

Table of Contents

Installation, upgrade and configuration of gLite VOMS 3.1 Patch 1629.....	1
1 Installation.....	1
1.1 Repositories setup.....	1
gLite repository.....	1
(a).....	1
DAG repository.....	1
JPACKAGE repository.....	1
CA repository.....	2
1.2 Software installation.....	2
1.2.1 Install CA RPMs.....	2
1.2.2 Install JRE 1.5.....	2
1.2.3 Install VOMS server packages.....	2
1.2.4 Install database software.....	2
(a) Mysql.....	3
1.2.5 Install the host certificate and key files.....	3
2 Database upgrade (only if you are upgrading a gLite VOMS 3.0 server).....	3
3 Configuration.....	4
3.1. Edit the VOMS server configuration files in /opt/glite/etc/config.....	4
3.2. Run the configuration process.....	5
3.3. Start the configured server.....	5
3.4. Check the Access control lists for each VO.....	5
4 Known issues.....	5
4.1. Database upgrade problems when migrating ACL data.....	5
4.2. Exception thrown when upgrading VOMS 1.2 database.....	6

Installation, upgrade and configuration of gLite VOMS 3.1 Patch 1629

1 Installation

1.1 Repositories setup

In order to install the glite-VOMS_mysql/glite-VOMS_oracle server you need to enable the following repositories

- gLite
- DAG
- Jpackage
- CA

via the corresponding yum repository files (see below)

gLite repository

(a)

```
[voms-mysql]
name=gLite 3.1
baseurl=http://grid-deployment.web.cern.ch/grid-deployment/glite/pps/3.1/glite-VOMS_mysql/s14/i38
enabled=1
protect=0
```

(b) Oracle

```
[voms-oracle]
name=gLite 3.1
baseurl=http://grid-deployment.web.cern.ch/grid-deployment/glite/pps/3.1/glite-VOMS_oracle/s14/i38
enabled=1
protect=0
```

DAG repository

```
[dag]
name=DAG rpms
baseurl=http://linuxsoft.cern.ch/dag/redhat/el4/en/$basearch/dag/
enabled=1
gpgcheck=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-dag
```

JPACKAGE repository

```
[jpackage17-generic]
name=JPackage 1.7, generic
baseurl=http://mirrors.dotsrc.org/jpackage/1.7/generic/free/
enabled=1
protect=1
gpgkey=http://www.jpackage.org/jpackage.asc
gpgcheck=1
```

```
[jpackage17-generic-nonfree]
name=JPackage 1.7, generic non-free
baseurl=http://mirrors.dotsrc.org/jpackage/1.7/generic/non-free/
enabled=1
```

```
protect=1
gpgkey=http://www.jpac.org/jpac.asc
gpgcheck=1
```

```
[jpackage5-generic]
name=JPackage 5, generic
baseurl=http://mirrors.dotsrc.org/jpackage/5.0/generic/free/
enabled=1
protect=1
gpgkey=http://www.jpac.org/jpac.asc
gpgcheck=1
```

```
[jpackage5-generic-nonfree]
name=JPackage 5, generic non-free
baseurl=http://mirrors.dotsrc.org/jpackage/5.0/generic/non-free/
enabled=1
protect=1
gpgkey=http://www.jpac.org/jpac.asc
gpgcheck=1
```

CA repository

```
[lcg-ca]
name=LCG CAs
baseurl=http://linuxsoft.cern.ch/LCG-CAs/current
enabled=1
gpgcheck=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-dag
```

1.2 Software installation

To install the necessary parts to run a glite-VOMS server you need to the following steps:

1.2.1 Install CA RPMs

```
yum install lcg-CA
```

1.2.2 Install JRE 1.5

Follow the steps described here

<https://twiki.cern.ch/twiki/bin/view/EGEE/GLite31JPackage>

1.2.3 Install VOMS server packages

(a) for Mysql backend

```
yum install cert-glite-VOMS_mysql
```

(b) for Oracle database backend

```
yum install cert-glite-VOMS_oracle
```

Note: This will install also Tomcat 5.5 from JPackage as a dependency.

1.2.4 Install database software

(a) Mysql

Database client only

```
yum install mysql
```

Database server and client

```
yum install mysql-server
```

The password for the root account should be set

```
/usr/bin/mysqladmin -u root password <password>
```

```
/usr/bin/mysqladmin -u root -h <hostname> password <password>
```

(b) Oracle

Database client

Download from the Oracle's website and install:

- oracle-instantclient-basic-10.2.0.3-1.i386.rpm
- oracle-instantclient-jdbc-10.2.0.3-1.i386.rpm

Database server

Refer to Oracle's documentation

1.2.5 Install the host certificate and key files

Make sure to place the two files in the target node into the directory and check the access right hostkey.pem only readable by root and the certificate readable by everybody.

```
/etc/grid-security
```

2 Database upgrade (only if you are upgrading a gLite VOMS 3.0 server)

gLite VOMS Server 3.1 ships with VOMS-ADMIN 2, which uses a new database schema. The old VO databases should be upgraded for VOMS 3.1

!!! You are strongly advised to backup your database before doing the upgrade !!! (see known issue 4.1)

The database upgrade program is part of VOMS-ADMIN 2 which is now installed on you new server.

!!! The database upgrade will work only if you use the latest database schema in production from gLite VOMS 3.0 !!!

Please also check the known issues before embarking on the upgrade - **pay particular attention to the advice about ACLs.**

Before proceeding with the database upgrade you should decide whether you want to keep the old database instance or to create a new one. If you run VOMS 3.0 with a MySQL database backend on the same machine you will probably want to use a new database instance on the 3.1 VOMS host. In this case you can copy the

database and then run the database upgrade script against the new instance.

- dump the old database

```
mysqldump -h <OLD_HOSTNAME> -u <PRIV_USER> -p --databases <DATABASE_NAME> > <DUMP_FILENAME>
```

- use the dump to create the new database

```
mysql -h <NEW_HOSTNAME> -u <PRIV_USER> -p < <DUMP_FILENAME>
```

- grant ALL PRIVILEGES to the user that the VOMS 3.1 instance will use to connect and use the database

```
mysql -h <NEW_HOSTNAME> -u <PRIV_USER> -p
```

```
mysql> GRANT ALL PRIVILEGES ON <DATABASE_NAME> TO <VOMS_USER>@localhost IDENTIFIED BY '<VOMS_PASSWORD>'
```

Follow these steps to upgrade the databases:

- Go to /var/glite/etc/voms-admin on the old VOMS 3.0 server and copy all subdirectories named after the VOs you want to upgrade to the server in the same place.
- In each of these subdirectories check the voms.database.properties file. It contains the database connection parameters. Edit these on the new 3.1 server if needed (the should point to the database you want to upgrade).
- Set the following variables with the appropriate values

```
export GLITE_LOCATION=/opt/glite
export GLITE_LOCATION_VAR=/var/glite
export GLITE_LOCATION_LOG=/var/log/glite
```

- Execute (bug 34112, <http://savannah.cern.ch/bugs/?34112>)

```
sed -i -e 's/@WEBUI.ENABLED@/WEBUI.ENABLED/' /opt/glite/etc/voms-admin/templates/voms.servi
```

- For each VO database you want to upgrade run:

```
/opt/glite/sbin/voms-admin-configure --vo=<VO_NAME> upgrade
```

Before this make sure your database is not in use by someone else. This script modifies the

- Execute

```
sed -i -e 's/WEBUI.ENABLED/@WEBUI.ENABLED@/' /opt/glite/etc/voms-admin/templates/voms.servi
```

You should complete successfully all database upgrades before running the VOMS configuration script (glite-voms-server-config.py).

3 Configuration

3.1. Edit the VOMS server configuration files in /opt/glite/etc/config

The RGMA cofiguration is not needed as opposed to the previous version. The RGMA client and servicetool are not configured on the VOMS server any more.

If you are doing an upgrade, you could use the old configuration files but pay attention to the following variables

- JAVA_HOME (in glite-global.cfg.xml)
- CATALINA_HOME (in glite-global.cfg.xml)
- tomcat.user.name (in glite-global.cfg.xml)
- tomcat.user.group (in glite-global.cfg.xml)
- voms.db.oracle.instantclient.location (in glite-voms-server.cfg.xml, if using Oracle backend)
- make sure you use the desired database connection parameters for the VOs (in vo-list.xml)

3.2. Run the configuration process

```
/opt/glite/etc/config/scripts/glite-voms-server-config.py --configure
```

3.3. Start the configured server

```
/opt/glite/etc/config/scripts/glite-voms-server-config.py --start
```

3.4. Check the Access control lists for each VO

Go to the VOMS-ADMIN web interface for each of your VOs

(https://SERVER_NAME:8443/voms/VO_NAME by default) and check the access control lists.

VOMS-ADMIN 2 has a redesigned security model. The Global ACL List is now deprecated. Grant to any authenticated user "Container rights: Read permission" and "Membership rights: Read permission" for the top group and all other subgroups that should be visible to the relevant grid hosts for the gridmap file generation.

4 Known issues

4.1. Database upgrade problems when migrating ACL data

Database upgrade procedure failures were observed during the ACL migration phase on Oracle. These problems are not fully understood yet. It was found out that they are non-deterministic (database containing the same ACL entries sometimes upgrades fine and sometimes not). One of the suspicions is that the order in which the database upgrade code processes the entries leads to different results. This behaviour was observed with ACL entries that grant a specific right (add, create, remove, delete, etc.) for a specific user (DN/CA pair), and has only been observed on Oracle. Despite the rare occurrence of this bug it is dangerous because

!!! if the upgrade program fails the database is left in an inconsistent state !!!

You would have to restore the database and remove the offending ACL. Therefore **it is recommended that you remove your custom ACL entries before upgrading the database**. This can be done from the voms-admin web interface.

Just leave the standard entries in the Global ACL list:

```
Allow    all    The Local Database Administrator
Allow    all    Anyone with role /<VO_NAME>/Role=VO-Admin
Allow    all    <VOMS_HOST_SUBJECT>    <VOMS_HOST_CA_SUBJECT>
Allow    all    <DEFAULT_ADMIN_SUBJECT>    <DEFAULT_ADMIN_CA_SUBJECT>
```

and remove the rest (in the Global ACL and those created for groups and roles).

!!! Please backup your database before doing the upgrade !!!

4.2. Exception thrown when upgrading VOMS 1.2 database

<https://savannah.cern.ch/bugs/?34112>

This topic: EGEE > Glite31VOMSp1629

Topic revision: r2 - 2008-03-16 - DimitarShiyachki



Copyright &© by the contributing authors. All material on this collaboration platform is the property of the contributing authors.

Ideas, requests, problems regarding TWiki? Ask a support question or Send feedback