MyProxy Server: installation, configuration & testing

Giuseppe La Rocca

INFN – Catania

giuseppe.larocca@ct.infn.it

EMBRACE-EGEE Tutorial

www.eu-egee.org

Outline

- **Why MyProxy ?**
  - Proxy Renewal mechanism
- **MyProxy Server Installation.**
  - Yaim profiles
  - Metapackage installation and configuration
- **Testing MyProxy Server.**
  - myproxy-init -s <myproxy server>
  - myproxy-get-delegation –s <myproxy server>

Long term proxy

- Proxy has limited lifetime (default is 12 h)
  - Long jobs may outlive the validity of the initial proxy; if happens the job will die prematurely.
  - To solve this WMS allows proxies to be renewed automatically if user's credentials are stored on a myproxy server (*proxy renewal service*).
- When a user's proxy is going to expire, proxy renewal daemon contacts MyProxy server and performs credentials renew
- For proxy renewal service user has to store credential using the command:

```
myproxy-init -s <server> -t <hours> -d -n
```

and specify which MyProxy server has to be contacted in jobs JDL: MyProxyServer = “grid001.ct.infn.it”;

Installing the MyProxy Server

Installation pre-requisites

- Start from the Virtual Machine Base that you can download from :

  `https://gilda.ct.infn.it/GILDAVM/GILDAVM_Base.tar.bz2`

- Verify that these packages are installed and properly configured:
  - Java SDK 1.4.2 (or greater)
  - edg_VO_Gilda rpm `(https://gilda.ct.infn.it/RPMS/)`
  - glite-yaim-3.0.0

    `(http://glitesoft.cern.ch/EGEE/gLite/APT/R3.0/rhel30/RPMS.Release3.0/)`
  - gilda_ig-yaim-3.0.0

    `(http://grid018.ct.infn.it/apt/gilda_app-i386/utils/)`

Install host certificates

- Request host certificates for the MyProxy Server to a CA
  - https://gilda.ct.infn.it/CA/mgt/restricted/srvreq.php
- Copy host certificate (hostcert.pem and hostkey.pem) in `/etc/grid-security`
- Change the permisions
  - `chmod 644 hostcert.pem`
  - `chmod 400 hostkey.pem`

Java SDK Installation

- Because of SUN licence used for Java SDK, it is not possible to redistribute it with the middleware.
- You have to download Java SDK 1.4.2 from Sun web site:

  http://java.sun.com/j2se/1.4.2/download.html
- Select ``Download J2SE SDK", and download the ``RPM in self-extracting file". Follow the instruction on the pages to extract the rpm.

Node Configuration

- A general requirement for the gLite nodes is that they are synchronized.
- Configure the file `/etc/ntp.conf` by adding the lines dealing with your time server configuration such as, for instance:

```
# Prohibit general access to this service.
restrict default ignore
restrict 193.206.144.10 mask 255.255.255.255
  nomodify notrap noquery

server  127.127.1.0     # local clock
fudge   127.127.1.0 stratum 10
server ntp-1.infn.it
```

Node Configuration

- Edit the file `/etc/ntp/step-tickers` adding a list of your time server(s) hostname(s)

```
cat /etc/ntp/step-tickers
193.206.144.10
```

- # If you are running a kernel firewall, you will have to allow inbound communication on the NTP port.
- If you are using iptables, you can add the following to `/etc/sysconfig/iptables`

```
-A INPUT -s <NTP-serverIP-1> -p udp --dport 123 -j
 ACCEPT
```

- You can then reload the firewall : `/etc/init.d/iptables restart`

Node Configuration

- Activate the ntpd service with the following commands:

```
# ntpdate <your ntp server name>
# service ntpd start
# chkconfig ntpd on
```

- You can check ntpd's status by running the following command :

```
# ntpq -p
```

Install glite-yaim and gilda_ig-yaim

- Download and install latest version of glite-yaim-3.0.0 -* on your machine

  http://glitesoft.cern.ch/EGEE/gLite/APT/R3.0/rhel30/RPMS.Release3.0/glite-yaim-3.0.0-11.noarch.rpm

- Download and install the latest version of gilda_ig-yaim-3.0.0 -* on your machine

  http://grid018.ct.infn.it/apt/gilda_app-i386/utils/gilda_ig-yaim-latest

- glite-yaim and gilda_ig-yaim provide a set of bash ``mini-scripts". Each ``mini-script" implements one bash function and it is stored in file with the same name of the function. Each function configures a specific middleware module. The functions are stored in the two directories:

  /opt/glite/yaim/functions (glite-yaim functions)
  /opt/glite/yaim/functions/local (gilda_ig-yaim functions)

Customize gilda_ig-site-info.def

- Copy the yaim configuration template file into the root dir:

```
cp /opt/glite/yaim/examples/gilda_ig-site-info.def
/root/my-site-info.def
```

- Open `/root/my-site-info.def` file using a text editor and set the following values according to your grid environment:

```
MY_DOMAIN=<your DOMAIN>
PX_HOST=grid001.ct.infn.it
MON_HOST=rgmasrv.ct.infn.it
REG_HOST=rgmasrv.ct.infn.it
NTP_HOSTS="193.206.144.10"
```

Customize gilda_ig-site-info.def

For this tutorial substitute grid018.ct.infn.it/rep with 192.168.0.50

```
OS_REPOSITORY="rpm
  http://grid018.ct.infn.it/rep slc306-i386 os
  updates extras"
LCG_REPOSITORY="rpm
  http://grid018.ct.infn.it/rep glite_sl3-i386
  3_0_0 3_0_0_externals 3_0_0_updates"
IG_REPOSITORY="rpm
  http://grid018.ct.infn.it/rep ig_sl3-i386
  3_0_0 utils"
GILDA_REPOSITORY="rpm
  http://grid018.ct.infn.it/rep gilda_app-i386
  app 3_0_0"
CA_REPOSITORY="rpm
  http://grid018.ct.infn.it/rep glite_sl3-i386
  security"
```

Customize gilda_ig-site-info.def

- **Check/Modify VO and VOMS specific configurations:**

```
VOS=“gilda ..”
ALL_VOMS=“gilda ..”
```

Customize gilda_ig-site-info.def

```
#Specific VO settings
VO_GILDA_SW_DIR=$VO_SW_DIR/gilda
VO_GILDA_DEFAULT_SE=$DPM_HOST
VO_GILDA_STORAGE_DIR=$CLASSIC_STORAGE_DIR//gilda
VO_GILDA_QUEUES="short long infinite"
VO_GILDA_VOMS_SERVERS="vomss://voms.ct.infn.it:8443/voms
/gilda?/gilda"VO_GILDA_VOMSES="'gilda voms.ct.infn.it
15001 /C=IT/O=GILDA/OU=Host/L=INFN
Catania/CN=voms.ct.infn.it/Email=emidio.giorgio@ct.infn.
it gilda'“

JAVA_LOCATION=“/usr/java/j2sdk1.4.2_12/”
```

MyProxy Installation

- We are ready to install the MyProxy Server:

```
/opt/glite/bin/gilda_ig_install_node
/root/my-site-info.def GILDA_ig_PX
```

- This command will download and install all the needed packages

- Now we can configure the node:

```
/opt/glite/bin/gilda_ig_configure_node
/root/my-site-info.def GILDA_ig_PX
```

MyProxy Settings

- Because of a bug in the gLte Middleware we have to fix the myproxy exec script
  - Edit `/etc/init.d/myproxy`
  - Comment the following lines
    - `{GLOBUS_LOCATION}/libexec/globus-script-initializer`
    - `{libexecdir}/globus-sh-tools.sh`
    - `MKCONFIG="/etc/rc.d/init.d/myproxy-generate-config.pl $CERTDIR $X509_USER_CERT ...`
  - Change the MYPROXY variable with
    - `MYPROXY=/opt/globus/sbin/myproxy-server`

Before to start…

- Listening port, storing directory for credentials and configuration file could be changed setting the appropriate variables (PORT, STORE, CONFIG) on init script.
  - PORT="-p 7512"
  - STORE="-s /var/myproxy"
  - CONFIG="-c $CONFIG"
- Pay attention to ownerships/permissions for $STORE ! (root / 700).

Iptables /1

```
# Firewall configuration wirtten by redhat-config-securitylevel
# Manual customization of this file is not recommeded.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -s 193.206.144.10 -p udp --dport 123 -j ACCEPT
```

Iptables /2

```
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -
  j ACCEPT
-A RH-Firewall-1-INPUT -m state --state
  ESTABLISHED,RELATED -j ACCEPT

# Enable incoming connection to 7512 port.
-A RH-Firewall-1-INPUT -m state --state NEW -m
  tcp -p tcp --dport 7512 -j ACCEPT

# REJECT all traffic not allowed.
-A RH-Firewall-1-INPUT -j REJECT --reject-with
  icmp-host-prohibited
COMMIT
```

Before to start… /2

- Edit /etc/myproxy-server.config and define your access policies
  - By default you will find all the EGEE policies

```
accepted_credentials "/C=IT/O=INFN/*"
accepted_credentials "/C=it/O=GILDA/*"
accepted_credentials "/C=IT/O=GILDA/*"      proxy certificate
                                            subjects accepted
                                            to be stored

authorized_retrievers "*"                   certificate subject
                                            allowed torequest
                                            credentials delegation

authorized_renewers "*"                     certificate subject
                                            allowed torequest
                                            credentials renew
```

..and finally

- **Start the service running the command**

```
/etc/init.d/myproxy start
```

MyProxy Testing

MyProxy commands

- **myproxy-init -s <host_name>**

  -s: <host_name> specifies the hostname of the myproxy server

- **myproxy-info -s <host_name>**
  - Get information about stored long living proxy

- **myproxy-get-delegation -s <host_name>**
  - Get a new proxy from the MyProxy server

- **myproxy-destroy -s <host_name>**
  - Destroy the credential into the server

Howto access to training240v.healthgrid.org

Login : clermontXX@training240v.healthgrid.org
where XX=01,..15

Password : GridCLEXX XX=01,..,15

PEM PASSPHRASE : CLERMONT

Store credentials on MyProxy Server

```
%myproxy-init -s <server name>
…
Enter GRID pass phrase for this identity:
…
Enter MyProxy pass phrase:
…
A proxy valid for 168 hours (7.0 days) for user xxx     now
   exists on ui-test.trigrid.it.
Now your credentials are stored on MyProxy server,   and
   are available for delegation or renewal by RB
```

Get delegation

```
%myproxy-get-delegation -s <server name>

Enter MyProxy pass phrase:
A proxy has been received for user XXX in /tmp/x509up_u5XX
```

Log file & init script

- Log messages can be found in

  ```
  /var/log/messages
  ```

- Init script can be found in /etc/init.d

  ```
  /etc/init.d/myproxy
  ```

Troubleshooting

Clock skew between the node /1

```
$_ myproxy-init -s giular.trigrid.it --voms bio

init.c:266: globus_gss_assist_init_sec_context: Error during context
initialization
init_sec_context.c:171: gss_init_sec_context: SSLv3 handshake
problemsglobus_i_gsi_gss_utils.c:881: globus_i_gsi_gss_handshake: Unable
to verify
remote side's credentials
globus_i_gsi_gss_utils.c:854: globus_i_gsi_gss_handshake: SSLv3
handshakeproblems: Couldn't do ssl handshake
OpenSSL Error: s3_clnt.c:840: in library: SSL routines, function
SSL3_GET_SERVER_CERTIFICATE: certificate verify failed
globus_gsi_callback.c:351: globus_i_gsi_callback_handshake_callback:
Could not verify credential
globus_gsi_callback.c:443: globus_i_gsi_callback_cred_verify: Could
not verify credential: self signed certificate in
certificate chain
```

Clock skew between the node /2

```
Sep  7 16:00:01 giular myproxy-server: <2319> Connection from
193.206.208.141
Sep  7 16:00:01 giular myproxy-server: <2349> Error authenticating
client: GSS Major Status: Authentication Failed GSS Minor
Status Error Chain: accept_sec_context.c:170: gss_accept_sec_context:
SSLv3 handshake problems globus_i_gsi_gss_utils.c:881:
globus_i_gsi_gss_handshake: Unable to verify remote side's credentials
globus_i_gsi_gss_utils.c:854: globus_i_gsi_gss_handshake: SSLv3
handshake problems: Couldn't do ssl handshake OpenSSL Error:
s3_srvr.c:1816: in library: SSL routines, function
SSL3_GET_CLIENT_CERTIFICATE: no certificate returned
globus_gsi_callback.c:351: globus_i_gsi_callback_handshake_callback:
Could not verify credential globus_gsi_callback.c:420:
globus_i_gsi_callback_cred_verify: The certificate is not yet valid:
Cert with subject: /C=IT/O=GILDA/OU=Personal Certificate/L=INFN
Catania/CN=Giuseppe La Rocca/Email=giuseppe.larocca@ct.infn.it/CN=proxy
```

is not yet valid- check clock skew between hosts.

```
Sep  7 16:00:01 giular myproxy-server: <2349> Exiting: authentication
failed
```

Not authorized to store cred.

```
$_ myproxy-init -s giular.trigrid.it --voms gilda
Cannot find file or dir: /home/larocca/.glite/vomsesYour identity:
/C=IT/O=GILDA/OU=Personal Certificate/L=INFN Catania/CN=Giuseppe La
Rocca/Email=giuseppe.larocca@ct.infn.it
Enter GRID pass phrase:
verify OK
Creating temporary
proxy ........................................ Done
Contacting  voms.ct.infn.it:15001 [/C=IT/O=GILDA/OU=Host/L=INFN
Catania/CN=voms.ct.infn.it/Email=emidio.giorgio@ct.infn.it] "gilda" Done
Creating proxy ............................. Done
Your proxy is valid until Thu Sep 14 16:44:02 2006
Enter MyProxy pass phrase:
Verifying password - Enter MyProxy pass phrase:
```

ERROR from server: "/C=IT/O=GILDA/OU=Personal Certificate/L=INFN Catania/CN=Giuseppe La Rocca/Email=giuseppe.larocca@ct.infn.it"

not authorized to store credentials on this server

Check if myproxy-server.conf of the server contain:

- **accepted_credentials "/C=IT/O=GILDA/*"**

References

- gLite v3.0 Advanced Installation and Configuration Guide
  - http://glite.web.cern.ch/glite/packages/R3.0/R20060502/doc/installation_guide_3.0-2.html
- GILDA gLite 3.0 installation notes wiki
  - https://grid.ct.infn.it/twiki/bin/view/GILDA/GliteElementsInstallation
- GILDA gLite-3.0 installation instructions
  - https://gilda.ct.infn.it/docs/GILDAsiteinstall-3_0_0.html

Questions…