

## Ubuntu ( Breezy 5.1 & Dapper 6.06.1 ) and Fedora Directory Server using LDAP

I still think Ubuntu is non-standard, it doesn't follow standards adopted by other distribution. Anyway I figured out how to bound Ubuntu clients to LDAP.

Before you proceed usually I enable root logins so you can edit files directly, log in with an administrator account and set the root password for the root user.

```
ashley@rain:/etc/apt# sudo passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

And after that enable root login through the graphical console by clicking

Systems->Administration->Login Screen Setup

Click login setup

Security -> Option -> Allow root to login with GDM

First thing first, by default when you install the Ubuntu (Breezy or Dapper) you will not be able to install the necessary PAM (Pluggable Authentication Module) necessary for LDAP authentication as it is not supported by the UBUNTU team.

You would think something important as PAM or LDAP would be supported but no its not, now if we look at the LDAP packages ie <http://packages.ubuntulinux.org/dapper/source/libpam-ldap>. It belongs to the universe package set which is not included in your apt-get list as its not supported.

So the first you would have to do is edit the site to include the universe packages.

Ie edit or replace /etc/apt/sources.list

I've replaced sources.list with the iiNET mirror site as the traffic is free because we are on waix, the contents should be something like this. Note this is dependent on the version of Ubuntu you are using.

For Ubuntu 5.10 Breezy Distro is should be something like this.

```
root@rain:/etc/apt# cat sources.list
deb cdrom:[Ubuntu 5.10 _Breezy Badger_ - Release i386 (20051012)]/ breezy main
restricted
```

```
#Main Ubuntu
```

```
deb ftp://ftp.iinet.net.au/linux/ubuntu breezy main restricted
deb ftp://ftp.iinet.net.au/linux/ubuntu breezy-updates main restricted
deb ftp://ftp.iinet.net.au/linux/ubuntu breezy-security main restricted
```

```
#Unsupported Ubuntu Repository
```

Ubuntu and Fedora Directory Server Binding via LDAP

Written by: Ashley Chew

Last Updated: 18082006

```
deb ftp://ftp.iinet.net.au/linux/ubuntu breezy universe multiverse
deb ftp://ftp.iinet.net.au/linux/ubuntu breezy-security universe multiverse
```

For Ubuntu 6.06.1 Dapper Distro is should be something like this.

```
root@rain:/etc/apt# cat sources.list
#deb cdrom:[Ubuntu 5.10 _Breezy Badger_ - Release i386 (20051012)]/ breezy main
restricted
```

```
deb ftp://ftp.iinet.net.au/linux/ubuntu dapper main restricted
deb ftp://ftp.iinet.net.au/linux/ubuntu dapper-updates main restricted
deb ftp://ftp.iinet.net.au/linux/ubuntu dapper-security main restricted
deb ftp://ftp.iinet.net.au/linux/ubuntu dapper universe multiverse
deb ftp://ftp.iinet.net.au/linux/ubuntu dapper-security universe multiverse
```

Once that's done you have to update the list of packages available from the mirror you do this by typing this and you should see the following for Ubuntu 5.1 Breezy distro, again you will see something similar with you use Ubuntu 6.06.1 Dapper distro.

```
root@rain:/etc/apt# apt-get update
Hit ftp://ftp.iinet.net.au breezy Release.gpg
Hit ftp://ftp.iinet.net.au breezy-updates Release.gpg
Hit ftp://ftp.iinet.net.au breezy-security Release.gpg
Hit ftp://ftp.iinet.net.au breezy Release
Get:1 ftp://ftp.iinet.net.au breezy-updates Release [30.9kB]
Get:2 ftp://ftp.iinet.net.au breezy-security Release [27.0kB]
Hit ftp://ftp.iinet.net.au breezy/main Packages
Hit ftp://ftp.iinet.net.au breezy/restricted Packages
Hit ftp://ftp.iinet.net.au breezy/universe Packages
Hit ftp://ftp.iinet.net.au breezy/multiverse Packages
Hit ftp://ftp.iinet.net.au breezy-updates/main Packages
Hit ftp://ftp.iinet.net.au breezy-updates/restricted Packages
Hit ftp://ftp.iinet.net.au breezy-security/main Packages
Hit ftp://ftp.iinet.net.au breezy-security/restricted Packages
Hit ftp://ftp.iinet.net.au breezy-security/universe Packages
Hit ftp://ftp.iinet.net.au breezy-security/multiverse Packages
Fetched 58.0kB in 0s (121kB/s)
Reading package lists... Done
```

Now I would install ssh and ssh daemon clients, as that's what I will be using to test if it binds and authenticates via LDAP instead of logging in and out of the console. So install ssh by doing

```
apt-get install ssh
```

With that installed we proceed to install the LDAP client packages required for authentication which include several packages which both work on Ubuntu Dapper and Breezy distro. Both distros modify the same set of files but the PAM configurations differs slightly.

Ubuntu and Fedora Directory Server Binding via LDAP  
Written by: Ashley Chew  
Last Updated: 18082006

```
apt-get install ldap-utils libpam-ldap libnss-ldap nscd
```

If should prompt you several questions, and I'm assuming you have a Fedora Directory LDAP server going so you should be to answer those questions which include

```
LDAP Server host: jhett.csse.uwa.edu.au
The distinguished name of the search base: dc=csse,dc=uwa,dc=edu,dc=au
LDAP Version to use: 3
Database requires login: no
Make configuration readable/writeable by owner only: yes
```

I would advice people to start nscd, this the name system caching daemon or something like that which will cache request to the LDAP server. Start it /etc/init.d/nscd start (Good idea to add it to startup)

Now this will generate a file in /etc/libnss-ldap.conf which we have to edit as the questions asked is not enough to described the Fedora LDAP Directory including custom schema. It find that funny most Unix/Linux system has a configuration file called ldap.conf but with ubuntu I find it odd as it has several references which are

```
/etc/libnss-ldap.conf
/etc/pam_ldap.conf
/etc/ldap/ldap.conf
```

But they are all the same file, so I deleted /etc/pam\_ldap.conf and /etc/ldap/ldap.conf and sym linked it to /etc/libnss-ldap.conf as they are one and the same configuration file ie

```
rm -rf /etc/pam_ldap.conf
rm -rf /etc/ldap/ldap.conf
ln -s /etc/libnss-ldap.conf /etc/pam_ldap.conf
ln -s /etc/libnss-ldap.conf /etc/ldap/ldap.conf
```

Now as all references of the LDAP configuration is in one place I just have to edit the one file which is /etc/libnss-ldap.conf, the contents of that file is shown below.

```
cat /etc/libnss-ldap.conf

###DEBCONF###
# the configuration of this file will be done by debconf as long as
the
# first line of the file says '###DEBCONF###'
#
# you should use dpkg-reconfigure libnss-ldap to configure this file.
#
@(#) $Id: ldap.conf,v 2.41 2005/03/23 08:30:16 lukeh Exp $
#
# This is the configuration file for the LDAP nameservice
# switch library and the LDAP PAM module.
#
```

```

# PADL Software
# http://www.padl.com
#

# Your LDAP server. Must be resolvable without using LDAP.
# Multiple hosts may be specified, each separated by a
# space. How long nss_ldap takes to failover depends on
# whether your LDAP client library supports configurable
# network or connect timeouts (see bind_timelimit).
host acm.csse.uwa.edu.au

# The distinguished name of the search base.
base dc=csse,dc=uwa,dc=edu,dc=au

# Another way to specify your LDAP server is to provide an
# uri with the server name. This allows to use
# Unix Domain Sockets to connect to a local LDAP Server.
#uri ldap://127.0.0.1/
#uri ldaps://127.0.0.1/
#uri ldapi://%2fvar%2frun%2fldapi_sock/
# Note: %2f encodes the '/' used as directory separator

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
#binddn cn=proxyuser,dc=padl,dc=com

# The credentials to bind with.
# Optional: default is no credential.
#bindpw secret

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
#rootbinddn cn=manager,dc=padl,dc=com

# The port.
# Optional: default is 389.
port 389

# The search scope.
#scope sub
#scope one
#scope base

# Search timelimit
#timelimit 30

# Bind/connect timelimit
#bind_timelimit 30

# Reconnect policy:
# hard_open: reconnect to DSA with exponential backoff if
#             opening connection failed
# hard_init: reconnect to DSA with exponential backoff if
#             initializing connection failed
# hard:      alias for hard_open
# soft:      return immediately on server failure

```

Ubuntu and Fedora Directory Server Binding via LDAP  
 Written by: Ashley Chew  
 Last Updated: 18082006

```

#bind_policy hard

# Idle timelimit; client will close connections
# (nss_ldap only) if the server has not been contacted
# for the number of seconds specified below.
#idle_timelimit 3600

# Pagesize: when configured with --enable-paged-results allow
# to set the pagesize to a custom value
#pagesize 1000

# Filter to AND with uid=%s
#pam_filter objectclass=account

# The user ID attribute (defaults to uid)
#pam_login_attribute uid

# Search the root DSE for the password policy (works
# with Netscape Directory Server)
#pam_lookup_policy yes

# Check the 'host' attribute for access control
# Default is no; if set to yes, and user has no
# value for the host attribute, and pam_ldap is
# configured for account management (authorization)
# then the user will not be allowed to login.
#pam_check_host_attr yes

# Check the 'authorizedService' attribute for access
# control
# Default is no; if set to yes, and the user has no
# value for the authorizedService attribute, and
# pam_ldap is configured for account management
# (authorization) then the user will not be allowed
# to login.
#pam_check_service_attr yes

# Group to enforce membership of
#pam_groupdn cn=PAM,ou=Groups,dc=padl,dc=com

# Group member attribute
#pam_member_attribute uniquemember

# Specify a minium or maximum UID number allowed
#pam_min_uid 0
#pam_max_uid 0

# Template login attribute, default template user
# (can be overridden by value of former attribute
# in user's entry)
#pam_login_attribute userPrincipalName
#pam_template_login_attribute uid
#pam_template_login nobody

# HEADS UP: the pam_crypt, pam_nds_passwd,
# and pam_ad_passwd options are no
# longer supported.
#
# If you are using XAD, you can set pam_password
# to racf, ad, or exop. Make sure that you have
# SSL enabled.

```

Ubuntu and Fedora Directory Server Binding via LDAP  
 Written by: Ashley Chew  
 Last Updated: 18082006

```

# Do not hash the password at all; presume
# the directory server will do it, if
# necessary. This is the default.
#pam_password clear

# Hash password locally; required for University of
# Michigan LDAP server, and works with Netscape
# Directory Server if you're using the UNIX-Crypt
# hash mechanism and not using the NT Synchronization
# service.
pam_password crypt

# Remove old password first, then update in
# cleartext. Necessary for use with Novell
# Directory Services (NDS)
#pam_password nds

# RACF is an alias for the above. For use with
# IBM RACF
#pam_password racf

# Update Active Directory password, by
# creating Unicode password and updating
# unicodePwd attribute.
#pam_password ad

# Use the OpenLDAP password change
# extended operation to update the password.
#pam_password exop

# Redirect users to a URL or somesuch on password
# changes.
#pam_password_prohibit_message Please visit http://internal to change
your password.

# RFC2307bis naming contexts
# Syntax:
# nss_base_XXX    base?scope?filter
# where scope is {base,one,sub}
# and filter is a filter to be &'d with the
# default filter.
# You can omit the suffix eg:
# nss_base_passwd ou=People,
# to append the default base DN but this
# may incur a small performance impact.
nss_base_passwd ou=People,dc=csse,dc=uwa,dc=edu,dc=au
nss_base_shadow ou=People,dc=csse,dc=uwa,dc=edu,dc=au
nss_base_group ou=Groups,dc=csse,dc=uwa,dc=edu,dc=au

#nss_base_passwdou=People,dc=padl,dc=com?one
#nss_base_shadowou=People,dc=padl,dc=com?one
#nss_base_group    ou=Group,dc=padl,dc=com?one
#nss_base_hosts    ou=Hosts,dc=padl,dc=com?one
#nss_base_servicesou=Services,dc=padl,dc=com?one
#nss_base_networksou=Networks,dc=padl,dc=com?one
#nss_base_protocolsou=Protocols,dc=padl,dc=com?one
#nss_base_rpc       ou=Rpc,dc=padl,dc=com?one
#nss_base_ethersou=Ethers,dc=padl,dc=com?one
#nss_base_netmasksou=Networks,dc=padl,dc=com?ne
#nss_base_bootparamsou=Ethers,dc=padl,dc=com?one

```

Ubuntu and Fedora Directory Server Binding via LDAP

Written by: Ashley Chew

Last Updated: 18082006

```

#nss_base_aliasesou=Aliases,dc=padl,dc=com?one
#nss_base_netgroupou=Netgroup,dc=padl,dc=com?one

# attribute/objectclass mapping
# Syntax:
#nss_map_attributerfc2307attribute mapped_attribute
#nss_map_objectclassrfc2307objectclass mapped_objectclass

# configure --enable-nds is no longer supported.
# NDS mappings
#nss_map_attribute uniqueMember member

# Services for UNIX 3.5 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount User
#nss_map_attribute uid msSFU30Name
#nss_map_attribute uniqueMember msSFU30PosixMember
#nss_map_attribute userPassword msSFU30Password
#nss_map_attribute homeDirectory msSFU30HomeDirectory
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_objectclass posixGroup Group
#pam_login_attribute msSFU30Name
#pam_filter objectclass=User
#pam_password ad

# configure --enable-mssfu-schema is no longer supported.
# Services for UNIX 2.0 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid msSFUName
#nss_map_attribute uniqueMember posixMember
#nss_map_attribute userPassword msSFUPassword
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup Group
#nss_map_attribute cn msSFUName
#pam_login_attribute msSFUName
#pam_filter objectclass=User
#pam_password ad

# RFC 2307 (AD) mappings
#nss_map_objectclass posixAccount user
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid sAMAccountName
#nss_map_attribute homeDirectory unixHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup group
#nss_map_attribute uniqueMember member
#pam_login_attribute sAMAccountName
#pam_filter objectclass=User
#pam_password ad

# configure --enable-authpassword is no longer supported
# AuthPassword mappings
#nss_map_attribute userPassword authPassword

# AIX SecureWay mappings
#nss_map_objectclass posixAccount aixAccount
#nss_base_passwd ou=aixaccount,?one
#nss_map_attribute uid userName
#nss_map_attribute gidNumber gid

```

```

#nss_map_attribute uidNumber uid
#nss_map_attribute userPassword passwordChar
#nss_map_objectclass posixGroup aixAccessGroup
#nss_base_group ou=aixgroup,?one
#nss_map_attribute cn groupName
#nss_map_attribute uniqueMember member
#pam_login_attribute userName
#pam_filter objectclass=aixAccount
#pam_password clear

# Netscape SDK LDAPS
#ssl on

# Netscape SDK SSL options
#sslpath /etc/ssl/certs/cert7.db

# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically 636
#ssl start_tls
#ssl on

# OpenLDAP SSL options
# Require and verify server certificate (yes/no)
# Default is to use libldap's default behavior, which can be
configured in
# /etc/openldap/ldap.conf using the TLS_REQCERT setting. The default
for
# OpenLDAP 2.0 and earlier is "no", for 2.1 and later is "yes".
#tls_checkpeer yes

# CA certificates for server certificate verification
# At least one of these are required if tls_checkpeer is "yes"
#tls_cacertfile /etc/ssl/ca.cert
#tls_cacertdir /etc/ssl/certs

# Seed the PRNG if /dev/urandom is not provided
#tls_randfile /var/run/egd-pool

# SSL cipher suite
# See man ciphers for syntax
#tls_ciphers TLSv1

# Client certificate and key
# Use these, if your server requires client authentication.
#tls_cert
#tls_key

# Disable SASL security layers. This is needed for AD.
#sasl_secprops maxssf=0

# Override the default Kerberos ticket cache location.
#krb5_ccname FILE:/etc/.ldapcache

```

I would pay special attention to nss\_base\_\* ie in this case I refer to nss\_base\_passwd, nss\_base\_shadow and nss\_base\_group. As in the Fedora Directory Default schema these information are stored in the organization unit People and Groups. If you didn't specify this and you tried logging later on it will try to look up the information from your base directive ie dc=csse,dc=uwa,dc=edu,dc=au instead of specified place ou=People,dc=csse,dc=uwa,dc=edu,dc=au for user

## Ubuntu and Fedora Directory Server Binding via LDAP

Written by: Ashley Chew

Last Updated: 18082006

information and similarly for group information  
ou=Groups,dc=csse,dc=uwa,dc=edu,dc=au.

Now basically you have configured the lookup information for LDAP but you haven't told the system to actually use LDAP. This basically is a two step process, which you have to tell it to use ldap by editing /etc/nsswitch.conf and altering PAM modules to use LDAP.

The contents of the nsswitch.conf is shown below

```
cat /etc/nsswitch.conf
```

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.
```

```
passwd:      files ldap
group:       files ldap
shadow:      files ldap
```

```
hosts:       files dns
networks:    files
```

```
protocols:   db files
services:    db files
ethers:      db files
rpc:         db files
```

```
netgroup:    nis
```

With the PAM authentication, you have to edit several files in /etc/pam.d, mainly all PAM modules including for login, ssh etc uses a common set of files which are common-account, common-auth, common-password and common-session. You have to alter all these file to include LDAP directives which I will show below.

Note these LDAP directives will only work with Ubuntu 5.1 (Breezy) and won't work with Ubuntu 6.06.1 (Dapper), the PAM modules directives are slightly different as I found out.

```
root@rain:/etc/pam.d# cat common-account
```

```
#
# /etc/pam.d/common-account - authorization settings common to all
services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authorization modules that define
# the central access policy for use on the system.  The default is to
# only deny service to users whose accounts are expired in
/etc/shadow.
#
account sufficient      pam_ldap.so
account required       pam_unix.so
```

```
root@rain:/etc/pam.d# cat common-auth
```

```
#
# /etc/pam.d/common-auth - authentication settings common to all
services
```

Ubuntu and Fedora Directory Server Binding via LDAP

Written by: Ashley Chew

Last Updated: 18082006

```

#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.). The default is to use
the
# traditional Unix authentication mechanisms.
#
auth    sufficient    pam_ldap.so
auth    required      pam_unix.so nullok_secure

root@rain:/etc/pam.d# cat common-password
#
# /etc/pam.d/common-password - password-related modules common to all
services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to
be
#used to change user passwords. The default is pam_unix

# The "nullok" option allows users to change an empty password, else
# empty passwords are treated as locked accounts.
#
# (Add `md5' after the module name to enable MD5 passwords)
#
# The "obscure" option replaces the old `OBSOLETE_CHECKS_ENAB' option
in
# login.defs. Also the "min" and "max" options enforce the length of
the
# new password.

password sufficient pam_ldap.so
password required pam_unix.so nullok obscure min=4 max=8 md5

# Alternate strength checking for password. Note that this
# requires the libpam-cracklib package to be installed.
# You will need to comment out the password line above and
# uncomment the next two in order to use this.
# (Replaces the `OBSOLETE_CHECKS_ENAB', `CRACKLIB_DICTPATH')
#
# password required pam_cracklib.so retry=3 minlen=6 difok=3
# password required pam_unix.so use_authok nullok md5

root@rain:/etc/pam.d# cat common-session
#
# /etc/pam.d/common-session - session-related modules common to all
services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be
performed
# at the start and end of sessions of *any* kind (both interactive
and
# non-interactive). The default is pam_unix.
#
session sufficient pam_ldap.so
session required pam_unix.so

```

As mentioned before the Ubuntu LDAP directives are slightly different for Ubuntu 6.06.1 Dapper, I'm not quite sure why.

```
rain% pwd
/etc/pam.d
rain% cat common-account
#
# /etc/pam.d/common-account - authorization settings common to all
services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authorization modules that define
# the central access policy for use on the system.  The default is to
# only deny service to users whose accounts are expired in
/etc/shadow.
#
account sufficient      pam_ldap.so
account required        pam_unix.so

rain% cat common-auth
#
# /etc/pam.d/common-auth - authentication settings common to all
services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  The default is to use
the
# traditional Unix authentication mechanisms.
#
auth      sufficient      pam_ldap.so
auth      required        pam_unix.so nullok_secure

rain% cat common-password
#
# /etc/pam.d/common-password - password-related modules common to all
services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to
be
#used to change user passwords.  The default is pam_unix

# The "nullok" option allows users to change an empty password, else
# empty passwords are treated as locked accounts.
#
# (Add `md5' after the module name to enable MD5 passwords)
#
# The "obscure" option replaces the old `OBSCURE_CHECKS_ENAB' option
in
# login.defs. Also the "min" and "max" options enforce the length of
the
# new password.

password  sufficient      pam_ldap.so
password  required        pam_unix.so nullok obscure min=4 max=8 md5

# Alternate strength checking for password. Note that this
# requires the libpam-cracklib package to be installed.
# You will need to comment out the password line above and
```

Ubuntu and Fedora Directory Server Binding via LDAP

Written by: Ashley Chew

Last Updated: 18082006

```

# uncomment the next two in order to use this.
# (Replaces the `OBSCURE_CHECKS_ENAB', `CRACKLIB_DICTPATH')
#
# password required      pam_cracklib.so retry=3 minlen=6 difok=3
# password required      pam_unix.so use_authtok nullok md5

rain% cat common-session
#
# /etc/pam.d/common-session - session-related modules common to all
services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be
performed
# at the start and end of sessions of *any* kind (both interactive
and
# non-interactive). The default is pam_unix.
#
session sufficient      pam_ldap.so
session required        pam_unix.so
#session                optional    pam_foreground.so

```

That's basically it, now if you have a user in your LDAP try ssh into your client machine. If you have problems make sure it is contacting your Fedora LDAP server by looking /opt/fedora-ds/slapd-machinename/logs/access.

It should show the machine name contacting your ldap server with the username ie this is a trace of a successful login attempt on the Directory Server.

```

Fedora-Directory/1.0.2 B2006.060.1951
jhett.csse.uwa.edu.au:389 (/opt/fedora-ds/slapd-jhett)

```

```

[18/Aug/2006:16:23:32 +0800] conn=0 fd=64 slot=64 connection from
130.95.1.126 to 130.95.1.71
[18/Aug/2006:16:23:32 +0800] conn=0 op=0 BIND dn="" method=128
version=3
[18/Aug/2006:16:23:32 +0800] conn=0 op=0 RESULT err=0 tag=97
nentries=0 etime=0 dn=""
[18/Aug/2006:16:23:32 +0800] conn=0 op=1 SRCH
base="ou=People,dc=csse,dc=uwa,dc=edu,dc=au" scope=2
filter="(&(objectClass=posixAccount)(uid=ashley))" attrs="uid
userPassword uidNumber gidNumber cn homeDirectory loginShell gecos
description objectClass"
[18/Aug/2006:16:23:32 +0800] conn=0 op=1 RESULT err=0 tag=101
nentries=1 etime=0
[18/Aug/2006:16:23:34 +0800] conn=1 fd=65 slot=65 connection from
130.95.1.126 to 130.95.1.71
[18/Aug/2006:16:23:34 +0800] conn=1 op=0 BIND dn="" method=128
version=3
[18/Aug/2006:16:23:34 +0800] conn=1 op=0 RESULT err=0 tag=97
nentries=0 etime=0 dn=""
[18/Aug/2006:16:23:34 +0800] conn=1 op=1 SRCH
base="ou=People,dc=csse,dc=uwa,dc=edu,dc=au" scope=2
filter="(uid=ashley)" attrs=ALL
[18/Aug/2006:16:23:34 +0800] conn=1 op=1 RESULT err=0 tag=101
nentries=1 etime=0
[18/Aug/2006:16:23:34 +0800] conn=1 op=2 BIND
dn="uid=ashley,ou=People,dc=csse,dc=uwa,dc=edu,dc=au" method=128
version=3

```

Ubuntu and Fedora Directory Server Binding via LDAP

Written by: Ashley Chew

Last Updated: 18082006

```

[18/Aug/2006:16:23:34 +0800] conn=1 op=2 RESULT err=0 tag=97
nentries=0 etime=0
dn="uid=ashley,ou=people,dc=csse,dc=uwa,dc=edu,dc=au"
[18/Aug/2006:16:23:34 +0800] conn=1 op=3 BIND dn="" method=128
version=3
[18/Aug/2006:16:23:34 +0800] conn=1 op=3 RESULT err=0 tag=97
nentries=0 etime=0 dn=""
[18/Aug/2006:16:23:34 +0800] conn=0 op=2 SRCH
base="ou=People,dc=csse,dc=uwa,dc=edu,dc=au" scope=2
filter="(&(objectClass=posixAccount)(uid=ashley))" attrs=ALL
[18/Aug/2006:16:23:34 +0800] conn=0 op=2 RESULT err=0 tag=101
nentries=1 etime=0
[18/Aug/2006:16:23:34 +0800] conn=0 op=3 SRCH
base="ou=Groups,dc=csse,dc=uwa,dc=edu,dc=au" scope=2
filter="(&(objectClass=posixGroup)(|(memberUid=ashley)(uniqueMember=uid=ashley,ou=People,dc=csse,dc=uwa,dc=edu,dc=au)))" attrs="gidNumber"
[18/Aug/2006:16:23:34 +0800] conn=0 op=3 RESULT err=0 tag=101
nentries=0 etime=0
[18/Aug/2006:16:23:34 +0800] conn=1 op=4 UNBIND
[18/Aug/2006:16:23:34 +0800] conn=1 op=4 fd=65 closed - U1
[18/Aug/2006:16:23:34 +0800] conn=0 op=4 SRCH
base="ou=People,dc=csse,dc=uwa,dc=edu,dc=au" scope=2
filter="(&(objectClass=posixAccount)(uidNumber=272))" attrs="uid
userPassword uidNumber gidNumber cn homeDirectory loginShell gecos
description objectClass"
[18/Aug/2006:16:23:34 +0800] conn=0 op=4 RESULT err=0 tag=101
nentries=1 etime=0
[18/Aug/2006:16:23:34 +0800] conn=0 op=5 SRCH
base="ou=People,dc=csse,dc=uwa,dc=edu,dc=au" scope=2
filter="(&(objectClass=posixAccount)(uid=ashley))" attrs="uid
userPassword uidNumber gidNumber cn homeDirectory loginShell gecos
description objectClass"
[18/Aug/2006:16:23:34 +0800] conn=0 op=5 RESULT err=0 tag=101
nentries=1 etime=0
[18/Aug/2006:16:23:34 +0800] conn=2 fd=65 slot=65 connection from
130.95.1.126 to 130.95.1.71
[18/Aug/2006:16:23:34 +0800] conn=2 op=0 BIND dn="" method=128
version=3
[18/Aug/2006:16:23:34 +0800] conn=2 op=0 RESULT err=0 tag=97
nentries=0 etime=0 dn=""
[18/Aug/2006:16:23:34 +0800] conn=2 op=1 SRCH
base="ou=People,dc=csse,dc=uwa,dc=edu,dc=au" scope=2
filter="(&(objectClass=posixAccount)(uidNumber=272))" attrs="uid
userPassword uidNumber gidNumber cn homeDirectory loginShell gecos
description objectClass"
[18/Aug/2006:16:23:34 +0800] conn=2 op=1 RESULT err=0 tag=101
nentries=1 etime=0
[18/Aug/2006:16:23:34 +0800] conn=3 fd=66 slot=66 connection from
130.95.1.126 to 130.95.1.71
[18/Aug/2006:16:23:34 +0800] conn=3 op=0 BIND dn="" method=128
version=3
[18/Aug/2006:16:23:34 +0800] conn=3 op=0 RESULT err=0 tag=97
nentries=0 etime=0 dn=""
[18/Aug/2006:16:23:34 +0800] conn=3 op=1 SRCH
base="ou=Groups,dc=csse,dc=uwa,dc=edu,dc=au" scope=2
filter="(&(objectClass=posixGroup)(cn=ashley))" attrs="cn
userPassword memberUid uniqueMember gidNumber"
[18/Aug/2006:16:23:34 +0800] conn=3 op=1 RESULT err=0 tag=101
nentries=0 etime=0
[18/Aug/2006:16:23:34 +0800] conn=3 op=-1 fd=66 closed - B1

```

```
[18/Aug/2006:16:23:37 +0800] conn=0 op=6 SRCH
base="ou=People,dc=csse,dc=uwa,dc=edu,dc=au" scope=2
filter="(&(objectClass=posixAccount)(uid=ashley))" attrs="uid
userPassword uidNumber gidNumber cn homeDirectory loginShell gecos
description objectClass"
[18/Aug/2006:16:23:37 +0800] conn=0 op=6 RESULT err=0 tag=101
nentries=1 etime=0
[18/Aug/2006:16:23:37 +0800] conn=0 op=-1 fd=64 closed - B1
[18/Aug/2006:16:23:37 +0800] conn=2 op=-1 fd=65 closed - B1
```

Other points of interest make sure you have a valid shell specified in your LDAP on your remote ssh connection to test the machine will not allow you in (I got caught by this silly mistake) the other thing you may find useful is to see if the LDAP is translated correctly similar to a passwd format which you can type 'getent passwd'

Another point seems like if you finished configuring it and it fails in terms of logging at the console screen saying can't because of some sort of group error. Just reboot the Ubuntu machine, then it works, I seriously don't know whats with this distro. I might look into it further down the line.