



HOWTO Install and Configure Grouper 2.1.5 on Ubuntu Linux 12.04

23 Giugno 2014

Author: Marco Malavolti, Andrea Biancini

Index

1) Introduction.....	3
2) Packages required.....	3
3) Phase 1 – Installation of Grouper.....	4
3.1) Install the Operating System (Ubuntu 12.04 – Precise Pangolin) on target machines.....	4
3.2) Prepare the environment.....	4
3.3) Install Grouper.....	5
4) Phase 2 – Shibbolize Grouper and add Subjects to DB.....	8
4.1) Install a Shibboleth Service Provider on Grouper machine.....	8
4.2) Add Subjects to Grouper DB.....	9
5) Phase 3 – Install the Grouper VOOT Connector.....	11
5.1) Prepare the environment.....	11
6) Phase 4 – Configure an Attribute Authority on Grouper machine.....	13
7) Phase 5 – Configure a Shibboleth SP to use the “isMemberOf” attribute.....	16
8) Phase 6 – Configure Grouper to release the “isMemberOf” attribute to a Service Provider.....	17

1 Introduction

This is a tutorial for users that want to know how to install Grouper on a Ubuntu Linux 12.04 machine and that want to know how to use the new “isMemberOf” attribute produced.

2 Packages required

- ntp
- vim

3 Phase 1 – Installation of Grouper

3.1 Install the Operating System (Ubuntu 12.04 – Precise Pangolin) on target machines

Install Ubuntu Linux 12.04 on the target machines, from the installation parameters, choose ONLY “Standard system utilities” and “SSH server” to minimize the number of packages to be installed on the target machine.

Configure the network and the name resolution so that the machine reachable with its FQDN (as returned by `hostname -f` command) from the Puppet Agents and the Puppet Master. It can be obtained by editing the `/etc/hosts` file.

Install the following packages and their dependencies:

- `sudo apt-get install vim ntp`

3.2 Prepare the environment

1. Assume the role of root user for all the process steps:

- `sudo su -`

2. Install the required packages and their dependencies:

- `apt-get install python-software-properties`
- `add-apt-repository ppa:webupd8team/java`
- `apt-get update ; sudo apt-get dist-upgrade`
- `apt-get install oracle-jdk7-installer ant tomcat7 dos2unix mysql-server`

3. Configure `JAVA_HOME` for correctly execution of tomcat7:

a) Select the ‘oracle’ version of Java after execute the command:

- `update-alternatives --config java`

b) Add the following line to “`/etc/default/tomcat7`” to set the `JAVA_HOME`:

- `JAVA_HOME="/usr/lib/jvm/java-7-oracle"`

4. Create the Grouper Log directories:

- `mkdir /var/log/grouperUi ; chown tomcat7:tomcat7 /var/log/grouperUi`
- `mkdir /var/log/grouperWs ; chown tomcat7:tomcat7 /var/log/grouperWs`

5. Create the Grouper DB:

- `mysql -u root -p`
- `mysql> create database grouper;`
- `mysql> create user 'grouperdb'@'localhost' identified by '###DB-PASSWORD###';`
- `mysql> grant all on grouper.* to 'grouperdb'@'localhost' identified by '###DB-PASSWORD###';`
- `mysql> flush privileges;`

- `mysql> exit;`

3.3 Install Grouper

1. Download the Grouper installer, extract it and move it in the `/opt` directory:

- `cd /usr/local/src`
- `wget http://software.internet2.edu/grouper/release/2.1.5/grouper.installer-2.1.5.tar.gz`
- `tar xzvf grouper.installer-2.1.5.tar.gz`
- `mv grouper.installer-2.1.5 /opt/grouper`

2. Execute the installer of Grouper:

- `cd /opt/grouper`
- `java -jar grouperInstaller.jar`

3. Answer to the questions as follows:

```
- Enter in the Grouper install directory (note: better if no spaces or special chars) [/usr/local/src/grouper.installer-2.1.5]: /opt/grouper
- Enter the default IP address for checking ports (just hit enter to accept the default unless on a machine with no network, might want to change to 127.0.0.1): [0.0.0.0]: 0.0.0.0
- Do you want to set gsh script to executable (t/f)? [t]: t
- Do you want to run dos2unix on gsh.sh (t/f)? [t]: t
- Do you want to use the default and included hsqldb database (t/f)? [t]: f
- Enter the database URL [jdbc:hsqldb:hsqldb://localhost:9001/grouper]: jdbc:mysql://localhost:3306/grouper
- Database user [sa]: grouperdb
- Database password (note, you aren't setting the pass here, you are using an existing pass, this will be echoed back) [<blank>]: ###DB-PASSWORD###
- Don't care if this message appears:
Checking database with query: select 1
giu 12, 2014 12:20:09 PM edu.internet2.middleware.grouperInstaller.util.GiDbUtils rollbackQuietly
GRAVE: Problem rolling back
com.mysql.jdbc.exceptions.jdbc4.MySQLNonTransientConnectionException: Can't call rollback when autocommit=true
at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)
at sun.reflect.NativeConstructorAccessorImpl.newInstance(NativeConstructorAccessorImpl.java:57)
at sun.reflect.DelegatingConstructorAccessorImpl.newInstance(DelegatingConstructorAccessorImpl.java:45)
at java.lang.reflect.Constructor.newInstance(Constructor.java:526)
at com.mysql.jdbc.Util.handleNewInstance(Util.java:411)
at com.mysql.jdbc.Util.getInstance(Util.java:386)
at com.mysql.jdbc.SQLError.createSQLException(SQLError.java:1013)
at com.mysql.jdbc.SQLError.createSQLException(SQLError.java:987)
at com.mysql.jdbc.SQLError.createSQLException(SQLError.java:982)
```

```
at com.mysql.jdbc.SQLException.createSQLException(SQLException.java:927)
at com.mysql.jdbc.ConnectionImpl.rollback(ConnectionImpl.java:4711)
at edu.internet2.middleware.grouperInstaller.util.GiDbUtils.rollbackQuietly(GiDbUtils.java:419)
at edu.internet2.middleware.grouperInstaller.util.GiDbUtils.listSelect(GiDbUtils.java:403)
at edu.internet2.middleware.grouperInstaller.util.GiDbUtils.listSelect(GiDbUtils.java:323)
at edu.internet2.middleware.grouperInstaller.util.GiDbUtils.select(GiDbUtils.java:334)
at edu.internet2.middleware.grouperInstaller.util.GiDbUtils.checkConnection(GiDbUtils.java:474)
at edu.internet2.middleware.grouperInstaller.GrouperInstaller.checkDatabaseConnection(GrouperInstaller.java:1663)
at edu.internet2.middleware.grouperInstaller.GrouperInstaller.mainLogic(GrouperInstaller.java:1027)
at edu.internet2.middleware.grouperInstaller.GrouperInstaller.main(GrouperInstaller.java:191)
```

It is enough that this message appears "Successfully tested database connection"

- Do you want to init the database (delete all existing grouper tables, add new ones) (t/f)? **t**
- Do you want to add quickstart subjects to DB (t/f)? [t]: **t**
- Do you want to add quickstart data to registry (t/f)? [t]: **t**
- Do you want to start the Grouper loader (daemons)?
(note, if it is already running, you need to stop it now, check ps -ef | grep gsh | grep loader) (t/f)? [f]: **t**
- Do you want to set the tomcat memory limit (t/f)? [t]: **t**
- Do you want to set tomcat scripts to executable (t/f)? [t]: **t**
- Do you want to run dos2unix on tomcat sh files (t/f)? [t]: **t**
- What ports do you want tomcat to run on (HTTP, JK, shutdown): [8080, 8009, 8005]: **8080, 8009, 8005**
- Should we check ports to see if tomcat was able to stop (t/f)? [t]: **t**
- Couldn't find the command 'sh'. Enter the path of 'sh' (e.g. /bin/sh): **/bin/bash**
- Do you want to set the log dir of UI (t/f)? [t]: **t**
- Enter the UI log dir: [/opt/grouper/apache-tomcat-6.0.35/logs/grouperUi]: **/var/log/grouperUi**
- Enter the URL path for the UI [grouper]: **grouper**
- Enter the GrouperSystem password: **###GROUPER-PASSWORD###**
- Do you want to set the GrouperSystem password in /opt/grouper/apache-tomcat-6.0.35/conf/tomcat-users.xml? [t]: **t**
- Should we stop tomcat anyway? (t/f)? [f]: **f**
- Should we check ports to see if tomcat was able to start (t/f)? [t]: **t**
- Do you want to build the Grouper WS? (t/f) [t]: **t**
- Should we check ports to see if tomcat was able to stop (t/f)? [t]: **t**
- Do you want to set the log dir of WS (t/f)? [t]: **t**
- Enter the WS log dir: [/opt/grouper/apache-tomcat-6.0.35/logs/grouperWs]: **/var/log/grouperWs**
- Enter the URL path for the WS [grouper-ws]: **grouper-ws**
- Should we stop tomcat anyway? (t/f)? [f]: **f**
- Should we check ports to see if tomcat was able to start (t/f)? [t]: **t**
- Do you want to install the provisioning service provider (t/f)? [t]: **t**

4. Test the correct execution of Grouper into the default environment by opening the web page:

- `http://###YOUR.GROUPER.FQDN###:8080/grouper/`

5. Remove all unnecessary files:

- `cd /opt/grouper ; rm -rf *.tar ; rm -f *.tar.gz`

6. Edit the `/usr/share/tomcat7/bin/catalina.sh` file by adding this under the “# JAVA_OPTS ...”:

```
JAVA_OPTS="-server -Xmx512M -XX:MaxPermSize=256M"
```

7. Replace the default `tomcat-users.xml` of Tomcat7 with the grouper's ones:

- `cp /opt/grouper/apache-tomcat-6.0.35/conf/tomcat-users.xml /etc/tomcat7/tomcat-users.xml`

8. Edit the `/etc/tomcat7/server.xml` as follows:

```
<Host name="localhost" appBase="webapps"
      unpackWARs="true" autoDeploy="true"
      xmlValidation="false" xmlNamespaceAware="false">
  <Context
docBase="/opt/grouper/grouper.ws-2.1.5/grouper-ws/build/dist/grouper-ws"
path="/grouper-ws" reloadable="false"/>
    <Context docBase="/opt/grouper/grouper.ui-2.1.5/dist/grouper" path="/grouper"
reloadable="false"/>
        ...other things...
</Host>
```

9. Replace “\$” with “#” on the value “`{uiException.class.simpleName}`” into `/opt/grouper/grouper.ui-2.1.5/dist/grouper/WEB-INF/jsp/dynamicTile.jsp` file.

10. Remove the “Log out” from Grouper with:

a) Edit the GrouperUI's “`build.properties`”:

- `vim /opt/grouper/grouper.ui-2.1.5/build.properties`

```
logout.link.show=false
```

b) Edit the GrouperUI's “`media.properties`”:

- `vim /opt/grouper/grouper.ui-2.1.5/dist/grouper/WEB-INF/classes/resources/grouper/media.properties`

```
logout.link.show=false
```

c) Recompile the code with:

- `cd /opt/grouper/grouper.ui-2.1.5 ; ant default`

11. Remove the log's files from their directories to permit to Tomcat7 to write its logs:

- `rm -f /var/log/grouperUi/*`
- `rm -f /var/log/grouperWs/*`

12. Shutdown the Grouper's Tomcat Server to leave place to the Apache Tomcat7 installed:

- `sh /opt/grouper/apache-tomcat-6.0.35/bin/shutdown.sh`

13. Start the Apache Tomcat7 server:

- `service tomcat7 start`

4 Phase 2 – Shibbolize Grouper and add Subjects to DB

4.1 Install a Shibboleth Service Provider on Grouper machine

1. Install a Shibboleth SP and exchange its metadata with your federation.

This SP will authenticate the users via EPPN attribute, then modify the “**shibboleth2.xml**” in this way:

```
...
<ApplicationDefaults entityID="https://grouper.fqdn.example.com/shibboleth"
REMOTE_USER="eppn">
...

```

2. Add AJP support to Tomcat7:

a) Modify the **/etc/tomcat7/server.xml** file by adding this:

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

b) Ensure that the mod “**proxy_ajp**” is enabled:

- `a2enmod proxy_ajp ; service apache2 restart`

3. Create the apache2 site “**/etc/apache2/sites-available/grouper**” with this content:

```
ProxyPass /grouper ajp://localhost:8009/grouper
ProxyPassReverse /grouper ajp://localhost:8009/grouper

ProxyPass /grouper-ws ajp://localhost:8009/grouper-ws
ProxyPassReverse /grouper-ws ajp://localhost:8009/grouper-ws

<Location /grouper>
    AuthType shibboleth
    ShibRequireSession On
    require valid-user
</Location>
```

And enable it:

- `a2ensite grouper ; service apache2 restart`

4.2 Add Subjects to Grouper DB

1. Comment out all the “<security-constraint>”, “<login-config>” and “<security-role>” from /opt/grouper/grouper.ui-2.1.5/dist/grouper/WEB-INF/web.xml.
2. Create the bash script “/root/addSubject.sh” that permits you to add a Subject to Grouper:

```
#!/bin/bash

function ask_param {
    local VALUE=$1
    local NAME=$2

    if [ -z "$VALUE" ]; then
        read -p "Insert the $NAME: " VALUE
    fi

    echo $VALUE
}

EPPN=$(ask_param "$1" "eppn")
NAME=$(ask_param "$2" "name")
SURNAME=$(ask_param "$3" "surname")
EMAIL=$(ask_param "$4" "email")

echo "The provided information for the user to be inserted in Grouper, are as follows:"

echo ""
echo "eppn:      $EPPN"
echo "name:      $NAME"
echo "surname:   $SURNAME"
echo "email:     $EMAIL"
echo ""
echo "Press ENTER to continue or CTRL+C to exit..."
read -p "" DEL

cd /opt/grouper/grouper.apiBinary-2.1.5
./bin/gsh <<EOF
addSubject("$EPPN", "person", "$NAME $SURNAME");
EOF
cd -

#GrouperSession.startRootSession();
#subj = findSubject("horberg@umu.se");
#attr = subj.getAttributes();
#attr.put("loginid", new HashSet(java.util.Arrays.asList(new String[]
{ "horberg@umu.se" })));

mysql -u grouperdb -password=###DB-PASSWORD### grouper <<EOF
insert into subjectattribute values('$EPPN','loginid','$EPPN','$EPPN');
insert into subjectattribute values('$EPPN','description','$NAME
$SURNAME',lower('$NAME $SURNAME'));
insert into subjectattribute values('$EPPN','name','$NAME $SURNAME',lower('$NAME
```

```

$SURNAME' ));
insert into subjectattribute values('$EPPN','email','$EMAIL','$EMAIL');
EOF
cd -

```

3. Create the bash script “**/root/addMemberToSysAdmin.sh**” that permits you to add a Member to the Sysadmin group:

```

#!/bin/bash
function ask_param {
    local VALUE=$1
    local NAME=$2

    if [ -z "$VALUE" ]; then
        read -p "Insert the $NAME: " VALUE
    fi
    echo $VALUE
}
EPPN=$(ask_param "$1" "eppn")

echo "The provided information for the user to be inserted in Grouper, are as follows:"
echo ""
echo "eppn:      $EPPN"
echo ""
echo "Press ENTER to continue or CTRL+C to exit..."
read -p "" DEL

cd /opt/grouper/grouper.apiBinary-2.1.5
./bin/gsh <<EOF
addMember("etc:sysadmingroup", "$EPPN");
EOF
cd -

```

4. Add the right privileges to **addSubject.sh**:

- `chmod +x /root/addSubject.sh /root/addMemberToSysAdmin.sh`

5. Execute the **addSubject.sh** script to add the user stored on you IdP (as many as you want):

- `/bin/bash /root/addSubject.sh`

6. Modify the callLogin path from “**login.to**” to “**home.to**” into “**struts-config.xml**” file:

- `vim /opt/grouper/grouper.ui-2.1.5/dist/grouper/WEB-INF/struts-config.xml`

```

<action path="/callLogin" scope="request"
    type="edu.internet2.middleware.grouper.ui.actions.CallLoginAction"
    unknown="false" validate="false">
    <forward name="callLogin" path="/home.do" redirect="true"/>
</action>

```

7. Edit the **grouper.properties** to be able to edit the system groups:

- `vim /opt/grouper/grouper.ui-2.1.5/dist/grouper/WEB-INF/classes/grouper.properties`

```
configuration.autocreate.system.groups = true
...
groups.wheel.use                       = true
```

8. Restart Tomcat7 service to apply the changes:

- `service tomcat7 restart`

9. Add a created Subject to SysAdmin group:

- `/bin/bash addMemberToSysAdmin.sh`

5 Phase 3 – Install the Grouper VOOT Connector

5.1 Prepare the environment

1. Install subversion on Grouper VM:

- `apt-get install subversion`

2. Download the code of Grouper VOOT Connector into **/usr/local/src**:

- `cd /usr/local/src`
- `svn checkout`
`http://anonsvn.internet2.edu/svn/i2mi/branches/GROUPER_2_0_BRANCH/grouper-misc/grouper-voot/`

3. Modify the “**build.properties**” file created by:

- `cd /usr/local/src/grouper-voot`
- `cp build.example.properties build.properties`
- `vim build.properties:`

```
grouper.dir = /opt/grouper/grouper.apiBinary-2.1.5
grouperWs.dir = /opt/grouper/grouper.ws-2.1.5/grouper-ws
```

4. Execute “**ant**” command to build the jar:

- `ant`

5. Copy the **grouperVoot.jar** into the right position:

- `cp /usr/local/src/grouper-voot/dist/grouperVoot.jar`
`/opt/grouper/grouper.ws-2.1.5/grouper-ws/build/dist/grouper-ws/WEB-INF/lib/grouperVoot.jar`

6. Modify the **source.xml** by removing every “**^M**” character:

- `vim`
`/opt/grouper/grouper.ws-2.1.5/grouper-ws/build/dist/grouper-ws/WEB-INF/classes/sources.xml`

and ensure to see this:

```
<!-- If using emails and need email addresses in sources, set which attribute has
the email address in this source -->
```

```
<init-param>
  <param-name>emailAttributeName</param-name>
  <param-value>email</param-value>
</init-param>
```

7. Setup the Grouper **web.xml**:

- vim
/opt/grouper/grouper.ws-2.1.5/grouper-ws/build/dist/grouper-ws/WEB-INF/web.xml

```
<!-- Add this to filter-mapping -->
<filter-mapping>
  <filter-name>Grouper service filter</filter-name>
  <url-pattern>/voot/*</url-pattern>
</filter-mapping>

<!-- Add this to servlet -->
<servlet>
  <servlet-name>VootServlet</servlet-name>
  <display-name>Voot Servlet</display-name>
  <servlet-class>edu.internet2.middleware.grouperVoot.VootServlet</servlet-class>
  <load-on-startup>1</load-on-startup>
</servlet>

<!-- Add this to servlet-mapping -->
<servlet-mapping>
  <servlet-name>VootServlet</servlet-name>
  <url-pattern>/voot/*</url-pattern>
</servlet-mapping>
```

8. Restart Tomcat server:

- service tomcat7 restart

6 Phase 4 – Configure an Attribute Authority on Grouper machine

1. Download the Shibboleth IdP package from Internet2 and store it into `/usr/local/src` directory:

- `cd /usr/local/src`
- `wget http://www.shibboleth.net/downloads/identity-provider/2.4.0/shibboleth-identityprovider-2.4.0-bin.zip`

2. Install the IdP on the Grouper VM into `/opt/shibboleth-idp` directory:

- `sudo apt-get install unzip ; unzip shibboleth-identityprovider-2.4.0-bin.zip`
- `export JAVA_HOME="/usr/lib/jvm/java-7-oracle"`
- `cd /usr/local/src/shibboleth-identityprovider-2.4.0 ; sh install.sh`

3. Copy the Xerces and Xalan libraries into the right position:

- `cp -r /usr/local/src/shibboleth-identityprovider-2.4.0/endorsed /usr/share/tomcat7`

4. Assign the right privileges by executing this:

- `chown tomcat7 /opt/shibboleth-idp/logs/`
- `chown tomcat7 /opt/shibboleth-idp/metadata/`
- `chown tomcat7 /opt/shibboleth-idp/credentials/`
- `chmod 400 /opt/shibboleth-idp/credentials/idp.key`
- `chmod 644 /opt/shibboleth-idp/credentials/idp.crt`
- `chown tomcat7 /opt/shibboleth-idp/credentials/idp.key`
- `chown tomcat7 /opt/shibboleth-idp/credentials/idp.crt`

5. Deploy the **idp.war** application:

- `vim /etc/tomcat7/Catalina/localhost/idp.xml:`

```
<Context docBase="/opt/shibboleth-idp/war/idp.war"
  privileged="true"
  antiResourceLocking="false"
  antiJARLocking="false"
  unpackWAR="false"
  swallowOutput="true" />
```

6. Modify the `“/etc/apache2/sites-enabled/default-ssl”` by adding the bold text under the VirtualHost:

```
<VirtualHost _default_:443>
  ServerName grouper.fqdn.example.com:443
  ...
  ProxyPass /idp ajp://localhost:8009/idp
  ProxyPassReverse /idp ajp://localhost:8009/idp
```

```
</VirtualHost>
```

7. Copy the “`/etc/apache2/sites-enabled/default-ssl`” to “`/etc/apache2/sites-enabled/default-ssl-8443`” and change all “443” port to “8443”, and add this:

```
<VirtualHost _default_:8443>
  ServerName grouper.fqdn.example.com:8443
  ...
  SSLCertificateFile /opt/shibboleth-idp/credentials/idp.crt
  SSLCertificateKeyFile /opt/shibboleth-idp/credentials/idp.key
  ...
  SSLVerifyClient optional_no_ca
</VirtualHost>
```

8. Add the port 8443 to those that Apache2 listen by editing the “`/etc/apache2/ports.conf`” file:

```
Listen 8443
NameVirtualHost *:8443
```

9. Install `mysql-java-connector`:

- `sudo apt-get install libmysql-java`
- `cp /usr/share/java/mysql-connector-java-5.1.16.jar /opt/shibboleth-idp/lib`
- `cp /usr/share/java/mysql-connector-java-5.1.16.jar /var/lib/tomcat7/common`

10. Restart the Tomcat7 and Apache2 service:

- `service tomcat7 restart`
- `service apache2 restart`

11. Configure the IdP to retrieve the federation’s metadata that contain the Grouper SP Metadata

12. Modify the “`attribute-resolver.xml`” by adding:

- A new DataConnector:

```
<!-- Grouper Database connector -->
<resolver:DataConnector xsi:type="RelationalDatabase"
xmlns="urn:mace:shibboleth:2.0:resolver:dc" id="grouper">
  <ApplicationManagedConnection jdbcDriver="com.mysql.jdbc.Driver"
    jdbcURL="jdbc:mysql://localhost:3306/grouper"
    jdbcUserName="grouperdb"
    jdbcPassword="geantdbpassword" />
  <QueryTemplate>
    <![CDATA[
      SELECT REPLACE(GROUP_NAME,
CONCAT(SUBSTRING_INDEX(SUBSTRING_INDEX('$requestContext.getPeerEntityId()', '/',
-1), '/', 1), ':'), '') AS GROUP_NAME FROM grouper_memberships_lw_v WHERE subject_id
= '$requestContext.principalName' AND GROUP_NAME LIKE
```

```

CONCAT(SUBSTRING_INDEX(SUBSTRING_INDEX('$requestContext.getPeerEntityId()', '/',
-1), '/', 1), '%') AND list_name = 'members'

    ]]>
</QueryTemplate>

    <Column columnName="GROUP_NAME" attributeID="isMemberOf" type="String" />
</resolver:DataConnector>

```

- A new AttributeDefinition:

```

<!-- AttributeDefinition for "isMemberOf" attribute -->
<resolver:AttributeDefinition id="isMemberOf" xsi:type="ad:Simple"
sourceAttributeID="isMemberOf">
    <resolver:Dependency ref="grouper" />
    <resolver:DisplayName xml:lang="en">Grouper groups</resolver:DisplayName>
    <resolver:DisplayName xml:lang="it">Gruppi Grouper</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">List of groups retrieved from
Grouper</resolver:DisplayDescription>
    <resolver:DisplayDescription xml:lang="it">Elenco dei gruppi ottenuti da
Grouper</resolver:DisplayDescription>
    <resolver:AttributeEncoder xsi:type="enc:SAML1String"
name="urn:mace:dir:attribute-def:isMemberOf" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
name="urn:oid:1.2.840.113556.1.666.1" friendlyName="isMemberOf" />
</resolver:AttributeDefinition>

```

- A change to the Principal Connector:

```

<!-- ===== -->
<!--      Principal Connectors      -->
<!-- ===== -->

<!--
    <resolver:PrincipalConnector xsi:type="pc:Transient" id="shibTransient"
nameIDFormat="urn:mace:shibboleth:1.0:nameIdentifier"/>

    <resolver:PrincipalConnector xsi:type="pc:Transient" id="saml1Unspec"
nameIDFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>

    <resolver:PrincipalConnector xsi:type="pc:Transient" id="saml2Transient"
nameIDFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
-->

    <resolver:PrincipalConnector xsi:type="pc:Direct" id="saml1Direct"
nameIDFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>

    <resolver:PrincipalConnector xsi:type="pc:Direct" id="saml2Direct"
nameIDFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified"/>

```

13. Modify the “**attribute-filter.xml**” of Grouper IdP by adding this:

```

<afp:AttributeFilterPolicy id="sp-test-4-grouper">
    <afp:PolicyRequirementRule xsi:type="basic:AttributeRequesterString"
value="https://sp-test-grouper.example.com/shibboleth" />
    <afp:AttributeRule attributeID="isMemberOf">
        <afp:PermitValueRule xsi:type="basic:ANY"/>
    </afp:AttributeRule>

    <afp:AttributeRule attributeID="eduPersonPrincipalName">

```



```
<afp:PermitValueRule xsi:type="basic:ANY" />  
</afp:AttributeRule>  
</afp:AttributeFilterPolicy>
```

14. Don't restart Tomcat7 before the end of Phase 5 !!!!

7 Phase 5 – Configure a Shibboleth SP to use the “isMemberOf” attribute

1. Install and Configure a Shibboleth SP (`sp-test-grouper.example.com`) and exchange its metadata with Grouper AA and Federation.
2. Modify the “**shibboleth2.xml**” by adding this AttributeResolver:

```
<!-- Use a SAML query if no attributes are supplied during SSO. -->
<AttributeResolver type="Query" subjectMatch="true"/>
  <AttributeResolver type="SimpleAggregation" attributeId="eppn"
    format="urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified">
    <Entity>https://grouper.fqdn.example.com/idp/shibboleth</Entity>
  </AttributeResolver>
```

3. Edit the “**attribute-map.xml**” to resolve the new attribute “**isMemberOf**”:

```
<Attribute name="urn:oid:1.2.840.113556.1.666.1" id="isMemberOf"/>
```

4. Restart the “**shibd**” service:
 - `service shibd restart`
5. Restart Tomcat7 on Grouper machine
6. Configure the Federation's IdPs to release the “**eduPersonPrincipalName**” of their users to the Grouper Application/SP.

NOTES:

The Federation's IDPs must know, by metadata exchange, the Grouper SP and the other SPs.

The Federation's Sps must know, by metadata exchange, the Grouper AA and the other IdPs.

8 Phase 6 – Configure Grouper to release the “isMemberOf” attribute to a Service Provider

1. Open <https://#YOUR.GROUPER.FQDN#/grouper> and, working as Admin:
 - Create a new Folder that have as FolderID the FQDN of the SP to which Grouper will give the *isMemberOf* attribute:

My tools

- Explore
- Search
- Folder workspace
- Group workspace
- Entity workspace
- Group types
- Lite UI
- Help

EXPLORE

Create folder

Current location is:
 Root

Folder name	A Folder Title that indicate your service
Folder ID	your.relying.party.fqdn
Description	A brief Description of the Folder

[Back to Manage folders](#)

- Create a new group into that folder and add a member (you) by searching your surname:

[Add to Folder workspace](#)
[Edit folder](#)
[Create folder](#)
[Create group](#)
[Moves and Copies](#)
[Audit log](#)

Name	An extended name for your new Group
ID	id-4-new-group
Alternate ID Path	
Description	Brief description of Group
Assign privileges to everyone	<input type="checkbox"/> admin <input type="checkbox"/> update <input checked="" type="checkbox"/> read <input checked="" type="checkbox"/> view <input type="checkbox"/> optin <input type="checkbox"/> optout
Select group types	<input type="checkbox"/> grouperLoader <input type="checkbox"/> teaching <input type="checkbox"/> mailingList

[Delete](#)
[Add to Group workspace](#)
[Edit group](#)
[Manage members](#)
[Add members](#)
[Manage members lite](#)
[Move group](#)
[Copy group](#)

[Audit log](#)
[View entity details](#)

This permits to Grouper to release the **isMemberOf** attribute to the **your.relying.party.fqdn**.

2. Try to login on a simple application protected by the SP for which you have created a directory into Grouper and see if the attribute “**isMemberOf**” is release by checking the **/Shibboleth.sso/Session** page of your SP.

```
Attributes  
affiliation: 1 value(s)  
cn: 1 value(s)  
displayName: 1 value(s)  
eppn: 1 value(s)  
givenName: 1 value(s)  
isMemberOf: 1 value(s)
```