

Managing Virtual Organizations (VO) at DESY using LDAP

- **Virtual Organizations (VO) – Overview**
- **Grid-vo.desy.de – Overview**
- **DESY LCG account requests analyzer**
- **DESY VO and LCG USERS Administration Tool**

Karen Mkoyan
Yerevan State University, Armenia
E-mail: karen.mkoyan@yepfi.am
07 September 2004
DESY, Hamburg

Virtual Organizations (VO) – Overview

- **A virtual organization is a dynamic collection of individuals, and resources which is defined by certain sharing rules.**
- **Technically, a user is represented by his/her certificate**
- **The collection of authorized users is defined on every machine in /etc/grid-security/grid-mapfile**
- **This file is regularly updated from VO server**
- **The server holds a list of all users belonging to a collection**
- **This collection we call a VO!**
- **A VO is defined in central list, e.g. a LDAP tree**

grid-vo.desy.de – Overview

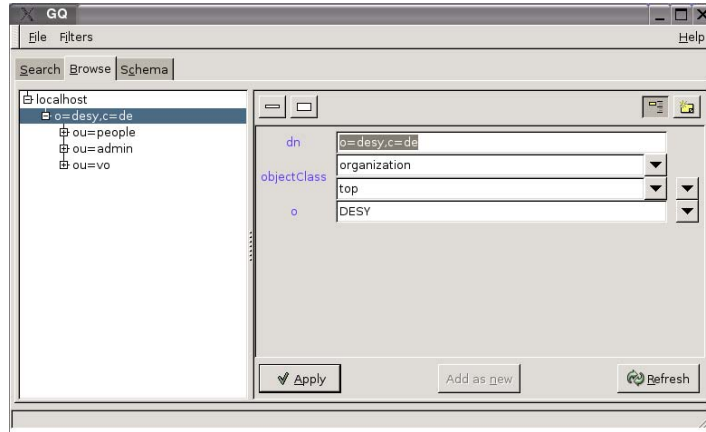


Figure 1: The LDAP server has 3 sub-trees, 'people', 'admin' and 'vo'

grid-vo.desy.de – Overview

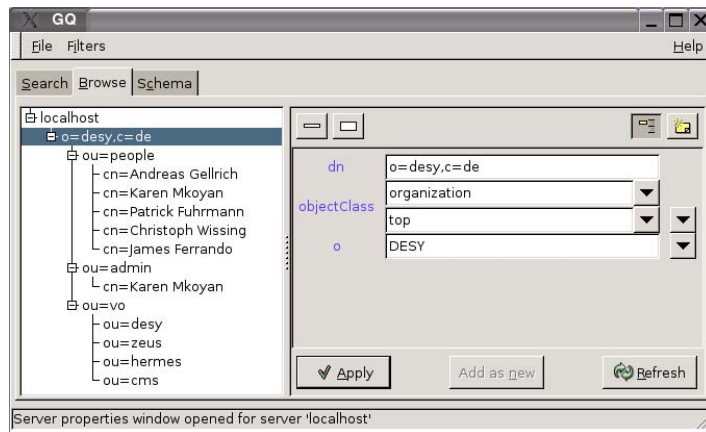


Figure 2: All trees are expanded.

grid-vo.desy.de – Overview

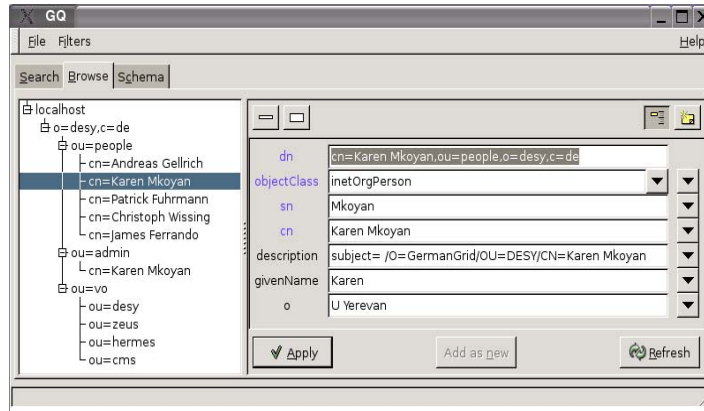


Figure 3: Person 'Karen Mkoyan' expanded, viewing details.

grid-vo.desy.de – Overview

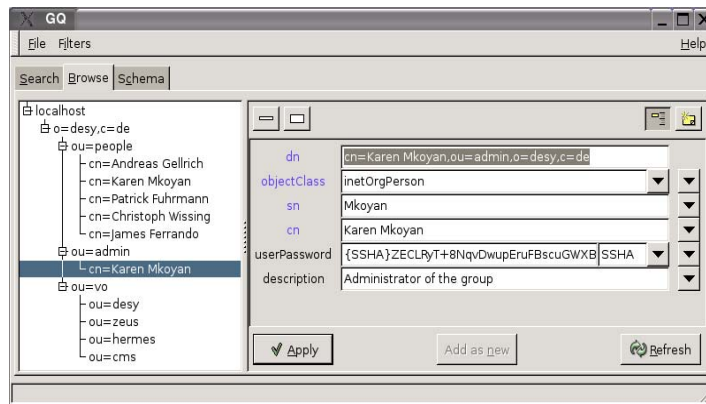


Figure 4: Group Administrator 'Karen Mkoyan' expanded, viewing details.

grid-vo.desy.de – Overview

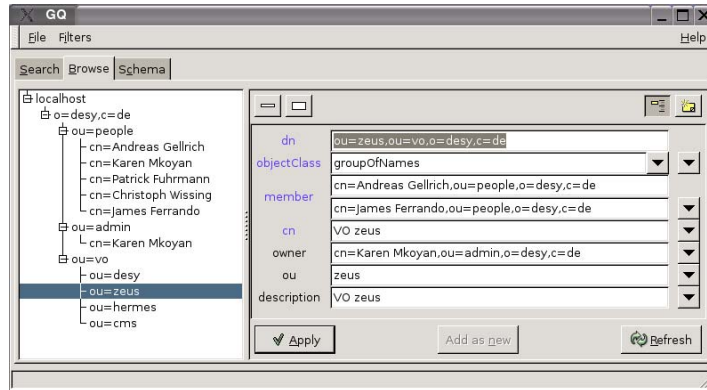


Figure 5: Group Administrator 'Karen Mkoyan' is the owner of VO 'zeus'.

grid-vo.desy.de – Overview

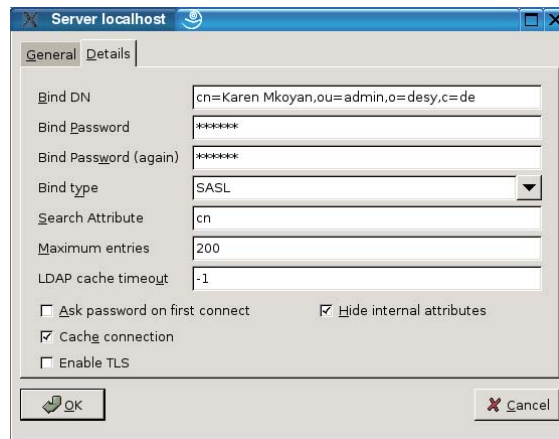
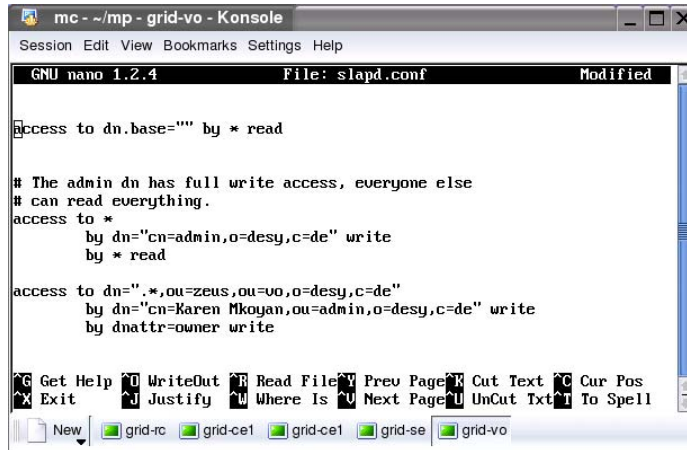


Figure 6: The DN to bind with to the LDAP server.

grid-vo.desy.de – Overview



```
mc - ~/mp - grid-vo - Konsole
Session Edit View Bookmarks Settings Help
GNU nano 1.2.4 File: slapd.conf Modified
# access to dn.base="" by * read

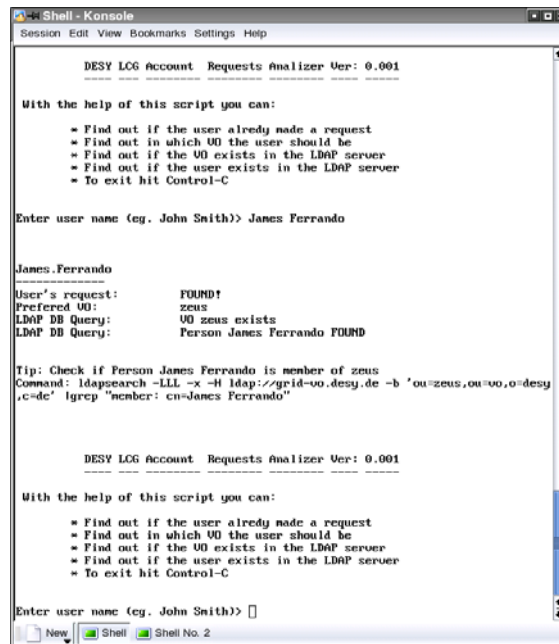
# The admin dn has full write access, everyone else
# can read everything.
access to *
  by dn="cn=admin,o=desy,c=de" write
  by * read

access to dn="*,ou=zeus,ou=vo,o=desy,c=de"
  by dn="cn=Karen Mkoyan,ou=admin,o=desy,c=de" write
  by dnattr=owner write

Get Help WriteOut Read File Prev Page Cut Text Cur Pos
Exit Justify Where Is Next Page UnCut Text To Spell
New grid-rc grid-ce1 grid-ce1 grid-se grid-vo
```

Figure 7: A part of the LDAP server configuration file, 'Karen Mkoyan' is VO 'zeus' admin.

DESY LCG account requests analyzer



```
Shell - Konsole
Session Edit View Bookmarks Settings Help

DESY LCG Account Requests Analyzer Ver: 0.001
-----

With the help of this script you can:
* Find out if the user already made a request
* Find out in which VO the user should be
* Find out if the VO exists in the LDAP server
* Find out if the user exists in the LDAP server
* To exit hit Control-C

Enter user name (eg. John Smith)> James Ferrando

James.Ferrando
-----
User's request:      FOUND!
Preferred VO:       zeus
LDAP DB Query:      VO zeus exists
LDAP DB Query:      Person James Ferrando FOUND

Tip: Check if Person James Ferrando is member of zeus
Command: ldapsearch -LLL -x -H ldap://grid-vo.desy.de -b 'ou=zeus,ou=vo,o=desy,c=de' |grep "member: cn=James Ferrando"

DESY LCG Account Requests Analyzer Ver: 0.001
-----

With the help of this script you can:
* Find out if the user already made a request
* Find out in which VO the user should be
* Find out if the VO exists in the LDAP server
* Find out if the user exists in the LDAP server
* To exit hit Control-C

Enter user name (eg. John Smith)> 
```

DESY LCG account requests analyzer

```
Shell - Konsole
Session Edit View Bookmarks Settings Help

DESY LCG Account Requests Analyzer Ver: 0.001

With the help of this script you can:

* Find out if the user already made a request
* Find out in which VO the user should be
* Find out if the VO exists in the LDAP server
* Find out if the user exists in the LDAP server
* To exit hit Control-C

Enter user name (eg. John Smith)> Luca Cinti

Luca.Cinti
-----
User's request:      FOUND!
Preferred VO:       zeus
LDAP DB Query:      VO zeus exists
LDAP DB Query:      Person Luca Cinti NOT FOUND

Tip: Add person Luca Cinti to LDAP DB, make him member of zeus
Tip: To generate LDIF file from request run this command:
Command: ./cert2ldif.pl -uo people,o=desy,c=de /afs/desy.de/group/grid/certs/zeus/Luca.Cinti

DESY LCG Account Requests Analyzer Ver: 0.001

With the help of this script you can:

* Find out if the user already made a request
* Find out in which VO the user should be
* Find out if the VO exists in the LDAP server
* Find out if the user exists in the LDAP server
* To exit hit Control-C

Enter user name (eg. John Smith)> 
```

DESY VO and LCG USERS Administration Tool

```
Shell - Konsole
Session Edit View Bookmarks Settings Help

DESY VO Administrative Tool Ver: 0.001

Choose one of the following (and hit enter):

[ v ]      List all VOs
[ lv ]     List VO
[ cv ]     Create VO
[ dv ]     Delete VO (be careful!)

[ i ]      Import LDIF file

[ u ]      List all Users
[ lu ]     List User

[ cu ]     Create User (interactive)
[ du ]     Delete User (interactive)

[ q ]      to exit

> lv

Enter VO name: cms

Listing VO cms
-----

dn: ou=cms,ou=vo,o=desy,c=de
ou: cms
cn: VO cms
owner: cn=Karen Mkogan,ou=admin,o=desy,c=de
member: cn=Andreas Gellrich,ou=people,o=desy,c=de
member: cn=Karen Mkogan,ou=people,o=desy,c=de
objectClass: groupOfNames
description: VO cms
```

DESY VO and LCG USERS Administration Tool

```
Shell - Konsole
Session Edit View Bookmarks Settings Help
DESY VO Administrative Tool Ver: 0.001

Choose one of the following (and hit enter):
[ l ] List all VOs
[ lv ] List VO
[ cv ] Create VO
[ dv ] Delete VO (be careful!)

[ i ] Import LDIF file
[ u ] List all Users
[ lu ] List User
[ cu ] Create User (interactive)
[ du ] Delete User (interactive)
[ q ] to exit

> cv

Enter VO name: hone

Creating VO hone
-----
Enter owner DN (eg. cn=John Smith,ou=people,o=desy,c=de):cn=John Smith,ou=pe
ople,o=desy,c=de
You need at least one member to be included in the VO hone
Enter member DN:cn=John Smith,ou=people,o=desy,c=de
ldap_initialize( ldap://grid-vo.desy.de )
add objectclass:
groupofnames
add ou:
hone
add cn:
VO hone
add description:
VO hone
add owner:
cn=John Smith,ou=people,o=desy,c=de
add member:
cn=John Smith,ou=people,o=desy,c=de
adding new entry "ou=hone, ou=vo, o=desy, c=de"
modify complete
```

DESY VO and LCG USERS Administration Tool

```
Shell - Konsole
Session Edit View Bookmarks Settings Help
DESY VO Administrative Tool Ver: 0.001

Choose one of the following (and hit enter):
[ l ] List all VOs
[ lv ] List VO
[ cv ] Create VO
[ dv ] Delete VO (be careful!)

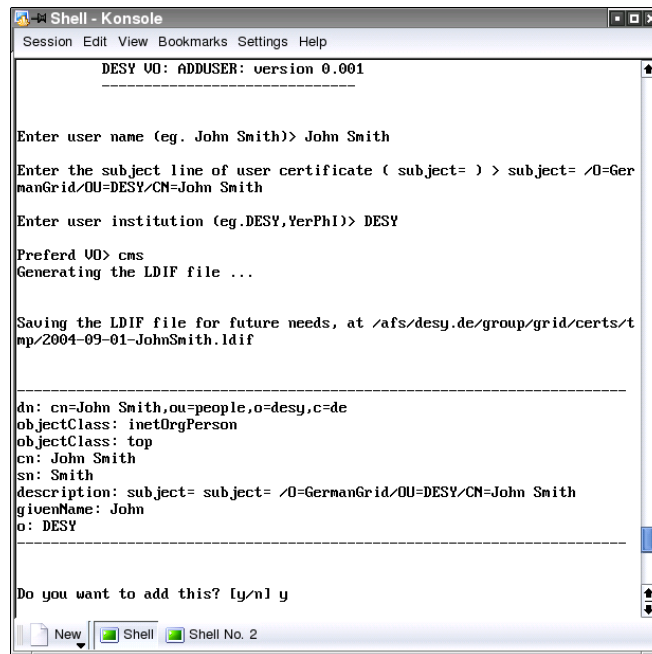
[ i ] Import LDIF file
[ u ] List all Users
[ lu ] List User
[ cu ] Create User (interactive)
[ du ] Delete User (interactive)
[ q ] to exit

> lv

Enter VO name: hone

Listing VO hone
-----
dn: ou=hone,ou=vo,o=desy,c=de
objectClass: groupofnames
ou: hone
cn: VO hone
description: VO hone
owner: cn=John Smith,ou=people,o=desy,c=de
member: cn=John Smith,ou=people,o=desy,c=de
```

DESY VO and LCG USERS Administration Tool



```
DESY VO: ADDUSER: version 0.001
-----
Enter user name (eg. John Smith)> John Smith
Enter the subject line of user certificate ( subject= ) > subject= /O=GermanGrid/OU=DESY/CN=John Smith
Enter user institution (eg.DESY,VerPhI)> DESY
Preferd UD> cms
Generating the LDIF file ...

Saving the LDIF file for future needs, at /afs/desy.de/group/grid/certs/tmp/2004-09-01-JohnSmith.ldif

-----
dn: cn=John Smith,ou=people,o=desy,c=de
objectClass: inetOrgPerson
objectClass: top
cn: John Smith
sn: Smith
description: subject= subject= /O=GermanGrid/OU=DESY/CN=John Smith
givenName: John
o: DESY
-----
Do you want to add this? [y/n] y
```

Full Report is available at
<http://grid.desy.de/talks/>

Karen Mkoyan
07 Sep. 2004
DESY, Hamburg