# Linux and NDS®, with LDAP

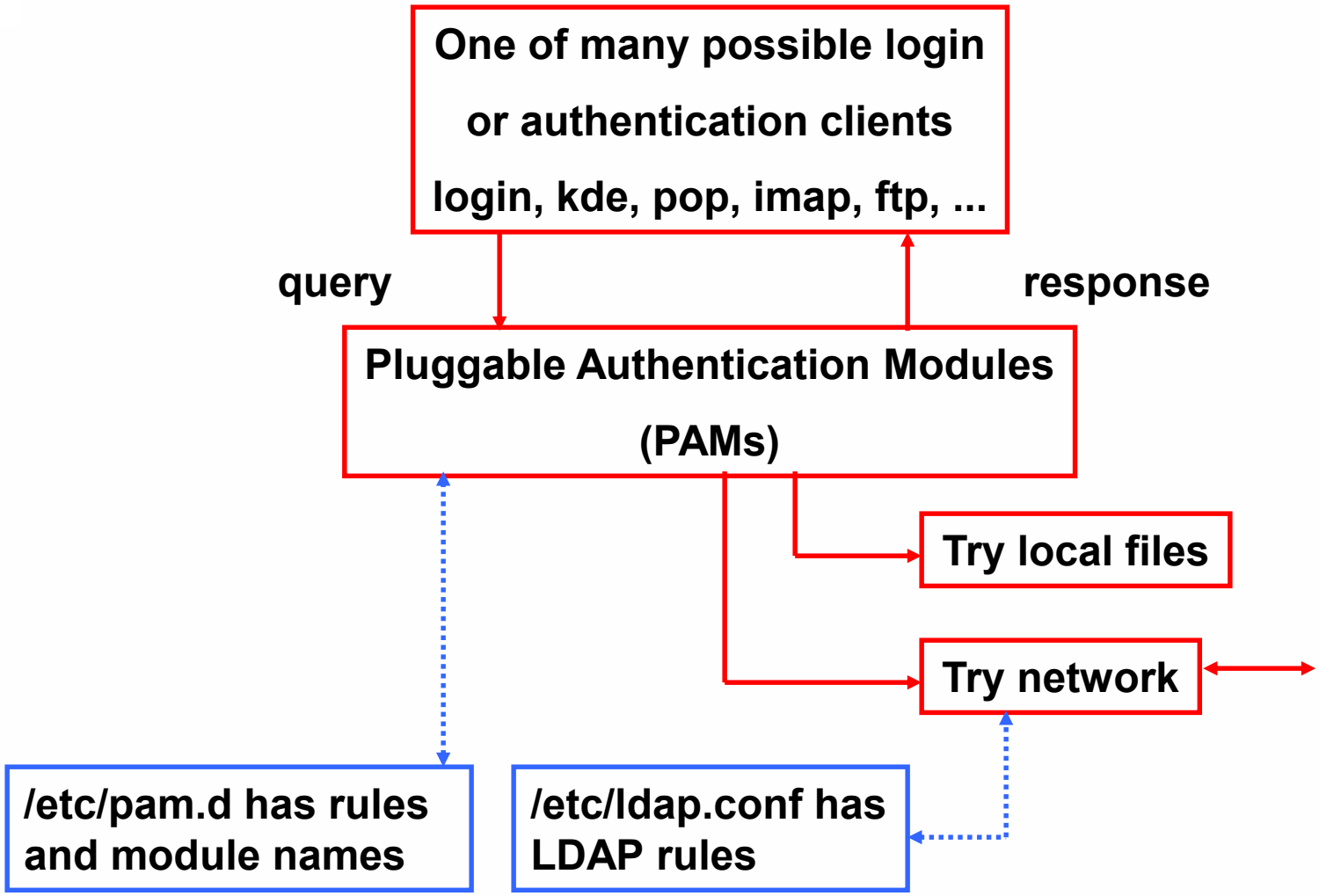
Joe R. Doupnik, Professor of ECE
*jrd@cc.usu.edu*
Utah State University

Based on a presentation by
Randy Cook, Calderasystems Inc

BrainShare2000

Novell.

# Login/authentication process




BrainShare2000

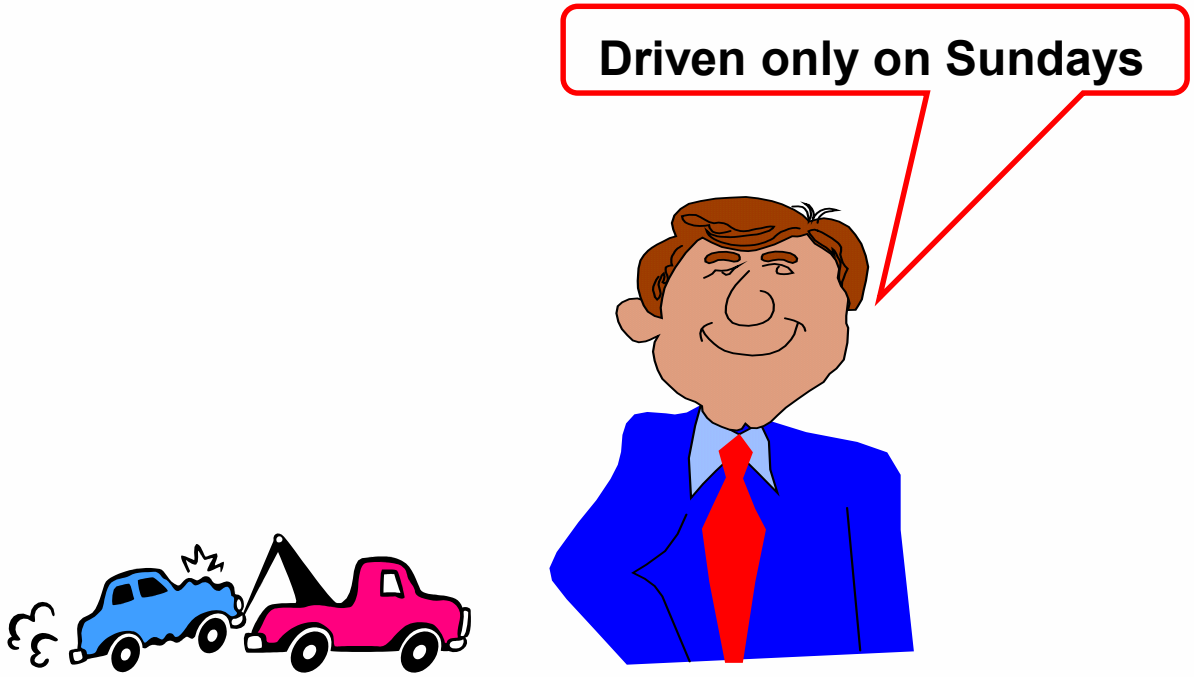
# Login control

- Login, check username and password
- Try various methods, allow some to fail and yet others to succeed

BrainShare2000

# Authentication

- Checks access to resources, vouches for user




BrainShare2000

# Session

- Add startup and shutdown procedures around a session
- Used by NDS connections, and others

BrainShare2000

# PAM's configuration options

- Things PAM can check upon
  - account = services
  - authentication = you know who I am
  - password = our little secret
  - session = wrapper around session
- Examination results, each rule
  - sufficient = passing this is enough
  - requisite = must pass this check
  - required = must pass, other checks done
  - optional = maybe, maybe not, shrug

BrainShare2006

# /etc/pam.d modules

```
[root@netlab4 pam.d]# ls

README  ftp.nds  login.nds     pop          rlogin.nds  su.nds
chfn    imap     netatalk.pamd pop+imap.nds rsh         xscreensaver
chsh    kde      other         rexec        samba
ftp     login    passwd        rlogin       su
```

Edit the kde file to add LDAP to NDS

BrainShare2000

# /etc/pam.d/kde, modified twice

```
[root@netlab4 pam.d]# more kde

#%PAM-1.0
auth    sufficient      /lib/security/pam_ldap.so          <--- Added LDAP
auth            required    /lib/security/pam_pwdb.so shadow nullok use_first_pass
auth            required    /lib/security/pam_nologin.so
account sufficient      /lib/security/pam_ldap.so          <--- Added LDAP
account     required    /lib/security/pam_pwdb.so
password    required    /lib/security/pam_cracklib.so type=user retry=3
password    required    /lib/security/pam_pwdb.so use_authtok # md5 shadow

session     required    /lib/security/pam_pwdb.so
```

# File /etc/ldap.conf

- **Original**

```
# Your LDAP server. Must be resolvable without using LDAP.
host 127.0.0.1
# The distinguished name of the search base.
base dc=padl,dc=com
```

- **Revised for local NDS properties**

```
# Your LDAP server. Must be resolvable without using LDAP.
host netlab2.usu.edu      <--- Your NetWare server's IP name
# The distinguished name of the search base.
base o=usu                <--- Where NDS object Ldap-group resides
deref always              <--- Dereference NDS "alias" usernames
```

BrainShare2000

# File /etc/nsswitch.conf excerpt

## Name Service Switch configuration file

- **Original**

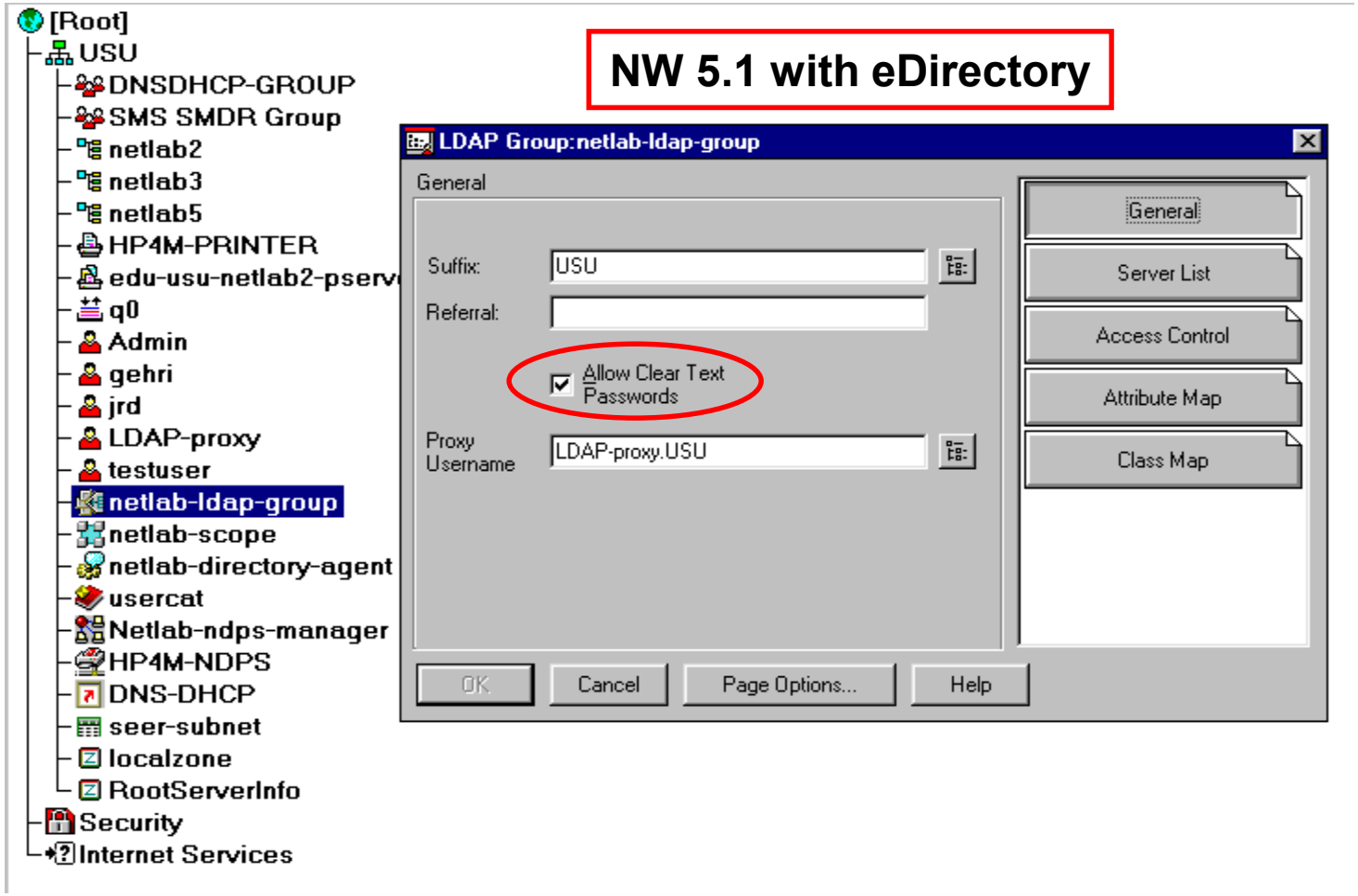
```
passwd:         compat
shadow:         compat
group:          compat
```

- **Revised to add LDAP password support**

```
passwd:         compat ldap
shadow:         compat
group:          compat
```

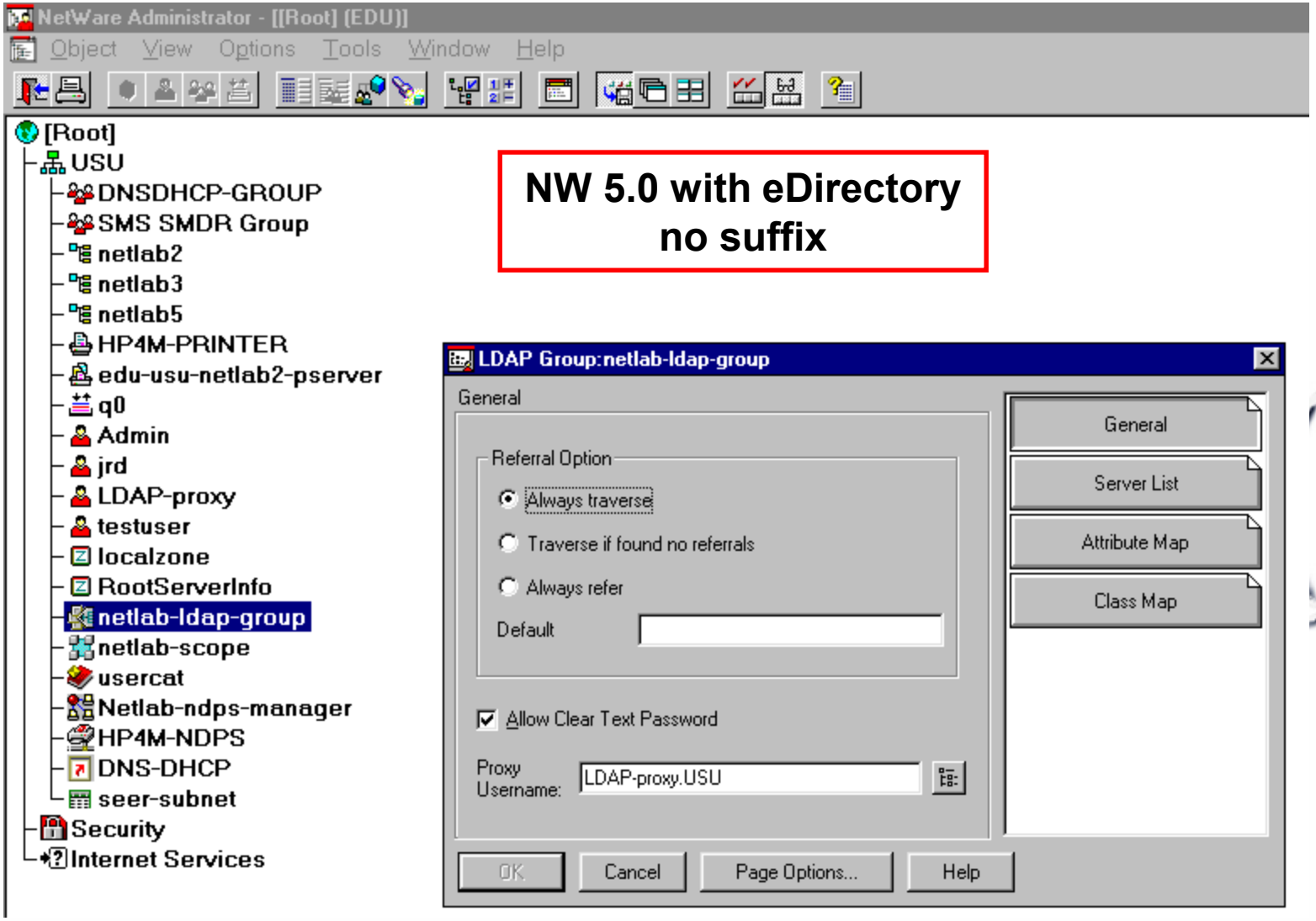
BrainShare2000

# NW 5 LDAP Group configuration



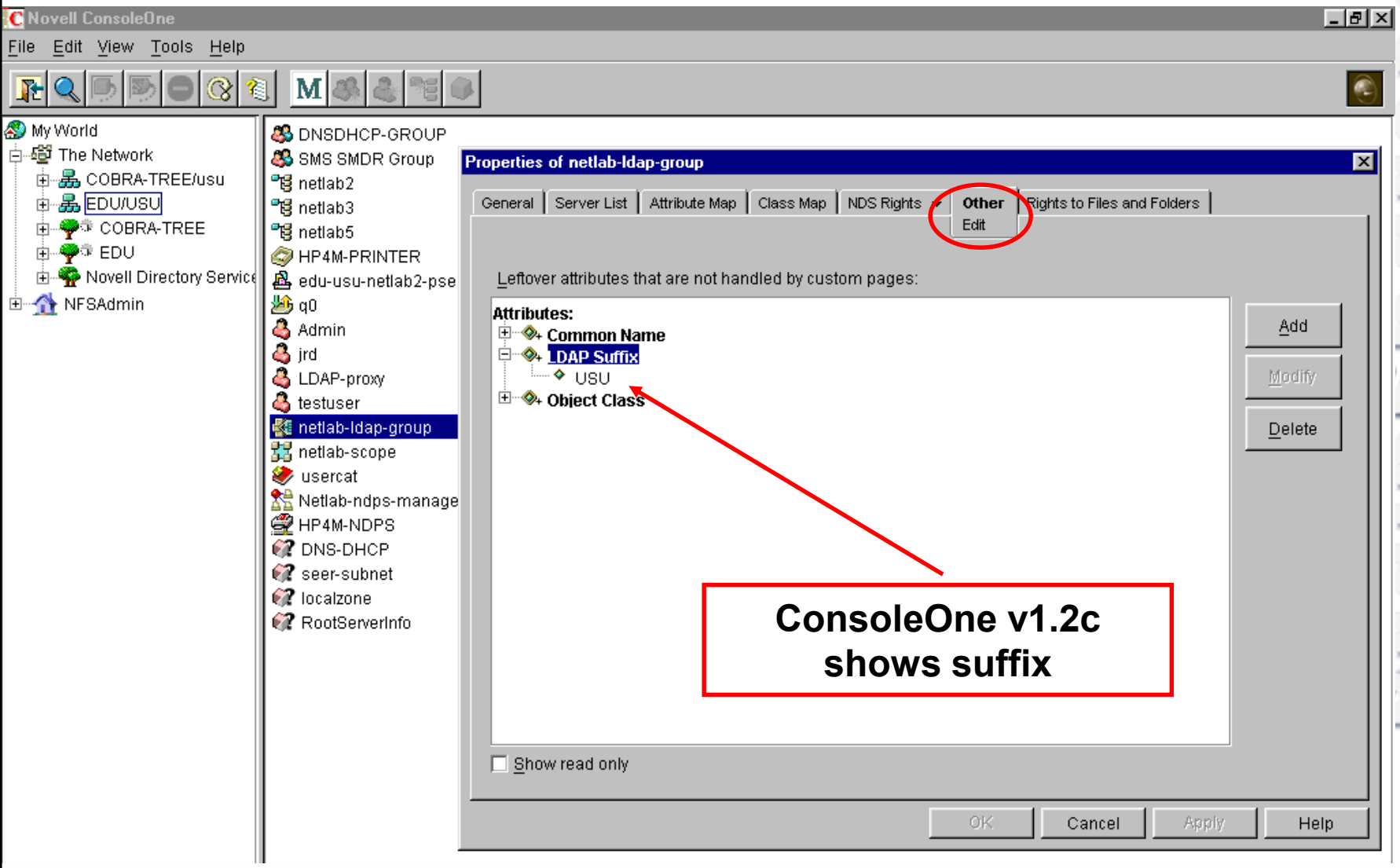

BrainShare2000

# NW 5 LDAP Group configuration



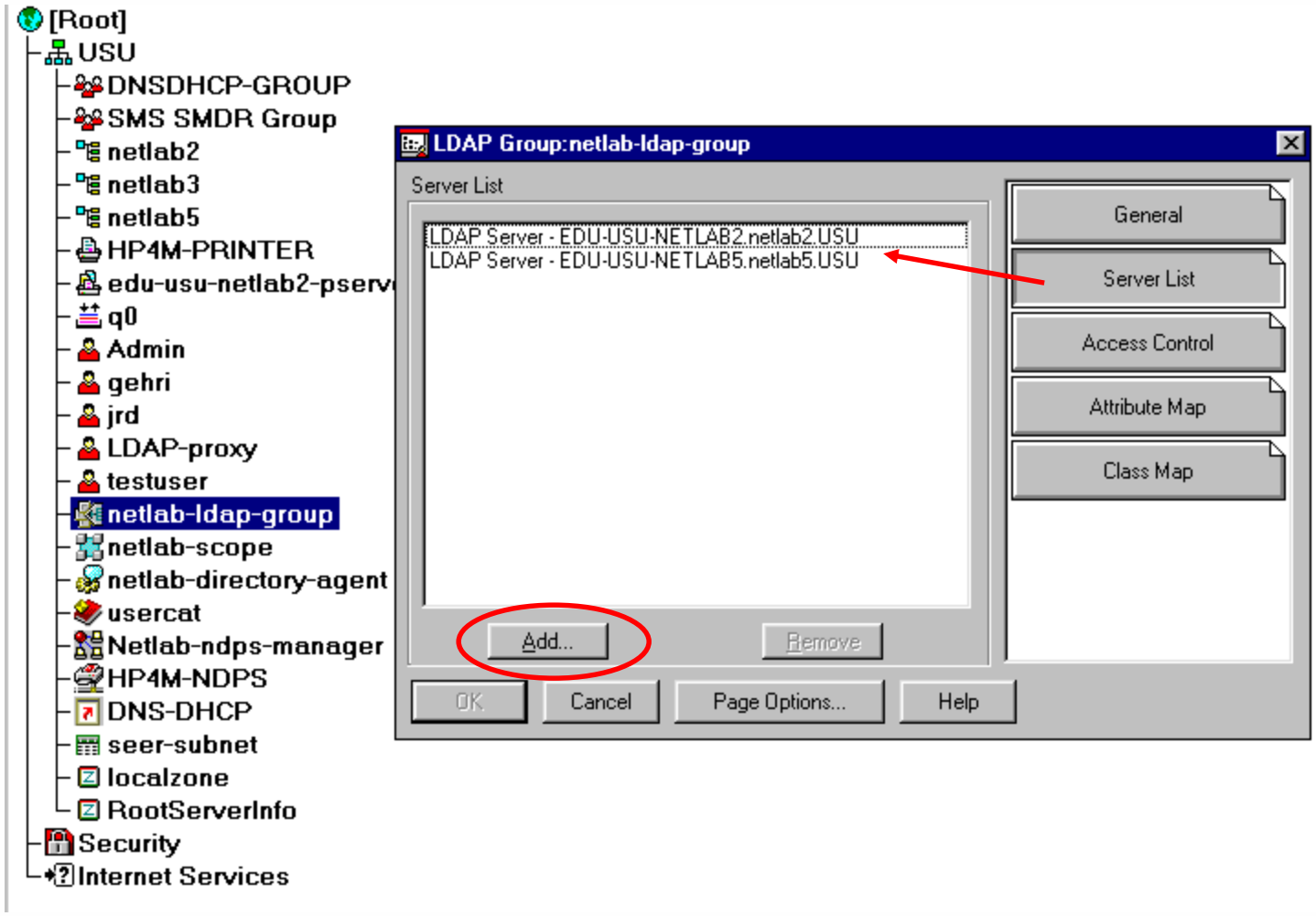

BrainShare2000

# NW 5 LDAP Group configuration



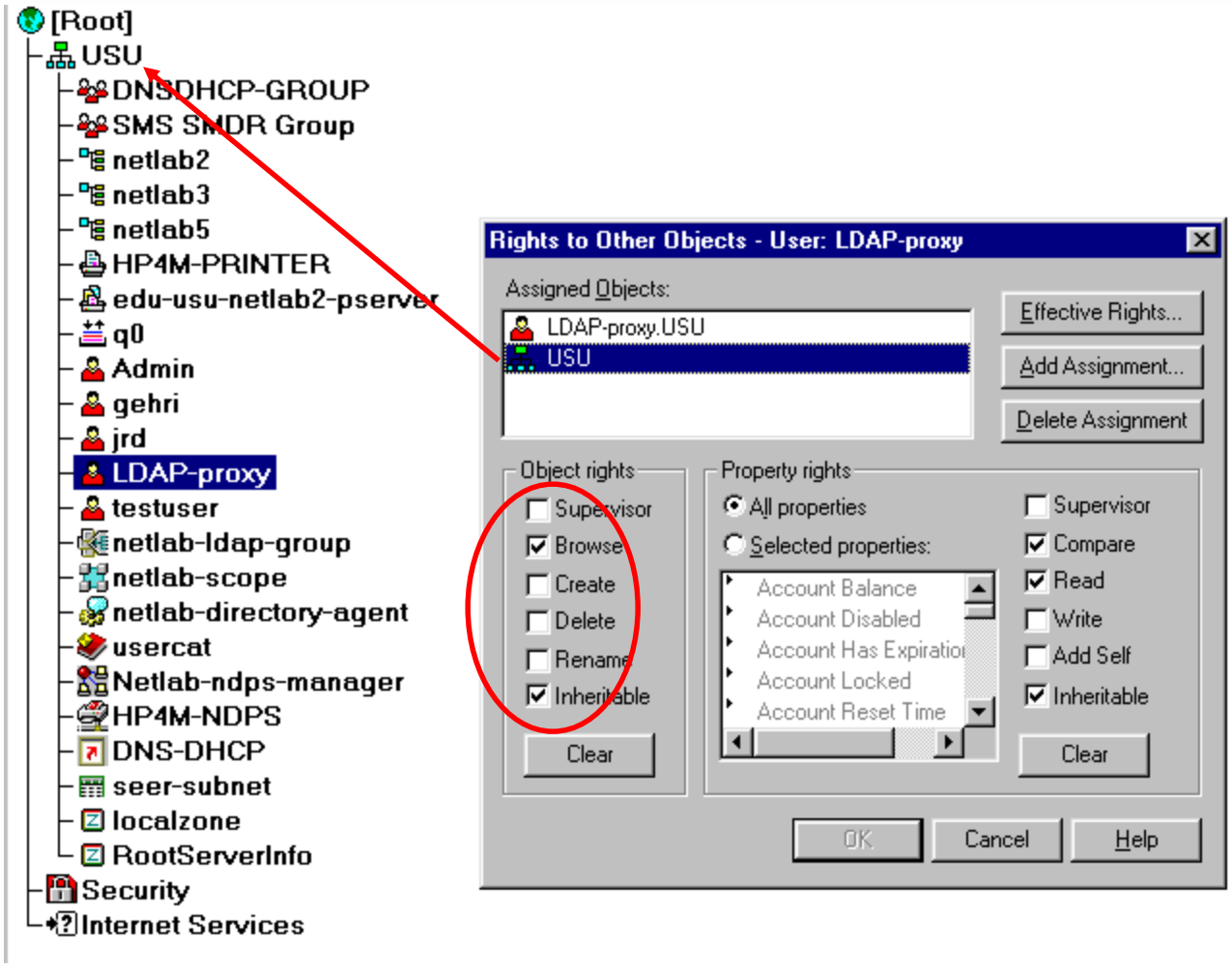

brainshare2000

# NDS, choosing LDAP servers



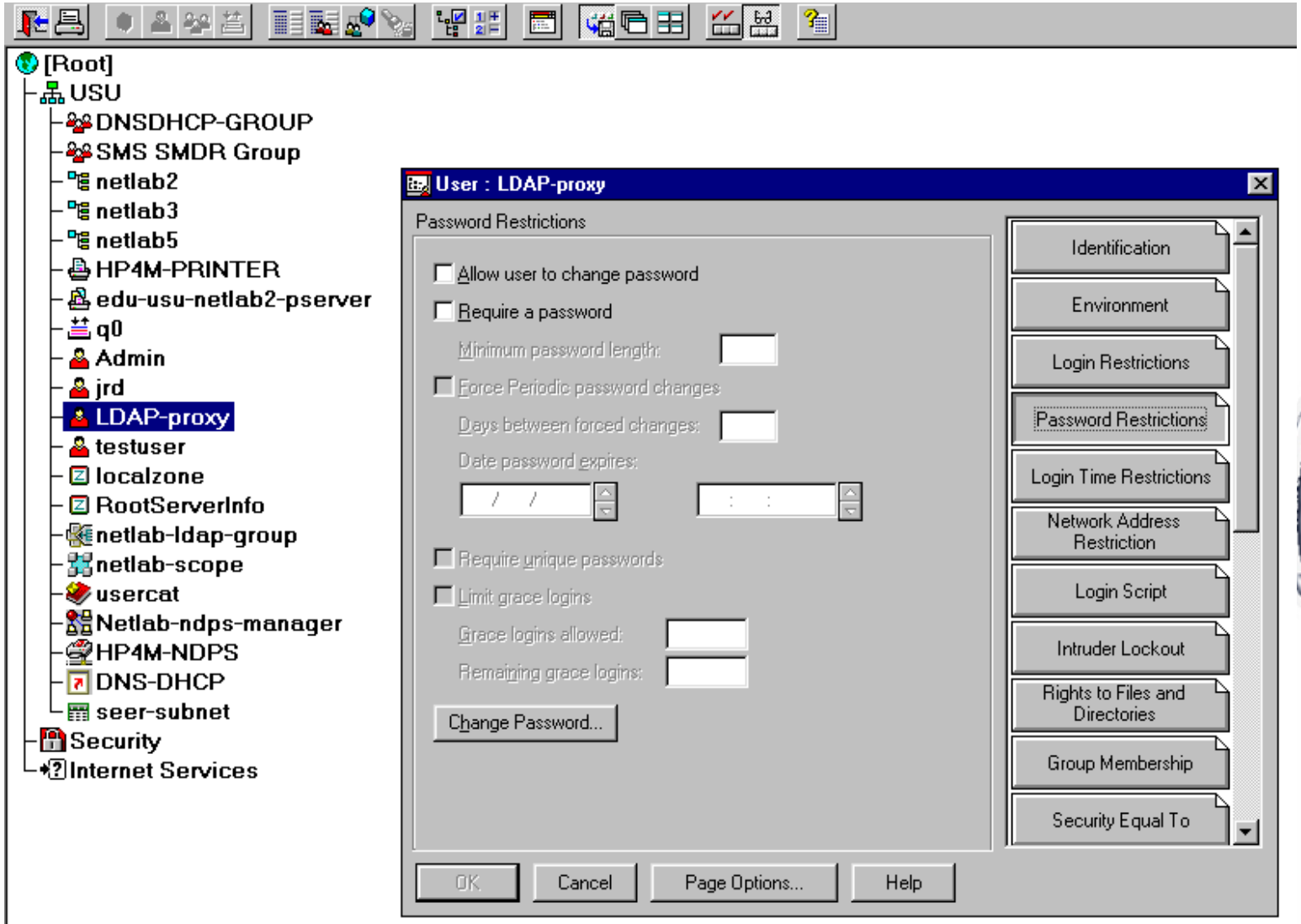

BrainShare2000

# LDAP Proxy, Browse rights to O=




BrainShare2000

# NW 5 LDAP Proxy user setup



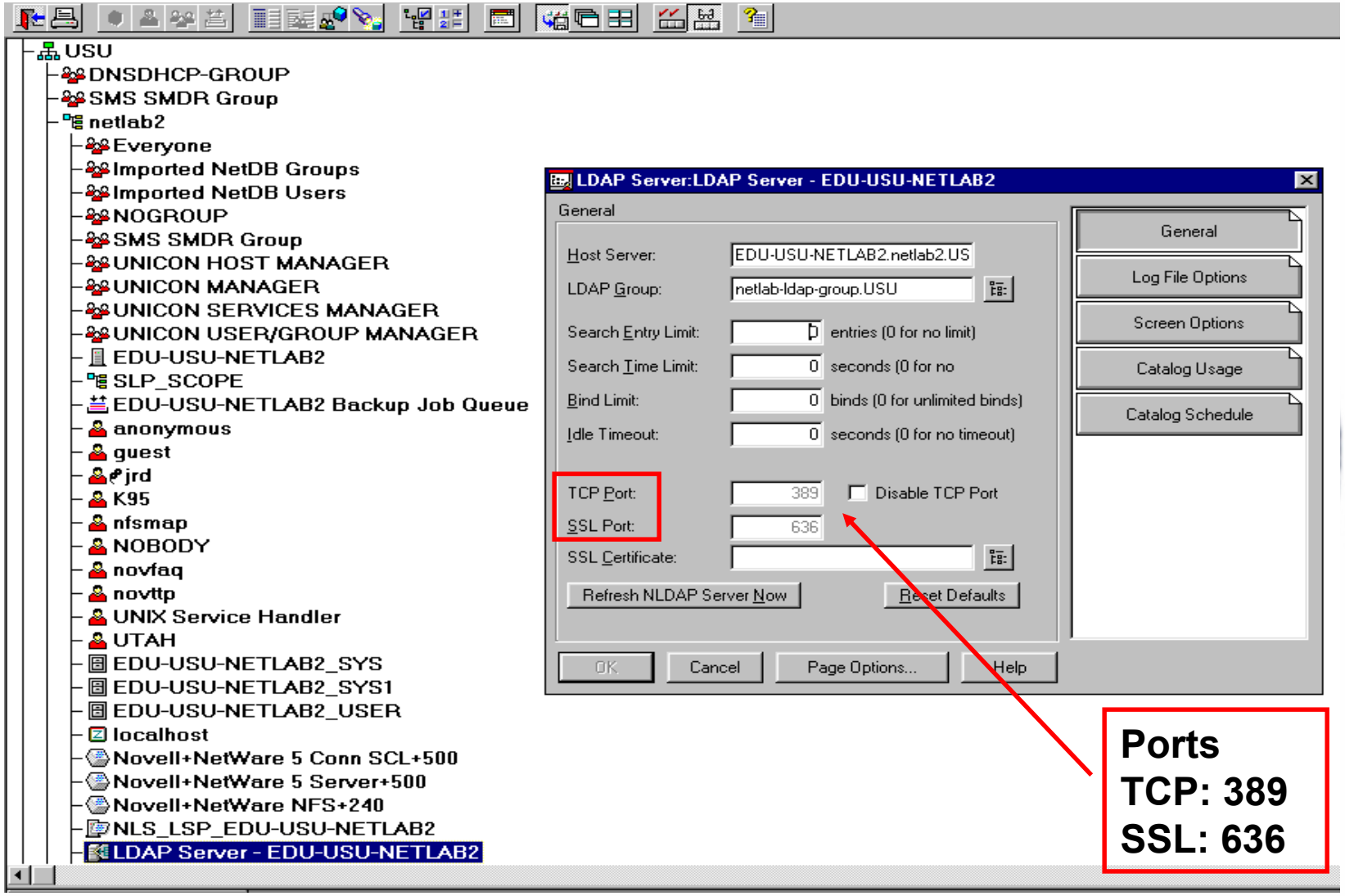

BrainShare2000

# LDAP Proxy user

- LDAP Proxy user is an NDS user
- Employed to do searches when LDAP request uses anonymous credentials
- Needs Browse rights to its part of the tree, often the entire tree
- No password, protect against bad guys guessing usernames

BrainShare2000

# NDS LDAP server object




BrainShare2000

# Check NDS LDAP from Linux

**ldapsearch is a Unix based LDAP query tool**

**-h host is NDS LDAP host IP name or number**

**-b “string” is base where NDS LDAP-group is defined**

**second “string” is the search pattern, here for CN of admin**

**Put quotes around strings containing spaces**

```
[jrd@(none) jrd]$ ldapsearch -h netlab2 -b o=usu cn=admin
```

**The query**

**The response**

```
cn=Admin,o=USU
objectClass=top
objectClass=person
objectClass=organizationalPerson
objectClass=inetOrgPerson
revision=1742
groupMembership=cn=DNSDHCP-GROUP,o=USU
sn=
uid=Admin
cn=Admin
```

BrainShare2000

# NDS LDAP response problems

- NDS aliased names can confuse LDAP responses
  - Configure LDAP with DEREF ALWAYS
- NDS usernames spelled the same but in different NDS contexts can produce multiple responses
  - Chose “base” to target desired container and lower in the NDS tree

BrainShare2000

# Configuring as NetWare client

- Configure IPX to start at boot time
  - with correct Ethernet frame kind
  - with correct IPX network number
- Configure automounter daemon to make NetWare volume(s) available transparently upon demand

BraInShare2000

# File /etc/sysconfig/ipx, configure IPX parameters

- Original

```
IPX_AUTO_PRIMARY=on
IPX_AUTO_INTERFACE=on
IPX_CONFIGURED=no
IPX_DEVICE=eth0
IPX_FRAME=802.2
IPX_INTERNAL_NET=no
IPX_NETNUM=0
```

- Revised

```
IPX_AUTO_PRIMARY=on
IPX_AUTO_INTERFACE=off
IPX_CONFIGURED=yes
IPX_DEVICE=eth0
IPX_FRAME=EtherII
IPX_INTERNAL_NET=no
IPX_NETNUM=817b0100
```

BrainShare2000

# Files in /etc/sysconfig/daemons, use “yes” for start upon booting

- **/etc/sysconfig/daemons/ipx**

  IDENT=IPX

  DESCRIPTIVE="Internetwork Packet eXchange (ipx)"

  ONBOOT="no” ----> *revise to be* ----> “yes”

- **/etc/sysconfig/daemons/nwclient**

  IDENT=nwclient

  DESCRIPTIVE="NetWare Client”

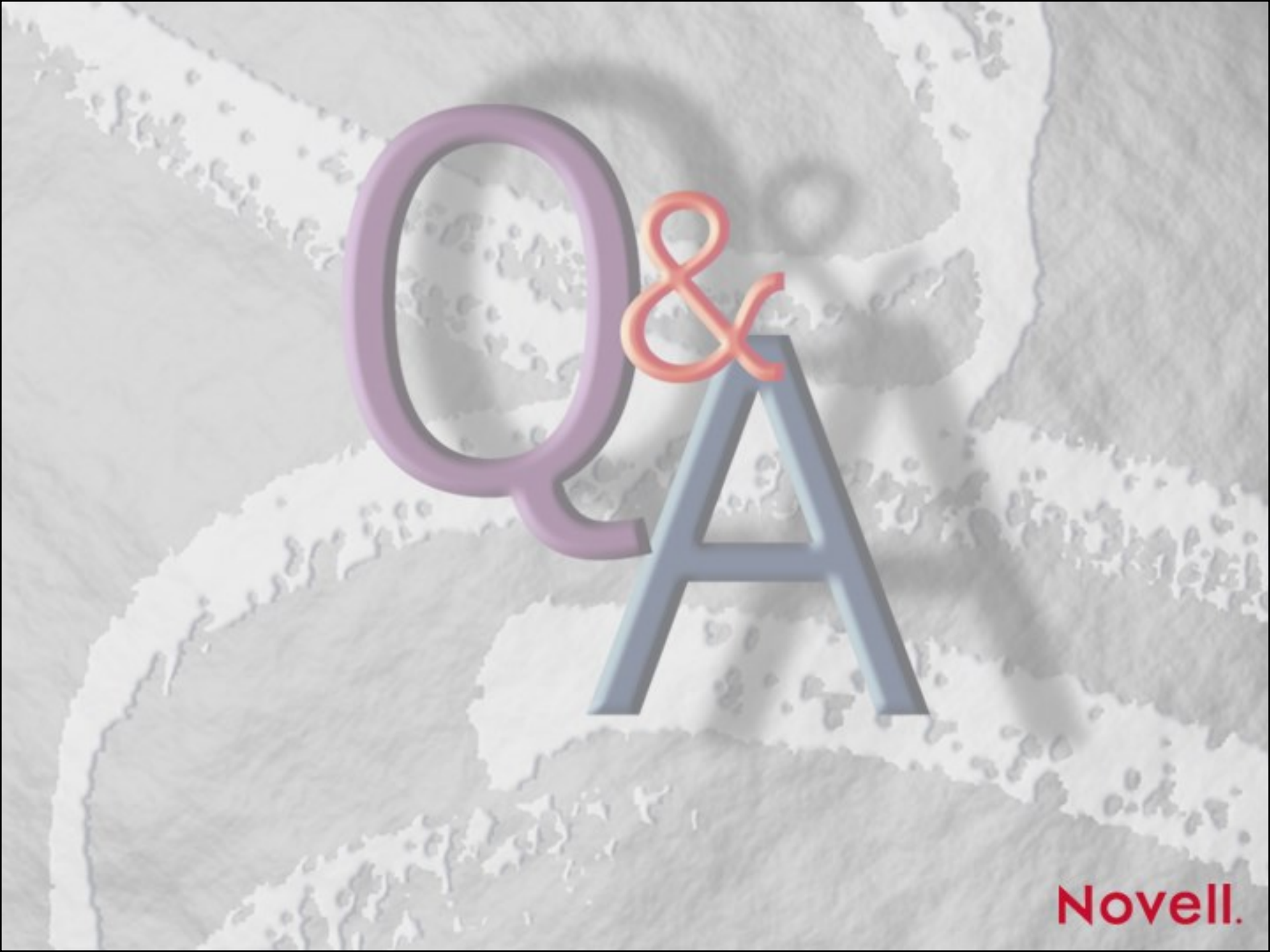
  ONBOOT=no ----> *revise to be* ----> “yes”

  # NWCLIENT_ACTIVE has been replaced with ONBOOT for consistency's sake

  NWCLIENT_SINGLE_CONNECTION_TABLE=no

BrainShare2000

Q&A
Novell.


Q&A
Novell.