# Contents

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>2</td>
</tr>
<tr>
<td>Objective</td>
<td>3</td>
</tr>
<tr>
<td>Authentication scheme</td>
<td>3</td>
</tr>
<tr>
<td>Recommendations</td>
<td>3</td>
</tr>
<tr>
<td>Server configuration</td>
<td>4</td>
</tr>
<tr>
<td>Edirectory install</td>
<td>4</td>
</tr>
<tr>
<td>eDirectory configuration for Linux client authentication.</td>
<td>8</td>
</tr>
<tr>
<td>LDAP Service Configuration</td>
<td>12</td>
</tr>
<tr>
<td>LDAP Trace</td>
<td>13</td>
</tr>
<tr>
<td>Connection Test</td>
<td>14</td>
</tr>
<tr>
<td>Linux client configuration</td>
<td>15</td>
</tr>
<tr>
<td>LDAP based eDirectory authentication</td>
<td>15</td>
</tr>
<tr>
<td>X Window Authentication</td>
<td>17</td>
</tr>
<tr>
<td>KDE Login testing</td>
<td>17</td>
</tr>
<tr>
<td>KDE Login Background</td>
<td>17</td>
</tr>
<tr>
<td>PAM Configuration examples</td>
<td>18</td>
</tr>
<tr>
<td>Security</td>
<td>19</td>
</tr>
<tr>
<td>LDAP Proxy User</td>
<td>19</td>
</tr>
<tr>
<td>Secure LDAP connections TLS/SSL</td>
<td>19</td>
</tr>
<tr>
<td>Enable secure LDAP connections (TLS/SSL) on server side</td>
<td>20</td>
</tr>
<tr>
<td>Enable secure LDAP connection on client side - TLS.</td>
<td>20</td>
</tr>
<tr>
<td>Enable secure LDAP connection on client side - SSL</td>
<td>23</td>
</tr>
<tr>
<td>Testing LDAP connection over TLS/SSL</td>
<td>24</td>
</tr>
<tr>
<td>PAM Modules</td>
<td>25</td>
</tr>
<tr>
<td>PAM MOUNT</td>
<td>25</td>
</tr>
<tr>
<td>ConsoleOne snapins for Unix Profile</td>
<td>26</td>
</tr>
</tbody>
</table>
Objective

To provide a guide to implement Linux authentication against eDirectory (no local users) based on PAM and LDAP.

Authentication scheme

Recommendations

Use LDAP APIs for cross-platform services that require accessing eDirectory objects and attribute information.

Use PAM-ldap for native Linux applications for Linux authentication and authorization.

Use DirXML (del text, JDBC, JMS drivers) when applications are not directory-enabled, PAM-enabled or cannot be customized.
Server configuration

**Edirectory install**

- Add multi-cast route
  - `route add -net 224.0.0.0 netmask 240.0.0.0 dev eth0`
- Add fixed ip address and verify dns information
- Install eDirectory on server
- Update PATH y MANPATH
- `/etc/profile`

```bash
edirlinux:~ # tail /etc/profile -n16
#
# Variables de eDir 8.7.3
#
#
# jre
PATH=$PATH:/usr/lib/nds-modules/embox/jre/bin
export PATH

# Novell LDAP Tools
PATH=$PATH:/usr/ldaptools/bin
export PATH

# Novell MAN Pages
MANPATH=$MANPATH:/usr/man:/usr/ldaptools/man
export MANPATH

edirlinux:~ #
```

- eDirectory configuration

```bash
/bin:/usr/X11R6:/bin:/usr/games:/opt/gnome:/bin:/opt/kde3/bin:/usr/lib/java
jre:/usr/lib/nds-modules/embox/jre/bin:/usr/ldaptools/bin:/usr/lib/nds-modules/
embox/jre/bin:/usr/ldaptools/bin

edirlinux:~ # man ndsconfig
Reformatting ndsconfig(8), please wait...

edirlinux:~ # ndsconfig def -t ndslab -n o=novell -a .cn=admin.o=novell -S edirl
ux
Enter the password for .cn=admin.o=novell:
Re-enter the password for .cn=admin.o=novell:
Starting the service 'ndsd'... Done.
Configuring Novell eDirectory server with following parameters
Admin name  = .cn=admin.o=novell
Tree name   = ndslab
Server Context = o=novell
Server name  = edirlinux
dibdir path  = /var/nds/dib

Searching for Duplicate Tree Name in the network. Please wait...
Configuring Novell eDirectory Server ...
```

---

Page 4 / 26  Adrián Malaguti, Consultant
- Verify eDir and server status

```
edirlinux:~ # /etc/init.d/mdsd status
Tree Name: NWLAB
Server Name: .CN=edirlinux.O=novell.T=NWLAB.
Binary Version: 10550.98
Root Most Entry Depth: 0
Product Version: NDS/Unix - NDS eDirectory v8.7.3 (DS)

edirlinux:~ # 
```

<table>
<thead>
<tr>
<th>Active Internet connections (servers and established)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Proto</td>
<td>Recv-Q</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
</tr>
</tbody>
</table>

- **DHost HTTP Server**
  - **DHost Console**
  - **NDS**
    - DS Trace
    - NDS iMonitor

Checking server: .edirlinux.novell
Address Type = TCP, dataf61 = 192.168.74.128:524
Address Type = UDP, dataf61 = 192.168.74.128:524
Checking server address in Replica ID : 1, .(Root).
Repairing replica ring
Start: Friday, April 09, 2004 16:59:40 Local Time
Replica Ring for replica: .(Root).
Remote server's local ID: 00032793
Remote server's replica root ID: 00032791
Remote server name is: .edirlinux.novell
OK - Authenticated to server
Finish: Friday, April 09, 2004 16:59:40 Local Time
Total repair time: 00:01:01
Total errors: 0
MDSRepair process completed.
edirlinux: ~ mdsrepair -0
• Instalar iManager 2

$ cd /tmp/install2/iManager/installs/linux 
$ ./install.sh 

Welcome to Novell's iManager.

This program will install or uninstall Novell's iManager 2.0.2 on your computer.

Choice

1) install
2) uninstall

----

Selection [install]: 1

![iManager installation screen]

• Install Console One, last version + snapins
  • Last version 1.3.6
  • It's not required to install JRE if previous one exists.
• Add C1_JRE_HOME=/path/to/jre to /etc/exports

• Verify server status and services

<table>
<thead>
<tr>
<th>PID</th>
<th>USER</th>
<th>PR</th>
<th>NI</th>
<th>VIRT</th>
<th>RES</th>
<th>SHR</th>
<th>%CPU</th>
<th>%MEM</th>
<th>TIME+</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>8141</td>
<td>root</td>
<td>21</td>
<td>0</td>
<td>1024</td>
<td>1024</td>
<td>764</td>
<td>R</td>
<td>28.4</td>
<td>0.4</td>
<td>0:00.48</td>
</tr>
<tr>
<td>5627</td>
<td>novlwww</td>
<td>15</td>
<td>0</td>
<td>75400</td>
<td>73m</td>
<td>18m</td>
<td>S</td>
<td>1.4</td>
<td>29.5</td>
<td>0:06.42</td>
</tr>
<tr>
<td>1</td>
<td>root</td>
<td>16</td>
<td>0</td>
<td>252</td>
<td>252</td>
<td>220</td>
<td>S</td>
<td>0.0</td>
<td>0.1</td>
<td>0:04.04</td>
</tr>
</tbody>
</table>

Note: This machine isn't running XDM.
eDirectory configuration for Linux client authentication

- Extend eDirectory schema
  - ndssch -h localhost -t treename cn=admin,o=novell rfc2307-usergroup.sch

```
# tail /var/nds/schema.log -n 20
Start: Friday April 09 2004 10:43:46
Starting schema update for: /usr/lib/nds-schema/rfc2307-usergroup.sch...
Resolved to Master of Server1: to extend the schema.
  Added schema attribute uidNumber.
  Added schema attribute gidNumber.
  Added schema attribute homeDirectory.
  Added schema attribute loginShell.
  Added schema attribute shadowLastChange.
  Added schema attribute shadowMin.
  Added schema attribute shadowMax.
  Added schema attribute shadowWarning.
  Added schema attribute shadowInactive.
  Added schema attribute shadowExpire.
  Added schema attribute shadowFlag.
  Added schema attribute memberld.
  Added schema class posixAccount.
  Added schema class shadowAccount.
  Added schema class posixGroup.
```

- Add eDir group and add extension “posixGroup” to it.
  - This/these group/s are used as primary groups for linux users.
• Create eDir user and extend it with posixAccount extension.
  • Populate user's primary group/gid with the posixGroup you created before.
• After the user is created, go to tab Other and add attribute loginshell.
• Set loginshell to /bin/bash or whatever shell you want.
- Verify LDAP service with some LDAP tool
- Example:

  We have three users, but only two of them have been extended as posixAccount (Amalaguti and Jdoe).

  So, when I do an ldap search I only get these two users, the third one is not displayed. Additionally, I get the primary group I created as posixGroup.

  ![LDAP Interface](image)

  The tool used here is “directory_administrator”, it allows to manage LDAP objects with Unix Profiles.
LDAP Service Configuration

- For testing purposes, you may want to set no proxy user and allow clear text connections. Also for testing purpose, proxy user could be configured with read and compare rights over all attributes.
  And that's what I did, just to be sure that basic things are working fine.

- Create proxy user for LDAP, set null password for this user and disable password changing.
- Configure LDAP Group to use proxy user.
- Enable TLS/SSL. Validate the certificates, server ip address and hostname. Also verify that ports 389 and 636 are not being blocked by some kind of firewall.
- Proxy user tree browsing restrictions, limit proxy user visibility of your eDirectory by granting specific rights to your tree.
  Make proxy user trustee of [root] and give him Browse entry rights, and read and compare property rights on the following attributes:
  - CN
  - Description
  - O
  - OU
  - Object Class
  - dc
  - gecos
  - gidNumber
  - homeDirectory
  - loginShell
  - memberUid
  - uidNumber
  - uniqueID

- Refresh LDAP service and verify if it's working fine, do an LDAP trace.

NOTE: During test lab I created proxy user for LDAP with Console One 1.3.6 for Linux. I don't know why but I had some LDAP errors with this user, so I deleted it and recreated it using iManager 2 and it worked fine.
LDAP Trace

16:22:11 94024 FFFFFFFF - LDAP: Refresh immediate has been issued from an NCP client
16:22:11 3800F FFFFFFFF - LDAP: ldapDefaultReferralBehavior: 2
16:22:11 3800F FFFFFFFF - LDAP: searchReferralUsage: 1
16:22:11 3800F FFFFFFFF - LDAP: otherReferralUsage: 1
16:22:11 3800F FFFFFFFF - LDAP: NDS attribute "NSCP:memberCertificateDesc" does not exist, mapping ignored
16:22:11 3800F FFFFFFFF - LDAP: NDS attribute "staticMember" does not exist, mapping ignored
16:22:11 3800F FFFFFFFF - LDAP: LDAP Referral: Not Defined
16:22:11 3800F FFFFFFFF - referralIncludeFilter: Not Defined
16:22:11 3800F FFFFFFFF - referralExcludeFilter: Not Defined
16:22:11 3800F FFFFFFFF - LDAP Screen Level: 29385
16:22:11 3800F FFFFFFFF - searchSizeLimit: 0
16:22:11 3800F FFFFFFFF - searchTimeLimit: 0
16:22:12 3800F FFFFFFFF - LDAP Server Bind Limit: 0
16:22:12 3800F FFFFFFFF - LDAP Server Idle Timeout: 0
16:22:12 3800F FFFFFFFF - LDAP Enable TCP: TRUE
16:22:12 3800F FFFFFFFF - LDAP Enable SSL: TRUE
16:22:12 3800F FFFFFFFF - LDAP TCP Port: 389
16:22:12 3800F FFFFFFFF - LDAP SSL Port: 636
16:22:12 3800F FFFFFFFF - filteredReplicaUsage: 0
16:22:12 3800F FFFFFFFF - LDAP:keyMaterialName: "SSL CertificateIP"
16:22:12 3800F FFFFFFFF - extensionInfo: OID:2.16.840.1.113719.1.142.100.1 lburp:ExtensionHandler
16:22:12 3800F FFFFFFFF - extensionInfo: OID:2.16.840.1.113719.1.27.100.1 ldapxs:ExtensionHandler
16:22:12 3800F FFFFFFFF - extensionInfo: OID:2.16.840.1.113719.1.39.42.100.1 nmasldap:ExtensionHandler
16:22:12 3800F FFFFFFFF - nonStdClientSchemaCompatMode: 0
16:22:12 3800F FFFFFFFF - ldapEnablePsearch: 1
16:22:12 3800F FFFFFFFF - ldapMaximumPsearchOperations: 0
16:22:12 3800F FFFFFFFF - ldapignorePsearchLimitsForEvents: 1
16:22:12 3800F FFFFFFFF - ldapEnableMonitorEvents: 1
16:22:12 3800F FFFFFFFF - ldapMaximumMonitorEventsLoad: 0
16:22:12 3800F FFFFFFFF - ldapTLSRequired: FALSE
16:22:12 3800F FFFFFFFF - ldapTLSVerifyClientCertificate: 0
16:22:12 3800F FFFFFFFF - ldapDerefAlias: FALSE
16:22:12 3800F FFFFFFFF - ldapNonStdAllUserAttrsMode: 1220218519
16:22:12 3800F FFFFFFFF - LDAP Bind Restrictions: 0
16:22:12 3800F FFFFFFFF - LDAP TLSTrustedRootContainer: Not Defined
16:22:12 3800F FFFFFFFF - LDAP:searchReferralUsage: Not Defined
16:22:12 3800F FFFFFFFF - LDAP:otherReferralUsage: Not Defined
16:22:12 3800F FFFFFFFF - LDAP DefaultReferralBehavior: Not Defined
16:22:12 3800F FFFFFFFF - LDAP Referral: Not Defined
16:22:12 3800F FFFFFFFF - Updating server configuration
16:22:17 4C014 FFFFFFFF - LDAP: Refresh immediate has been issued from an NCP client
16:22:17 3800F FFFFFFFF - LDAP: ldapDefaultReferralBehavior: 2
16:22:17 3800F FFFFFFFF - LDAP: searchReferralUsage: 1
16:22:17 3800F FFFFFFFF - LDAP:otherReferralUsage: 1
16:22:17 3800F FFFFFFFF - LDAP Allow Clear Text Password: TRUE
16:22:17 3800F FFFFFFFF - LDAP: NDS attribute "NSCP:memberCertificateDesc" does not exist, mapping ignored
16:22:17 3800F FFFFFFFF - LDAP: NDS attribute "staticMember" does not exist, mapping ignored
16:22:17 3800F FFFFFFFF - LDAP Referral: Not Defined
16:22:17 3800F FFFFFFFF - referralIncludeFilter: Not Defined
16:22:17 3800F FFFFFFFF - referralExcludeFilter: Not Defined
16:22:17 3800F FFFFFFFF - LDAP Screen Level: 29385
16:22:17 3800F FFFFFFFF - searchSizeLimit: 0
16:22:17 3800F FFFFFFFF - searchTimeLimit: 0
16:22:17 3800F FFFFFFFF - LDAP Server Bind Limit: 0
16:22:17 3800F FFFFFFFF - LDAP Server Idle Timeout: 0
16:22:17 3800F FFFFFFFF - LDAP Enable TCP: TRUE
16:22:17 3800F FFFFFFFF - LDAP Enable SSL: TRUE
16:22:17 3800F FFFFFFFF - LDAP TCP Port: 389
16:22:17 3800F FFFFFFFF - LDAP SSL Port: 636
16:22:17 3800F FFFFFFFF - filteredReplicaUsage: 0
16:22:17 3800F FFFFFFFF - LDAP:keyMaterialName: "SSL CertificateIP"
Connection Test

- Run ldap searches and verify results.
- Anonymous ldapsearch from remote client searching for cn=amalaguti object, no TLS/SSL:
  ```
  linux:/home/amalaguti # ldapsearch -h 192.168.74.128 -x -b o=novell -s sub "(cn=amalaguti)"
  
  # extended LDIF
  #
  # LDAPv3
  # base <o=novell> with scope sub
  # filter: (cn=amalaguti)
  # requesting: ALL
  #
  # AMalaguti, novell
dn: cn=AMalaguti,o=novell
loginShell: /bin/bash
homeDirectory: /home/malaguti
gidNumber: 700
uidNumber: 600
uid: AMalaguti
Language: ENGLISH
sn: Malaguti
passwordAllowChange: TRUE
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: Person
objectClass: ndsLoginProperties
objectClass: Top
objectClass: posixAccount
loginTime: 20040410191121Z
cn: AMalaguti
cn: Adrian Malaguti
ACL: 2#subtree#cn=AMalaguti,o=novell#[All Attributes Rights]
ACL: 6#entry#cn=AMalaguti,o=novell#loginScript
ACL: 2#entry#[Public]#messageServer
ACL: 2#entry#[Root]#groupMembership
ACL: 6#entry#cn=AMalaguti,o=novell#printJobConfiguration
ACL: 2#entry#[Root]#networkAddress

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```
Linux client configuration

LDAP based eDirectory authentication

/etc/ldap.conf file: Configuration file for pam_ldap and nss_ldap modules
/etc/openldap/ldap.conf file: Holds configuration and default settings for openldap utilities
Not used for PAM configuration

- Run your distro's configuration tool for authentication configuration.
  - Redhat: authconfig
  - Suse: YaST -> Network Services -> LDAP client.

Modify /etc/ldap.conf to suite your environment requirements
(Sin tls/ssl, usando usuario admin)

```
host 192.168.74.128
base o=novell
ldap_version 3
binddn cn=admin,o=novell
bindpwd novell
scope sub
pam_check_host_attr no
pam_password ngs
nss_map_attribute uniqueMember member
ssl no
nss_base_passwd o=novell
nss_base_shadow o=novell
nss_base_group o=novell
```

Testing configuration:
No anonymous bind and clear text connection.
Verify your LDAP service settings

- Modify /etc/nsswitch.conf to suite your authentication order needs

```
password: files ldap
group: files ldap
```

- Modify /etc/pam.d/login to suite your needs
  - The following is just an example and may vary for your distro, verify modules path and
parameters. Read your PAM documentation

```
auth  required  pam_securetty.so
auth  required  pam_nologin.so
auth  sufficient  pam_lgadj.so
auth  required  pam_unix_auth.so try_first_pass
auth  requisite  pam_unix2.so  nullok msecrpc
auth  required  pam_homecheck.so
auth  required  pam_env.so
auth  required  pam_mail.so
account  sufficient  pam_ldap.so
account  required  pam_unix_acct.so
account  required  pam_unix2.so
password  required  pam_cracklib.so
password  required  pam_lgadj.so
session  required  pam_unix_session.so
session  required  pam_unix2.so  none # debug or trace
session  required  pam_limits.so
session  required  pam_mkhomedir.so  skel=/etc/skel  umask=0022
```

- Try LDAP auth first, if it fails, try local auth.
  ```
  auth  sufficient  pam_lgadj.so
  auth  required  pam_unix_auth.so try_first_pass
  ```

- Create home directory $HOME automatically during login if it doesn't exist
  ```
  session  required  pam_mkhomedir.so skel=/etc/skel umask=0022
  ```

```
linux login: amalgutri
Password:
Creating directory `/home/amalaguti`
Creating directory `/home/amalaguti/bin`.
Creating directory `/home/amalaguti/Documents`.
Creating directory `/home/amalaguti/public_html`.
Creating directory `/home/amalaguti/.xemacs`.
Creating directory `/home/amalaguti/.fonts`.
Last login: Sat Apr 10 02:22:02 on tty3
Have a lot of fun...
```
```
AMalaguti@linux:~> pwd
/home/amalaguti
AMalaguti@linux:~> ls -lh
total 0
  drwxr-xr-x  2 AMalaguti linuxuser  48 2004-04-10 02:37 bin
  drwxr-xr-x  2 AMalaguti linuxuser  80 2004-04-10 02:37 Documents
  drwxr-xr-x  2 AMalaguti linuxuser  80 2004-04-10 02:37 public_html
```
X Window Authentication

- Modify /etc/pam.d/xdm, follow same rules as /etc/pam.d/login

KDE Login testing

- NDS/LDAP username: cn=user1.ou=users.o=novell
- NDS/LDAP password: 123
- Local user -> /etc/passwd: Not Available (authentication forwarded to eDirectory LDAP)
- User's $HOME: Not Available (will be created after login)
- Login KDE Prompt
  Username: user1
  Password: 123

KDE Login Background

1. LDAP query filtering “user1”
2. User and password validation against eDirectory
3. KDE Login's startups scripts begin running
4. Service pam.d/xdm creates user's $HOME in local file system based on user's Unix Profile

User1 is logged in

There is no local user, exception for system users.

$HOME was created for user1 and other previously logged users
PAM Configuration examples

```
# # PAM NNLS
# #%PAM-1.0

# This is required for console ownership access
session optional /lib/security/pam_console.so

# First try through NDS
auth sufficient /lib/security/pam_nam.so.0
account sufficient /lib/security/pam_nam.so.0
password sufficient /lib/security/pam_nam.so.0
session sufficient /lib/security/pam_nam.so.0

# Fall back to flat file authentication, try first password first
auth required /lib/security/pam_securetty.so
auth required /lib/security/pam_pwdb.so shadow nullok try_first_pass
auth required /lib/security/pam_nologin.so
account required /lib/security/pam_pwdb.so
password required /lib/security/pam_cracklib.so
password required /lib/security/pam_pwdb.so nullok use_authtok md5 shadow
session required /lib/security/pam_pwdb.so

# PAM - Ldap login
# #%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth required /lib/security/pam_env.so
auth sufficient /lib/security/pam_unix.so likeauth nullok
auth required /lib/security/pam_deny.so
account required /lib/security/pam_unix.so
password required /lib/security/pam_cracklib.so retry=3 type=
password sufficient /lib/security/pam_unix.so nullok use_authtok md5 shadow
password required /lib/security/pam_deny.so
session required /lib/security/pam_limits.so
session required /lib/security/pam_unix.so

# PAM Login, source documentation
# #%PAM-1.0
auth required pam_securetty.so
auth required pam_nologin.so
auth sufficient pam_ldap.so
auth required pam_unix2.so nullok try_first_pass #set_secrpc
account sufficient pam_ldap.so
account required pam_unix2.so
password required pam_pwcheck.so nullok
password required pam_unix2.so use_first_pass use_authok
password required pam_unix2.so nullok use_first_pass use_authok
session required pam_unix2.so none # debug or trace
session required pam_limits.so
session required pam_env.so
session optional pam_mail.so
```
Security

**LDAP Proxy User**

- Crear usuario proxy ldap, asignar atributos correspondientes. Ver Configuración del servicio LDAP.

**Secure LDAP connections TLS/SSL**

- Use the ldapsearch command-line tool to perform a TLS-enabled search
  
  example: `ldapsearch -h 10.0.0.100 -D cn=admin,o=novell -W -x -b -s one -ZZ`

Packet capture and trace of a no secure (no TLS/SSL) connection, binding user is `cn=admin,o=novell` with password `novell` (no proxy user)
Enable secure LDAP connections (TLS/SSL) on server side

- Edit /etc/ldap.conf, set “ssl start_tls”

Enable secure LDAP connection on client side - TLS

- LDAP bind with username and password (not required nor recommended)

  Recommendation:
  Use anonymous bind, by setting #binddn and #bindpwd not configured.

TLS habilitado
• LDAP Trace: TLS Enabled, logged in as username “amalaguti”, ldap bind as admin.novell (No anonymous bind)

02:35:36 40012 D.B.P. New Client connection 0x530250 from 192.168.74.20:33121 monitor = 0x54016, index = 1
02:35:36 20008 D.B.P. (192.168.74.20:33121) [0x0000:0x07] implied anonymous bind by operation 0x1:0x7 on connection 0x8530250
02:35:36 20008 D.B.P. (192.168.74.20:33121) [0x0000:0x07] DoExtended on connection 0x8530250
02:35:36 20008 D.B.P. (192.168.74.20:33121) [0x0000:0x07] Start TLS request issued from connection 0x8530250
02:35:36 20008 D.B.P. (192.168.74.20:33121) [0x0000:0x07] Sending operation result 0:*:* to connection 0x8530250
02:35:36 04014 D.B.P. Monitor 0x54016 initiating TLS handshake on connection 0x8530250
02:35:36 60013 D.B.P. (192.168.74.20:33121) [0x0000:0x00] DoTLSHandshake on connection 0x8530250
02:35:36 60013 D.B.P. (192.168.74.20:33121) [0x0000:0x00] Completed TLS handshake on connection 0x8530250
02:35:36 04012 D.B.P. (192.168.74.20:33121) [0x0000:0x06] DoBind on connection 0x8530250
02:35:36 04014 D.B.P. (192.168.74.20:33121) [0x0000:0x00] Activating pending operation 0x2:0x60 on connection 0x8530250
02:35:36 04002 D.B.P. (192.168.74.20:33121) [0x0000:0x06] DoBind on connection 0x8530250
02:35:36 04002 D.B.P. (192.168.74.20:33121) [0x0000:0x06] DoBind on connection 0x8530250
02:35:36 04002 D.B.P. (192.168.74.20:33121) [0x0000:0x06] Bind name=amalaguti@novell.version:3:authentication=system
02:35:36 04002 D.B.P. (192.168.74.20:33121) [0x0000:0x06] Sending operation result 0:*:* to connection 0x8530250
02:35:36 04002 D.B.P. (192.168.74.20:33121) [0x0000:0x06] DoSearch on connection 0x8530250
02:35:36 04002 D.B.P. (192.168.74.20:33121) [0x0000:0x06] Search request:

base: "o=novell"
scope:2 dereference 0 sizelimit:1 timelimit:0 anonymous:0
filter: "(objectClass=posixAccount) (uid=amalaguti)"
attribute: "uid"
attribute: "userPassword"
attribute: "uidNumber"
attribute: "gidNumber"
attribute: "cn"
attribute: "homeDirectory"
attribute: "loginsShell"
attribute: "gecos"
attribute: "description"
attribute: "objectClass"

02:35:36 04002 D.B.P. (192.168.74.20:33121) [0x0000:0x63] Sending search result entry "cn=Amalaguti=novell" to connection 0x8530250

• LDAP Trace: TLS Enabled, logged in as username “amalaguti”, anonymous bind

02:35:38 40012 D.B.P. New Client connection 0x530440 from 192.168.74.20:33131 monitor = 0x54016, index = 4
02:35:38 20006 D.B.P. (192.168.74.20:33131) [0x0000:0x07] implied anonymous bind by operation 0x1:0x77 on connection 0x856e40
02:35:38 20006 D.B.P. (192.168.74.20:33131) [0x0000:0x07] DoExtended on connection 0x856e40
02:35:38 20011 D.B.P. (192.168.74.20:33131) [0x0000:0x07] Start TLS request issued from connection 0x856e40
02:35:38 20011 D.B.P. (192.168.74.20:33131) [0x0000:0x07] Sending operation result 0:*:* to connection 0x856e40
02:35:38 50014 D.B.P. Monitor 0x54016 initiating TLS handshake on connection 0x856e40
02:35:38 12007 D.B.P. (192.168.74.20:33131) [0x0000:0x00] DoTLSHandshake on connection 0x856e40
02:35:38 12007 D.B.P. (192.168.74.20:33131) [0x0000:0x00] Completed TLS handshake on connection 0x856e40
02:35:38 00002 D.B.P. (192.168.74.20:33131) [0x0000:0x06] DoBind on connection 0x856e40
02:35:38 12007 D.B.P. (192.168.74.20:33131) [0x0000:0x00] Activating pending operation 0x2:0x60 on connection 0x856e40
02:35:38 04011 D.B.P. (192.168.74.20:33131) [0x0000:0x06] DoBind on connection 0x856e40
02:35:38 04011 D.B.P. (192.168.74.20:33131) [0x0000:0x06] Initiating simple bind with empty DN and no password as anonymous
02:35:38 04011 D.B.P. (192.168.74.20:33131) [0x0000:0x06] bind name=ANONYMOUS version:4: authentication=system
02:35:38 04011 D.B.P. (192.168.74.20:33131) [0x0000:0x06] Sending operation result 0:*:* to connection 0x856e40
02:35:38 00002 D.B.P. (192.168.74.20:33131) [0x0000:0x03] DoSearch on connection 0x856e40
02:35:38 00002 D.B.P. (192.168.74.20:33131) [0x0000:0x03] Search request:

base: "o=novell"
scope:2 dereference 0 sizelimit:1 timelimit:0 anonymous:0
filter: "(objectClass=posixAccount) (uidNumber=600)"
attribute: "uid"
attribute: "userPassword"
attribute: "uidNumber"
attribute: "gidNumber"
attribute: "cn"
attribute: "homeDirectory"
attribute: "loginsShell"
attribute: "gecos"
attribute: "description"
attribute: "objectClass"

02:35:38 00002 D.B.P. (192.168.74.20:33131) [0x0000:0x63] Sending search result entry "cn=Amalaguti=novell" to connection 0x856e40
Enable secure LDAP connection on client side - SSL

- For PAM LDAP, edit `/etc/ldap.conf`, set “ssl on” and “port 636”

For OpenLdap based tools, like ldapsearch, edit `/etc/openldap/ldap.conf`. OpenLdap need to be configured to allow self signed certificates to prevent certificate errors during TLS/SSL handshaking, set “TLS_REQCERT allow”.
Some applications could require importing the Trusted Root Certificate. Obtain it from ConsoleOne in DER format and execute this command:

```
#openssl x509 -in trustedroot.der -inform DER -out /etc/ssl/certs/trustedroot.pem -outform PEM.
```

**Testing LDAP connection over TLS/SSL**

```
#ldapsearch -H ldaps://192.168.74.128 -x -b o=novell -s sub -Z
```
PAM Modules

PAM MOUNT

The pam_mount module allows users to have NCP (Netware), SMB (Windows/Samba), NFS, or loopback-encrypted volumes mounted upon login, using the same passwords they typed to log in. A remote volume can even be used as a user's $HOME. Volumes mounted this way are automatically unmouted on logout.

- It has two configuration files
  - /etc/security/pam_mount.conf, global configuration file
  - $HOME/.pam_mount.conf, per user configuration file.
ConsoleOne snapins for Unix Profile

- Not recommended, see Note below
- Install Unix snapins for ConsoleOne.
  - File: AccountManagementUnix.zip
  - copy unixSnapinRes.jar -> ../ConsoleOne/resources
  - copy unixsnapin.jar -> ../ConsoleOne/snapins/unix

Note: I got some anomalies using this snapins, for example: to be unable to save changes to user’s Unix Profile.
I reverted back deleting both .jar files.