

Dante, Module LDAP

Inferno Nettverk A/S
Oslo Research Park
Gaustadalleen 21
NO-0349 Oslo
Norway

Date: 2011/06/13 13:19:23

1 Description

The *LDAP* module provides LDAP based user access control for the *Dante* SOCKS server.

Based on a users LDAP group membership or LDAP attributes, the module can be used to e.g., limit users access to web/ftp sites, or to only allow access for temporary staff to work related web/ftp sites.

If the username contains a domain extension, the module determines the LDAP server in an automatic way using the following method:

1. Extract the domain name from the username e.g. *DOMAIN.COM* from *user@DOMAIN.COM* when GSSAPI authentication is used.
2. Perform a DNS SRV record lookup (typically available in a Windows environment with Active Directory),
 - (a) without SSL, from *_ldap._tcp.DOMAIN.COM*.
 - (b) with SSL, from *_ldaps._tcp.DOMAIN.COM*, or if this entry does not exist, from *_ldap._tcp.DOMAIN.COM*.
3. Perform a DNS *A record* lookup of *DOMAIN.COM*.
4. Use */etc/hosts* file entry for *DOMAIN.COM*.
5. Sort entries by weight and priority and remove duplicates.

If the username does not contain any domain extension a pre-configured LDAP URL can be used to verify the LDAP group membership of users.

The module authenticates to the LDAP server using SASL/GSSAPI with the appropriate entry of the GSSAPI or LDAP specific keytab or the username/password provided as part of the LDAP URL.

2 Syntax

The syntax used to control the behavior of the LDAP module is as follows:

```
ldap.group: <LDAP-GROUP | LDAP-GROUP@ | LDAP-GROUP@DOMAIN.COM>
```

The parameters are defined as follows:

LDAP-GROUP name of LDAP group to be used for any user.

LDAP-GROUP@ name of LDAP group to be used for users who have a domain extension in their username (e.g. *user@DOMAIN.COM*).

LDAP-GROUP@DOMAIN.COM name of LDAP group to be used only for users who have a domain extension of *DOMAIN.COM* in their username.

This statement can be repeated.

```
ldap.group.hex: <LDAP-GROUP | LDAP-GROUP@ | LDAP-GROUP@DOMAIN.COM>
```

The parameters are defined as follows:

LDAP-GROUP name of LDAP group in hex UTF-8 to be used for any user.

LDAP-GROUP@ name of LDAP group in hex UTF-8 to be used for users who have a domain extension in their username (e.g. *user@DOMAIN.COM*).

LDAP-GROUP@DOMAIN.COM name of LDAP group in hex UTF-8 to be used only for users who have a domain extension of *DOMAIN.COM* (not in UTF-8) in their username.

For a translation of hex UTF-8 see for example <http://www.utf8-chartable.de/unicode-utf8-table.pl>

This statement can be repeated.

```
ldap.group.hex.all: <LDAP-GROUP | LDAP-GROUP@ | LDAP-GROUP@DOMAIN.COM>
```

The parameters are defined as follows:

LDAP-GROUP name of LDAP group in hex UTF-8 to be used for any user.

LDAP-GROUP@ name of LDAP group in hex UTF-8 to be used for users who have a domain extension in their username (e.g. *user@DOMAIN.COM*).

LDAP-GROUP@DOMAIN.COM name of LDAP group in hex UTF-8 to be used only for users who have a domain extension of *DOMAIN.COM* in hex UTF-8 in their username.

For a translation of hex UTF-8 see for example <http://www.utf8-chartable.de/unicode-utf8-table.pl>

This statement can be repeated.

```
ldap.domain: <DOMAIN>
```

The parameter is defined as follows:

DOMAIN default Kerberos domain to be used for pam/username authentication to emulate a GSSAPI user.

ldap.url: <URL>

The parameter is defined as follows:

URL LDAP URL of the form

ldap(s)://<username>:<password>@<Host:Port>/<basedn>.

This statement can be repeated.

ldap.server: <server@DOMAIN.COM>

The parameter is defined as follows:

server@DOMAIN.COM LDAP server name of the LDAP server for domain *DOMAIN.COM*. This setting avoids the automated server determination via DNS SRV or *A records*.

This statement can be repeated.

ldap.basedn: <base DN|base DN@DOMAIN.COM>

The parameters are defined as follows:

base DN base DN for LDAP search for any LDAP server.

base DN@DOMAIN.COM the base DN for LDAP search for LDAP server for domain *DOMAIN.COM*.

This statement can be repeated.

ldap.basedn.hex: <base DN|base DN@DOMAIN.COM>

The parameters are defined as follows:

base DN base DN in hex UTF-8 for LDAP search for any LDAP server.

base DN@DOMAIN.COM base DN for LDAP search for LDAP server for domain *DOMAIN.COM*.

This statement can be repeated.

ldap.basedn.hex.all: <base DN|base DN@DOMAIN.COM>

The parameters are defined as follows:

base DN base DN in hex UTF-8 for LDAP search for any LDAP server.

base DN@DOMAIN.COM base DN for LDAP search for LDAP server for domain *DOMAIN.COM* in hex UTF-8.

This statement can be repeated.

ldap.port: <PORT>

The parameter is defined as follows:

PORT LDAP port to be used for automatic LDAP server determination if no SRV DNS records exist.

`ldap.port.ssl: <PORT>`

The parameter is defined as follows:

PORT LDAP SSL port to be used for automatic LDAP server determination if no SRV DNS records exist.

`ldap.ssl: no|yes`

Require SSL for LDAP connection. The default value is no.

`ldap.certcheck: no|yes`

Require SSL certificate check. The default value is no.

`ldap.certfile: <filename>`

The parameter is defined as follows:

filename OpenLDAP CA certificate file name.

`ldap.certpath: <pathname>`

The parameter is defined as follows:

pathname Sun/Mozilla LDAP SDK certificate database location.

`ldap.debug: <debug level>`

The parameter is defined as follows:

debug level OpenLDAP debug level to set when OpenLDAP is used. The default value is 0.

`ldap.mdepth: <maximal search depth>`

The parameter is defined as follows:

maximal search depth maximal depth of recursive group searches in Active Directory. The default value is 0.

`ldap.keeprealm: no|yes`

Keep the realm name when comparing username with LDAP user attribute. The default value is no.

`ldap.filter: <filter>`

The parameter is defined as follows:

filter search filter for an OpenLDAP server. The default filter is `(memberuid=%s)` and assumes a `rfc2307bis` schema.

`ldap.filter.hex`: <filter>

The parameter is defined as follows:

filter search filter in hex UTF-8 for an OpenLDAP server. The default filter is (`memberid=%s`) and assumes a `rfc2307bis` schema.

`ldap.filter.ad`: <filter>

The parameter is defined as follows:

filter search filter for an Active Directory server. The default filter is (`samaccountname=%s`).

`ldap.filter.ad.hex`: <filter>

The parameter is defined as follows:

filter search filter in hex UTF-8 for an Active Directory server. The default filter is (`samaccountname=%s`).

`ldap.attribute`: <attribute>

The parameter is defined as follows:

attribute OpenLDAP server to be matched against the `ldap.group` values to identify the users group membership. The default attribute is `cn`.

`ldap.attribute.hex`: <attribute>

The parameter is defined as follows:

attribute hex UTF-8 for an OpenLDAP server to be matched against the `ldap.group` values to identify the users group membership. The default attribute is `cn`.

`ldap.attribute.ad`: <attribute>

The parameter is defined as follows:

attribute Active Directory server to be matched against the `ldap.group` values to identify the users group membership. The module will search recursively through groups. The default attribute is `memberof`.

`ldap.attribute.ad.hex`: <attribute>

The parameter is defined as follows:

attribute hex UTF-8 for an Active Directory server to be matched against the `ldap.group` values to identify the users group membership. The module will search recursively through groups. The default attribute is `memberof`.

`ldap.keytab`: <keytab>

The parameter is defined as follows:

keytab file containing the Kerberos principals to authenticate the module to the LDAP servers. The default keytab is *FILE:/etc/sockd.keytab* or the value of *gssapi.keytab* if it is set.

`ldap.auto.off: no|yes`

Disable automatic determination of LDAP server. The default value is no.

3 Semantics

The LDAP module statements described above are generally only used as a part of Dante socks-rules.

4 Special notes

The *Dante* server uses a set of timeout values defined in the Dante source code.

The following values are defined in the file *include/sockd.h*:

SOCKD_LDAP_DEADTIME the time a dead LDAP server should not be retried.

SOCKD_LDAP_SEARCHTIME the maximal time an LDAP search can take.

SOCKD_LDAP_TIMEOUT the maximal network connect time for an LDAP connection.

The following value is defined in *include/config.h*:

SOCKD_LDAPCACHE_TIMEOUT is the maximal time a LDAP group result is cached.

Should it be necessary to change these values, the above values will need to be redefined and the Dante server recompiled.

5 Examples

This section shows several examples of how it is possible to use the *LDAP* module. The first examples require GSSAPI user authentication. For Windows clients, the OpenText (formerly Hummingbird) client can be used (see <http://connectivity.opentext.com/products/socks-client.aspx>).

5.1 Limiting access to web/http

The rules below shows how one can limit access to web sites from clients on the 10.0.0.0/8 network to members of the *SOCKS_ALLOW* LDAP group.

```
# client-rule, no ldap statements.
client pass {
    from: 10.0.0.0/8 to: 0.0.0.0/0
    gssapi enctype: clear integrity confidentiality
}

# socks-rule, including a ldap statement.
pass {
    from: 10.0.0.0/8 to: 0.0.0.0/0 port = http
    command: connect
    ldap.group: SOCKS_ALLOW
}
```

For an OpenLDAP server with a rfc2307bis schema or an Active Directory server, *User1* and *User2* will be allowed, whereas *User3* would be refused access (see Appendix for additional details).

5.2 Limiting access to SSL VPNs

The next rule, if placed before other general rules, shows how one can limit access for temporary staff on the 10.0.0.0/8 network to only a specific work related site.

```
client pass {
    from: 10.0.0.0/8 to: 0.0.0.0/0
    gssapi enctype: clear integrity confidentiality
}

pass {
    from: 10.0.0.0/8 to: sslvpn.example.com port = 443
    command: connect
    ldap.group: Temporary
    ldap.filter: (uid=%s)
    ldap.attribute: employeeType
}

pass {
    from: 10.0.0.0/8 to: 0.0.0.0/0 port = 443
    command: connect
    ldap.group: Permanent
    ldap.filter: (uid=%s)
}
```



```
    ldap.attribute: employeeType
}
```

Assuming the OpenLDAP configuration in the Appendix example is used, the temporary user *User3* is only allowed to connect to *sslvpn.example.com* on port 443 whereas the permanent users *User1* and *User2* can connect to any secure website via https.

5.3 Limiting ftp to company employees only

The next rule shows how one can limit access to ftp sites to company employees on the 10.0.0.0/8 network.

Note that this example will only work for *active* ftp, because there are no fixed port numbers for *passive* ftp.

```
client pass {
    from: 10.0.0.0/8 to: 0.0.0.0/0
    gssapi.enctype: clear integrity confidentiality
}

pass {
    from: 0.0.0.0/0 port = ftp-data to: 10.0.0.0/8
    command: bindreply
    ldap.group: MyCompany
    ldap.keeprealm: yes
    ldap.filter.ad: (userprincipalname=%s)
    ldap.attribute.ad: company
}

pass {
    from: 10.0.0.0/8 port = ftp to: 0.0.0.0/0
    command: connect
    ldap.group: MyCompany
    ldap.keeprealm: yes
    ldap.filter.ad: (userprincipalname=%s)
    ldap.attribute.ad: company
}
```

Assuming the Active Directory example in the Appendix is used, *User3* is only allowed to connect to ftp data whereas the users *User1* and *User2* are not allowed.

5.4 Using an LDAP URL to determine LDAP group membership

The next rule shows how one can limit access to ftp sites for company employees on the 10.0.0.0/8 network without requiring GSSAPI authentication. An LDAP URL with a directly specified username (here *user*) and password (here *pass*) is used for authentication.

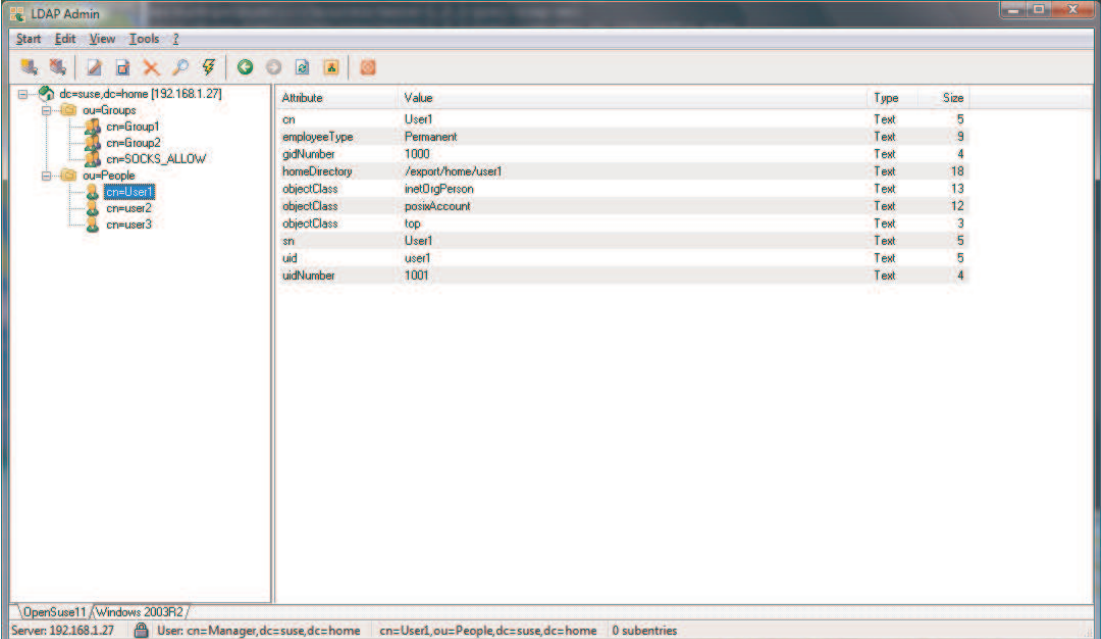
```
client pass {
    from: 10.0.0.0/8 to: 0.0.0.0/0
}

pass {
    from: 0.0.0.0/0 port = ftp-data to: 10.0.0.0/8
    command: bindreply
    ldap.group: SOCKS_ALLOW
    ldap.auto.off: yes
    ldap.url: ldap://user:pass@ldap1.example.com:389/OU=SALES,DC=MYCOMPANY,DC=COM
    ldap.url: ldap://user:pass@ldap2.example.com:389/OU=SALES,DC=MYCOMPANY,DC=COM
}

pass {
    from: 10.0.0.0/8 port = ftp to: 0.0.0.0/0
    command: connect
    ldap.group: SOCKS_ALLOW
    ldap.auto.off: yes
    ldap.url: ldap://user:pass@ldap1.example.com:389/OU=SALES,DC=MYCOMPANY,DC=COM
    ldap.url: ldap://user:pass@ldap2.example.com:389/OU=SALES,DC=MYCOMPANY,DC=COM
}
```

6 Appendix

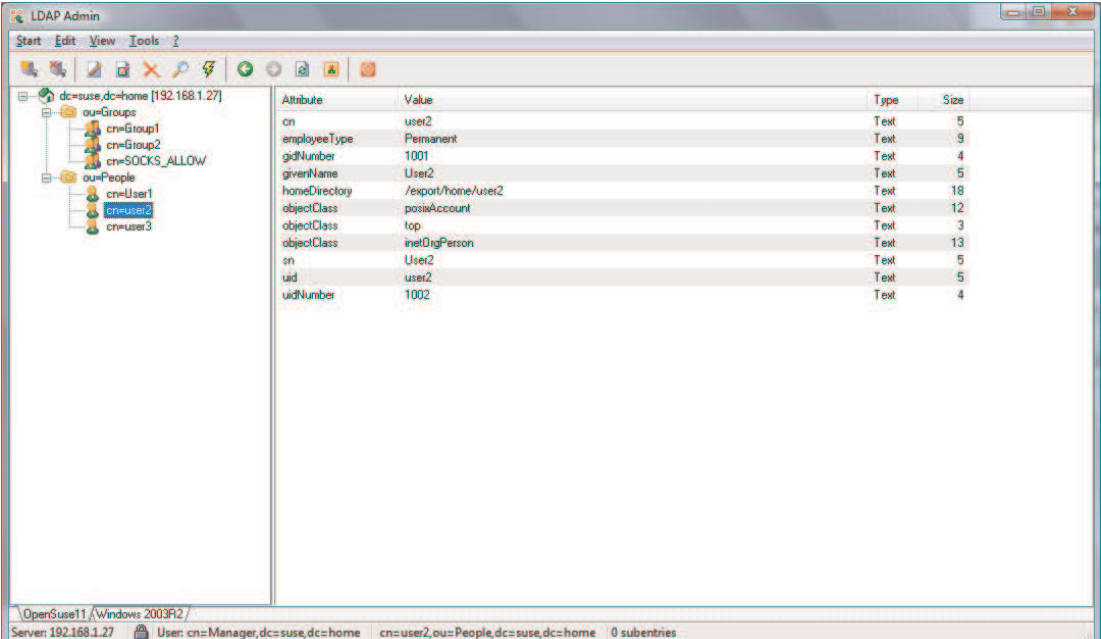
6.1 OpenLdap



The screenshot shows the LDAP Admin interface for a server at 192.168.1.27. The left pane shows a tree view with 'ou=People' selected, containing 'cn=User1', 'cn=user2', and 'cn=user3'. The right pane displays the details for 'cn=User1' in a table format.

Attribute	Value	Type	Size
cn	User1	Text	5
employeeType	Permanent	Text	9
gidNumber	1000	Text	4
homeDirectory	/export/home/User1	Text	18
objectClass	inetOrgPerson	Text	13
objectClass	posixAccount	Text	12
objectClass	top	Text	3
sn	User1	Text	5
uid	user1	Text	5
uidNumber	1001	Text	4

Server: 192.168.1.27 User: cn=Manager,dc=suse,dc=home cn=User1,ou=People,dc=suse,dc=home 0 subentries



The screenshot shows the LDAP Admin interface for a server at 192.168.1.27. The left pane shows a tree view with 'ou=People' selected, containing 'cn=User1', 'cn=user2', and 'cn=user3'. The right pane displays the details for 'cn=user2' in a table format.

Attribute	Value	Type	Size
cn	user2	Text	5
employeeType	Permanent	Text	9
gidNumber	1001	Text	4
givenName	User2	Text	5
homeDirectory	/export/home/user2	Text	18
objectClass	posixAccount	Text	12
objectClass	top	Text	3
objectClass	inetOrgPerson	Text	13
sn	User2	Text	5
uid	user2	Text	5
uidNumber	1002	Text	4

Server: 192.168.1.27 User: cn=Manager,dc=suse,dc=home cn=user2,ou=People,dc=suse,dc=home 0 subentries

LDAP Admin

Start Edit View Tools ?

dc=suse,dc=home [192.168.1.27]

- ou=Groups
 - cn=Group1
 - cn=Group2
 - cn=SOCKS_ALLOW
- ou=People
 - cn=User1
 - cn=user2
 - cn=user3

Attribute	Value	Type	Size
cn	user3	Text	5
displayName	User3	Text	5
employeeType	Temporary	Text	9
gidNumber	1002	Text	4
givenName	User3	Text	5
homeDirectory	/export/home/user3	Text	18
mail	user3@SUSE.HOME	Text	15
objectClass	posixAccount	Text	12
objectClass	top	Text	3
objectClass	inetOrgPerson	Text	13
sn	User3	Text	5
uid	user3	Text	5
uidNumber	1003	Text	4

Server: 192.168.1.27 User: cn=Manager,dc=suse,dc=home cn=user3,ou=People,dc=suse,dc=home 0 subentries

LDAP Admin

Start Edit View Tools ?

dc=suse,dc=home [192.168.1.27]

- ou=Groups
 - cn=Group1
 - cn=Group2
 - cn=SOCKS_ALLOW
- ou=People
 - cn=User1
 - cn=user2
 - cn=user3

Attribute	Value	Type	Size
cn	Group1	Text	6
gidNumber	1001	Text	4
objectClass	posixGroup	Text	10
objectClass	namedObject	Text	11
objectClass	top	Text	3

Server: 192.168.1.27 User: cn=Manager,dc=suse,dc=home cn=Group1,ou=Groups,dc=suse,dc=home 0 subentries

LDAP Admin

Start Edit View Tools ?

dc=suse,dc=home [192.168.1.27]

- ou=Groups
 - cn=Group1
 - cn=Group2
 - cn=SOCKS_ALLOW
- ou=People
 - cn=User1
 - cn=user2
 - cn=user3

Attribute	Value	Type	Size
cn	Group2	Text	6
gidNumber	1002	Text	4
objectClass	posixGroup	Text	10
objectClass	namedObject	Text	11
objectClass	top	Text	3

Server: 192.168.1.27 User: cn=Manager,dc=suse,dc=home cn=Group2,ou=Groups,dc=suse,dc=home 0 subentries

LDAP Admin

Start Edit View Tools ?

dc=suse,dc=home [192.168.1.27]

- ou=Groups
 - cn=Group1
 - cn=Group2
 - cn=SOCKS_ALLOW
- ou=People
 - cn=User1
 - cn=user2
 - cn=user3

Attribute	Value	Type	Size
cn	SOCKS_ALLOW	Text	11
gidNumber	1000	Text	4
memberUid	user2	Text	5
objectClass	posixGroup	Text	10
objectClass	namedObject	Text	11
objectClass	top	Text	3

Server: 192.168.1.27 User: cn=Manager,dc=suse,dc=home cn=SOCKS_ALLOW,ou=Groups,dc=suse,dc=home 0 subentries

6.2 Active Directory

The screenshot shows the LDAP Admin console window. On the left is a tree view of the directory structure, with 'CN=User1' selected. The main pane displays a list of attributes for this user object.

Attribute	Value	Type	Size
accountExpires	3223372036854775807	Text	19
badPasswordTime	0	Text	1
badPwdCount	0	Text	1
cn	User1	Text	5
codePage	0	Text	1
countryCode	0	Text	1
displayName	User1	Text	5
distinguishedName	CN=User1,CN=Users,DC=win2003r2,DC=home	Text	38
givenName	User1	Text	5
instanceType	4	Text	1
lastLogoff	0	Text	1
lastLogon	0	Text	1
logonCount	0	Text	1
memberOf	CN=SOCKS_ALLOW,OU=Groups,DC=win2003r2,DC=home	Text	45
name	User1	Text	5
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=win2003r2,DC=home	Text	57
objectClass	top	Text	3
objectClass	person	Text	6
objectClass	organizationalPerson	Text	20
objectClass	user	Text	4
objectGUID	A6 37 1F E5 82 8F DD 4D AD 33 75 C1 2F 90 08 D3	Binary	16
objectSid	01 05 00 00 00 00 00 05 15 00 00 00 A6 5A 02 6D 64 EE 7D 41 4F 5A 88 9A 8D 04 00 00	Binary	28
primaryGroupID	513	Text	3
pwdLastSet	129068531831093750	Text	18
sAMAccountName	user1	Text	5
sAMAccountType	805306368	Text	9
userAccountControl	66048	Text	5
userPrincipalName	user1@win2003r2.home	Text	20
uSNChanged	957170	Text	6
uSNCreated	957165	Text	6
whenChanged	20091230132623.0Z	Text	17
whenCreated	20091230132623.0Z	Text	17

The status bar at the bottom indicates the server path: \\OpenSuse11\Windows 2003R2\ and the current user: User: CN=Administrator,CN=Users,DC=win2003r2,DC=home. It also shows the current object: CN=User1,CN=Users,DC=win2003r2,DC=home with 0 subentries.

LDAP Admin

Start Edit View Tools

CN=ForeignSecurityPrincipals
 CN=Infrastructure
 CN=LostAndFound
 CN=NTDS Quotas
 CN=Program Data
 CN=System
 CN=Users
 CN=Administrator
 CN=Cert Publishers
 CN=CERTSVC_DCDM_ACCE
 CN=DHCP Administrators
 CN=DHCP Users
 CN=DnsAdmins
 CN=DnsUpdateProxy
 CN=Domain Admins
 CN=Domain Computers
 CN=Domain Controllers
 CN=Domain Guests
 CN=Domain Users
 CN=Enterprise Admins
 CN=Group Policy Creator Ovrn
 CN=Guest
 CN=IIS_WPG
 CN=USR_WIN2003R2
 CN=WAM_WIN2003R2
 CN=krbtgt
 CN=RAS and IAS Servers
 CN=Schema Admins
 CN=Session Directory Comput
 CN=SQLARIS.HOME\$
 CN=SQLServer2005MSSQLS
 CN=SQLServer2005MSSQLU
 CN=SQLServer2005QLBrow
 CN=SUSE.HOME\$
 CN=User1
 CN=User2
 CN=User3
 CN=Win2003R2Users
 CN=WINS Users

Attribute	Value	Type	Size
accountExpires	9223372036854775807	Text	19
badPasswordTime	0	Text	1
badPwdCount	0	Text	1
cn	User2	Text	5
codePage	0	Text	1
countryCode	0	Text	1
displayName	User2	Text	5
distinguishedName	CN=User2,CN=Users,DC=win2003r2,DC=home	Text	38
givenName	User2	Text	5
instanceType	4	Text	1
lastLogoff	0	Text	1
lastLogon	0	Text	1
logonCount	0	Text	1
memberOf	CN=SOCKS_GROUP1,OU=Groups,DC=win2003r2,DC=home	Text	46
name	User2	Text	5
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=win2003r2,DC=home	Text	57
objectClass	top	Text	3
objectClass	person	Text	6
objectClass	organizationalPerson	Text	20
objectClass	user	Text	4
objectGUID	2F E7 1D 81 03 A5 8A 40 A3 D 8 7A 05 2D 9E CA 9A	Binary	16
objectSid	01 05 00 00 00 00 00 05 15 00 00 00 A6 5A 02 6D 64 EE 7D 41 4F 5A 88 9A 8E 04 00 00	Binary	28
primaryGroupID	513	Text	3
pwdLastSet	129066532149218750	Text	18
sAMAccountName	user2	Text	5
sAMAccountType	805306368	Text	9
userAccountControl	66048	Text	5
userPrincipalName	user2@win2003r2.home	Text	20
uSNCreated	557172	Text	6
whenChanged	20091230132654.0Z	Text	17
whenCreated	20091230132654.0Z	Text	17

\OpenUse11\Windows 2003R2/
 Server: 192.168.1.12 User: CN=Administrator,CN=Users,DC=win2003r2,DC=home CN=User2,CN=Users,DC=win2003r2,DC=home 0 subentries

LDAP Admin

Start Edit View Tools ?

CN=ForeignSecurityPrincipals
 CN=Infrastructure
 CN=LostAndFound
 CN=NTDS Quotas
 CN=Program Data
 CN=System
 CN=Users
 CN=Administrator
 CN=Cert Publishers
 CN=CERTSVC_DCOM_ACCE
 CN=DHCP Administrators
 CN=DHCP Users
 CN=DnsAdmins
 CN=DnsUpdateProxy
 CN=Domain Admins
 CN=Domain Computers
 CN=Domain Controllers
 CN=Domain Guests
 CN=Domain Users
 CN=Enterprise Admins
 CN=Group Policy Creator Ovr
 CN=Guest
 CN=IS_wFG
 CN=USR_WIN2003R2
 CN=IWAM_WIN2003R2
 CN=krbtgt
 CN=RAS and IAS Servers
 CN=Schema Admins
 CN=Session Directory Comput
 CN=SQLARIS.HOME\$
 CN=SQLServer2005MSSQLS
 CN=SQLServer2005MSSQLU
 CN=SQLServer2005QLBrow
 CN=SUSE.HOME\$
 CN=User1
 CN=User2
 CN=User3
 CN=win2003R2Users
 CN=WIN5 Users

Attribute	Value	Type	Size
accountExpires	3223372036854775807	Text	19
badPasswordTime	0	Text	1
badPwdCount	0	Text	1
cn	User3	Text	5
codePage	0	Text	1
company	MyCompany	Text	9
countryCode	0	Text	1
displayName	User3	Text	5
distinguishedName	CN=User3,CN=Users,DC=win2003r2,DC=home	Text	38
givenName	User3	Text	5
instanceType	4	Text	1
lastLogoff	0	Text	1
lastLogon	0	Text	1
logonCount	0	Text	1
name	User3	Text	5
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=win2003r2,DC=home	Text	57
objectClass	top	Text	3
objectClass	person	Text	6
objectClass	organizationalPerson	Text	20
objectClass	user	Text	4
objectGUID	FC E1 77 A3 CD A7 DD 4C 9A 35 D0 31 FB ED 1B 50	Binary	16
objectSid	01 05 00 00 00 00 05 15 00 00 00 A6 5A 02 6D 64 EE 7D 41 4F 5A 88 9A 8F 04 00 00	Binary	28
primaryGroupID	513	Text	3
pwdLastSet	12908853294375000	Text	18
sAMAccountName	user3	Text	5
sAMAccountType	805306368	Text	9
userAccountControl	66048	Text	5
userPrincipalName	user3@win2003r2.home	Text	20
uSNChanged	957193	Text	6
uSNCreated	957179	Text	6
whenChanged	20091230132931.0Z	Text	17
whenCreated	20091230132719.0Z	Text	17

\OpenSuse11\Windows 2003R2/
 Server: 192.168.1.12 User: CN=Administrator,CN=Users,DC=win2003r2,DC=home CN=User3,CN=Users,DC=win2003r2,DC=home 0 subentries

LDAP Admin

Start Edit View Tools ?

dc=win2003r2,DC=home [192.168.1.12]
 OU=Domain Controllers
 OU=Groups
 CN=Group1
 CN=Group2
 CN=SOCKS_ALLOW
 CN=SOCKS_GROUP1
 OU=Ldapconfig
 OU=NetGroups
 OU=SambaServers
 OU=ServicePrincipals
 CN=Builtin
 CN=Computers
 CN=defaultMigrationContainer30
 CN=ForeignSecurityPrincipals
 CN=Infrastructure
 CN=LostAndFound
 CN=NTDS Quotas
 CN=Program Data
 CN=System
 CN=Users

Attribute	Value	Type	Size
cn	Group1	Text	6
distinguishedName	CN=Group1,OU=Groups,DC=win2003r2,DC=home	Text	40
groupType	-2147483646	Text	11
instanceType	4	Text	1
member	CN=Markus Moeller,CN=Users,DC=win2003r2,DC=home	Text	47
name	Group1	Text	6
objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=win2003r2,DC=home	Text	56
objectClass	top	Text	3
objectClass	group	Text	5
objectGUID	50 26 D1 AF 0A 6E 22 4D A3 A1 39 48 91 C4 C7 5E	Binary	16
objectSid	01 05 00 00 00 00 05 15 00 00 00 A6 5A 02 6D 64 EE 7D 41 4F 5A 88 9A 75 04 00 00	Binary	28
sAMAccountName	Group1	Text	6
sAMAccountType	268435456	Text	9
uSNChanged	156509	Text	6
uSNCreated	156469	Text	6
whenChanged	20080629114222.0Z	Text	17
whenCreated	20080629113642.0Z	Text	17

\OpenSuse11\Windows 2003R2/
 Server: 192.168.1.12 User: CN=Administrator,CN=Users,DC=win2003r2,DC=home CN=Group1,OU=Groups,DC=win2003r2,DC=home 0 subentries

LDAP Admin

Start Edit View Tools ?

dc=win2003r2,DC=home [192.168.1.12]

- OU=Domain Controllers
 - OU=Groups
 - CN=Group1
 - CN=Group2**
 - CN=SOCKS_ALLOW
 - CN=SOCKS_GROUP1
 - OU=Ldapconfig
 - OU=NetGroups
 - OU=SambaServers
 - OU=ServicePrincipals
 - CN=Builtin
 - CN=Computers
 - CN=defaultMigrationContainer30
 - CN=ForeignSecurityPrincipals
 - CN=Infrastructure
 - CN=LostAndFound
 - CN=NTDS Quotas
 - CN=Program Data
 - CN=System
 - CN=Users

Attribute	Value	Type	Size
cn	Group2	Text	6
distinguishedName	CN=Group2,OU=Groups,DC=win2003r2,DC=home	Text	40
groupType	-2147483646	Text	11
instanceType	4	Text	1
member	CN=Matkus Moeller,CN=Users,DC=win2003r2,DC=home	Text	47
memberOf	CN=SOCKS_ALLOW,CN=Users,DC=win2003r2,DC=home	Text	44
name	Group2	Text	6
objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=win2003r2,DC=home	Text	56
objectClass	top	Text	3
objectClass	group	Text	5
objectGUID	C2 0E 96 10 C6 A0 18 4E B1 37 28 A1 11 C9 C1 60	Binary	16
objectSid	01 05 00 00 00 00 05 15 00 00 00 A6 5A 02 6D 64 EE 7D 41 4F 5A 88 9A 76 04 00 00	Binary	28
sAMAccountName	Group2	Text	6
sAMAccountType	268435456	Text	9
uSNCreated	156512	Text	6
uSNCreated	156473	Text	6
whenChanged	20080629114222.0Z	Text	17
whenCreated	20080629113711.0Z	Text	17

OpenSuse11 / Windows 2003R2 /

Server: 192.168.1.12 User: CN=Administrator,CN=Users,DC=win2003r2,DC=home CN=Group2,OU=Groups,DC=win2003r2,DC=home 0 subentries

LDAP Admin

Start Edit View Tools ?

dc=win2003r2,DC=home [192.168.1.12]

- OU=Domain Controllers
 - OU=Groups
 - CN=Group1
 - CN=Group2
 - CN=SOCKS_ALLOW**
 - CN=SOCKS_GROUP1
 - OU=HomeUsers
 - OU=Ldapconfig
 - OU=NetGroups
 - OU=SambaServers
 - OU=ServicePrincipals
 - CN=Builtin
 - CN=Computers
 - CN=defaultMigrationContainer30
 - CN=ForeignSecurityPrincipals
 - CN=Infrastructure
 - CN=LostAndFound
 - CN=NTDS Quotas
 - CN=Program Data
 - CN=System
 - CN=Users

Attribute	Value	Type	Size
cn	SOCKS_ALLOW	Text	11
distinguishedName	CN=SOCKS_ALLOW,OU=Groups,DC=win2003r2,DC=home	Text	45
groupType	-2147483646	Text	11
instanceType	4	Text	1
member	CN=User1,CN=Users,DC=win2003r2,DC=home	Text	38
member	CN=SOCKS_GROUP1,OU=Groups,DC=win2003r2,DC=home	Text	46
name	SOCKS_ALLOW	Text	11
objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=win2003r2,DC=home	Text	56
objectClass	top	Text	3
objectClass	group	Text	5
objectGUID	DD 38 F2 25 3D 8C 07 41 90 33 3C 24 89 3D 96 18	Binary	16
objectSid	01 05 00 00 00 00 05 15 00 00 00 A6 5A 02 6D 64 EE 7D 41 4F 5A 88 9A 88 04 00 00	Binary	28
sAMAccountName	SOCKS_ALLOW	Text	11
sAMAccountType	268435456	Text	9
uSNCreated	557266	Text	6
uSNCreated	557154	Text	6
whenChanged	20100101122514.0Z	Text	17
whenCreated	20091230132506.0Z	Text	17

Windows 2003R2 /

Server: 192.168.1.12 User: CN=Administrator,CN=Users,DC=win2003r2,DC=home CN=SOCKS_ALLOW,OU=Groups,DC=win2003r2,DC=home 0 subentries

LDAP Admin

Start Edit View Tools ?

dc=win2003r2,DC=home [192.168.1.12]

- OU=Domain Controllers
 - OU=Groups
 - CN=Group1
 - CN=Group2
 - CN=SOCKS_ALLOW
 - CN=SOCKS_GROUP1**
 - OU=HomeUsers
 - OU=Ldapconfig
 - OU=NetGroups
 - OU=SambaServers
 - OU=ServicePrincipals
 - CN=Builtin
 - CN=Computers
 - CN=defaultMigrationContainer30
 - CN=ForeignSecurityPrincipals
 - CN=Infrastructure
 - CN=LostAndFound
 - CN=NTDS Quotas
 - CN=Program Data
 - CN=System
 - CN=Users

Attribute	Value	Type	Size
cn	SOCKS_GROUP1	Text	12
distinguishedName	CN=SOCKS_GROUP1,OU=Groups,DC=win2003r2,DC=home	Text	46
groupType	-2147483646	Text	11
instanceType	4	Text	1
member	CN=User2,CN=Users,DC=win2003r2,DC=home	Text	38
memberOf	CN=SOCKS_ALLOW,OU=Groups,DC=win2003r2,DC=home	Text	45
name	SOCKS_GROUP1	Text	12
objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=win2003r2,DC=home	Text	56
objectClass	top	Text	3
objectClass	group	Text	5
objectGUID	D2 52 90 DD 9A 2F ED 4F 9A CE AF AE 1D 25 C9 C8	Binary	16
objectSid	01 05 00 00 00 00 05 15 00 00 00 A6 5A 02 6D 64 EE 7D 41 4F 5A 88 9A 8A 04 00 00	Binary	28
sAMAccountName	SOCKS_GROUP1	Text	12
sAMAccountType	269435456	Text	9
uSNChanged	557263	Text	6
uSNCreated	557190	Text	6
whenChanged	20100101122514.0Z	Text	17
whenCreated	20091230132451.0Z	Text	17

Windows 2003R2 /
 Server: 192.168.1.12 User: CN=Administrator,CN=Users,DC=win2003r2,DC=home CN=SOCKS_GROUP1,OU=Groups,DC=win2003r2,DC=home 0 subentries