# Contents



# Lightweight Directory Access Protocol

Ldap commands:

```
ldapsearch -x  //list all ldap info for users
ldapsearch -x uid=username   //list ldap info for a particular user
```

## ldapmodify

```
echo "dn: uid=$User,ou=People,dc=skynet,dc=ie
loginShell: $Shell
" | ldapmodify -x -D "uid=$User,ou=People,dc=skynet,dc=ie" -W
```

After a good bit of checking and looking, the -x and -W values make this work. The above code was obtained from /usr/bin/chsh which is a modified/fixed version of chsh especially for ldap. It did need a little modification however.

## Debug ldapsearch | ldapmodify

If you are getting errors similar to:

```
ldap_bind: Can't contact LDAP server (-1)
        additional info: error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify
```

There are problems with your ldap server. Passwd and other commands may work, but ldapsearch or ldapmodify may not work. To debug whats happenning type:

```
ldapsearch -x -d 9
```

You will see exactly whats happenning.

## ldapmodify - modify privileged user details

The above ldapmodify code will work for changing details which the user themselves have access to. If you want to change privileged information, you need to run ldapmodify with root or Account privileges. The following works fine:

```
echo "dn: uid=steviewdr,ou=People,dc=skynet,dc=ie
altShell: /bin/bash
" | ldapmodify -x -D "cn=Accounts,dc=skynet,dc=ie" -W
```

The above will connect as "cn=Accounts" and will prompt for the Accounts password. Run a "ldapsearch -x uid=steviewdr" afterwards to check that altShell was changed. Thats is.

## ldapvi - Perform an LDAP search and update results using a text editor.

```
apt-get install ldapvi

ldapvi
```

~~Although I didnt test it fully, it seems nice.~~ You may have to provide a better start command to auth yourself as "Accounts" etc. You also may have to export vi as your editor.

```
export EDITOR="/usr/bin/vi"
ldapvi --user cn=Accounts,dc=skynet,dc=ie -w`cat /etc/ldap.secret`
```

### Issues with ldapvi

I was continually getting the error '**ldap_bind: Can't contact LDAP server (-1)**'. Commands such as ldapsearch, ldapmodify worked ok. It turns out with an strace and some googling that it was TLS Certs causing the issue.

**Solution: to use "--tls allow"**

```
ldapvi -D "uid=steviewdr,ou=People,dc=skynet,dc=ie" -h ldaps://ldap.skynet.ie --tls allow

#To connect as Accounts/root instead of a user:
ldapvi -D "cn=Accounts,dc=skynet,dc=ie" -h ldaps://ldap.skynet.ie --tls allow
```

The command above, reads /etc/ldap/ldap.conf, and looks for the TLS_Cert. You do need the Cert to connect to ldaps.

```
#Contents of above file
BASE dc=skynet,dc=ie
URI ldaps://ldap.skynet.ie
TLS_CACERT  /etc/ssl/certs/cacert.class1.pem
```

So not only can the main accounts user use ldapvi to change other peoples details, the ldap user themselves can change their own details instead of using ldapmodify or patched chsh or chfn.

#### ldap limit of 500 entries

Another issue I had with ldapvi, albeit not specifically an ldapvi issue, was that it was limited to 500 entries.

```
   500 entries read
Search failed: Size limit exceeded
Continue anyway? [yn] n

On the old ldap:
vi /etc/ldap/slapd.conf
#add the following:
sizelimit 3000

On the new ldap:
vi /etc/ldap/slapd.d/cn=config/olcDatabase={1}bdb.ldif
#Add in olcSizeLimit: 3000 underneath "olcRootPW"
olcRootPW:: xxxx
olcSizeLimit: 3000

/etc/init.d/slapd restart
```

---

## Allow users to change their LDAP Password

After an upgrade from hardy to lucid, ldap changed, and no longer used /etc/ldap/slapd.conf, and instead used many smaller ldif files in /etc/ldap/slapd.d/

```
vi /etc/ldap/slapd.d/cn\=config/olcDatabase\=\{1\}bdb.ldif
#make sure the "by self write" is present in the userPassword line.
olcAccess: {2}to attrs=userPassword by self write by dn.base="cn=admin,dc=skynet,dc=ie" write by ano
/etc/init.d/slapd restart
```

## Ldap commands

```
* Authed ldapsearch
ldapsearch -x -D "uid=steviewdr,ou=People,dc=skynet,dc=ie" -W
* UnAuthed ldapsearch
ldapsearch -x
* Change ldap password method 2
ldappasswd -D 'uid=steviewdr,ou=People,dc=skynet,dc=ie' -W -S
```

Useful links:

http://docs.sun.com/source/816-6400-10/lsearch.html

http://docs.sun.com/source/816-6400-10/lmodify.html

http://docsrv.sco.com/INT_DirectoryAG/modify.htm#1021458

http://docsrv.sco.com/INT_DirectoryAG/modify.htm#1006755