VOMS: installation, configuration & testing

Giuseppe La Rocca
INFN – Catania
giuseppe.larocca@ct.infn.it

EMBRACE-EGEE Tutorial

www.eu-egee.org

Information Society and Media

Outline

- Introduction to VOMS Architecture
- Installing VOMS
  - Installation via apt
- Configuring VOMS & testing
- Registering VOMS admin
- VOMS server web interface
- VOMS Admin command line interface

Introduction to VOMS

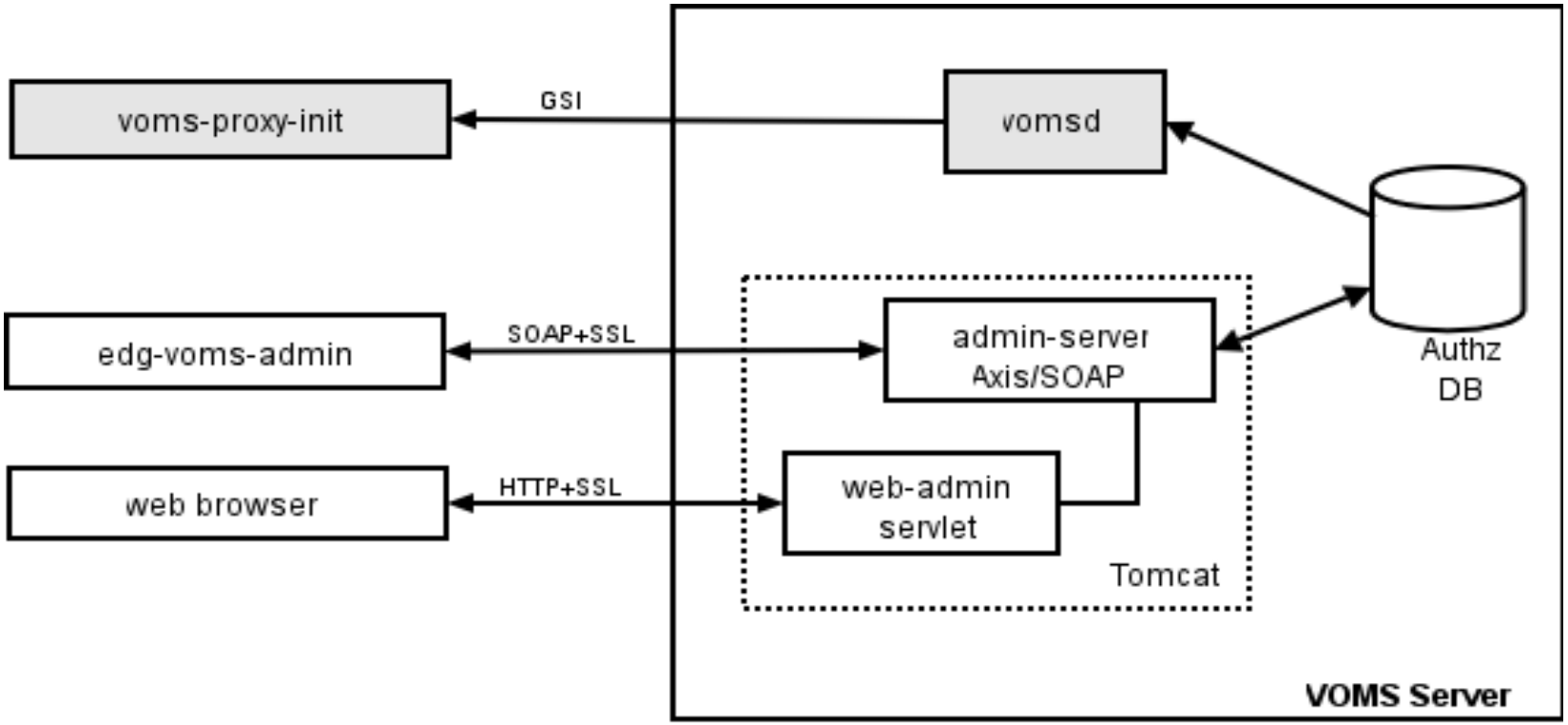
- **Virtual Organization Membership Service (VOMS)**
  - Account Database
    - Serving information in a special format (VOMS credentials)
    - Can be administered via command line & via web interface
  - Provides information on the user's relationship with his/her Virtual Organization (VO)
    - VO - Membership
    - Group membership
    - Roles of user

VOMS - components

- VOMS Core Services
  - Server - returns authorization info to the client.
  - Client
    - voms-proxy-init
      queries the server for authorization info and create a proxy certificate including it.
    - voms-proxy-info
      shows the info included in a proxy.
    - voms-proxy-destroy

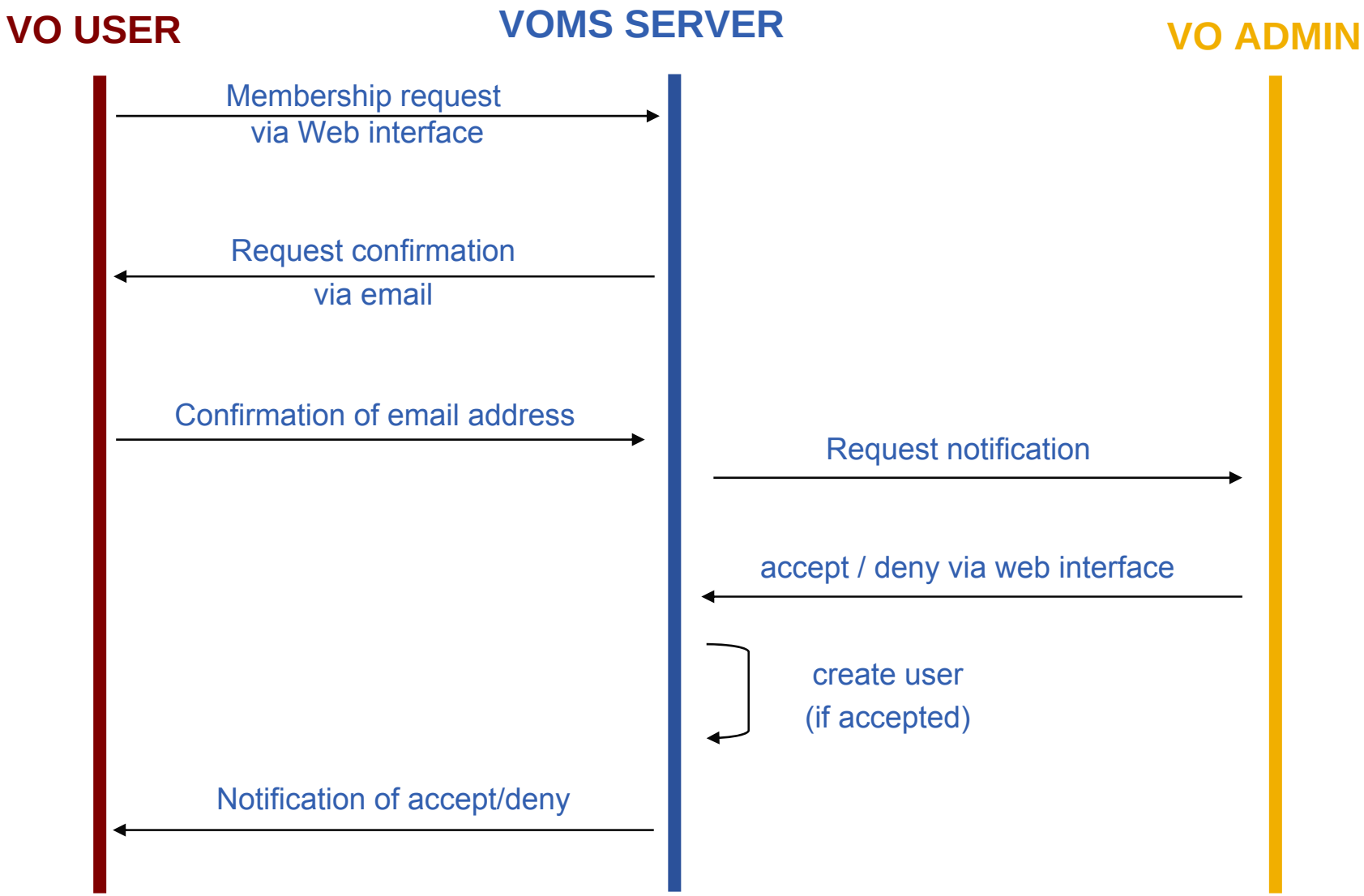
- VOMS Admin
  A Java server application used to manage users and their privileges for a VO.

VOMS Server architecture



The server is essentially a front-end where all the information about users are kept.

Registration process



Groups

- The number of users of a VO can be very high:
  - E.g. the experiment ATLAS has 2000 member

- Make VO manageable by organizing users in groups:
  Examples:
  - VO BIOMED-FRANCE
    - Group Paris
      - *Sorbonne University*
        - Group Prof. de Gaulle
      - *Central University*
    - Group Lyon
    - Group Marseille
  - VO BIOMED-FRANCE
    - BIOMED-FRANCE/STAFF — can write to normal storage
    - BIOMED-FRANCE/STUDENT — can only to volatile space

- Groups can have a hierarchical structure

- **Group membership is added automatically to your proxy when doing a *voms-proxy-init***

Roles

- **Roles are specific roles a user has and that distinguishes him from others in his group:**
  - **Software manager**
  - **Administrator**
  - **Manager**
- **Difference between roles and groups:**
  - **Roles have no hierarchical structure – there is no sub-role**
  - **Roles are not used in 'normal operation'**
    - **They are not added to the proxy by default when running *voms-proxy-init***
    - **But they can be added to the proxy for special purposes when running *voms-proxy-init***

Installation of a VOMS Server based on MySql database

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)**
  - **CA_Gilda rpm** `(https://gilda.ct.infn.it/RPMS/)`

Install host certificates

- Request host certificates for the VOMS 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
```

- Currently, there's no YAIM profile for the installation of VOMS
- We are going to proceed with the manual installation !
- VOMS Server can be installed using:
  - Installer script
  - APT
    - During the installation will be installed dependencies and other necessary modules.

Installing VOMS via apt

1. Verify apt is present:
   - rpm -qa | grep apt
   - Install apt if necessary:
     - rpm -ivh http://linuxsoft.cern.ch/cern/slc30X/i386/SL/RPMS/apt-0.5.15cnc6-8.SL.cern.i386.rpm

2. Add gLite apt repository:
   - Fill up a file (e.g. `glite.list`) under the `/etc/apt/sources.list.d` directory (R 1.4)

```
rpm http://192.168.0.50 glite-1.4-i386 1_4 externals updates
```

3. Update apt repository:
   - `apt-get update`
   - `apt-get upgrade`

4. Install VOMS server:
   - `apt-get install glite-voms-server-mysql-config`

Configure the VOMS server

- Go to configuration directory and copy templates
  - `cd /opt/glite/etc/config`
  - `cp templates/*.xml .`
- Customize configuration files by replacing all '**changeme**' values with the proper values

- **List of the mandatory XML files to configure VOMS Server**

glite-global.cfg.xml
glite-security-utils.cfg.xml
glite-rgma-common.cfg.xml
glite-rgma-servicetool.cfg.xml
glite-voms-server.cfg.xml

- **glite-global.cfg.xml**
  - Contains general aspects. Typically just the JAVA_HOME attribute needs to be changed specifying in the location of your JVM.
- **glite-rgma-common.cfg.xml**
  - Specify the configuration parameters for R-GMA.
- **glite-rgma-servicetool.cfg.xml**
  - Configuration parameters for RGMA servicetool Service.
- **glite-security-utils.cfg.xml**
  - Just set the cron.mailto attribute value

VOMS Server configuration aspects

- Virtual organization description (one instance per VO)
  - **name** of the VO (i.e. newVO)
  - VOMS (core) service TCP **port** number on which the server VO instance will listen
    - must be a valid, unique port number – typically from 15000 upwards
  - **e-mail** address used to send emails on behalf of the VOMS server

```
<instance name="florence">
        <parameters>
           <voms.vo.name
            description="Name of the VO associated with
             this VOMS instance.
            [Example: 'EGEE'] [Type: 'string']"
            value="florence"/>

            <voms.port.number
            description="Port number listening for request
             for this VO instance
            [Example: '15001'][Type: 'string']"
            value="15001"/>
```

```
<voms.admin.notification.e-mail
    description="E-mail address that is used to send
    notification mails from the VOMS-admin.
     [Example: name.surname@domain.org][Type: 'string']"
     value="giuseppe.larocca@ct.infn.it"/>

<voms.admin.certificate
     description="The certificate file (in pem format) of an
     initial VO administrator. The VO will be set up so that
     this user has full VO administration privileges.
     Remove parameter or leave parameter empty if you don't
     want to create an initial VO administartor.
     value="/etc/grid-security/admin-usercert.pem"/>
```

- **Copy the admin certificate** (`admin-usercert.pem`) **on** `/etc/grid-security/`

Configure MySQL

- **MySQL database configuration**
  - Administrator **password** of used MySQL database (it has to be set **before** configuration)

```
/usr/bin/mysqladmin -u root \
  password <your passwd>
```

VOMS firewall configuration

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

Iptables /2

```
# Enable incoming SSH Connection.
-A RH-Firewall-1-INPUT -m state --state NEW -m
  tcp -p tcp -s XXX.XXX.XXX.XXX --dport 22 -j
  ACCEPT
# VOMS ports.
-A RH-Firewall-1-INPUT -m state --state NEW -m
  tcp -p tcp --dport 8443 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m
  tcp -p tcp --dport 15001 -j ACCEPT
# REJECT all traffic not allowed.
-A RH-Firewall-1-INPUT -j REJECT --reject-with
  icmp-host-prohibited
COMMIT
```

VOMS configuration & start up

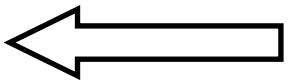
- Go to the scripts directory and execute the VOMS Server configuration script
  - `cd /opt/glite/etc/config/scripts`
  - `./glite-voms-server-config.py --configure`
- Start the VOMS server
  - `./glite-voms-server-config.py --start`
- Check if the environment variables have been properly exported:

```
source /etc/glite/profile.d/glite_setenv.sh
```

more configuration..

- **Configure the /opt/glite/etc/voms/florence/voms.conf file as follow:**

```
--vo=florence
--port=15001
--code=15001
--username=voUser
--passfile=/opt/glite/etc/voms/florence/voms.pass
--logfile=/var/log/glite/voms.florence
--loglevel=4
--logtype=7
--sqlloc=/opt/glite/lib/libvomsmysql.so
--dbname=VOMS_florence
--timeout=864000
```



`10gg * 24h * 60min * 60sec`

Upgrade the VOMS Server to gLite-3.0

- **Upgrade the glite.list file with the link to the gLite-3.0 repository to use during the upgrading of the VOMS Server.**

For this tutorial use http://192.168.0.50 glite_sl3-i386 3_0_0 3_0_0_updates 3_0_0_externals

and run..

```
apt-get update
apt-get upgrade
```

Register VOMS administrator

The first VOMS administrator has to be added manually using the command line tools:

- Copy your public grid certificate to your VOMS server
- Run voms-admin command to add yourself as admin

```
$GLITE_LOCATION/bin/voms-admin \
            --vo <VO name> \
            create-user <admincert.pem> \
            assign-role <VO name> \
            VO-Admin <admincert.pem>
```

VOMS testing

Using gLite configuration script

```
./glite-voms-server-config.py --status
```

Connect to the VOMS server via browser

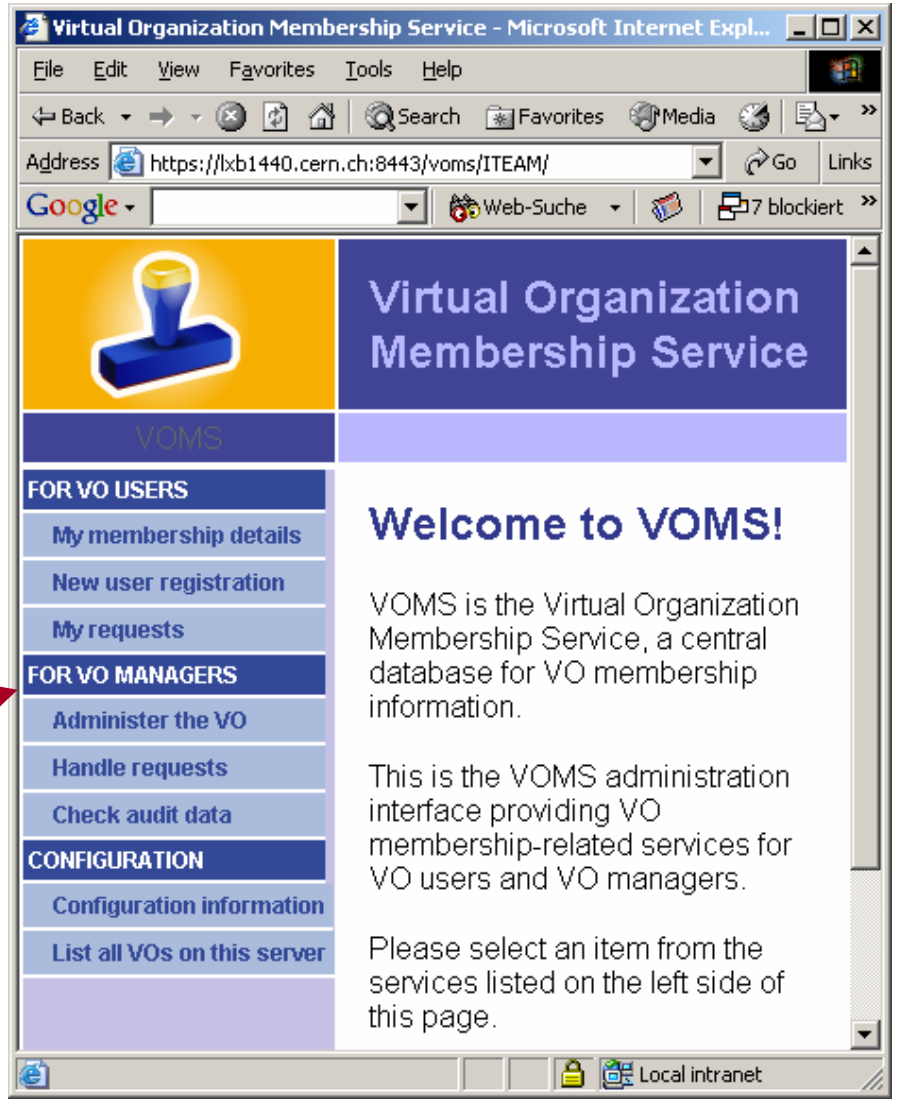
```
https://<voms-server>:8443/voms/florence
```

(requires personal certificate loaded on browser)

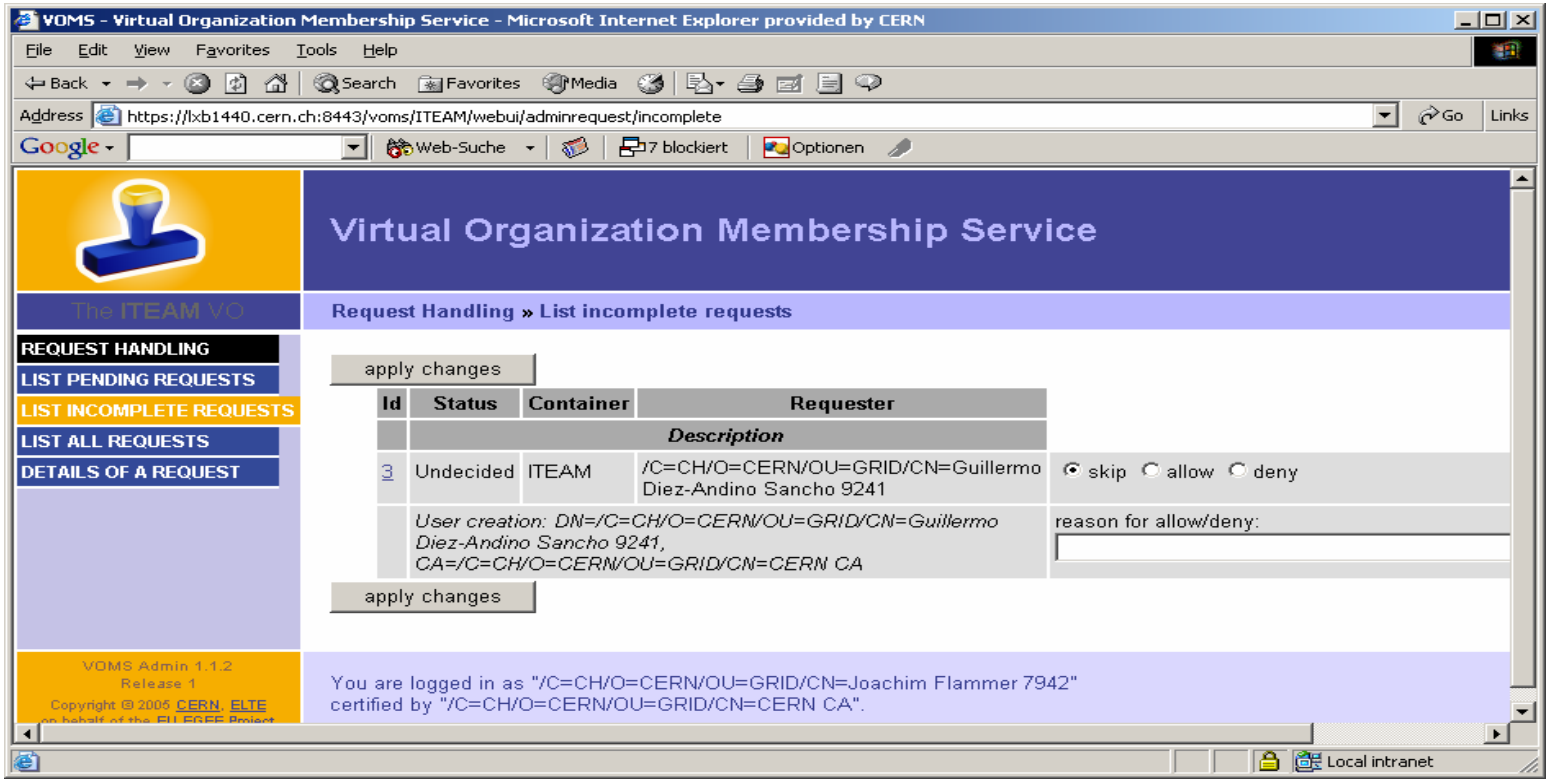
VOMS Server web interface

VOMS Web interface

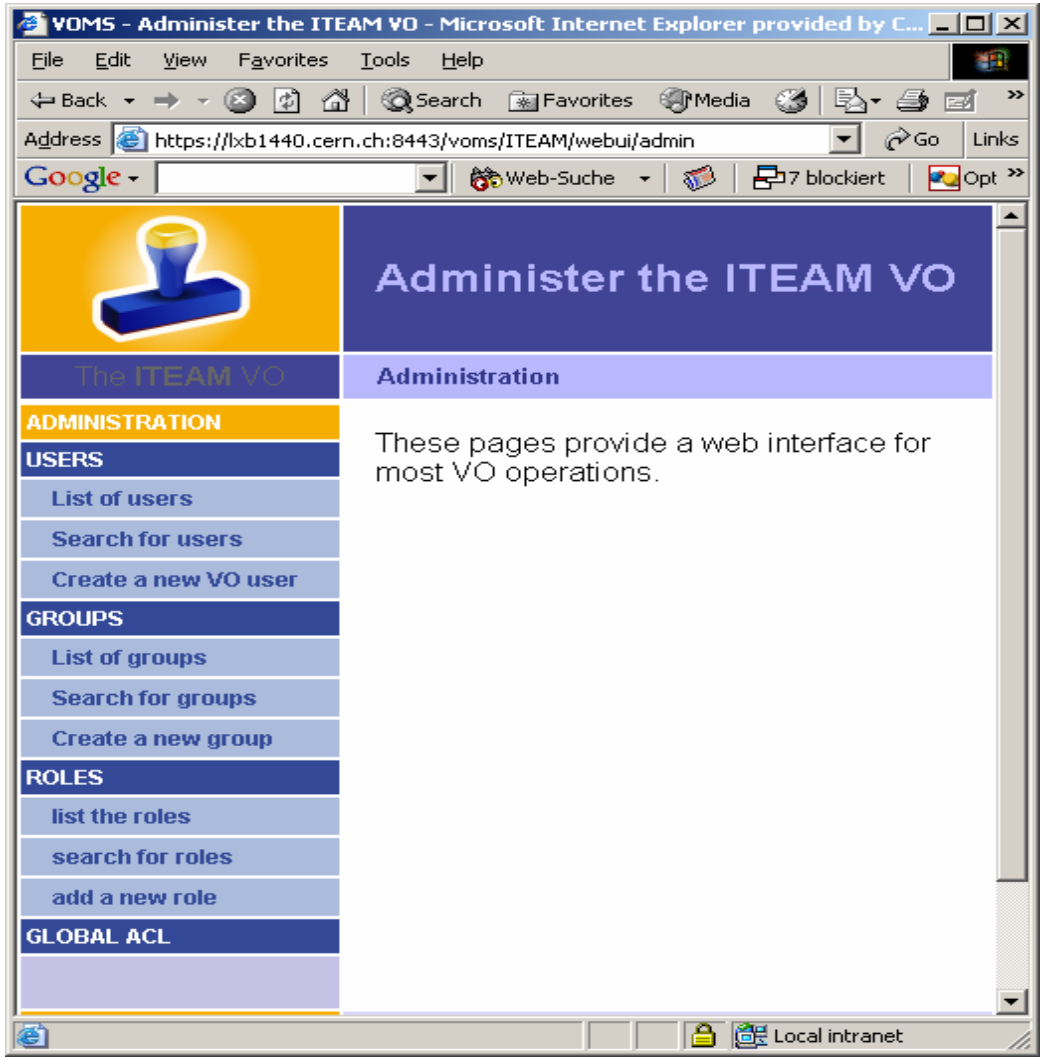
- VO user can
  - Query membership details
  - Register himself in the VO
    - You will need a valid certificate
  - Track his requests
- VO manager can
  - Handle request from users
  - Administer the VO



- VO manager will be informed of new requests via mail
  - Query requests
  - Accept / Deny requests



- The administrator interface allows you to
  - Manage users
    - List users
    - Search for users
    - Create users
  - Manage groups
    - List groups
    - Search for groups
    - Create groups
  - Manage roles
    - List roles
    - Search for roles
    - Create roles



VOMS command line interface

Command line interface

```
voms-admin [OPTIONS] --vo=NAME [-h HOST]
[-p PORT] COMMAND PARAM

voms-admin [OPTIONS] --url=URL COMMAND PARAM
```

COMMAND

- get-vo-name
- list-users — list all users of VO
- create-user <CERTIFICATE.PEM>
- delete-user USER
- list-cas — list certificate auth. accepted by VO
- list-roles
- ....

See VOMS admin user guide for entire list and details

Command line interface /2

```
#_ ${GLITE_LOCATION}/bin/voms-admin --vo
florence get-vo-name

/florence

#_ ${GLITE_LOCATION}/bin/voms-admin --vo
florence list-users

CN |certUri |mail |DN |CA
Giuseppe La Rocca
giuseppe.larocca@ct.infn.it|/C=IT/O=GILDA/OU=Personal
Certificate/L=INFN Catania/CN=Giuseppe La Rocca
/Email=giuseppe.larocca@ct.infn.it
/C=IT/O=GILDA/CN=GILDA Certification Authority
```

Command line interface /3

```
#_ ${GLITE_LOCATION}/bin/voms-admin --vo
florence list-roles

Role=VO-Admin

#_ ${GLITE_LOCATION}/bin/voms-admin --vo
florence create-user <usercert.pem>
```

Log files & init scripts

Logs and scripts

- **Log files can be found in**

```
/var/log/messages
/var/log/glite/voms.<VO NAME>
```

- **Init scripts can be found in**

```
/opt/glite/etc/config/scripts/
```

Testing the VOMS Server from a User Interface

Use the configuration info of the VOMS Server you have already installed …

to create `.glite/vomses` file in your UI's account.

Initialize the proxy

- `$ voms-proxy-init --voms florence`

```
Your 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:
Creating temporary proxy
..................................... Done
Contacting  giular.trigrid.it:15001
[/C=IT/O=GILDA/OU=Host/L=INFN
Catania/CN=giular.trigrid.it/Email=giuseppe.la
rocca@ct.infn.it] "florence" Done
Creating proxy
.......................................
Done
Your proxy is valid until Tue Sep 19 00:05:36
2006
```

Check your local proxy

```
$ voms-proxy-info --all
   subject   : /C=IT/O=GILDA/OU=Personal Certificate/L=INFN
   Catania/CN=Giuseppe La
   Rocca/Email=giuseppe.larocca@ct.infn.it/CN=proxy
   issuer    : /C=IT/O=GILDA/OU=Personal Certificate/L=INFN
   Catania/CN=Giuseppe La Rocca/Email=giuseppe.larocca@ct.infn.it
   identity  : /C=IT/O=GILDA/OU=Personal Certificate/L=INFN
   Catania/CN=Giuseppe La Rocca/Email=giuseppe.larocca@ct.infn.it
   type      : proxy
   strength  : 512 bits
   path      : /tmp/x509up_u512
   timeleft  : 11:59:56
   === VO florence extension information ===
   VO        : florence
   subject   : /C=IT/O=GILDA/OU=Personal Certificate/L=INFN
   Catania/CN=Giuseppe La Rocca/Email=giuseppe.larocca@ct.infn.it
   issuer    : /C=IT/O=GILDA/OU=Host/L=INFN
   Catania/CN=giular.trigrid.it/Email=giuseppe.larocca@ct.infn.it
   attribute : /florence/Role=NULL/Capability=NULL
   timeleft  : 11:59:55
```

Troubleshooting

Troubleshooting

The client side message is like in the following example:

```
$_ voms-proxy-init -voms france
Your identity: /C=CH/O=CERN/OU=GRID/CN=Maria
Alandes Pradillo 5561 Enter GRID pass phrase:
Creating temporary proxy
..................................... Done
Contacting lxb0769.cern.ch:15001
[/C=CH/O=CERN/OU=GRID/CN=lxb0769.cern.ch] "france"
```

Failed Error: Could not establish authenticated connection with the server. GSS Major Status: Unexpected Gatekeeper or Service Name GSS Minor Status Error Chain: an unknown error occurred Failed to contact servers for france.

Troubleshooting

The server log file (/var/log/glite/voms.france) contains the following lines:

```
Wed Aug 16 11:04:48
2006:lxb0769.cern.ch:vomsd(4341):ERROR:REQUEST:Acc
eptGSIAuthentication
home/glbuild/GLITE_3_0_0_final/org.glite.security.
voms/src/socklib/Server.cpp:259):Failed to
establish security context (accept):.GSS Major
Status: General failure.GSS Minor Status Error
Chain:..accept_sec_context.c:305:gss_accept_sec_co
ntext: Error during delegation: Delegation
protocol violation
```

Solution (I)

In this case check whether the *vomses* file contains the correct host certificate subject.

To check what's your VOMS host certificate subject, run the following command:

```
openssl x509 -in /etc/grid-
security/hostcert.pem -noout -subject

subject=/C=CH/O=CERN/OU=GRID/CN=host/lxb0769.cern
.ch
```

Solution (I)

And check in the *vomses* file whether the certificate subject is correct:

```
more vomses
...
france" "lxb0769.cern.ch" "15001"
"/C=CH/O=CERN/OU=GRID/CN=host/lxb0769.cern.
ch" "france"
...
```

Solution (II)

Verify the synchronization between the UI and the VOMS Server.

```
Check if nptd is running
/etc/init.d/ntpd status
ntpd (pid 1742) is running...
```

and if the date is correctly !

Solution (III)

Check if both VOMS and UI have the same CRL installed.

Questions...