VO Server Information

J. A. Templon
NIKHEF

23 October 2001
Last Edit: 29.10.2001

Abstract

This is a work in progress which attempts to explain how to administer the LDAP server which at the moment is responsible for enabling user access to the Grid via the Virtual Organization (VO) mechanism. Suggestions for improvements and/or corrections are welcomed.

1 Introduction

On the EU Data Grid, "users" of the Grid will not have "accounts" in the usual sense of the word. That is, they will not have a login name and password via which they can log in to Grid computer nodes via `ssh` or `telnet` or somesuch. Rather, users will have a "X.509 Identity Certificate" which has been issued by some "Certificate Authority" which is recognized by the EU Data Grid organization. This certificate serves to "prove" a user's identity, but somehow the user's authorization to perform the requested task must be authorized.

The Virtual Organization (VO) construct is used in the implementation of the authorization phase of user task instantiation. Basically, VOs are used to organize the credentials (certificate subject lines for example) of sets of users into various subgroups. When a user submits a task request, the user's certificate information is compared with a file which is populated by information from the various VOs. "Roberto Barbera" may have been added to the Alice VO, in which case the file referred to will have an entry for "Roberto Barbera" along with a directive to map his requests onto a local Alice environment. On the other hand, Roberto would not be allowed to run jobs under other environments (at least for PM9).

Somewhere there needs to be a database which lists the people in each VO. LDAP has been chosen to implement this database. NIKHEF has experience in other contexts with LDAP, so the institute volunteered to administer the LDAP server containing this person/VO mapping. Experiments themselves need to administer the VO directories which reside on the server. The main purpose of this document is to explain how to do that.

2 The Roles of Managers and Administrators

NIKHEF (actually the CT group at NIKHEF) will physically maintain the computer system on which the VO LDAP server runs. This computer has the host name `grid-vo.nikhef.nl`. David Groep (NIKHEF) will also maintain the LDAP server program running on this computer. NIKHEF staff (at the moment, David Groep and Jeff Templon) will take care of *management* of the VO database. Each VO in turn will need to appoint a *VO Manager*. (S)he may appoint one or more *VO Group Administrator(s)*.

2.1 Database Manager

The Database Manager(s) are primarily concerned with making it possible for the VOs to do their job. The Database Manager(s) is the person(s) who

1. creates new Virtual Organizations in the database
2. specify the initial VO Manager corresponding to each VO

At the moment, this can only be done by the NIKHEF staff mentioned above.

2.2 VO Manager

The VO Manager has the following rights and responsibilities:

1. to maintain the list of people belonging to his/her VO (by adding/removing them from a list on the VO directory)
2. to add or delete new "groups" within the VO. For example, the "biology" VO might have two groups: "imageproc" and "bioinformatics". The "lhcb" VO might have "trigger", "outertracker", and "prodsim" groups.
3. to specify the Administrator(s) for each group within the VO.

There is are only two restrictions on who can be a VO Manager:

1. the VO Manager needs to be entered into the directory by the Database Manager, and
2. there can initially only be one VO Manager.

VO Managers should not share their passwords with others. There is a possibility that a VO could be munged by having multiple copies of the manager doing administration in parallel. If experience proves that the restriction of a single VO Manager is problematic, the Database Managers can assign additional VO Managers.

2.3 VO Group Administrator

The VO Group Administrator has the following rights and responsibilities:

1. to add people to his/her group *providing that they are already members of the VO.*
2. to remove people from his/her group.

3 General Information on LDAP

There is a general web page set up with information on OpenLDAP which is the version of LDAP we're using (are there others?) The web address is `http://www.openldap.org/`. One of the links on this page is to the FAQ-O-Matic, where one of the FAQs is "Where can I get more information on LDAP?" I downloaded the free book published by IBM called "Understanding LDAP":

`http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg244986.pdf`.

This book thoroughly explains the concepts involved behind LDAP. It is quite basic (the level is a bit too basic) — but I prefer such a book to one for which the level is not basic enough.

4 LDAP structure of VOs

I assume that you are a bit familiar with X.50X terminology, but in case you forgot, here is a short cheat sheet:

dc domain component (like an internet domain, and you can't "just choose", there are standards organizations which hand these things out)

cn common name, for example for a person this would be the normal "name" you'd use to look in a phone book

sn surname (last name)

o organization, for example NIKHEF or INFN

ou organizational unit, for example the CT group at NIKHEF or the CNAF unit of INFN

The LDAP server runs on the internet host `grid-vo.nikhef.nl`. To access the VO directories, one has to connect to this host with the following information:

`o=alice,dc=eu-datagrid,dc=org`

where `alice` is the name of the organization of this VO, and could also be at the moment `lhcb`, `atlas`, or `cms`. This specifies that you want to connect to the directory of the **organization** `alice` of the **domain** `eu-datagrid.org`.

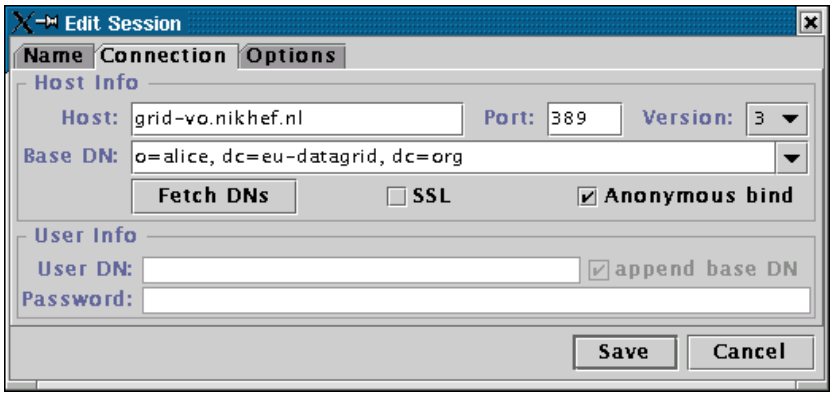

Figure 1: Dialog box showing the LDAP parameters needed to connect anonymously (as a "user" of information) to a VO.

5 Connecting to the VO directory as an information User

Using the LDAP browser referred in Sec. 7, Fig. 1 shows how you would connect anonymously (*ie* as some random unprivileged user) to the alice VO.

The next screen (Fig. 2) shows the view provided to you if you connect as an anonymous user. You can clearly see all the information needed to fill a grid-mapfile.

6 Connecting to the VO directory as a VO Manager

Fig. 3 shows a connection dialog for the case of where the VO Manager wants to make a connection (so (s)he can e.g. delete or add some people, or change some group attributes, etc.) Notes:

1. the Manager will be prompted for a password!
2. read further before trying to change anything in the directory. It is possible to corrupt the directory by changing the wrong thing.

7 Software Tools for VO Administration and Management

In principle, one can construct and/or modify VO directories with any LDAP tool which provides directory update capability. However it is possible to change

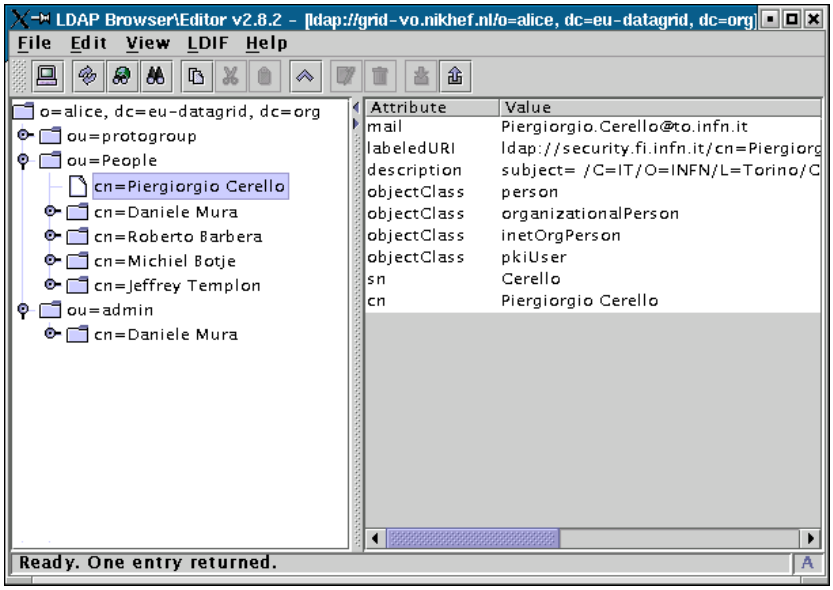

Figure 2: View of Alice VO seen via an anonymous connection to the LDAP server & Alice VO directory.

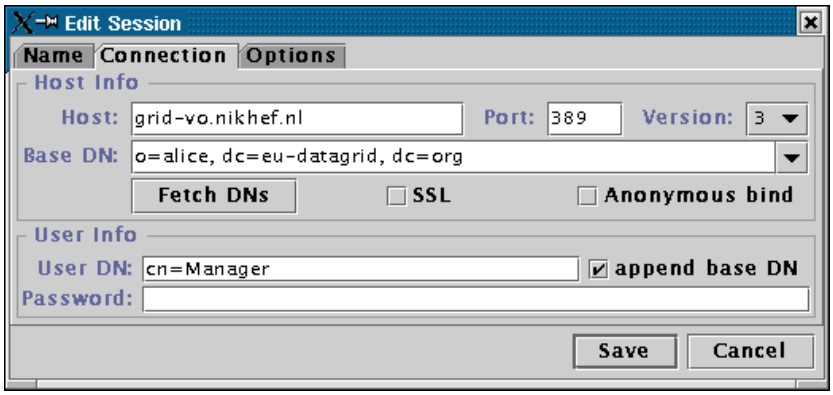

Figure 3: Dialog box showing the connection to a VO directory for a VO manager.

something you shouldn't change which may break other software. In order to limit the possibility of corruption, several tools have been developed to assist in administration and management of the VO database by the various classes of managers/administrators. Some of them are available from the DataGrid Authorization Working Group:

`http://cvs.infn.it/cgi-bin/cvsweb.cgi/Auth/VO/sbin/`

The other tools have been "baked" at NIKHEF by David Groep and are available at

`http://www.dutchgrid.nl/DataGrid/apps`

These tools assume that your workstation has the basic LDAP client-side tools installed. This is standard on Solaris systems. On Linux you might need to install it. At NIKHEF for example we have `openldap-1.2.9-6`. You also will need Perl installed (blech) with LDAP and Tk support enabled.

Finally, a general-purpose LDAP browser will be useful. You can get one at the following web site:

`http://www.iit.edu/~gawojar/ldap/`.

This tool can edit LDAP directory information (given that you have permission) as well as browse it. If you just want to browse and not edit, you can use Netscape 4.X (or MS Internet Exploder).

8 Tools for the VO Manager

The following tools are available for a VO Manager.

- `scripts/vop.pl` - add people to the VO
- `sbin/makegroup.sh` - add a new group to the VO
- `scripts/cert2ldif.pl` - is used to generate user information to be added to a VO database in the case that the user's CA doesn't have an ldap server. In this case, you can feed the user's `usercert.pem` to this script to generate LDIF format input for adding to the VO directory. The invocation format is

  ```
  cert2ldif.pl -vo alice usercert.pem > tmp.ldif
  ```

  and this output file `tmp.ldif` is suitable for import into the directory via the "import" function of the Manager's LDAP browser. Alternatively it could be added via the `ldapadd` command:

```
ldapadd -h grid-vo.nikhef.nl -W -D "cn=Manager,o=alice,dc=eu-datagrid,dc=org" -f tmp.ldif
```

9 Tools for the VO Group Administrator

The following tool is available for a VO Group Administrator:

- `scripts/group.pl` - add "existing" people (already within the VO) to "existing" groups (already added by the VO Manager)