

**NAME**

ldapcompare - LDAP compare tool

**SYNOPSIS**

```
ldapcompare [-V[V]] [-d debuglevel] [-n] [-v] [-z] [-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]] DN {attr:value | attr::b64value}
```

**DESCRIPTION**

*ldapcompare* is a shell-accessible interface to the **ldap\_compare\_ext**(3) library call.

**ldapcompare** opens a connection to an LDAP server, binds, and performs a compare using specified parameters. The *DN* should be a distinguished name in the directory. *Attr* should be a known attribute. If followed by one colon, the assertion *value* should be provided as a string. If followed by two colons, the base64 encoding of the value is provided. The result code of the compare is provided as the exit code and, unless ran with **-z**, the program prints TRUE, FALSE, or UNDEFINED on standard output.

**OPTIONS****-V[V]**

Print version info. If **-VV** is given, only the version information is printed.

**-d *debuglevel***

Set the LDAP debugging level to *debuglevel*. **ldapcompare** 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 compare. Useful for debugging in conjunction with **-v**.

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

**-z** Run in quiet mode, no output is written. You must check the return status. Useful in shell scripts.

**-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. Note that *complete* means that any leading or trailing whitespaces, including newlines, will be considered part of the password and, unlike other software, they will not be stripped. As a consequence, passwords stored in files by commands like **echo**(1) will not behave as expected, since **echo**(1) by default appends a trailing newline to the echoed string. The recommended portable way to store a cleartext password in a file for use with this option is to use **slappasswd**(8) with *{CLEARTEXT}* as hash and the option **-n**.

**-H** *ldapuri*

Specify URI(s) referring to the ldap server(s); only the protocol/host/port fields are allowed; a list of URI, separated by whitespace or commas is expected.

**-P** {2|3}

Specify the LDAP protocol version to use.

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

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

Specify general extensions with **-e** and compare 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)

Compare extensions:

!dontUseCopy

**-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.

**EXAMPLES**

```
ldapcompare "uid=babs,dc=example,dc=com" sn:Jensen
ldapcompare "uid=babs,dc=example,dc=com" sn::SmVuc2Vu
```

are all equivalent.

**LIMITATIONS**

Requiring the value be passed on the command line is limiting and introduces some security concerns. The command should support a mechanism to specify the location (file name or URL) to read the value from.

**SEE ALSO**

**ldap.conf(5)**, **ldif(5)**, **ldap(3)**, **ldap\_compare\_ext(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.