VO Server Information

J. A. Templon, D. Groep
NIKHEF

23 October 2001
Last Edit: 08.01.2002

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" (CA) 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`.

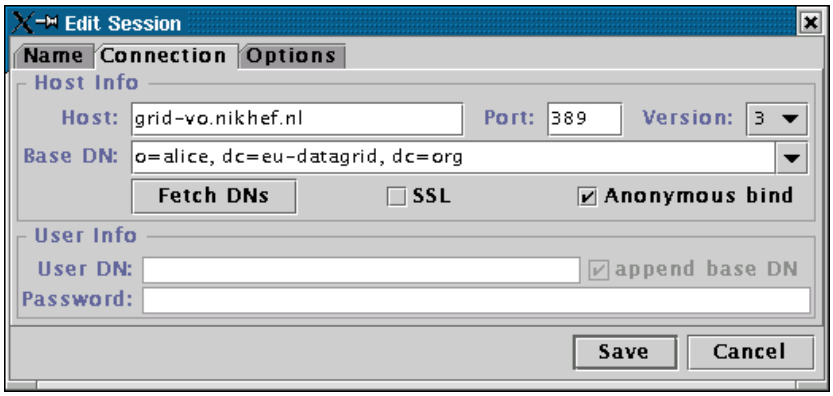

Figure 1: Dialog box showing the LDAP parameters needed to connect anonymously (as a "user" of information) to a VO.

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

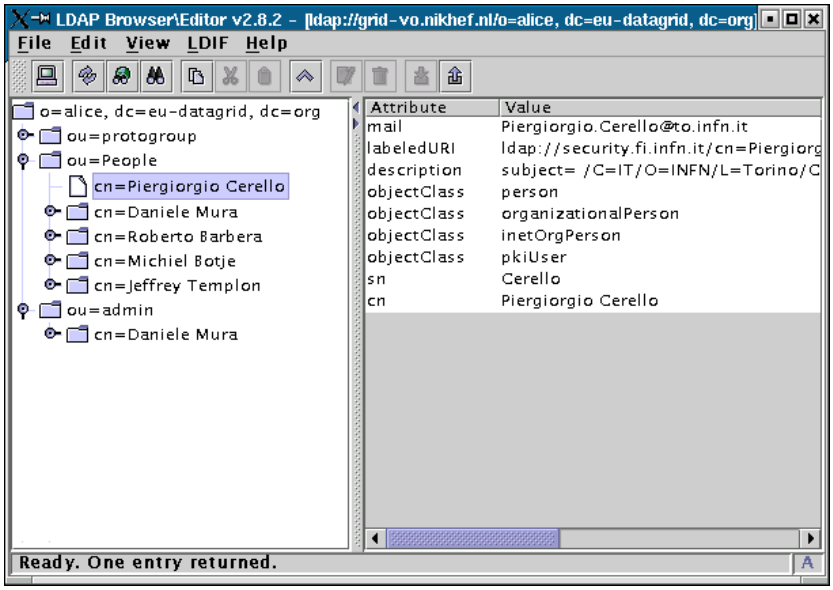

Figure 2: View of Alice VO seen via an anonymous connection to the LDAP server & Alice VO directory.

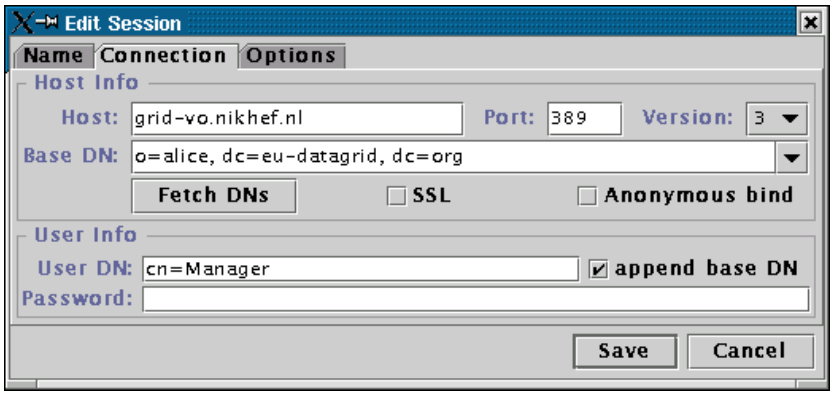

Figure 3: Dialog box showing the connection to a VO directory for a VO manager.

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. See Appendix A for information on how to get the correct Perl modules installed.

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.

- `vop.pl` - add people to the VO. The information on the people is retrieved from an LDAP server run by a Certification Authority (CA). Not all CA's have LDAP servers, so some people must be added using `cert2ldif.pl` (see below).

- `makegroup.sh` - add a new group to the VO. This command-line tool allows you to specify the Group Administrator (see sec. 2.3) at creation time.

- `creategroup.pl` - add a new group to the VO. Does the same as makegroup; it has a nice GUI but you can't specify the Group Administrator.

- `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
```

8.1 vop.pl operation

vop.pl is used to populate a VO with people who are known to a CA LDAP server. At the moment there are only three CA LDAP servers so this tool is not sufficient to completely populate most VOs.

You start `vop.pl` on a Linux machine by typing `./vop.pl` . When you start VOP, you get a new window (Tk style) with on the top a pull-down button to select the CA directory (at the moment only INFN, NIKHEF or CESnet). Furthermore there are four boxes to type in your VO information (LDAP server, VO basename, bind name and password). Following this there is a pane with a list of all people with valid certificates issued by the selected CA. This list is a list of "candidates" to join your VO.

The tool comes up with a default of the INFN CA. Suppose for example you wanted to add the Dutch Guy David Groep to your VO.

1. select the dutchgrid CA (certificate.nikhef.nl) from the pull-down button, wait some time, and the window will reappear with a list of Dutch people instead of a list of Italian people.

2. set the fields as follows (this example is for the "earthob" VO):

   VO hostname grid-vo.nikhef.nl

   VO basename o=earthob,dc=eu-datagrid,dc=org

   VO bindname cn=Manager,o=earthob,dc=eu-datagrid,dc=org

   VO password ¡¡your manager password¿¿

Then, click on the checkbox next to David Groep's name in the list of people, possibly select other people to add to your VO and click on "Go!". When you click Go, the selected people will be added to your VO. You may then either continue or click "Quit".

8.2 makegroup.sh operation

The function of this tool is to create a new group (sometimes called a subgroup) in your VO, and to specify the Group Administrator and his/her password. The Group Administrator can add or remove people from his/her group provided that they already belong to the VO as a whole. That is, Group Administrators cannot add just *anyone* to their Group; the VO Manager controls who belongs to the VO as a whole, and an Administrator decides which of the VO people belong to his/her Group.

Here is an example command line for makegroup.sh:

```
makegroup.sh -owner "David Grissom" -sn Grissom -desc "Test Group" \
"o=earthob,dc=eu-datagrid,dc=org" wolfpack
```

This creates a group called "wolfpack" within the "earthob" VO. The owner of the *Group* will be David Grissom, whose surname (sn) is Grissom, and the Group will contain a description field containing the phrase "Test Group".

Once this command is entered, you will get three prompts, that look like this:

```
New password:
Re-enter new password:
You will need to enter the VO main manager password ...
Enter LDAP Password:
```

Recall this command is being run by the VO Manager, who is the only person with the permission to create a group. The VO Manager's password is the third one asked for ("Enter LDAP Password:"). The first two prompts are asking you to first enter, and then confirm, the password that will be set for the Group Administrator you specified on the command line (in this case David Grissom). If the command was successful, you will see the following:

```
adding new entry "ou=wolfpack,o=earthob,dc=eu-datagrid,dc=org"
adding new entry "cn=David Grissom,ou=admin,o=earthob,dc=eu-datagrid,dc=org"
*** You have created group wolfpack ***
In order to satisfy the schema and as an illustration, this group has been
given one single member, named <cn=empty>. You should remove this entry
after adding the first real user to this group.
```

8.3 creategroup.pl operation

Creategroup.pl does the same thing as makegroup.pl with the following differences:

- it has a graphical interface in place of the command-line style of makegroup.sh
- it does not allow for specification of the "description" field
- it does not allow for specification of a separate Group Administrator.

The VO Manager becomes in effect the Group Administrator. You (the VO Manager) can always "give" the group afterwards to an aminstrator, using an LDAP browser/editor. Instructions for doing that are beyond the scope of this document.

Below (Fig. 4) is a snapshot of creategroup.pl in action, creating the same group as described in the makegroup.pl example.

If the command is successful, the word "Done!" will appear at the command prompt where you typed "creategroup.pl".

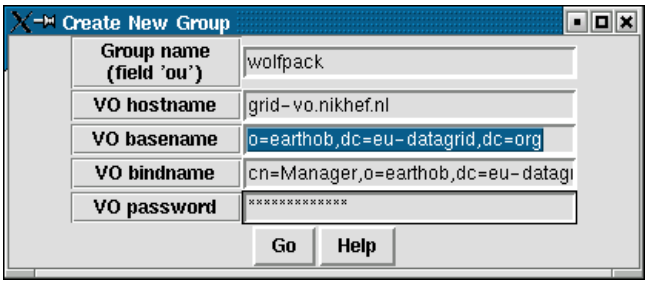

Figure 4: Screen shot on how to fill in the fields for creategroup.pl. As shown, the group "wolfpack" will be created inside the VO "earthob". The VO bindname box isn't big enough to display everything here; the entire bindname is the VO Manager name (cn=Manager) plus the VO basename (o=earthob,dc=eu-datagrid,dc=org).

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).

The operation of `group.pl` is similar to that of `vop.pl` above. Fig. 5 shows a snapshot of how to fill in the fields. Once you have filled in these fields and clicked "Go", you will get something that looks like Fig. 6.

Unfortunately, group.pl doesn't give you any idea about whether the command was successful. You have to start it again (or use an LDAP browser) and see whether it worked.

A Perl Installation

You will likely need some extra Perl modules installed in order to use the LDAP tools (*e.g.,* `vop.pl` and `cert2ldif.pl`). It is not possible to provide complete information here that would work for every possible site, so I provide the steps I needed to get it running on my machine as an example. I start with the example of `vop.pl`. However, the best solution is to convince your system administrator to install the needed modules for you. The advantage here is that they are placed in the system space, so you don't need to define any environment variables, and as well they don't take up any of your disk quota.

Start by downloading the latest release of `vop.pl` from the Authorization Working Group web site:

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

Make it executable (`chmod 755 vop.pl`) and execute it (under Linux by typing `./vop.pl`). This resulted here in:

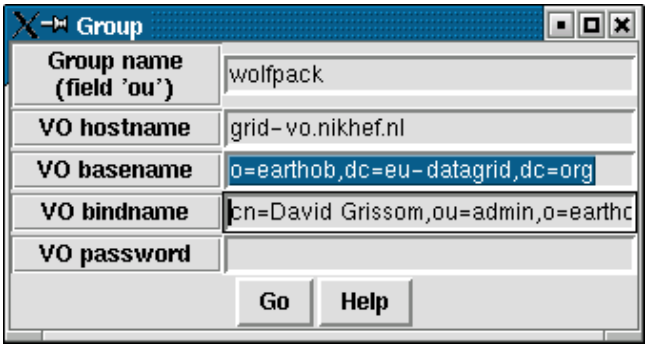

Figure 5: Example of how to fill in the fields for `group.pl`. In this case, the Group Adminstrator is not the same as the VO Manager, so the full VO bindname consists of the Administrator field (cn=David Grissom,ou=admin) plus the VO basename (o=earthob,dc=eu-datagrid,dc=org). If the Group had been created using creategroup.pl, the VO bindname would be the same as in the creategroup.pl example (cn=Manager,o=earthob,dc=eu-datagrid,dc=org).

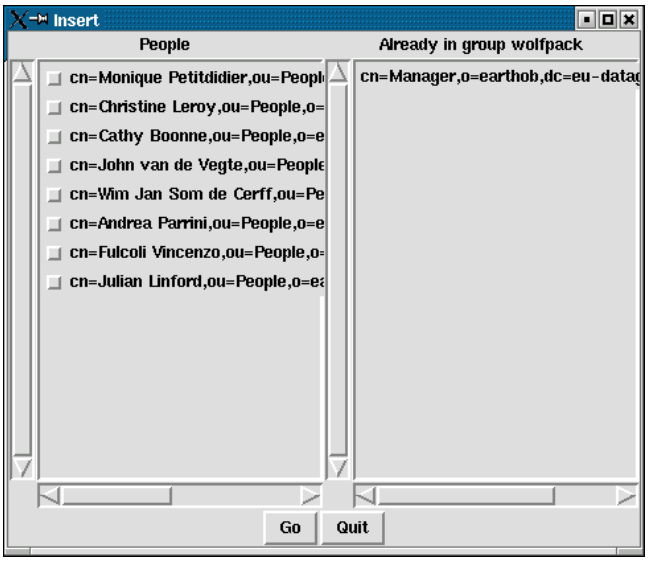

Figure 6: How to choose people to belong to your Group (using group.pl). On the left are shown all the people in the VO (in this example, earthob VO). On the right are shown all the people who are already in your Group (in this case, wolfpack). Click on the box next to the people you wish to add, and then click "Go".

```
Can't locate Tk.pm in @INC (@INC contains:
/usr/lib/perl5/5.00503/i386-linux
/usr/lib/perl5/5.00503
/usr/lib/perl5/site_perl/5.005/i386-linux
/usr/lib/perl5/site_perl/5.005 .) at ./vop.pl line 4.
BEGIN failed--compilation aborted at ./vop.pl line 4.
```

The most important part of this error message is the phrase `Can't locate Tk.pm`. This indicates that the `Tk` Perl module is missing. In the instructions below, you will see how to find, download, and install these missing modules. I list some other missing modules below. Unless otherwise stated, I found out that they were missing via the above method: try to run the script, and look at the first line of output to find the name of the missing module.

A.1 How to find and download Perl modules

Go to `http://search.cpan.org` and type the name of the desired module into the "Search" box on the left hand side of the page. When I typed in `Tk` I got back a page with 506 hits. Describing the format of this output is beyond the scope of this document. The desired hit is the one for Tk800.023 which provides the module "Tk" standalone (the first entry in the list of Tk800.023 is just "Tk"). Click on Tk800.023. At the top of the resulting page, you see "Latest Release" - right click on this to download it. Here are the steps I did to unpack and install the modules in my home directory:

```
tar xvzf Tk800.023.tar.gz
cd Tk800.023
perl Makefile.PL PREFIX=/user/templon # puts it in my home dir
make
make test         # skip if you're impatient
make install
```

You also need to set an environment variable to let Perl know where you put this library (in my case it is a subdirectory of `/user/templon`). Here is what I needed to do:

```
export PERLLIB=/user/templon/lib/perl5/site_perl/5.005:\
/user/templon/lib/perl5/site_perl/5.005/i386-linux
```

Now when I run the script `./vop.pl` I get the following:

```
Can't locate Net/LDAP.pm in @INC (@INC contains:
/user/templon/lib/perl5/site_perl/5.005/i386-linux
/usr/lib/perl5/5.00503/i386-linux
/usr/lib/perl5/5.00503
/usr/lib/perl5/site_perl/5.005/i386-linux
/usr/lib/perl5/site_perl/5.005 .) at ./vop.pl line 5.
BEGIN failed--compilation aborted at ./vop.pl line 5.
```

As you can see, the `Can't locate` phrase has changed, which is good.

A.2 Further steps needed at NIKHEF to install all Perl modules

Here is a list of what I had to do at NIKHEF.

1. download and install module Convert::ASN1 (needed before Net::LDAP would install)
2. download and install module Net::LDAP (actually I tried this first, but the Makefile.PL command complained that it could not find prerequisite Convert::ASN1)

At this point, when I typed `./vop.pl` I got the tool screen and everything worked OK.