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