OpenLDAP client tools Query LDAP directories

CONCEPTS

Connect -H uri, -Z StartTLS
↓ bind
Bind -x -D -W or SASL
↓ search
Search -b base -s scope filter
↓ return
Entries attrs, LDIF output
One ldapsearch run

Always add -x unless you want SASL: without it the tools try SASL and often fail with confusing errors.

Directory data is a tree: a DN names an entry, the base picks the subtree, the scope picks how deep.

Put the filter in quotes; shell characters like ( ) and * would otherwise be eaten.

CONNECT AND BIND

-H ldap://<host>[:<port>]
Server URI (plain or StartTLS)

-H ldaps://<host>
TLS from the first byte

-H ldapi:///
Local socket (as root, with -Y EXTERNAL)

-x
Simple bind instead of SASL

-D <binddn>
Bind as this DN

-W
Prompt for the password

-y <file>
Read password from a file

-w <password>
Password on command line

-ZZ
StartTLS, fail if it cannot be used

-Y EXTERNAL -H ldapi:///
SASL EXTERNAL over the local socket

-Y GSSAPI
Kerberos login

SEARCHING

-b <base>
Search base DN

SEARCHING (cont.)

-b ""
Empty base: rootDSE with -s base

-s base / one / sub / children
Search scope (default sub)

"(<attr>=<value>)"
Equality filter

"(<attr>=<pre>*)"
Substring/wildcard match

"(<attr>=*)"
Attribute is present

"(&(<f1>)(<f2>))"
AND of filters

"(|(<f1>)(<f2>))"
OR of filters

"(!(<f>))"
Negate a filter

"(<attr>≥<n>)"
Greater or equal (<= for less)

-z <n>
Max entries returned

-l <seconds>
Time limit for the search

\28 \29 \2a \5c
Escape ( ) * \ in values

ATTRIBUTES AND OUTPUT

... <filter> cn mail
Return only listed attributes

"*" "+"
User plus operational attributes

1.1
Return DNs only

-LLL
Plain LDIF, no comments or version

-L
LDIF v1 with comments

-S <attr>
Sort entries client-side

-o ldif_wrap=no
Don't wrap long LDIF lines

-E pr=<n>/noprompt
Paged results

-v
Verbose diagnostics

CHANGE ENTRIES

ldapadd -x -D <binddn> -W -f <file>
Add entries from LDIF

ldapmodify -x -D <binddn> -W -f <file>
Apply LDIF changes

ldapdelete -x -D <binddn> -W "<dn>"
Delete an entry

ldappasswd -x -D <binddn> -W -S "<dn>"
Set a password (prompts)

ldapwhoami -x -D <binddn> -W
Show the identity after bind

ldapmodify -c -S <skipfile>
Keep going, save failed records

ldapmodify -a
Treat input as adds

ldapmodify -n -v
Dry run with verbose output

LDIF change record

Line	Meaning
`dn: <dn>`	Entry to change
`changetype: modify`	Modify (also add, delete, modrdn)
`add: / replace: / delete: <attr>`	Operation on an attribute
`-`	Ends one operation block

Separate records in an LDIF file with a blank line; the lone - line closes each modify block.

RECIPES

Export a subtree

```
# dump a whole subtree to a file
ldapsearch -x -LLL -H ldaps://
<host> -D <binddn> -W \
  -b "<base>" "(objectClass=*)" >
backup.ldif
```

Discover the base DN

```
# find the naming contexts the
server offers
ldapsearch -x -LLL -H ldap://
<host> -s base -b "" \
  namingContexts
supportedSASLMechanisms
```