JAVA based portable GRID storage access tools installation (no root access required)

For the impatient: skip text and jump to the installation walk-through. (Assumes you have a grid certificate available and have been placed in the VOMS /lofar/user group.)

Installation of grid middleware used to be quite challenging although their is now often reasonable support via linux installation packages (see e.g. the page on SRM software installation. It is however possible to deploy the required client tools without the need for root access and reasonably independent of the OS, The setup below has been tested on Kubuntu 12.10 and Mac OS X 10.6.8. Since all programs are JAVA based, it is very likely that these packages can be made to work on other systems as well. However, the tools would require customized scripts as provided in the (s)bin directories.

General requirements

Given the title of this page, it is obviously necessary to start with a system with a JAVA VM installed (1.5 or higher). NB Since there is a known issue for the dCache/FNAL SRM client tools on openjdk-7, it may be required to install an alternative JVM than the system default and point `JAVA_HOME` to the alternative location.

The key elements in any minimal installation are:

- A valid (personal) grid certificate.
- Functionality to generate a proxy with VOMS attributes
- Functionality to initiate data transfers using SRM and the gsiftp protocol

Below, we will take a detailed look at each individual element.

Grid certificate

The procedure for obtaining a personal grid certificate is described here. The default locations for the private key and the signed certificate are respectively `$HOME/.globus/userkey.pem` and `$HOME/.globus/usercert.pem`. Alternative locations may be used but should than be configured by setting appropriate values for the `X509_USER_KEY` and `X509_USER_CERT` environment variables.

NB It is not required to store the personal certificate on the system that has the SRM clients installed. These clients only require a valid 'proxy' generated from the certificate and it is perfectly possible to generate the proxy elsewhere and copy it to the SRM client system using e.g. `scp` or 'MyProxy' (to be further documented).

Note on security: By whatever means the certificate and/or proxy are generated, it is critical that the private key (stored as `userkey.pem` or in any other form) and the generated proxy (see below) are kept secure. These files should have set read/write access for only the owner (e.g. `chmod 600 userkey.pem`) and it is good practice to be very restrictive regarding the creation of copies, in

particular on shared systems. In addition, the private key should always be secured by setting a (good) encryption password when it is generated.

Proxy generation

To generate a proxy with VOMS attributes from the personal certificate, the `proxy-init.sh` script provided by jLite can be used. The package includes a manual in the 'doc' subdirectory. To allow setting of VOMS attributes for the LOFAR VO (Virtual Organisation), there are three additional steps to take:

- Create a `vomses` file to allow `proxy-init` to contact the relevant VOMS server
- Create a file that contains the certificate chain for authentication of the VOMS server
- Install the set of trusted grid Certificate Authority (CA) certificates (these are also required by the SRM tools).

The 'vomses' file

To allow generation of proxies with LOFAR voms attributes, a 'vomses' file must exist that contains at least the following line:

```
"lofar" "voms.grid.sara.nl" "30019"
"/O=dutchgrid/O=hosts/OU=sara.nl/CN=voms.grid.sara.nl" "lofar"
```

jLite expects this file to be located at `$JLITE_HOME/etc/vomses`, in the location pointed to by the `$VOMS_USERCONF` environment or in the default 'gLite' locations, usually: `$HOME/.glite/vomses`

VOMS server certificate chain

To allow the proxy generator to check the authenticity of the voms server, the chain of certificates for the the VOMS server must be provided in a file named '<voms_server_address>.lsc'. This file must be placed in a subdirectory with the name of the virtual organization which is placed in the VOMS directory (see below). For the lofar VO, this file is `lofar/voms.grid.sara.nl.lsc` which should contain the following lines:

```
/O=dutchgrid/O=hosts/OU=sara.nl/CN=voms.grid.sara.nl
/C=NL/O=NIKHEF/CN=NIKHEF medium-security certification auth
```

The default VOMS directory for jLite is `$JLITE_HOME/etc/certs/voms`. An alternative location can be configured by setting the `$X509_VOMS_DIR` environment value and if neither locations contains a valid configuration, jLite will also look in the default (system-wide) gLite location `/etc/grid-security/vomsdir` directory.

Trusted grid CA certificates

If your system has been installed with grid software already, it is likely that the trusted CA certificates

can be found in the default directory `/etc/grid-security/certificates`. If this is not the case, or you receive error messages related to not being able to determine the authenticity of a certificate, you can retrieve the latest certificates, e.g. from EUGridPMA, and place them in a directory of your choosing. jLite will expect them in the directory `$JLITE_HOME/etc/certs/ca` but will also look in the directory set by the `$X509_CERT_DIR` variable or in the default system wide directory.

Prepackaged tarball

The jLite with lofar voms tarball comes prepackaged with the above as required to access the LOFAR VO. The executable files are in the `jlite-0.2/cli` subdirectory. The relevant commands are `proxy-init.sh` for generating a proxy and `proxy-info.sh` for inspecting the generated proxy.

SRM client tools

There are (at least) two JAVA based packages that provide the required SRM client functionality, including support for the gsiftp (a.k.a. 'gridftp') protocol. One has been developed by Fermilab and is hosted by dCache. Another has been developed at Berkeley.

NB If the client srm copy call returns timeout messages, the most likely cause is that a firewall is blocking outward connections. The following ports are typically needed by the srm client tools: 8443/8444, 2811, and any port in the gridftp port range (typically in the range 20000 - 25000). Note that these ports are configured on the server side so this list may not be complete for all situations. If at all possible, it is advisable to configure the firewall to allow all outward connections. The next best option is to allow all outward connections to the domains that provide LOFAR LTA services (currently grid.sara.nl, fz-juelich.de, and target.rug.nl)

NB2 If you want to enable 'active' transfers, firewalls should allow incoming access to the ports configured as the globus port range (look in client documentation for more details). This type of transfer can improve performance as it will use multiple parallel connections for retrieving a file. For the FNAL/dCache client, 'active' transfers are initiated if the `-server_mode=passive` setting is omitted. For the Berkely client, parallel transfers will be initiated when the `-parallelism` parameter is set to a value larger than 1. Since in most cases LOFAR datasets consist of a large number of files, a similar performance improvement can be achieved by splitting the set of files over multiple srm copy processes.

FNAL/dCache client tools

We provide a slightly modified package: srm client tools. This contains updated scripts that allow installation in any directory. The tarball can be unpacked anywhere after which the `$SRM_PATH` environment variable should be set to the root directory of the unpacked tarball. Additionally, the `$SRM_PATH/bin` directory should be added to `$PATH` and trusted CA certificates must be installed. Finally, a valid proxy must be available in the default grid location (`/tmp/x509up_u<UID>`) or in the location configured as `$X509_USER_PROXY`. Note that jLite does not store the proxy in the default grid location so an appropriate setting of the environment is required for it. You should now be able to retrieve a file from the LOFAR LTA:

```
srmcp -server_mode=passive
srm://srm.grid.sara.nl/pnfs/grid.sara.nl/data/lofar/ops/fifotest/file1M
file:///`pwd`/file1M
```

Berkeley client tools

The Berkely client tools can be downloaded from the bestman repository. After unpacking, perform:

```
cd bestman-client/setup
./configure  --enable-clientonly
cd ..
export PATH=`pwd`/bin:$PATH
```

Just like for the FNAL/dCache client tools, trusted CA certificates must be installed and a valid proxy must be available in the default grid location (`/tmp/x509up_u<UID>`) or in the location configured as `$X509_USER_PROXY`.

Note that the Berkeley client tools work slightly different as compared to the FNAL/dCache client tools. Most notably, they require explicit setting of the server 'WSDL' url which for dCache installations is the host URL, including port, plus the path `srm/managerv2`, e.g.:

```
srm-copy
srm://srm.grid.sara.nl/pnfs/grid.sara.nl/data/lofar/ops/fifotest/file1M
file:///`pwd`/file1M  -serviceurl srm://srm.grid.sara.nl:8443/srm/managerv2
```

Walkthrough

This walkthrough utilizes the FNAL/dCache SRM client tools and assumes a bash-like shell is used for setting the environment variables..

- Store your private key in `$HOME/.globus/userkey.pem`
- Execute:

  ```
  chmod 600 $HOME/.globus/userkey.pem
  ```

- Store your signed certificate in `$HOME/.globus/usercert.pem`
- Download jLite with lofar voms
- Untar package in directory of your choosing:

  ```
  tar -xvzf jlite-0.2-lofar-vo.tgz
  ```

- Update path:

  ```
  export PATH=`pwd`/jlite-0.2/cli:$PATH
  ```

- Set CA certificate environment variable (required by srm tools):

```
export X509_CERT_DIR=`pwd`/jlite-0.2/etc/certs/ca
```

- Generate a proxy:

```
proxy-init.sh lofar:/lofar/user
```

- Set proxy environment variable to location provided in 'Proxy location: <proxy_location>':

```
export X509_USER_PROXY=<proxy_location>
```

- Download srm client tools
- Untar package in directory of your choosing:

```
tar -xvzf srm.tar.gz
```

- Set srm path variable:

```
export SRM_PATH=`pwd`/srm
```

- Update path:

```
export PATH=$SRM_PATH/bin:$PATH
```

- Test data retrieval:

```
srmcp -server_mode=passive
srm://srm.grid.sara.nl/pnfs/grid.sara.nl/data/lofar/ops/fifotest/file1M
file:///file1M
```

- Done! *NB You will off course need to put all `export` commands (with full paths where appropriate) in a shell start-up script to make them permanent.*

These are the shell commands you have to use for (t)csh:

```
> setenv mypath `pwd`
> setenv PATH ${mypath}/jlite-0.2/cli:${PATH}
> setenv X509_CERT_DIR ${mypath}/jlite-0.2/etc/certs/ca
> proxy-init.sh lofar:/lofar/user
Enter your private key passphrase:
Created VOMS proxy: O=dutchgrid,O=users,O=astron,CN=User,CN=proxy
Proxy is valid until: Tue Jun 25 04:29:11 2013 CEST
Proxy location:
/var/folders/kp/jvqqvjyd3k119ryygxm3qlpm0000gn/T/x509up_u_user

> setenv X509_USER_PROXY
/var/folders/kp/jvqqvjyd3k119ryygxm3qlpm0000gn/T/x509up_u_user
> setenv SRM_PATH ${mypath}/srm
> setenv PATH ${mypath}/srm/bin:${PATH}
```