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

-x
Simple bind instead of SASL

-D <binddn>
Bind as this DN

-W
Prompt for the password

-ZZ
StartTLS, fail if it cannot be used

SEARCHING

-b <base>
Search base DN

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

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

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

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

SEARCHING (cont.)

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

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

-E pr=<n>**/noprompt**
Paged results

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

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