NAME

ldapsearch - LDAP search tool

SYNOPSIS

ldapsearch [**-V**[**V**]] [**-d** *debuglevel*] [**-n**] [**-v**] [**-c**] [**-u**] [**-t**[**t**]] [**-T** *path*] [**-F** *prefix*] [**-A**] [**-L**[**L**[**L**]]] [**-S** *attribute*] [**-b** *searchbase*] [**-s** {**base**|**one**|**sub**|**children**}] [**-a** {**never**|**always**|**search**|**find**}] [**-l** *timelimit*] [**-z** *sizelimit*] [**-f** *file*] [**-M**[**M**]] [**-x**] [**-D** *binddn*] [**-W**] [**-w** *passwd*] [**-y** *passwdfile*] [**-H** *ldapuri*] [**-P** {**2**|**3**}] [**-e** [**!**]*ext*[**=***extparam*]] [**-E** [**!**]*ext*[**=***extparam*]] [**-o** *opt*[**=***optparam*]] [**-O** *security-properties*] [**-I**] [**-Q**] [**-N**] [**-U** *authcid*] [**-R** *realm*] [**-X** *authzid*] [**-Y** *mech*] [**-Z**[**Z**]] *filter* [*attrs...*]

DESCRIPTION

ldapsearch is a shell-accessible interface to the **ldap_search_ext**(3) library call.

ldapsearch opens a connection to an LDAP server, binds, and performs a search using specified parameters. The *filter* should conform to the string representation for search filters as defined in RFC 4515. If not provided, the default filter, **(objectClass=*)**, is used.

If **ldapsearch** finds one or more entries, the attributes specified by *attrs* are returned. If ***** is listed, all user attributes are returned. If **+** is listed, all operational attributes are returned. If no *attrs* are listed, all user attributes are returned. If only 1.1 is listed, no attributes will be returned.

The search results are displayed using an extended version of LDIF. Option *-L* controls the format of the output.

OPTIONS

-V[**V**]

Print version info. If **-VV** is given, exit after providing version info. Otherwise proceed with the specified search

-d *debuglevel*

Set the LDAP debugging level to *debuglevel*. **ldapsearch** must be compiled with LDAP_DEBUG defined for this option to have any effect.

-n Show what would be done, but don't actually perform the search. Useful for debugging in conjunction with **-v**.

-v Run in verbose mode, with many diagnostics written to standard output.

-c Continuous operation mode. Errors are reported, but ldapsearch will continue with searches. The default is to exit after reporting an error. Only useful in conjunction with **-f**.

-u Include the User Friendly Name form of the Distinguished Name (DN) in the output.

-t[**t**]
A single **-t** writes retrieved non-printable values to a set of temporary files. This is useful for dealing with values containing non-character data such as jpegPhoto or audio. A second **-t** writes all retrieved values to files.

-T *path*
Write temporary files to directory specified by *path* (default: **system default tmp directory**). The environment variables **TMPDIR**, **TMP**, or **TEMP** will override the default path.

-F *prefix*
URL prefix for temporary files. Default is **file://***path* **where** *path* **is the system default tmp directory or the value specified with -T.**

-A Retrieve attributes only (no values). This is useful when you just want to see if an attribute is present in an entry and are not interested in the specific values.

-L Search results are display in LDAP Data Interchange Format detailed in **ldif**(5). A single **-L** restricts the output to LDIFv1.
A second **-L** disables comments. A third **-L** disables printing of the LDIF version. The default is to use an extended version of LDIF.

-S *attribute*
Sort the entries returned based on *attribute*. The default is not to sort entries returned. If *attribute* is a zero-length string (""), the entries are sorted by the components of their Distinguished Name. See **ldap_sort**(3) for more details. Note that **ldapsearch** normally prints out entries as it receives them. The use of the **-S** option defeats this behavior, causing all entries to be retrieved, then sorted, then printed.

-b *searchbase*
Use *searchbase* as the starting point for the search instead of the default.

-s {**base**|**one**|**sub**|**children**}
Specify the scope of the search to be one of **base**, **one**, **sub**, or **children** to specify a base object, one-level, subtree, or children search. The default is **sub**. Note: *children* scope requires LDAPv3 subordinate feature extension.

-a {**never**|**always**|**search**|**find**}
Specify how aliases dereferencing is done. Should be one of **never**, **always**, **search**, or **find** to

specify that aliases are never dereferenced, always dereferenced, dereferenced when searching, or dereferenced only when locating the base object for the search. The default is to never dereference aliases.

-l *timelimit*
wait at most *timelimit* seconds for a search to complete. A timelimit of *0* (zero) or *none* means no limit. A timelimit of *max* means the maximum integer allowable by the protocol. A server may impose a maximal timelimit which only the root user may override.

-z *sizelimit*
retrieve at most *sizelimit* entries for a search. A sizelimit of *0* (zero) or *none* means no limit. A sizelimit of *max* means the maximum integer allowable by the protocol. A server may impose a maximal sizelimit which only the root user may override.

-f *file*
Read a series of lines from *file*, performing one LDAP search for each line. In this case, the *filter* given on the command line is treated as a pattern where the first and only occurrence of **%s** is replaced with a line from *file*. Any other occurrence of the the **%** character in the pattern will be regarded as an error. Where it is desired that the search filter include a **%** character, the character should be encoded as **\25** (see RFC 4515). If *file* is a single **-** character, then the lines are read from standard input. **ldapsearch** will exit when the first non-successful search result is returned, unless **-c** is used.

-M[**M**]
Enable manage DSA IT control. **-MM** makes control critical.

-x Use simple authentication instead of SASL.

-D *binddn*
Use the Distinguished Name *binddn* to bind to the LDAP directory. For SASL binds, the server is expected to ignore this value.

-W Prompt for simple authentication. This is used instead of specifying the password on the command line.

-w *passwd*
Use *passwd* as the password for simple authentication.

-y *passwdfile*
Use complete contents of *passwdfile* as the password for simple authentication.

-H *ldapuri*

Specify URI(s) referring to the ldap server(s); a list of URI, separated by whitespace or commas is expected; only the protocol/host/port fields are allowed. As an exception, if no host/port is specified, but a DN is, the DN is used to look up the corresponding host(s) using the DNS SRV records, according to RFC 2782. The DN must be a non-empty sequence of AVAs whose attribute type is "dc" (domain component), and must be escaped according to RFC 2396.

-P {**2**|**3**}

Specify the LDAP protocol version to use.

-e [**!**]*ext*[**=***extparam*]

-E [**!**]*ext*[**=***extparam*]

Specify general extensions with **-e** and search extensions with **-E**. '**!**' indicates criticality.

General extensions:
[!]assert=<filter> (an RFC 4515 Filter)
!authzid=<authzid> ("dn:<dn>" or "u:<user>")
[!]bauthzid (RFC 3829 authzid control)
[!]chaining[=<resolve>[/<cont>]]
[!]manageDSAit
[!]noop
ppolicy
[!]postread[=<attrs>] (a comma-separated attribute list)
[!]preread[=<attrs>] (a comma-separated attribute list)
[!]relax
sessiontracking[=<username>]
abandon,cancel,ignore (SIGINT sends abandon/cancel,
or ignores response; if critical, doesn't wait for SIGINT.
not really controls)

Search extensions:
!dontUseCopy
[!]domainScope (domain scope)
[!]mv=<filter> (matched values filter)
[!]pr=<size>[/prompt|noprompt] (paged results/prompt)
[!]sss=[-]<attr[:OID]>[/[-]<attr[:OID]>...] (server side sorting)
[!]subentries[=true|false] (subentries)
[!]sync=ro[/<cookie>] (LDAP Sync refreshOnly)

rp[/<cookie>][/<slimit>] (LDAP Sync refreshAndPersist)
[!]vlv=<before>/<after>(/<offset>/<count>|:<value>) (virtual list view)
[!]deref=derefAttr:attr[,attr[...]][;derefAttr:attr[,attr[...]]]
[!]<oid>[=:<value>|::<b64value>]

-o *opt*[=*optparam*]

Specify any **ldap.conf**(5) option or one of the following:
nettimeout=<timeout> (in seconds, or "none" or "max")
ldif_wrap=<width> (in columns, or "no" for no wrapping)

-O *security-properties*
Specify SASL security properties.

-I Enable SASL Interactive mode. Always prompt. Default is to prompt only as needed.

-Q Enable SASL Quiet mode. Never prompt.

-N Do not use reverse DNS to canonicalize SASL host name.

-U *authcid*
Specify the authentication ID for SASL bind. The form of the ID depends on the actual SASL mechanism used.

-R *realm*
Specify the realm of authentication ID for SASL bind. The form of the realm depends on the actual SASL mechanism used.

-X *authzid*
Specify the requested authorization ID for SASL bind. *authzid* must be one of the following formats: **dn:**<*distinguished name*> or **u:**<*username*>

-Y *mech*
Specify the SASL mechanism to be used for authentication. If it's not specified, the program will choose the best mechanism the server knows.

-Z[**Z**]
Issue StartTLS (Transport Layer Security) extended operation. If you use **-ZZ**, the command will require the operation to be successful.

OUTPUT FORMAT

If one or more entries are found, each entry is written to standard output in LDAP Data Interchange Format or **ldif**(5):

```
version: 1

# bjensen, example, net
dn: uid=bjensen,dc=example,dc=net
objectClass: person
objectClass: dcObject
uid: bjensen
cn: Barbara Jensen
sn: Jensen
...
```

If the **-t** option is used, the URI of a temporary file is used in place of the actual value. If the **-A** option is given, only the "attributename" part is written.

EXAMPLE

The following command:

```
ldapsearch -LLL "(sn=smith)" cn sn telephoneNumber
```

will perform a subtree search (using the default search base and other parameters defined in **ldap.conf**(5)) for entries with a surname (sn) of smith. The common name (cn), surname (sn) and telephoneNumber values will be retrieved and printed to standard output. The output might look something like this if two entries are found:

```
dn: uid=jts,dc=example,dc=com
cn: John Smith
cn: John T. Smith
sn: Smith
sn;lang-en: Smith
sn;lang-de: Schmidt
telephoneNumber: 1 555 123-4567

dn: uid=sss,dc=example,dc=com
cn: Steve Smith
cn: Steve S. Smith
sn: Smith
```

```
sn;lang-en: Smith
sn;lang-de: Schmidt
telephoneNumber: 1 555 765-4321
```

The command:

```
ldapsearch -LLL -u -t "(uid=xyz)" jpegPhoto audio
```

will perform a subtree search using the default search base for entries with user id of "xyz". The user friendly form of the entry's DN will be output after the line that contains the DN itself, and the jpegPhoto and audio values will be retrieved and written to temporary files. The output might look like this if one entry with one value for each of the requested attributes is found:

```
dn: uid=xyz,dc=example,dc=com
ufn: xyz, example, com
audio:< file:///tmp/ldapsearch-audio-a19924
jpegPhoto:< file:///tmp/ldapsearch-jpegPhoto-a19924
```

This command:

```
ldapsearch -LLL -s one -b "c=US" "(o=University*)" o description
```

will perform a one-level search at the c=US level for all entries whose organization name (o) begins with **University**. The organization name and description attribute values will be retrieved and printed to standard output, resulting in output similar to this:

```
dn: o=University of Alaska Fairbanks,c=US
o: University of Alaska Fairbanks
description: Naturally Inspiring
description: leaf node only

dn: o=University of Colorado at Boulder,c=US
o: University of Colorado at Boulder
description: No personnel information
description: Institution of education and research

dn: o=University of Colorado at Denver,c=US
o: University of Colorado at Denver
o: UCD
o: CU/Denver
```

o: CU-Denver
description: Institute for Higher Learning and Research

dn: o=University of Florida,c=US
o: University of Florida
o: UFl
description: Warper of young minds

...

DIAGNOSTICS

Exit status is zero if no errors occur. Errors result in a non-zero exit status and a diagnostic message being written to standard error.

SEE ALSO

ldapadd(1), **ldapdelete**(1), **ldapmodify**(1), **ldapmodrdn**(1), **ldap.conf**(5), **ldif**(5), **ldap**(3), **ldap_search_ext**(3), **ldap_sort**(3)

AUTHOR

The OpenLDAP Project <http://www.openldap.org/>

ACKNOWLEDGEMENTS

OpenLDAP Software is developed and maintained by The OpenLDAP Project <http://www.openldap.org/>. **OpenLDAP Software** is derived from the University of Michigan LDAP 3.3 Release.