.9.1.tar.gz
[esup@test]$ cp xerces-2_9_1/xercesImpl.jar /esup/webapps/probe/WEB-INF/lib
[esup@test]$ rm -rf /tmp/xerces-2_9_1

[esup@test]$ cp /esup/webapps/uPortal/WEB-INF/classes/org/esupportail/portal/utils/filter
/SimpleCASAAuthorizationFilter.class /esup/webapps/probe/WEB-INF/classes/org/esupportail/portal/utils/filter
/SimpleCASAAuthorizationFilter.class

[esup@test]$ vi /esup/webapps/probe/WEB-INF/web.xml

# se reporter à la partie "Les filtres CAS" > "Cassifier le manager Tomcat"
# se reporter à la partie "Les mappings" > "Cassifier le manager Tomcat"
# se reporter à la partie "Le Listener" > "Cassifier le manager Tomcat"
```

Nettoyage web.xml

Supprimer les parties :

- <security-constraint>...</security-constraint>
- <login-config>...</login-config>
- <security-role>...</security-role>