



Sun Java System Directory Server 5.2 2005Q1 Man Page Reference

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 817-7620-10
Feb 2005

Copyright 2005 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, docs.sun.com, AnswerBook, AnswerBook2, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2005 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées du système Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux États-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, et Solaris sont des marques de fabrique ou des marques déposées, de Sun Microsystems, Inc. aux États-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux États-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



041125@10536



Contents

Preface 5

DS 1 11

account-activate(1)	12
account-inactivate(1)	14
account-status(1)	16
entrycmp(1)	18
fildif(1)	21
insync(1)	23
ldapcompare(1)	26
ldapdelete(1)	32
ldapmodify(1)	38
ldapsearch(1)	46
ldif(1)	57
mmldif(1)	58
monitor(1)	59
ns-accountstatus.pl(1)	61
ns-activate.pl(1)	63
ns-inactivate.pl(1)	65
pwdhash(1)	67
repldisc(1)	69

DS 1m 73

bak2db(1M)	74
bak2db.pl(1M)	75
bak2db-task(1M)	76

db2bak(1M) 77
db2bak.pl(1M) 78
db2bak-task(1M) 80
db2ldif(1M) 82
db2ldif.pl(1M) 84
db2ldif-task(1M) 86
directoryserver(1M) 88
ldif2db(1M) 95
ldif2db.pl(1M) 97
ldif2db-task(1M) 99
ldif2ldap(1M) 101
migrateinstance5(1M) 103
ns-ldapagt(1M) 105
restart(1M) 106
restart-slapd(1M) 107
restoreconfig(1M) 108
saveconfig(1M) 109
schema_push.pl(1M) 110
start(1M) 111
start-slapd(1M) 112
stop(1M) 113
stop-slapd(1M) 114
suffix2instance(1M) 115
sync-cds(1M) 116
vlvindex(1M) 117

Preface

Both novice users and those familiar with the Solaris Operating System can use online man pages to obtain information about their SPARC™ or x86 based system and its features.

Note – In this document, the term “x86” refers to the Intel 32-bit family of microprocessor chips and compatible microprocessor chips made by AMD.

A man page is intended to answer concisely the question “What does it do?” The man pages in general comprise a reference manual. They are not intended to be a tutorial.

Note – Sun Cluster software runs on two platforms, SPARC and x86. The information in this document pertains to both platforms unless otherwise specified in a special chapter, section, note, bulleted item, figure, table, or example.

Overview

The following contains a brief description of each man page section and the information it references:

- Section 1 describes, in alphabetical order, commands available with the operating system.
- Section 1M describes, in alphabetical order, commands that are used chiefly for system maintenance and administration purposes.
- Section 2 describes all of the system calls. Most of these calls have one or more error returns. An error condition is indicated by an otherwise impossible returned value.

- Section 3 describes functions found in various libraries, other than those functions that directly invoke UNIX system primitives, which are described in Section 2.
- Section 4 outlines the formats of various files. The C structure declarations for the file formats are given where applicable.
- Section 5 contains miscellaneous documentation such as character-set tables.
- Section 6 contains available games and demos.
- Section 7 describes various special files that refer to specific hardware peripherals and device drivers. STREAMS software drivers, modules and the STREAMS-generic set of system calls are also described.
- Section 9 provides reference information needed to write device drivers in the kernel environment. It describes two device driver interface specifications: the Device Driver Interface (DDI) and the Driver/Kernel Interface (DKI).
- Section 9E describes the DDI/DKI, DDI-only, and DKI-only entry-point routines a developer can include in a device driver.
- Section 9F describes the kernel functions available for use by device drivers.
- Section 9S describes the data structures used by drivers to share information between the driver and the kernel.

Below is a generic format for man pages. The man pages of each manual section generally follow this order, but include only needed headings. For example, if there are no bugs to report, there is no BUGS section. See the `intro` pages for more information and detail about each section, and `man(1)` for more information about man pages in general.

NAME	This section gives the names of the commands or functions documented, followed by a brief description of what they do.
SYNOPSIS	This section shows the syntax of commands or functions. When a command or file does not exist in the standard path, its full path name is shown. Options and arguments are alphabetized, with single letter arguments first, and options with arguments next, unless a different argument order is required.
	The following special characters are used in this section:
	[] Brackets. The option or argument enclosed in these brackets is optional. If the brackets are omitted, the argument must be specified.

- . . . Ellipses. Several values can be provided for the previous argument, or the previous argument can be specified multiple times, for example, "filename ...".
- | Separator. Only one of the arguments separated by this character can be specified at a time.
- { } Braces. The options and/or arguments enclosed within braces are interdependent, such that everything enclosed must be treated as a unit.

PROTOCOL	This section occurs only in subsection 3R to indicate the protocol description file.
DESCRIPTION	This section defines the functionality and behavior of the service. Thus it describes concisely what the command does. It does not discuss OPTIONS or cite EXAMPLES. Interactive commands, subcommands, requests, macros, and functions are described under USAGE.
IOCTL	This section appears on pages in Section 7 only. Only the device class that supplies appropriate parameters to the ioctl(2) system call is called ioctl and generates its own heading. ioctl calls for a specific device are listed alphabetically (on the man page for that specific device). ioctl calls are used for a particular class of devices all of which have an io ending, such as mtio(7I).
OPTIONS	This section lists the command options with a concise summary of what each option does. The options are listed literally and in the order they appear in the SYNOPSIS section. Possible arguments to options are discussed under the option, and where appropriate, default values are supplied.
OPERANDS	This section lists the command operands and describes how they affect the actions of the command.
OUTPUT	This section describes the output – standard output, standard error, or output files – generated by the command.

RETURN VALUES	<p>If the man page documents functions that return values, this section lists these values and describes the conditions under which they are returned. If a function can return only constant values, such as 0 or -1, these values are listed in tagged paragraphs. Otherwise, a single paragraph describes the return values of each function. Functions declared void do not return values, so they are not discussed in RETURN VALUES.</p>
ERRORS	<p>On failure, most functions place an error code in the global variable <code>errno</code> indicating why they failed. This section lists alphabetically all error codes a function can generate and describes the conditions that cause each error. When more than one condition can cause the same error, each condition is described in a separate paragraph under the error code.</p>
USAGE	<p>This section lists special rules, features, and commands that require in-depth explanations. The subsections listed here are used to explain built-in functionality:</p>
	<ul style="list-style-type: none"> Commands Modifiers Variables Expressions Input Grammar
EXAMPLES	<p>This section provides examples of usage or of how to use a command or function. Wherever possible a complete example including command-line entry and machine response is shown. Whenever an example is given, the prompt is shown as <code>example%</code>, or if the user must be superuser, <code>example#</code>. Examples are followed by explanations, variable substitution rules, or returned values. Most examples illustrate concepts from the SYNOPSIS, DESCRIPTION, OPTIONS, and USAGE sections.</p>
ENVIRONMENT VARIABLES	<p>This section lists any environment variables that the command or function affects, followed by a brief description of the effect.</p>

EXIT STATUS	This section lists the values the command returns to the calling program or shell and the conditions that cause these values to be returned. Usually, zero is returned for successful completion, and values other than zero for various error conditions.
FILES	This section lists all file names referred to by the man page, files of interest, and files created or required by commands. Each is followed by a descriptive summary or explanation.
ATTRIBUTES	This section lists characteristics of commands, utilities, and device drivers by defining the attribute type and its corresponding value. See <code>attributes(5)</code> for more information.
SEE ALSO	This section lists references to other man pages, in-house documentation, and outside publications.
DIAGNOSTICS	This section lists diagnostic messages with a brief explanation of the condition causing the error.
WARNINGS	This section lists warnings about special conditions which could seriously affect your working conditions. This is not a list of diagnostics.
NOTES	This section lists additional information that does not belong anywhere else on the page. It takes the form of an aside to the user, covering points of special interest. Critical information is never covered here.
BUGS	This section describes known bugs and, wherever possible, suggests workarounds.

DS 1

account-activate(1)

NAME	account-activate, ns-activate.pl – activate an entry or a group of entries
SYNOPSIS	directoryserver [{-s -server} server-instance] account-activate [-D <i>rootDN</i>] {-w <i>password</i> -w - -j <i>filename</i> } [-h <i>host</i>] [-p <i>port</i>] -I <i>DN-to-activate</i> <i>ServerRoot</i> / slapd-serverID/ns-activate.pl [-D <i>rootDN</i>] {-w <i>password</i> -w - -j <i>filename</i> } [-h <i>host</i>] [-p <i>port</i>] -I <i>DN-to-activate</i>
DESCRIPTION	The <code>account-activate</code> command activates an entry or group of entries.
OPTIONS	The following options are supported: -? Provides help -D Directory Server user DN with root permissions, such as Directory Manager. -h Host name of Directory Server. The default value is the full host name of the machine on which Directory Server is installed. -I <i>DN-to-activate</i> Entry DN or role DN to activate. -j File from which the bind password is read. Used for simple authentication. If this option is specified the -w option must not be specified. -p Directory Server port. The default value is the Directory Server LDAP port specified at installation time. -w Password associated with the user DN. If you do not specify this option anonymous access is used. If you specify -w -, the utility prompts for the password. If either -w option is specified, the -j option must not be specified. For example, -w diner892.
EXIT STATUS	The following exit values are returned: 0 Successful completion. 1 An error occurred. On error, verbose error messages are output to standard output.
ATTRIBUTES	See <code>attributes(5)</code> for descriptions of the following attributes:

account-activate(1)

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M),ns-activate.pl(1)account-inactivate(1)account-status(1)`

account-inactivate(1)

NAME	account-inactivate, ns-inactivate.pl – inactivate an entry or a group of entries
SYNOPSIS	<pre>directoryserver [{-s -server} server-instance] account-inactivate [-D <i>rootDN</i>] {-w <i>password</i> -w - -j <i>filename</i>} [-h <i>host</i>] [-p <i>port</i>] -I <i>DN-to-inactivate</i> <i>ServerRoot</i>/slapd-serverID/ns-inactivate.pl [-D <i>rootDN</i>] {-w <i>password</i> -w - -j <i>filename</i>} [-h <i>host</i>] [-p <i>port</i>] -I <i>DN-to-inactivate</i></pre>
DESCRIPTION	The <code>account-inactivate</code> command inactivates an entry or group of entries.
OPTIONS	The following options are supported: <ul style="list-style-type: none">-? Provides help-D Directory Server user DN with root permissions, such as Directory Manager.-h Host name of Directory Server. The default value is the full host name of the machine on which Directory Server is installed.-I <i>DN-to-inactivate</i> Entry DN or role DN to inactivate.-j File from which the bind password is read. Used for simple authentication. If this option is specified the <code>-w</code> option must not be specified.-p Directory Server port. The default value is the Directory Server LDAP port specified at installation time.-w Password associated with the user DN. If you do not specify this option anonymous access is used. If you specify <code>-w -</code>, the utility prompts for the password. If either <code>-w</code> option is specified, the <code>-j</code> option must not be specified. For example, <code>-w diner892</code>.
EXIT STATUS	The following exit values are returned: <ul style="list-style-type: none">0 Successful completion.1 An error occurred. On error, verbose error messages are output to standard output.
ATTRIBUTES	See <code>attributes(5)</code> for descriptions of the following attributes:

account-inactivate(1)

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `ns-inactivate.pl(1)`, `account-activate(1)`,
`account-status(1)`

account-status(1)

NAME	account-status, ns-accountstatus.pl – provide status information to establish whether or not an entry or group of entries is inactivated
SYNOPSIS	directoryserver [{-s -server} server-instance] account-status [-D <i>rootDN</i>] {-w <i>password</i> -w - -j <i>filename</i> } [-h <i>host</i>] [-p <i>port</i>] -I <i>DN-to-get-status-of</i> <i>ServerRoot/slaped-serverID/ns-accountstatus.pl</i> [-D <i>rootDN</i>] {-w <i>password</i> -w - -j <i>filename</i> } [-h <i>host</i>] [-p <i>port</i>] -I <i>DN-to-get-status-of</i>
DESCRIPTION	The <code>account-status</code> command provides status information to establish whether an entry or group of entries is inactivated or not.
OPTIONS	The following options are supported: -? Provides help -D Directory Server user DN with root permissions, such as Directory Manager -h Host name of Directory Server. The default value is the full host name of the machine on which Directory Server is installed. -I <i>DN-to-get-status-of</i> Entry DN or role DN to obtain status for. -j File from which the bind password is read. Used for simple authentication. If this option is specified the <code>-w</code> option must not be specified. -p Directory Server port. The default value is the Directory Server LDAP port specified at installation time. -w Password associated with the user DN. If you do not specify this option anonymous access is used. If you specify <code>-w -</code> , the utility prompts for the password. If either <code>-w</code> option is specified, the <code>-j</code> option must not be specified. For example, <code>-w diner892</code> .
EXIT STATUS	The following exit values are returned: 0 Successful completion. 1 An error occurred. On error, verbose error messages are output to standard output.
ATTRIBUTES	See <code>attributes(5)</code> for descriptions of the following attributes:

account-status(1)

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO directoryserver(1M), ns-accountstatus.pl(1), account-activate(1),
account-inactivate(1)

entrycmp(1)

NAME	entrycmp – compare the same entry on two or more different servers
SYNOPSIS	<i>ServerRoot</i> / shared/bin/entrycmp [-D <i>bindDN</i>] [-w <i>password</i>] [-n] [-p <i>port</i>] [-j <i>file</i>] [-T <i>timeout</i>] [-J <i>file</i>] [-w <i>keypassword</i>] [-K <i>keydbpath</i>] [-N <i>certname</i>] [-P <i>certdbpath</i>] [-e <i>SSL port</i>] <i>ServerSpec</i> <i>entryDN</i>
DESCRIPTION	The entrycmp command compares the same entry on two or more different servers. An entry is retrieved from the master and the entry's nsuniqueid is used to retrieve the same entry from a specified consumer. All the attributes and values of the two entries are compared. If they are identical, the entries are considered to be the same.
OPTIONS	The following options are supported: -D The distinguished name with which to bind to the server. This parameter is optional if the server is configured to support anonymous access. If a DN is specified in the <i>ServerSpec</i> , this overrides the -D option -j If specifying the default password at the command-line poses a security risk, the password can be stored in a file. The -j option specifies this file. -n Specifies that entrycmp should not run in interactive mode. Running in interactive mode allows you to re-enter the bindDN, password, host and port, if a bind error occurs. -p The TCP port used by the Directory Server. The default port is 389. If a port is specified in the <i>ServerSpec</i> , this overrides the -p option. -T Specifies the number of seconds after which entrycmp will time out if the server connection goes down. -w The password associated with the distinguished name specified by the -D option. If a password is specified in the <i>ServerSpec</i> , this overrides the -w option. <i>entryDN</i> The DN of the entry that you wish to compare. <i>ServerSpec</i> The server specification. This can be: -s -S <i>HostSpec</i> [-c -C <i>HostSpec</i> -c -C <i>HostSpec</i>]... or -c -C [-s -S -s -S]... where -s is the supplier replica and -c is the consumer replica. Lower case specifies non-SSL options and upper case specifies SSL options. <i>Host Spec</i> The host specification, which takes the form [bindDN: [password]]@] <i>host</i> [:port]

Example: **"cn=directory manager":mypword@myserver:5201**. If you are using SSL, use `-s` and `-C` in the server specification. In this case, *HostSpec* specifies the certificate name and key password, rather than the bindDN and password. Specifying more than one `-s` and more than one `-c` will generate an error. If no `-c` option is specified, the `-s` *HostSpec* may refer to any server, either a consumer or a supplier.

SSL OPTIONS

You can use the following options to specify that `entrycmp` uses LDAPS when communicating with the Directory Server. You can also use these options if you want to use certificate-based authentication. These options are valid only when LDAPS has been turned on and configured. For more information on certificate-based authentication and how to create a certificate database for use with LDAP clients, see "Managing SSL" in the *Directory Server Administration Guide*.

- `-e`
Default SSL port
- `-J`
This option has the same function as the `-j` option, for the key password.
- `-K`
Specifies the name of the certificate key used for certificate-based client authentication. For example, `-K Server-Key`.
- `-N`
Specifies the certificate name to use for certificate-based client authentication. For example, `-N Server-Cert`. If this option is specified, the `-W` option is required.
- `-P`
Specifies the location of the certificate database.
- `-W`
Specifies the password for the certificate database identified by the `-P` option. For example, `-W serverpassword`.

EXAMPLES

EXAMPLE 1 Specifying an entry DN

```
# entrycmp -D "cn=directory manager" -w mypword \\  
-s myserver:1389 "uid=csmith,ou=people,dc=example,dc=com"
```

EXIT STATUS

The following exit values are returned:

- 0 Successful completion, that is a match was found.
- 1 An error occurred, and no match was found.

ATTRIBUTES

See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu

entrycmp(1)

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Stability Level	Committed Private

SEE ALSO `insync(1)`, `repldisc(1)`

NOTES The node on which you are running the `entrycmp`, `insync`, and `repldisc` tools must be able to reach all the specified hosts. If these hosts are unavailable due to a firewall, VPN, or other network setup reasons, you will encounter difficulties using these tools. For the same reason ensure that all servers are up and running before using these tools.

When identifying hosts, you must use either symbolic names or IP addresses for all hosts since the replication monitoring commands do not address resolution between symbolic names and IP addresses. Using a combination of the two can cause problems, especially on multi-homed hosts.

When SSL is enabled, the directory server on which you are running the tools must have a copy of all the certificates used by the other servers in the topology.

The replication monitoring tools rely on access to `cn=config` to obtain the replication status. This should be taken into account particularly when replication is configured over SSL.

NAME	fildif – creates a filtered version of an LDIF input file
SYNOPSIS	<code>ServerRoot/shared/bin/fildif -i input_file [-f] [-o output_file] -c config_file -b pointer_entry [-a pointer_attr]</code>
DESCRIPTION	<p>The <code>fildif</code> command creates a filtered version of an LDIF input file. <code>fildif</code> takes a configuration file as an input parameter. This configuration file must conform to the configuration rules of the filtering service included as part of Directory Server, and must contain the specific set and element entries that define these rules. The configuration rules can be defined by using the console or at the command-line. For more information on the Filtering Service and how it is configured, see the <i>Directory Server Administration Guide</i>.</p> <p><code>fildif</code> does not require the directory server to be running.</p> <p>A filtering service configuration is accessed through a pointer entry. The pointer entry is provided to <code>fildif</code> with the <code>-b</code> parameter. A pointer attribute within this entry (provided by the <code>-a</code> parameter) determines the RDN of the filtering service configuration entry to be used for the filtering.</p>
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none"> <code>-a</code> The attribute that will be used inside the pointer entry to point to a particular filtering service configuration definition. If this parameter is not present, the default <code>ds5partialReplConfiguration</code> is used. <code>-b</code> The pointer entry. This parameter is mandatory and specifies the DN of the entry that will be used as the filtering service configuration entry point. The entry specified by this DN must exist in the configuration file, specified by the <code>-c</code> parameter. <code>-c</code> The configuration file in which the filtering configuration is stored. <code>-f</code> Forces <code>fildif</code> to overwrite the contents of the specified output file, if it exists. <code>-i</code> The input LDIF file whose contents will be filtered. <code>-o</code> The output LDIF file in which the filtered results will be stored. If no output file is specified, the default output file is <code>./output.ldif</code>.
EXAMPLES	<p>EXAMPLE 1 Specifying the pointer attribute and overwriting an existing output file</p> <pre># fildif -i data.ldif -o filt_data.ldif -f -c config_fildif.ldif -b "cn=conf_20,cn=sets,cn=filtering service,cn=features,cn=config" -a ds5PartialReplConfiguration</pre>
EXIT STATUS	The following exit values are returned:

fldif(1)

0 Successful completion.

1 An error occurred.

On error, verbose error messages are output to standard output.

ATTRIBUTES

See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO

`insync(1)`, `entrycmp(1)`

NAME	insync – indicate the synchronization state between a supplier replica and one or more consumer replicas
SYNOPSIS	<i>ServerRoot</i> / shared/bin/insync [-D <i>bindDN</i>] [-w <i>password</i>] [-t] [-n] [-d] [-j <i>file</i>] [-p <i>port</i>] [-T <i>timeout</i>] [-J <i>file</i>] [-W <i>keypassword</i>] [-K <i>keydbpath</i>] [-N <i>certname</i>] [-P <i>certdbpath</i>] [-e <i>SSL port</i>] [-b <i>ReplicaRoot</i>] <i>ServerSpec</i> [<i>interval</i>]
DESCRIPTION	The insync command indicates the synchronization state between a supplier replica and one or more consumer replicas. insync compares the RUVs of replicas and displays the time difference or delay (in seconds) between the servers.
OPTIONS	The following options are supported: <ul style="list-style-type: none"> -b The suffix (replica root) that has been specified for replication. If -b is not specified, the delay for all suffixes is displayed. -d Displays the date of the last change recorded on the master. Using the -d option twice (-d -d) displays the time difference (in days, minutes and seconds) between the time of the last change and the current time. -D The distinguished name with which to bind to the server. This parameter is optional if the server is configured to support anonymous access. If a DN is specified in the <i>ServerSpec</i>, this overrides the -D option -j If specifying the default password at the command-line poses a security risk, the password can be stored in a file. The -j option specifies this file. -n Specifies that insync should not run in interactive mode. Running in interactive mode allows you to re-enter the bindDN, password, host and port, if a bind error occurs. -p The TCP port used by the Directory Server. The default port is 389. If a port is specified in the <i>ServerSpec</i>, this overrides the -p option. -t Displays the mode of transport (SSL or CLEAR) -T Specifies the number of seconds after which insync will time out if the server connection goes down. -w The password associated with the distinguished name specified by the -D option. If a password is specified in the <i>ServerSpec</i>, this overrides the -w option.

insync(1)

ServerSpec

The server specification. This can be: *-s/-S HostSpec [-c/-C HostSpec -c/-C HostSpec]...* or *-c/-C [-s/-S -s/-S]...* where *-s* is the supplier replica and *-c* is the consumer replica. Lower case specifies non-SSL options and upper case specifies SSL options.

Host Spec

The host specification, which takes the form
[bindDN[: [password]]@]host[:port]

Example: **"cn=directory manager":mypword@myserver:5201**. If you are using SSL, use *-s* and *-C* in the server specification. In this case, *HostSpec* specifies the certificate name and key password, rather than the bindDN and password. Specifying more than one *-s* and more than one *-c* will generate an error. If no *-c* option is specified, the *-s HostSpec* may refer to any server, either a consumer or a supplier.

interval

The amount of time (in seconds) after which the synchronization query will start again (in an infinite loop). If no interval is specified, the synchronization query will run only once.

SSL OPTIONS

You can use the following options to specify that *insync* uses LDAPS when communicating with the Directory Server. You can also use these options if you want to use certificate-based authentication. These options are valid only when LDAPS has been turned on and configured. For more information on certificate-based authentication and how to create a certificate database for use with LDAP clients, see the *Directory Server Administration Guide*.

-e

Default SSL port

-J

This option has the same function as the *-j* option, for the key password.

-K

Specifies the name of the certificate key used for certificate-based client authentication. For example, *-K Server-Key*.

-N

Specifies the certificate name to use for certificate-based client authentication. For example, *-N Server-Cert*. If this option is specified, the *-w* option is required.

-P

Specifies the location of the certificate database.

-W

Specifies the password for the certificate database identified by the *-P* option. For example, *-W serverpassword*.

EXAMPLES

EXAMPLE 1 Specifying a single server and a repetition interval of 30 seconds

Note that the delay changes to 5, indicating that the consumer is 5 seconds behind the supplier.

insync(1)

EXAMPLE 1 Specifying a single server and a repetition interval of 30 seconds (Continued)

```
# insync -D "cn=directory manager" -w mypwd \\
-s portugal:1389 30
ReplicaDn      Consumer      Supplier      Delay
dc=example,dc=com france.example.com:2389 portugal:1389 0
dc=example,dc=com france.example.com:2389 portugal:1389 5
dc=example,dc=com france.example.com:2389 portugal:1389 0
```

EXAMPLE 2 Requesting the date of the last change and restricting the output data to the DN o=rtest

```
# insync -D "cn=directory manager" -w mypwd \\
-s portugal:1389 -b o=rtest -d
```

EXIT STATUS The following exit values are returned:

- 0 Successful completion.
- 1 An error occurred.

ATTRIBUTES See attributes(5) for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO entrycmp(1), repldisc(1)

NOTES The node on which you are running the entrycmp, insync, and repldisc tools must be able to reach all the specified hosts. If these hosts are unavailable due to a firewall, VPN, or other network setup reasons, you will encounter difficulties using these tools. For the same reason ensure that all servers are up and running before using these tools.

When identifying hosts, you must use either symbolic names or IP addresses for all hosts since the replication monitoring commands do not address resolution between symbolic names and IP addresses. Using a combination of the two can cause problems, especially on multi-homed hosts.

When SSL is enabled, the directory server on which you are running the tools must have a copy of all the certificates used by the other servers in the topology.

If a delay of -1 is returned, insync was unable to obtain any replication information. This may indicate that a Total Update has just been run, or that no changes have been sent to the supplier server.

The replication monitoring tools rely on access to cn=config to obtain the replication status. This should be taken into account particularly when replication is configured over SSL.

ldapcompare(1)

NAME	ldapcompare – compare a value with an LDAP entry attribute value
SYNOPSIS	<pre>\$ cd ServerRoot/shared/bin ./ldapcompare [options] 'attrtype:attrvalue' ["dn"...] ./ldapcompare [options] 'attrtype:base64value' ["dn"...] ./ldapcompare [options] 'attrtype:<fileurl' ["dn"...]</pre>
DESCRIPTION	<p>The <code>ldapcompare</code> command asserts that a value you specify is the same as an entry attribute value stored by the directory server.</p> <p>Specify the attribute type, followed by the attribute value, either as a string, a base64–encoded value, or a URL to a file containing the attribute value (such as a photo or certificate). You typically enclose the attribute type/value pair in single quotes (' ') for the shell.</p> <p>Also specify one or more entry DN's, separated by space, and typically enclosed in double quotes (" ") for the shell. The <code>ldapcompare</code> command then compares the specified attribute value to that of attributes on each of the entries indicated by the DN's you provide.</p>
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none">-0 Ignore LDAP library version mismatches. When this option is omitted, the default behavior is to assert that the revision number of the LDAP API be greater than or equal to that used to compile the tool. Also, if the library and the tool have the same vendor name, the tool will assert that the vendor version number of the API be greater than or equal to that used to compile the tool. Revision and version numbers are based on the contents of the <code>LDAPAPIINFO</code> structure defined in <code><ldap.h></code> or header files included by <code><ldap.h></code>.-3 Check host names in SSL certificates.-D <i>bindDN</i> Use the specified bind DN to authenticate to the directory server. If the bind DN and its password are omitted, the <code>ldapcompare</code> command binds anonymously. The bind DN determines what entries and attributes appear in the comparison results, according to the DN's search permissions.-E Request that the directories expose (report) bind identities.-H Display usage information.-I <i>pin</i> Use the specified SSL card password file (<i>pin</i>).

- J *controloid*[:*criticality*[:*value* | ::*base64value* | :<*fileurl*]]
Use the specified control OID.

The *criticality*, a boolean, is false by default.
- K *pathname*
Use the certificate private key database located in the specified directory.

You may omit the -K option if the key database location is provided as an argument to the -P option.
- M
Manage referrals, comparing the entry containing the referral instead of the entry obtained by following the referral.
- N *certificate*
Use the specified *certificate* for certificate-based client authentication, for example: -N "Client-Cert", where Client-Cert is the subject name of the user's certificate.
- O *limit*
Follow at maximum *limit* referral hops. Default is 5.
- P *filename*
Use the certificate database located in *filename*, the full path to the certificate database file.
- Q [*token*][:*certificate-name*]
Use PKCS 11.
- R
Do not follow referrals automatically.
- V *n*
Use LDAP protocol version *n*, where *n* is 2 or 3. Default is 3.
- W *password*
Specify the password for the client's key database specified using the -K or -P option.

The -w option is required for certificate-based client authentication.
- Y *proxydn*
Use the rights of the entry having the specified DN for performing LDAP operations. When using this option, you must also specify how to bind before you assume the rights of the proxy. Thus, when using simple authentication, you would also use the -D and -w options with this option.

Before proxy authentication can work in Directory Server, you must set up the appropriate access control instructions.
- Z
Use SSL to provide certificate-based client authentication.

ldapcompare(1)

The `-Z` option requires the `-N` and `-W` options and any other SSL options needed to identify the certificate and the key database.

`-c`

Run in continuous mode, not stopping on errors.

In continuous mode, errors are reported but the `ldapcompare` command continues performing comparisons. When not running in continuous mode, the `ldapcompare` command quits after the first error.

`-d level`

Set LDAP debug level to the specified value.

The following debug levels are supported:

- 1 Display verbose debugging messages; `LDAP_DEBUG_TRACE`.
- 2 Display messages about the content of network packets;
`LDAP_DEBUG_PACKETS`.
- 320 Display messages about LDIF parsing; `LDAP_DEBUG_PARSE`.
- 16384 Display informational messages; `LDAP_DEBUG_ANY`.

Use the sum of the levels to specify more than one debug level.

`-f filename`

Read DN's from the specified file.

The file format is one DN per line without quotes around DN's. The `ldapcompare` command reads each line as one literal DN, performing the comparison for each entry whose DN is specified.

`-h host`

Contact the LDAP server on the specified host, which may be a host name or an IP address. Enclose IPv6 addresses in brackets (`[]`) as described in RFC 2732.

For example, when mapping the IPv4 address `192.168.0.99` to IPv6, pass the `-h` option with its argument as `-h [::ffff:192.168.0.99]`. Notice the brackets.

The default is `localhost`.

`-i charset`

Use the specified character set as opposed to the character set specified as the value of the `LANG` environment variable.

Use this option for example to perform the conversion from the specified character set to UTF8, thus overriding the `LANG` setting.

`-j filename`

Read the bind password for simple authentication from the specified file.

`-k pathname`

Use the conversion routines located in the specified directory.

The default is to use the current directory. Use the `-k` option to specify a sorting language that is not supported by the directory server.

`-m pathname`

Use the security module database located in the specified directory.

Use the `-m` option if the security module database is in a different directory from the certificate database itself.

`-n`

Show what would be done, but do not actually do it.

`-o attrname=attrvalue`

Use the specified attribute values when performing SASL authentication.

The following *attrname* arguments are supported:

`authid` Use the specified authentication identity.

`authzid` Use the specified authorization identity.

`mech` Request the specified SASL mechanism for the bind.

`realm` Use the specified realm to complete the bind.

`secProp` Use the specified security level.

`-p port`

Contact the LDAP server on the specified port.

The default is 389 (636 if SSL is used).

`-q`

Run in quiet mode, displaying no information about results of comparisons, but only about LDAP errors.

`-v`

Run in verbose mode, displaying diagnostics on standard output.

`-w -`

Prompt for the bind password for simple authentication.

`-w password`

Use the specified bind password for simple authentication.

EXAMPLES

Examples in this section use the following conventions:

- The directory server is located on a system named *host*.
- The directory server has been configured to support anonymous access for search and read. Therefore, you do not have to specify bind information.
- The directory server listens on port number 389, the default.

EXAMPLE 1 Comparing String Values

The following command compares a specified string with an attribute value:

ldapcompare(1)

EXAMPLE 1 Comparing String Values (Continued)

```
$ ./ldapcompare -h host 'givenname:Barbara' "uid=bjensen,ou=People,dc=example,dc=com"
comparing type: "givenname" value: "Barbara" in entry "uid=bjensen,ou=People,dc=example,dc=com"
compare TRUE
```

EXAMPLE 2 Comparing Base 64 Encoded Values

The following command compares a base64–encoded value with an attribute value:

```
$ ./ldapcompare -h host 'cn::QmFicyBKZW5zZW4='
"uid=bjensen,ou=People,dc=example,dc=com"
comparing type: "cn" value: "Babs Jensen" in entry "uid=bjensen,ou=People,dc=example,dc=com"
compare TRUE
```

EXAMPLE 3 Comparing Binary Values in Files

The following command compares an image with an attribute value:

```
$ ./ldapcompare -h host 'jpegphoto:<file:///home/bjensen/bjensen.jpg'
"uid=bjensen,ou=People,dc=example,dc=com"
comparing type: "jpegphoto" value: "NOT ASCII (3674 bytes)" in entry "uid=bjensen,ou=People,dc=example,dc=com"
compare TRUE
```

EXIT STATUS

The exit status returned either corresponds to 5 (LDAP_COMPARE_FALSE) or 6 (LDAP_COMPARE_TRUE), or reflects the return values of the underlying functions used, which may depend on return values sent by the server. Common exit status codes follow:

- 1 Server encountered errors while processing the request;
LDAP_OPERATIONS_ERROR; 0x01.
- 2 Server encountered errors, such as a BER-decoding error, while processing the request; LDAP_PROTOCOL_ERROR; 0x02.
- 3 Search exceeded the time limit for operations on the server;
LDAP_TIMELIMIT_EXCEEDED; 0x03.
- 5 Operation was successful but the values did not match;
LDAP_COMPARE_FALSE; 0x05.
- 6 Operation was successful and the values match; LDAP_COMPARE_TRUE;
0x06.
- 10 DN of the entry to compare belongs to an entry handled by neither server, and the referral URL identifies another server that handles the entry;
LDAP_REFERRAL; 0x0a.
- 32 DN of the entry to compare belongs to an entry handled by neither server, and no referral URL is available for the entry; LDAP_NO_SUCH_OBJECT;
0x20.
- 34 DN of the entry to compare is not a valid DN;
LDAP_INVALID_DN_SYNTAX; 0x22.

ldapcompare(1)

- 50 Bind DN user does not have permission to read the entry from the directory; LDAP_INSUFFICIENT_ACCESS; 0x32.
- 81 One of the directories did not respond to the request, or the connection was lost; LDAP_SERVER_DOWN; 0x51.
- 82 An error occurred while receiving results; LDAP_LOCAL_ERROR; 0x52.
- 83 The request could not be BER-encoded; LDAP_ENCODING_ERROR; 0x53.
- 84 A result could not be decoded; LDAP_DECODING_ERROR; 0x54.
- 89 An option or argument is not valid; LDAP_PARAM_ERROR; 0x59.
- 90 Needed memory could not be allocated; LDAP_NO_MEMORY; 0x5a.
- 91 A specified host name or port is not valid; LDAP_CONNECT_ERROR; 0x5b.
- 92 At least one server supports only LDAPv2, and the -v 2 option was not used, or the -v 2 option was used, but the server no longer supports LDAP v2; LDAP_NOT_SUPPORTED; 0x5c.

ATTRIBUTES See attributes(5) for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWldk
Stability Level	Evolving

SEE ALSO ldapdelete(1), ldapmodify(1), ldapsearch(1)

ldapdelete(1)

NAME	ldapdelete – delete LDAP entries
SYNOPSIS	<pre>\$ cd ServerRoot/shared/bin ./ldapdelete [options] ["dn"...] ./ldapdelete [options] < filename</pre>
DESCRIPTION	<p>The <code>ldapdelete</code> command requests deletion of entries stored by a directory server. You must bind as a user having access to delete the entries specified.</p> <p>Specify one or more entry DN's, separated by space, and typically enclosed in double quotes (" ") for the shell. Alternatively, include DN's in a file, one per line without quotes around DN's. The <code>ldapdelete</code> command reads each line as one literal DN.</p> <p>When deleting a subtree, you must delete child entries before you delete their parent entries.</p>
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none">-0 Ignore LDAP library version mismatches. When this option is omitted, the default behavior is to assert that the revision number of the LDAP API be greater than or equal to that used to compile the tool. Also, if the library and the tool have the same vendor name, the tool will assert that the vendor version number of the API be greater than or equal to that used to compile the tool. Revision and version numbers are based on the contents of the <code>LDAPAPIInfo</code> structure defined in <code><ldap.h></code> or header files included by <code><ldap.h></code>.-3 Check host names in SSL certificates.-D <i>bindDN</i> Use the specified bind DN to authenticate to the directory server. If the bind DN and its password are omitted, the <code>ldapdelete</code> command binds anonymously. The bind DN determines what entries and attributes appear in the comparison results, according to the user's search permissions.-E Request that the directories expose (report) bind identities.-H Display usage information.-I <i>pin</i> Use the specified SSL card password file (<i>pin</i>).-J <i>controloid[:criticality[:value ::base64value :<fileurl>]]</i> Use the specified control OID. The <i>criticality</i>, a boolean, is false by default.

- K *pathname*
Use the certificate private key database located in the specified directory.

You may omit the -K option if the key database location is provided as an argument to the -P option.
- M
Manage referrals, deleting the entry containing the referral instead of the entry obtained by following the referral.
- N *certificate*
Use the specified *certificate* for certificate-based client authentication, for example:
-N "Client-Cert", where Client-Cert is the subject name of the user's certificate.
- O *limit*
Follow at maximum *limit* referral hops. Default is 5.
- P *filename*
Use the certificate database located in *filename*, the full path to the certificate database file.
- Q [*token*][:*certificate-name*]
Use PKCS 11.
- R
Do not follow referrals automatically.
- V *n*
Use LDAP protocol version *n*, where *n* is 2 or 3. Default is 3.
- W *password*
Specify the password for the client's key database specified using the -K or -P option.

The -w option is required for certificate-based client authentication.
- Y *proxydn*
Use the rights of the entry having the specified DN for performing LDAP operations. When using this option, you must also specify how to bind before you assume the rights of the proxy. Thus, when using simple authentication, you would also use the -D and -w options with this option.

Before proxy authentication can work in Directory Server, you must set up the appropriate access control instructions.
- Z
Use SSL to provide certificate-based client authentication.

The -Z option requires the -N and -W options and any other SSL options needed to identify the certificate and the key database.
- c
Run in continuous mode, not stopping on errors.

ldapdelete(1)

In continuous mode, errors are reported but the `ldapdelete` command continues performing comparisons. When not running in continuous mode, the `ldapdelete` command quits after the first error.

`-d level`

Set LDAP debug level to the specified value.

The following debug levels are supported:

- 1 Display verbose debugging messages; `LDAP_DEBUG_TRACE`.
- 2 Display messages about the content of network packets;
`LDAP_DEBUG_PACKETS`.
- 320 Display messages about LDIF parsing; `LDAP_DEBUG_PARSE`.
- 16384 Display informational messages; `LDAP_DEBUG_ANY`.

Use the sum of the levels to specify more than one debug level.

`-f filename`

Read DN's from the specified file.

The file format is one DN per line without quotes around DN's. The `ldapdelete` command reads each line as one literal DN.

This option has no effect when you also specify DN's on standard input.

`-h host`

Contact the LDAP server on the specified host, which may be a host name or an IP address. Enclose IPv6 addresses in brackets ([]) as described in RFC 2732.

For example, when mapping the IPv4 address `192.168.0.99` to IPv6, pass the `-h` option with its argument as `-h [::ffff:192.168.0.99]`. Notice the brackets.

The default is `localhost`.

`-i charset`

Use the specified character set as opposed to the character set specified as the value of the `LANG` environment variable.

Use this option for example to perform the conversion from the specified character set to UTF8, thus overriding the `LANG` setting.

`-j filename`

Read the bind password for simple authentication from the specified file.

`-k pathname`

Use the conversion routines located in the specified directory.

The default is to use the current directory. Use the `-k` option to specify a sorting language that is not supported by the directory server.

`-m pathname`

Use the security module database located in the specified directory.

Use the `-m` option if the security module database is in a different directory from the certificate database itself.

- `-n`
Show what would be done, but do not actually do it.
- `-o attrname=attrvalue`
Use the specified attribute values when performing SASL authentication.

The following *attrname* arguments are supported:

authid	Use the specified authentication identity.
authzid	Use the specified authorization identity.
mech	Request the specified SASL mechanism for the bind.
realm	Use the specified realm to complete the bind.
secProp	Use the specified security level.
- `-p port`
Contact the LDAP server on the specified port.

The default is 389 (636 if SSL is used).
- `-v`
Run in verbose mode, displaying diagnostics on standard output.
- `-w -`
Prompt for the bind password for simple authentication.
- `-w password`
Use the specified bind password for simple authentication.

EXAMPLES

Examples in this section use the following conventions:

- The bind DN given corresponds to a user with permission to delete entries.
- The directory server is located on a system named *host*.
- The directory server listens on port number 389, the default for non-SSL traffic.
- The directory server listens on port number 636, the default for SSL traffic. SSL is enabled.

EXAMPLE 1 Deleting an Entry

The following command deletes a single entry from the directory:

```
$ ./ldapdelete -h host -D "uid=bjensen,ou=people,dc=example,dc=com" -w -
"uid=scarter,ou=People,dc=example,dc=com"
Enter bind password:
$
```

EXAMPLE 2 Deleting an Entry Interactively

The following commands demonstrate deleting an entry whose DN is specified on standard input:

ldapdelete(1)

EXAMPLE 2 Deleting an Entry Interactively (Continued)

```
$ ./ ldapdelete -h host -c -v -D "uid=bjensen,ou=People,dc=example,dc=com" -w -
Enter bind password:
ldapdelete: started Fri Jul  2 08:31:14 2004

ldap_init( host, 389 )

uid=kvaughan, ou=People, dc=example,dc=com
deleting entry uid=kvaughan, ou=People, dc=example,dc=com
entry removed
^D
$
```

EXAMPLE 3 Deleting Multiple Entries Specified in a File

The following commands demonstrate reading DNs of entries to delete from a file. Notice that the `-c` option is used to continue if an error occurs.

```
$ cat DNfile
uid=scarter, ou=People, dc=example,dc=com
uid=kvaughan, ou=People, dc=example,dc=com
$ ./ldapdelete -h host -c -f DNfile -D "uid=bjensen,ou=People,dc=example,dc=com" -w -
Enter bind password:
$
```

EXAMPLE 4 Using Server Authentication

The following command uses server authentication during the bind, where the server only accepts binds by clients with trusted certificates. Notice only the `-P` option is used without other SSL-related options.

```
$ ./ldapdelete -h host -p 636 -c -f DNfile -P /home/bjensen/security
-D "uid=bjensen,ou=People,dc=example,dc=com" -w -
Enter bind password:
```

EXAMPLE 5 Using Client Authentication

The following command uses client authentication during the bind, where the server only accepts binds by clients with trusted certificates, and the client must sign the certificate with a password-protected private key. Notice the options used in this example.

```
$ ./ldapdelete -h host -p 636 -c -f DNfile -Z -P /home/bjensen/security
-N "bjscert" -K /home/bjensen/security -W keypassword
```

EXIT STATUS

The exit status returned reflects the return values of the underlying functions used, which may depend on return values sent by the server. Common exit status codes follow:

0	Successful completion; LDAP_SUCCESS; 0x00.
1	Server encountered errors while processing the request; LDAP_OPERATIONS_ERROR; 0x01.

ldapdelete(1)

- 2 Server encountered errors, such as a BER-decoding error, while processing the request; LDAP_PROTOCOL_ERROR; 0x02.
- 10 DN of the entry to delete belongs to an entry handled by neither server, and the referral URL identifies another server that handles the entry; LDAP_REFERRAL; 0x0a.
- 32 DN of the entry to delete belongs to an entry handled by neither server, and no referral URL is available for the entry; LDAP_NO_SUCH_OBJECT; 0x20.
- 34 DN of the entry to delete is not a valid DN; LDAP_INVALID_DN_SYNTAX; 0x22.
- 50 Bind DN user does not have permission to read the entry from the directory; LDAP_INSUFFICIENT_ACCESS; 0x32.
- 53 Directory is read-only; LDAP_UNWILLING_TO_PERFORM; 0x35.
- 66 Entry specified has child-entries that must be deleted first; LDAP_NOT_ALLOWED_ON_NONLEAF; 0x42.
- 81 One of the directories did not respond to the request, or the connection was lost; LDAP_SERVER_DOWN; 0x51.
- 82 An error occurred while receiving results; LDAP_LOCAL_ERROR; 0x52.
- 83 The request could not be BER-encoded; LDAP_ENCODING_ERROR; 0x53.
- 84 A result could not be decoded; LDAP_DECODING_ERROR; 0x54.
- 89 An option or argument is not valid; LDAP_PARAM_ERROR; 0x59.
- 90 Needed memory could not be allocated; LDAP_NO_MEMORY; 0x5a.
- 91 A specified host name or port is not valid; LDAP_CONNECT_ERROR; 0x5b.
- 92 At least one server supports only LDAPv2, and the -v 2 option was not used, or the -V 2 option was used, but the server no longer supports LDAP v2; LDAP_NOT_SUPPORTED; 0x5c.

ATTRIBUTES See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWldk
Stability Level	Evolving

SEE ALSO `ldapcompare(1)`, `ldapmodify(1)`, `ldapsearch(1)`

ldapmodify(1)

NAME	ldapmodify – add, modify, rename, move, or delete LDAP entries
SYNOPSIS	<pre>\$ cd ServerRoot/shared/bin ./ldapmodify [options]</pre>
DESCRIPTION	<p>The <code>ldapmodify</code> command requests the addition, modification, rename, move, or deletion of entries stored by a directory server.</p> <p>You must bind as a user having access to perform the requested operation.</p> <p>The directory server may check all modifications against its schema, and reject updates that cause entries not to conform to the schema.</p> <p>You must specify additions and modifications in the proper order, because the directory server performs the updates in the order you request them. For example, to add entries to a subtree that does not yet exist, you must first update the base entry at the root of the subtree before adding entries under the base entry. When a requested operation fails, the <code>ldapmodify</code> command stops processing further input unless you use the <code>-c</code> option. The <code>ldapmodify</code> command does not save rejected entries unless you use the <code>-e</code> option.</p>
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none">-0 Ignore LDAP library version mismatches. When this option is omitted, the default behavior is to assert that the revision number of the LDAP API be greater than or equal to that used to compile the tool. Also, if the library and the tool have the same vendor name, the tool will assert that the vendor version number of the API be greater than or equal to that used to compile the tool. Revision and version numbers are based on the contents of the <code>LDAPAPIInfo</code> structure defined in <code><ldap.h></code> or header files included by <code><ldap.h></code>.-3 Display non-ASCII values when the <code>-v</code> option is used.-A Check host names in SSL certificates.-B <i>baseDN</i> Bulk import entries into the suffix under the specified DN. Bulk import using the <code>ldapmodify</code> command does not erase entries that already exist.-D <i>bindDN</i> Use the specified bind DN to authenticate to the directory server. If the bind DN and its password are omitted, the <code>ldapmodify</code> command binds anonymously. The bind DN determines what entries and attributes appear in the comparison results, according to the DN's search permissions.

- E
Request that the directories expose (report) bind identities.
- F
Force application of all modifications, even if some lines are duplicates.
- H
Display usage information.
- I *pin*
Use the specified SSL card password file (*pin*).
- J *controloid[:criticality[:value | ::base64value | :<fileurl]]*
Use the specified control OID.

The *criticality*, a boolean, is false by default.
- K *pathname*
Use the certificate private key database located in the specified directory.

You may omit the -K option if the key database location is provided as an argument to the -P option.
- M
Manage referrals, modifying the entry containing the referral instead of the entry obtained by following the referral.
- N *certificate*
Use the specified *certificate* for certificate-based client authentication, for example:
-N "Client-Cert", where Client-Cert is the subject name of the user's certificate.
- O *limit*
Follow at maximum *limit* referral hops. Default is 5.
- P *filename*
Use the certificate database located in *filename*, the full path to the certificate database file.
- Q [*token*][:*certificate-name*]
Use PKCS 11.
- R
Do not follow referrals automatically.
- V *n*
Use LDAP protocol version *n*, where *n* is 2 or 3. Default is 3.
- W *password*
Specify the password for the client's key database specified using the -K or -P option.

The -W option is required for certificate-based client authentication.

ldapmodify(1)

-Y *proxydn*

Use the rights of the entry having the specified DN for performing LDAP operations. When using this option, you must also specify how to bind before you assume the rights of the proxy. Thus, when using simple authentication, you would also use the -D and -w options with this option.

Before proxy authentication can work in Directory Server, you must set up the appropriate access control instructions.

-Z

Use SSL to provide certificate-based client authentication.

The -Z option requires the -N and -W options and any other SSL options needed to identify the certificate and the key database.

-a

Add LDAP entries, rather than modifying existing entries.

-b

Handle binary files.

Note – This option is deprecated. Use standard LDIF notation as described in RFC 2849 instead.

When you use the -b option, the `ldapmodify` command scans every attribute value to determine whether it specifies a valid file reference, such as `/home/bjensen/bjensen.jpg`. If so, the `ldapmodify` command uses the content of the specified file as the attribute value.

-c

Run in continuous mode, not stopping on errors.

In continuous mode, errors are reported but the `ldapmodify` command continues performing comparisons. When not running in continuous mode, the `ldapmodify` command quits after the first error.

-d *level*

Set LDAP debug level to the specified value.

The following debug levels are supported:

- | | |
|-------|--|
| 1 | Display verbose debugging messages; LDAP_DEBUG_TRACE. |
| 2 | Display messages about the content of network packets; LDAP_DEBUG_PACKETS. |
| 320 | Display messages about LDIF parsing; LDAP_DEBUG_PARSE. |
| 16384 | Display informational messages; LDAP_DEBUG_ANY. |

Use the sum of the levels to specify more than one debug level.

-e *filename*

Save rejected entries in the specified file.

- f *filename***
 Read modifications from the specified file.
- The file format is standard LDIF notation as described in RFC 2849.
- h *host***
 Contact the LDAP server on the specified host, which may be a host name or an IP address. Enclose IPv6 addresses in brackets (`[]`) as described in RFC 2732.
- For example, when mapping the IPv4 address `192.168.0.99` to IPv6, pass the `-h` option with its argument as `-h [::ffff:192.168.0.99]`. Notice the brackets.
- The default is `localhost`.
- i *charset***
 Use the specified character set as opposed to the character set specified as the value of the `LANG` environment variable.
- Use this option for example to perform the conversion from the specified character set to UTF8, thus overriding the `LANG` setting.
- j *filename***
 Read the bind password for simple authentication from the specified file.
- k *pathname***
 Use the conversion routines located in the specified directory.
- The default is to use the current directory. Use the `-k` option to specify a sorting language that is not supported by the directory server.
- m *pathname***
 Use the security module database located in the specified directory.
- Use the `-m` option if the security module database is in a different directory from the certificate database itself.
- n**
 Show what would be done, but do not actually do it.
- o *attrname=attrvalue***
 Use the specified attribute values when performing SASL authentication.
- The following *attrname* arguments are supported:
- | | |
|----------------------|--|
| <code>authid</code> | Use the specified authentication identity. |
| <code>authzid</code> | Use the specified authorization identity. |
| <code>mech</code> | Request the specified SASL mechanism for the bind. |
| <code>realm</code> | Use the specified realm to complete the bind. |
| <code>secProp</code> | Use the specified security level. |
- p *port***
 Contact the LDAP server on the specified port.

ldapmodify(1)

The default is 389 (636 if SSL is used).

- q
Run in quiet mode, not displaying information about the operations performed.
- v
Run in verbose mode, displaying diagnostics on standard output.
- w -
Prompt for the bind password for simple authentication.
- w *password*
Use the specified bind password for simple authentication.

EXAMPLES Examples in this section use the following conventions:

- The bind DN given corresponds to a user with permission to update entries.
- The directory server is located on a system named *host*.
- The directory server listens on port number 389, the default for non-SSL traffic.
- The directory server listens on port number 636, the default for SSL traffic. SSL is enabled.

EXAMPLE 1 Adding an Entry

The following commands demonstrate adding a single entry to the directory:

```
$ cat add.ldif
dn: uid=bcubbins,ou=People,dc=example,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
uid: bcubbins
givenName: Bartholomew
sn: Cubbins
cn: Bartholomew Cubbins
mail: bcubbins@example.com
userPassword: bcubbins
facsimiletelephonenumber: +1 234 567 8910

$ ldapmodify -a -h host -D "uid=bjensen,ou=people,dc=example,dc=com"
-w - -f add.ldif
Enter bind password:
adding new entry uid=bcubbins,ou=People,dc=example,dc=com

$
```

EXAMPLE 2 Modifying an Entry

The following commands demonstrate modifying an entry. Notice a line with a single dash (-) separates multiple modifications to a single entry.

```
$ cat modify.ldif
dn: uid=bcubbins,ou=People,dc=example,dc=com
changetype: modify
```

EXAMPLE 2 Modifying an Entry (Continued)

```

add: description
description: Added with ldapmodify
-
replace: mail
mail: bart@example.com

$ ./ldapmodify -h host -c -v
-D "uid=bjensen,ou=People,dc=example,dc=com" -w - -f modify.ldif
Enter bind password:
modifying entry uid=bcubbins,ou=People,dc=example,dc=com

$

```

EXAMPLE 3 Deleting an Entry Interactively

The following commands delete the entry added and modified in previous examples.

```

$ ./ldapmodify -h host -D "uid=bjensen,ou=People,dc=example,dc=com" -w -
Enter bind password:
dn: uid=bcubbins,ou=People,dc=example,dc=com
changetype: delete

deleting entry uid=bcubbins,ou=People,dc=example,dc=com
^D

$

```

EXAMPLE 4 Using Server Authentication

The following command uses server authentication during the bind, where the server only accepts binds by clients with trusted certificates. Notice only the `-P` option is used without other SSL-related options.

```

$ ./ldapmodify -h host -p 636 -c -f modify.ldif
-P /home/bjensen/security -D "uid=bjensen,ou=People,dc=example,dc=com" -w -
Enter bind password:

```

EXAMPLE 5 Using Client Authentication

The following command uses client authentication during the bind, where the server only accepts binds by clients with trusted certificates, and the client must sign the certificate with a password-protected private key. Notice the options used in this example.

```

$ ldapmodify -h host -p 636 -c -f modify.ldif -Z -P /home/bjensen/security
-N "bjscert" -K /home/bjensen/security -W keypassword

```

EXAMPLE 6 Moving an Entry

The following command moves an entry from one branch of a suffix to another:

```

$ ./ldapmodify -h host -D "uid=hmiller,ou=people,dc=example,dc=com" -w -
Enter bind password:
dn: uid=jwallace,ou=people,dc=example,dc=com

```

ldapmodify(1)

EXAMPLE 6 Moving an Entry (Continued)

```
changetype: modrdn
newrdn: uid=jwallace
deleteoldrdn: 0
newsuperior: ou=special users,dc=example,dc=com
^D
```

EXIT STATUS

The exit status returned reflects the return values of the underlying functions used, which may depend on return values sent by the server. Common exit status codes follow:

- | | |
|----|---|
| 0 | Successful completion; LDAP_SUCCESS; 0x00. |
| 1 | Server encountered errors while processing the request; LDAP_OPERATIONS_ERROR; 0x01. |
| 2 | Server encountered errors, such as a BER-decoding error, while processing the request; LDAP_PROTOCOL_ERROR; 0x02. |
| 10 | DN of the entry to modify belongs to an entry handled by neither server, and the referral URL identifies another server that handles the entry; LDAP_REFERRAL; 0x0a. |
| 16 | Attribute to be modified does not exist; LDAP_NO_SUCH_ATTRIBUTE; 0x10. |
| 19 | Attribute modification requested is not a proper modification. For example, a requested change to <code>userpassword</code> would result in a user password shorter than the minimum length allowed; LDAP_CONSTRAINT_VIOLATION; 0x13. |
| 20 | Attribute to add already exists with the specified value; LDAP_TYPE_OR_VALUE_EXISTS; 0x14. |
| 21 | The value modified does not respect the syntax for the attribute type; LDAP_INVALID_SYNTAX; 0x15. |
| 32 | DN of the entry to modify belongs to an entry handled by neither server, and no referral URL is available for the entry; LDAP_NO_SUCH_OBJECT; 0x20. |
| 34 | DN of the entry to modify is not a valid DN; LDAP_INVALID_DN_SYNTAX; 0x22. |
| 50 | Bind DN user does not have permission to read the entry from the directory; LDAP_INSUFFICIENT_ACCESS; 0x32. |
| 53 | Directory is read-only; LDAP_UNWILLING_TO_PERFORM; 0x35. |
| 65 | Requested modification would cause the entry not to comply with the directory schema; LDAP_OBJECT_CLASS_VIOLATION; 0x41. |
| 66 | Entry specified has child-entries that must be deleted first; LDAP_NOT_ALLOWED_ON_NONLEAF; 0x42. |

ldapmodify(1)

- 67 Requested modification would cause the entry to be missing attributes that are components of the entry DN; LDAP_NOT_ALLOWED_ON_RDN; 0x43.
- 68 An entry already exists with the same DN as the entry to add; LDAP_ALREADY_EXISTS; 0x44.
- 81 One of the directories did not respond to the request, or the connection was lost; LDAP_SERVER_DOWN; 0x51.
- 82 An error occurred while receiving results; LDAP_LOCAL_ERROR; 0x52.
- 83 The request could not be BER-encoded; LDAP_ENCODING_ERROR; 0x53.
- 84 A result could not be decoded; LDAP_DECODING_ERROR; 0x54.
- 89 An option or argument is not valid; LDAP_PARAM_ERROR; 0x59.
- 90 Needed memory could not be allocated; LDAP_NO_MEMORY; 0x5a.
- 91 A specified host name or port is not valid; LDAP_CONNECT_ERROR; 0x5b.
- 92 At least one server supports only LDAPv2, and the -v 2 option was not used, or the -V 2 option was used, but the server no longer supports LDAP v2; LDAP_NOT_SUPPORTED; 0x5c.

ATTRIBUTES See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWldk
Stability Level	Evolving

SEE ALSO `ldapcompare(1)`, `ldapdelete(1)`, `ldapsearch(1)`

ldapsearch(1)

NAME	ldapsearch – find LDAP entries		
SYNOPSIS	<pre>\$ cd ServerRoot/shared/bin ./ldapsearch -b baseDN [options] filter [attribute...] ./ldapsearch -b baseDN [options] -f filename [attribute...]</pre>		
DESCRIPTION	<p>The <code>ldapsearch</code> command searches for entries stored by a directory server based on the specified LDAP filter.</p> <p>The <code>ldapsearch</code> command displays results found in LDIF format, including the specified attributes, or all attributes returned if none are specified. Filter files contain one filter per line. Specified LDAP filters must comply with RFC 2254.</p>		
OPTIONS	<p>Unless the <code>LDAP_BASEDN</code> environment variable is set, you must at minimum provide a <i>baseDN</i> argument to the <code>-b</code> option. The <i>baseDN</i> argument specifies the distinguished name (DN) of the LDAP entry at the base of the search scope.</p> <p>The following options are supported:</p> <ul style="list-style-type: none">-0 Ignore LDAP library version mismatches. When this option is omitted, the default behavior is to assert that the revision number of the LDAP API be greater than or equal to that used to compile the tool. Also, if the library and the tool have the same vendor name, the tool will assert that the vendor version number of the API be greater than or equal to that used to compile the tool. Revision and version numbers are based on the contents of the <code>LDAPAPIInfo</code> structure defined in <code><ldap.h></code> or header files included by <code><ldap.h></code>.-1 Omit leading <code>version: 1</code> indication in LDIF output, meaning the output is not RFC 2849 compliant.-3 Check host names in SSL certificates.-A Display non-ASCII values when the <code>-v</code> option is used.-C <i>ps:changetype[:changesonly[:entrychangecontrols]]</i> Perform a persistent search that stops when you type Control-C. By default, when used with the <code>-C</code> option the <code>ldapsearch</code> command requests that the directory server return entry change controls with persistent search results. Adjust this behavior with the following arguments: <table><tr><td><i>changetype</i></td><td>Determines which modifications to an entry are detected and displayed in the output. Possible values include:</td></tr></table>	<i>changetype</i>	Determines which modifications to an entry are detected and displayed in the output. Possible values include:
<i>changetype</i>	Determines which modifications to an entry are detected and displayed in the output. Possible values include:		

	add	
	any	
	delete	
	modify	
	moddn	
<i>changesonly</i>		Determines when to display search results. Possible values include:
	0	
	f	
	false	Display initial search results immediately, not waiting for changes. Then display new changes as they occur.
	1	Display changes when they occur (default).
<i>entrychangecontrols</i>		Determines whether to display entry change controls. Possible values include:
	0	
	f	
	false	Do not display entry change controls.
	1	Display entry change controls (default).
-D <i>bindDN</i>		Use the specified bind DN to authenticate to the directory server.
		If the bind DN and its password are omitted, the <code>ldapsearch</code> command binds anonymously. The bind DN determines what entries and attributes appear in the comparison results, according to the DN's search permissions.
-E		Request that the directories expose (report) bind identities.
-F <i>sep</i>		Print specified separator character instead of <code>:</code> between attribute types and values.
-G <i>pattern</i>		Retrieve a virtual list view displaying a portion of the total search results. Use this option with the <code>-S</code> and <code>-x</code> options to sort entries returned.
		The specified pattern may take one of two forms to specify the size of the virtual list view around a <i>target entry</i> :
		<i>entriesbefore:entriesafter:value</i>
		Return the target entry, which is the first entry in the sorted results whose sort attribute is greater than or equal to the specified value, as well as the specified number of entries before the target entry and the specified number of entries after the target entry.

ldapsearch(1)

For example, `-S sn -x -G 5:10:johnson` returns 16 entries in alphabetical order of the surname attribute: 5 less than `johnson`, the entry equal to or following `johnson`, and the 10 subsequent entries.

entriesbefore:entriesafter:index:count

Return the target entry, as well as the specified number of entries before the target entry and the specified number of entries after the target entry. The target entry depends on the *index* and estimated *count* arguments.

The *count* argument may take the following values, with the following results:

count == 0

The target is the entry at the specified *index* position, starting from 1, and relative to the entire list of sorted results.

count == 1

The target is the first entry in the list of sorted results.

count > 1

The target is the first entry in the slice of the list represented by the fraction *index/count*.

Use an *index* argument greater than the *count* argument to target the last result in the list.

For example, `-G 5:10:2:4` specifies the *index* closest to the beginning of the second quarter of the entire list. If the search yielded 100 entries, the target index would be 26, and this pattern would return entries 21 through 36.

The number of entries displayed before and after the target entry may be limited by the beginning and end of the virtual list. The `ldapsearch` command displays the control response, giving the count of entries in the virtual list and the index of the target entry. Use these values to refine *index* and *count* arguments.

-H

Display usage information.

-I *pin*

Use the specified SSL card password file (*pin*).

-J *controloid[:criticality[:value|::base64value|:<fileurl]]*

Use the specified control OID.

The *criticality*, a boolean, is false by default.

-K *pathname*

Use the certificate private key database located in the specified directory.

You may omit the `-K` option if the key database location is provided as an argument to the `-P` option.

- M
Manage referrals, searching the entry containing the referral instead of the entry obtained by following the referral.
- N *certificate*
Use the specified *certificate* for certificate-based client authentication, for example:
-N "Client-Cert", where Client-Cert is the subject name of the user's certificate.
- O *limit*
Follow at maximum *limit* referral hops. Default is 5.
- P *filename*
Use the certificate database located in *filename*, the full path to the certificate database file.
- Q [*token*][:*certificate-name*]
Use PKCS 11.
- R
Do not follow referrals automatically.
- S *attrtype*
Sort the results based on the specified attribute.
- T
Do not break long lines within individual attribute values.

Default is to break long attribute values according to LDIF rules.
- U
When generating temporary file output using the -t option, include URLs as attribute types whose value is a file, such as a photo or certificate.
- V *n*
Use LDAP protocol version *n*, where *n* is 2 or 3. Default is 3.
- W *password*
Specify the password for the client's key database specified using the -K or -P option.

The -w option is required for certificate-based client authentication.
- X *attrlist*
When performing a search to get effective rights using the -c option, use the list of attributes provided.
- Y *proxydn*
Use the rights of the entry having the specified DN for performing LDAP operations. When using this option, you must also specify how to bind before you assume the rights of the proxy. Thus, when using simple authentication, you would also use the -D and -w options with this option.

Before proxy authentication can work in Directory Server, you must set up the appropriate access control instructions.

ldapsearch(1)

- Z**
Use SSL to provide certificate-based client authentication.
- The **-Z** option requires the **-N** and **-W** options and any other SSL options needed to identify the certificate and the key database.
- a *deref***
Dereference aliases as specified during a search. Possible values for the *deref* argument include the following values:
- | | |
|---------------|---|
| always | Dereference aliases both when finding the base DN, and when searching below it. |
| find | Dereference aliases when finding the base DN. |
| never | Never dereference aliases (default). |
| search | Dereference aliases when searching below the base DN, but not when finding the base DN. |
- This option has no effect when used with directories that do not support alias dereferencing.
- c *authzid***
Use the specified authorization ID when to perform a get effective rights search. The following authorization IDs are supported:
- | | |
|-------------------------|---|
| " (empty string) | Use the authorization ID already specified for the operation. |
| "bindDN" | Use the specified bind DN, such as
uid=bjensen,ou=People,dc=example,dc=com |
| "dn:" | Use anonymous as the authorization ID. |
- d *level***
Set LDAP debug level to the specified value.
- The following debug levels are supported:
- | | |
|--------------|---|
| 1 | Display verbose debugging messages; LDAP_DEBUG_TRACE. |
| 2 | Display messages about the content of network packets;
LDAP_DEBUG_PACKETS. |
| 320 | Display messages about LDIF parsing; LDAP_DEBUG_PARSE. |
| 16384 | Display informational messages; LDAP_DEBUG_ANY. |
- Use the sum of the levels to specify more than one debug level.
- e**
Minimize base64-encoding of resulting attribute values.

- f *filename*
Read the search filters from the specified file.

File format is one search filter per line, where search filters conform to RFC 2254.
- h *host*
Contact the LDAP server on the specified host, which may be a host name or an IP address. Enclose IPv6 addresses in brackets ([]) as described in RFC 2732.

For example, when mapping the IPv4 address 192.168.0.99 to IPv6, pass the -h option with its argument as -h [: : f f f f : 192 . 168 . 0 . 99] . Notice the brackets.

The default is localhost.
- i *charset*
Use the specified character set as opposed to the character set specified as the value of the LANG environment variable.

Use this option for example to perform the conversion from the specified character set to UTF8, thus overriding the LANG setting.
- j *filename*
Read the bind password for simple authentication from the specified file.
- k *pathname*
Use the conversion routines located in the specified directory.

The default is to use the current directory. Use the -k option to specify a sorting language that is not supported by the directory server.
- l *timelimit*
Interrupt the comparison if the specified time limit is exceeded.
- m *pathname*
Use the security module database located in the specified directory.

Use the -m option if the security module database is in a different directory from the certificate database itself.
- n
Show what would be done, but do not actually do it.
- o *attrname=attrvalue*
Use the specified attribute values when performing SASL authentication.

The following *attrname* arguments are supported:

authid	Use the specified authentication identity.
authzid	Use the specified authorization identity.
mech	Request the specified SASL mechanism for the bind.
realm	Use the specified realm to complete the bind.
secProp	Use the specified security level.

ldapsearch(1)

- p** *port*
Contact the LDAP server on the specified port.
The default is 389 (636 if SSL is used).
- s** *scope*
Use the specified search scope.
The following values are supported for *scope*:
- | | |
|------|--|
| base | Examine only the entry specified by the argument to the -b option. |
| one | Examine only to the entry specified by the argument to the -b option and its immediate children. |
| sub | (Default) Examine the subtree whose base is the entry specified by the argument to the -b option. |
- t**
Write a temporary file as output for each attribute of each entry in the search results. Such files are written to the system temporary directory, typically `/tmp`. On standard output, write file names in place of attribute values.
When the **-t** option is used, no base64 encoding is performed on any attribute values, regardless of their content.
- u**
Include user friendly entry names (`ufn: userfriendly`) in the results returned.
- v**
Run in verbose mode, displaying diagnostics on standard output.
- w** `-`
Prompt for the bind password for simple authentication.
- w** *password*
Use the specified bind password for simple authentication.
- x**
Have the directory server sort results based on entry DN's before returning the results.
- z** *sizelimit*
Interrupt the comparison if the specified maximum number of entries returned is exceeded.

EXAMPLES Examples in this section use the following conventions:

- The directory server is located on a system named `host`.
- The directory server has been configured to support anonymous access for search and read. Therefore, you do not have to specify bind information.
- The directory server listens on port number 389, the default for non-SSL traffic.

- The directory server listens on port number 636, the default for SSL traffic. SSL is enabled.

EXAMPLE 1 Returning All Entries

The following command returns all entries in the suffix under the base DN. Use this only when you need to retrieve all entries and attributes:

```
$ ./ldapsearch -h host -b "dc=example,dc=com" "(objectclass=*)"
```

EXAMPLE 2 Narrowing a Search

The following command employs a more specific filter to narrow the search:

```
$ ./ldapsearch -h host -b "dc=example,dc=com" "(cn=Babs Jensen)"
```

EXAMPLE 3 Searching the Root DSE Entry

The following command searches the root DSE entry, requesting supported naming contexts and supported LDAP versions. Notice you specify the scope as only the base entry:

```
$ ./ldapsearch -h host -b "" -s base "(objectclass=*)"
namingContexts supportedLDAPVersion
version: 1
dn:
namingContexts: dc=example,dc=com
namingContexts: o=NetscapeRoot
supportedLDAPVersion: 2
supportedLDAPVersion: 3
```

EXAMPLE 4 Searching the Schema Entry

The following command searches the schema entry, which contains the directory schema. Notice that you can request the operational attribute `subSchemaSubEntry` on any entry to determine which entry holds the schema attributes, in this case `cn=schema`. Then you specify the scope as only the base entry:

```
$ ./ldapsearch -h host -b "" -s base "(objectclass=*)" subSchemaSubEntry
version: 1
dn:
subSchemaSubEntry: cn=schema
$ ./ldapsearch -h host -b "cn=schema" -s base "(objectclass=*)"
version: 1
dn: cn=schema
...
```

EXAMPLE 5 Setting the Base DN

The following commands set the `LDAP_BASEDN` environment variable, and then use it when searching the directory. The syntax of the first command may not work for your shell. Refer to the documentation about your shell for instructions on setting environment variables.

ldapsearch(1)

EXAMPLE 5 Setting the Base DN (Continued)

```
$ export LDAP_BASEDN="dc=example,dc=com"
$ ./ldapsearch -h host "(givenname=Barbara)" cn uid
version: 1
dn: uid=bjablons, ou=People, dc=example,dc=com
cn: Barbara Jablonski
uid: bjablons

dn: uid=bhal2, ou=People, dc=example,dc=com
cn: Barbara Hall
uid: bhal2

dn: uid=bjensen, ou=People, dc=example,dc=com
cn: Barbara Jensen
cn: Babs Jensen
uid: bjensen

dn: uid=bmaddox, ou=People, dc=example,dc=com
cn: Barbara Maddox
uid: bmaddox

dn: uid=bfrancis, ou=People, dc=example,dc=com
cn: Barbara Francis
uid: bfrancis
```

EXAMPLE 6 Using a Filter File

The following commands demonstrate use of a filter file. The results show the directory server responds to separate searches for each filter.

```
$ cat filters
sn=Francis
givenname=Barbara
$ ./ldapsearch -b "dc=example,dc=com" -h host -f filters cn uid
version: 1
dn: uid=rfrancis, ou=People, dc=example,dc=com
cn: Richard Francis
uid: rfrancis

dn: uid=bfrancis, ou=People, dc=example,dc=com
cn: Barbara Francis
uid: bfrancis

dn: uid=bjablons, ou=People, dc=example,dc=com
cn: Barbara Jablonski
uid: bjablons

dn: uid=bhal2, ou=People, dc=example,dc=com
cn: Barbara Hall
uid: bhal2

dn: uid=bjensen, ou=People, dc=example,dc=com
cn: Barbara Jensen
cn: Babs Jensen
uid: bjensen
```

EXAMPLE 6 Using a Filter File (Continued)

```
dn: uid=bmaddox, ou=People, dc=example,dc=com
cn: Barbara Maddox
uid: bmaddox
```

```
dn: uid=bfrancis, ou=People, dc=example,dc=com
cn: Barbara Francis
uid: bfrancis
$
```

EXAMPLE 7 Escaping Commas

The following command demonstrates use of the backslash (\) to escape a comma within a base DN.

```
$ ./ldapsearch -b "o=Example Company\, Inc.,dc=example,dc=com"
-h host "(givenname=Barbara)"
```

EXAMPLE 8 Using Server Authentication

The following command uses server authentication during the bind, where the server only accepts binds by clients with trusted certificates. Notice only the `-P` option is used without other SSL-related options.

```
$ ./ldapsearch -h host -p 636 -b "dc=example,dc=com" -P /home/bjensen/security
-D "uid=bjensen,ou=People,dc=example,dc=com" -w - "(givenname=Barbara)"
Enter bind password:
```

EXAMPLE 9 Using Client Authentication

The following command uses client authentication during the bind, where the server only accepts binds by clients with trusted certificates, and the client must sign the certificate with a password-protected private key. Notice the options used in this example.

```
$ ldapsearch -h host -p 636 -b "dc=example,dc=com" -P /home/bjensen/security
-N "bjscert" -K /home/bjensen/security -W keypassword "(givenname=Barbara)"
```

EXIT STATUS

The exit status returned reflects the return values of the underlying functions used, which may depend on return values sent by the server. Common exit status codes follow:

- | | |
|---|---|
| 0 | Successful completion; LDAP_SUCCESS; 0x00. |
| 1 | Server encountered errors while processing the request; LDAP_OPERATIONS_ERROR; 0x01. |
| 2 | Server encountered errors, such as a BER-decoding error, while processing the request; LDAP_PROTOCOL_ERROR; 0x02. |
| 3 | Search exceeded the time limit for operations on the server; LDAP_TIMELIMIT_EXCEEDED; 0x03. |

ldapsearch(1)

- 4 Search returned more results than the maximum number allowed by the server; LDAP_SIZELIMIT_EXCEEDED; 0x04.
- 10 Base DN belongs to an entry handled by neither server, and the referral URL identifies another server that handles the entry; LDAP_REFERRAL; 0x0a.
- 11 Search returned more results than the maximum number a client application is allowed by the server to retrieve; LDAP_ADMINLIMIT_EXCEEDED; 0x0b.
- 32 Base DN belongs to an entry handled by neither server, and no referral URL is available for the entry; LDAP_NO_SUCH_OBJECT; 0x20.
- 34 Base DN is not a valid DN; LDAP_INVALID_DN_SYNTAX; 0x22.
- 50 Bind DN user does not have permission to read the entry from the directory; LDAP_INSUFFICIENT_ACCESS; 0x32.
- 53 Directory is read-only; LDAP_UNWILLING_TO_PERFORM; 0x35.
- 81 One of the directories did not respond to the request, or the connection was lost; LDAP_SERVER_DOWN; 0x51.
- 82 An error occurred while receiving results; LDAP_LOCAL_ERROR; 0x52.
- 83 The request could not be BER-encoded; LDAP_ENCODING_ERROR; 0x53.
- 84 A result could not be decoded; LDAP_DECODING_ERROR; 0x54.
- 85 The search exceeded the time limit specified using the -l option; LDAP_TIMEOUT; 0x55.
- 87 An error occurred while parsing and BER-encoding the specified filter; LDAP_FILTER_ERROR; 0x57.
- 89 An option or argument is not valid; LDAP_PARAM_ERROR; 0x59.
- 90 Needed memory could not be allocated; LDAP_NO_MEMORY; 0x5a.
- 91 A specified host name or port is not valid; LDAP_CONNECT_ERROR; 0x5b.
- 92 At least one server supports only LDAPv2, and the -v 2 option was not used, or the -v 2 option was used, but the server no longer supports LDAP v2; LDAP_NOT_SUPPORTED; 0x5c.

ATTRIBUTES See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWldk
Stability Level	Evolving

SEE ALSO `ldapcompare(1)`, `ldapdelete(1)`, `ldapmodify(1)`

NAME	ldif – format input by adding base 64 encoding to make it suitable for inclusion in an LDIF file.						
SYNOPSIS	directoryserver ldif [-b] <i>attrtype</i> <i>ServerRoot</i> bin/slapd/server/ldif [-b] <i>attrtype</i>						
DESCRIPTION	The <code>ldif</code> command formats input by adding base 64 encoding to make it suitable for inclusion in an LDIF file. This makes it easy to include binary data, such as JPEG images, along with other textual attribute values. In an LDIF file, base 64 encoded attribute values are indicated by a <code>: : encoded data</code> . In addition to binary data, other values that must be base 64 encoded include: any value that begins with a semicolon (<code>;</code>) or a space, and any value that contains non-ASCII data, including newlines. The <code>ldif</code> command takes any input and formats it with the correct line continuation and appropriate attribute information. See the <i>Directory Server Administration Guide</i> .						
OPTIONS	The following options are supported: -b Specifies that the <code>ldif</code> command should interpret the entire input as a single binary value. As an alternative to the <code>-b</code> option, you can use the <code>:<URL</code> specifier notation, which is simpler to use. For example: <code>jpegphoto:<file:///tmp/myphoto.jpg</code> . Although the official notation requires three <code>///</code> the user of one <code>/is</code> tolerated.						
EXIT STATUS	The following exit values are returned: 0 Successful completion. 1 An error occurred. On error, verbose error messages are output to standard output.						
ATTRIBUTES	See <code>attributes(5)</code> for descriptions of the following attributes:						
	<table border="1"> <thead> <tr> <th>ATTRIBUTE TYPE</th> <th>ATTRIBUTE VALUE</th> </tr> </thead> <tbody> <tr> <td>Availability</td> <td>SUNWdsvu</td> </tr> <tr> <td>Stability Level</td> <td>Committed Private</td> </tr> </tbody> </table>	ATTRIBUTE TYPE	ATTRIBUTE VALUE	Availability	SUNWdsvu	Stability Level	Committed Private
ATTRIBUTE TYPE	ATTRIBUTE VALUE						
Availability	SUNWdsvu						
Stability Level	Committed Private						
SEE ALSO	<code>directoryserver(1M)</code> , <code>ldapmodify(1)</code>						

mmldif(1)

- NAME** mmldif – combine multiple ldif files into a single, authoritative set of entries
- SYNOPSIS** **directoryserver mmldif** [-c] [-D] [-o *out.ldif*] *inputFiles*
ServerRoot/bin/slapd/server/mmldif [-c] [-D] [-o *out.ldif*] *inputFiles*
- DESCRIPTION** The mmldif command combines multiple LDIF files into a single authoritative set of entries. Typically each LDIF file is from a master server cooperating in a multi-master replication environment (for example, masters that refuse to sync up). Optionally, the mmldif command can generate LDIF change files that could be applied to the original file to bring it up to date with the authoritative version. At least two input files must be specified.
- OPTIONS** The following options are supported:
- c Write a change file (.delta) for each input file.
 - D Print debugging information.
 - o Write authoritative data to this file. If not specified, the command compares the input files, but does not generate output LDIF files.
- inputFiles* Two or more LDIF files to combine into a single set of entries. For example, *in1.ldif in2.ldif*
- ATTRIBUTES** See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `insync(1)`

NAME	monitor – retrieve performance monitoring information
SYNOPSIS	directoryserver [{-s -server} server-instance] monitor <i>ServerRoot/slaped-serverID/monitor</i>
DESCRIPTION	The monitor command retrieves performance monitoring information using the ldapsearch command-line utility. Directory Server must be running for this tool to function.
OPTIONS	There are no options for the monitor command.
EXIT STATUS	The exit status returned reflects the return values of the underlying functions used, which may depend on return values sent by the server. The return values are defined through <ldap.h> files both on the client side and on the server side. Common exit status codes follow: <ul style="list-style-type: none"> 0 Successful completion; LDAP_OPERATIONS_ERROR; 0x00. 1 Server encountered errors while processing the request; LDAP_OPERATIONS_ERROR; 0x01. 2 Server encountered errors, such as a BER-decoding error, while processing the request; LDAP_PROTOCOL_ERROR; 0x02. 3 Search exceeded the time limit for operations on the server; LDAP_TIMELIMIT_EXCEEDED; 0x03. 4 Search returned more results than the maximum number allowed by the server; LDAP_SIZELIMIT_EXCEEDED; 0x04. 10 Base DN belongs to an entry handled by neither server, and the referral URL identifies another server that handles the entry; LDAP_REFERRAL; 0x0a. 11 Search returned more results than the maximum number a client application is allowed by the server to retrieve; LDAP_ADMINLIMIT_EXCEEDED; 0x0b. 32 Base DN belongs to an entry handled by neither server, and no referral URL is available for the entry; LDAP_NO_SUCH_OBJECT; 0x20. 50 Bind DN user does not have permission to read the entry from the directory; LDAP_INSUFFICIENT_ACCESS; 0x32. 53 Directory is read-only; LDAP_UNWILLING_TO_PERFORM; 0x35. 81 One of the directories did not respond to the request, or the connection was lost; LDAP_SERVER_DOWN; 0x51. 82 An error occurred while receiving results; LDAP_LOCAL_ERROR; 0x52. 83 The request could not be BER-encoded; LDAP_ENCODING_ERROR; 0x53. 84 A result could not be decoded; LDAP_DECODING_ERROR; 0x54.

monitor(1)

- 85 The search exceeded the time limit specified using the -l option;
LDAP_TIMEOUT; 0x55.
- 87 An error occurred while parsing and BER-encoding the specified filter;
LDAP_FILTER_ERROR; 0x57.
- 89 An option or argument is not valid; LDAP_PARAM_ERROR; 0x59.
- 90 Needed memory could not be allocated; LDAP_NO_MEMORY; 0x5a.
- 91 A specified host name or port is not valid; LDAP_CONNECT_ERROR; 0x5b.
- 92 At least one server supports only LDAPv2, and the -v 2 option was not
used; LDAP_NOT_SUPPORTED; 0x5c, or the -V 2 option was specified but
the server no longer supports LDAPv2.

ATTRIBUTES See attributes(5) for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO directoryserver(1M), ldapsearch(1)

NAME	account-status, ns-accountstatus.pl – provide status information to establish whether or not an entry or group of entries is inactivated
SYNOPSIS	<pre> directoryserver [{-s -server} server-instance] account-status [-D rootDN] {-w <i>password</i> -w - -j <i>filename</i>} [-h <i>host</i>] [-p <i>port</i>] -I DN-to-get-status-of ServerRoot/slapd-serverID/ns-accountstatus.pl [-D <i>rootDN</i>] {-w <i>password</i> -w - -j <i>filename</i>} [-h <i>host</i>] [-p <i>port</i>] -I DN-to-get-status-of </pre>
DESCRIPTION	The <code>account-status</code> command provides status information to establish whether an entry or group of entries is inactivated or not.
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none"> -? <ul style="list-style-type: none"> Provides help -D <ul style="list-style-type: none"> Directory Server user DN with root permissions, such as Directory Manager -h <ul style="list-style-type: none"> Host name of Directory Server. The default value is the full host name of the machine on which Directory Server is installed. -I <i>DN-to-get-status-of</i> <ul style="list-style-type: none"> Entry DN or role DN to obtain status for. -j <ul style="list-style-type: none"> File from which the bind password is read. Used for simple authentication. If this option is specified the <code>-w</code> option must not be specified. -p <ul style="list-style-type: none"> Directory Server port. The default value is the Directory Server LDAP port specified at installation time. -w <ul style="list-style-type: none"> Password associated with the user DN. If you do not specify this option anonymous access is used. If you specify <code>-w -</code>, the utility prompts for the password. If either <code>-w</code> option is specified, the <code>-j</code> option must not be specified. For example, <code>-w diner892</code>.
EXIT STATUS	<p>The following exit values are returned:</p> <ul style="list-style-type: none"> 0 Successful completion. 1 An error occurred. <p>On error, verbose error messages are output to standard output.</p>
ATTRIBUTES	See <code>attributes(5)</code> for descriptions of the following attributes:

ns-accountstatus.pl(1)

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `ns-accountstatus.pl(1)`, `account-activate(1)`,
`account-inactivate(1)`

NAME	account-activate, ns-activate.pl – activate an entry or a group of entries
SYNOPSIS	<pre> directoryserver [{-s -server} server-instance] account-activate [-D <i>rootDN</i>] {-w <i>password</i> -w - -j <i>filename</i>} [-h <i>host</i>] [-p <i>port</i>] -I <i>DN-to-activate</i> <i>ServerRoot/slaped-serverID/ns-activate.pl</i> [-D <i>rootDN</i>] {-w <i>password</i> -w - -j <i>filename</i>} [-h <i>host</i>] [-p <i>port</i>] -I <i>DN-to-activate</i> </pre>
DESCRIPTION	The <code>account-activate</code> command activates an entry or group of entries.
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none"> -? <ul style="list-style-type: none"> Provides help -D <ul style="list-style-type: none"> Directory Server user DN with root permissions, such as Directory Manager. -h <ul style="list-style-type: none"> Host name of Directory Server. The default value is the full host name of the machine on which Directory Server is installed. -I <i>DN-to-activate</i> <ul style="list-style-type: none"> Entry DN or role DN to activate. -j <ul style="list-style-type: none"> File from which the bind password is read. Used for simple authentication. If this option is specified the <code>-w</code> option must not be specified. -p <ul style="list-style-type: none"> Directory Server port. The default value is the Directory Server LDAP port specified at installation time. -w <ul style="list-style-type: none"> Password associated with the user DN. If you do not specify this option anonymous access is used. If you specify <code>-w -</code>, the utility prompts for the password. If either <code>-w</code> option is specified, the <code>-j</code> option must not be specified. For example, <code>-w diner892</code>.
EXIT STATUS	<p>The following exit values are returned:</p> <ul style="list-style-type: none"> 0 Successful completion. 1 An error occurred. <p>On error, verbose error messages are output to standard output.</p>
ATTRIBUTES	See <code>attributes(5)</code> for descriptions of the following attributes:

ns-activate.pl(1)

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M),ns-activate.pl(1)account-inactivate(1)account-status(1)`

NAME	account-inactivate, ns-inactivate.pl – inactivate an entry or a group of entries
SYNOPSIS	<pre> directoryserver [{-s -server} server-instance] account-inactivate [-D <i>rootDN</i>] {-w <i>password</i> -w - -j <i>filename</i>} [-h <i>host</i>] [-p <i>port</i>] -I <i>DN-to-inactivate</i> <i>ServerRoot/slaped-serverID/ns-inactivate.pl</i> [-D <i>rootDN</i>] {-w <i>password</i> -w - -j <i>filename</i>} [-h <i>host</i>] [-p <i>port</i>] -I <i>DN-to-inactivate</i> </pre>
DESCRIPTION	The <code>account-inactivate</code> command inactivates an entry or group of entries.
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none"> -? <ul style="list-style-type: none"> Provides help -D <ul style="list-style-type: none"> Directory Server user DN with root permissions, such as Directory Manager. -h <ul style="list-style-type: none"> Host name of Directory Server. The default value is the full host name of the machine on which Directory Server is installed. -I <i>DN-to-inactivate</i> <ul style="list-style-type: none"> Entry DN or role DN to inactivate. -j <ul style="list-style-type: none"> File from which the bind password is read. Used for simple authentication. If this option is specified the <code>-w</code> option must not be specified. -p <ul style="list-style-type: none"> Directory Server port. The default value is the Directory Server LDAP port specified at installation time. -w <ul style="list-style-type: none"> Password associated with the user DN. If you do not specify this option anonymous access is used. If you specify <code>-w -</code>, the utility prompts for the password. If either <code>-w</code> option is specified, the <code>-j</code> option must not be specified. For example, <code>-w diner892</code>.
EXIT STATUS	<p>The following exit values are returned:</p> <ul style="list-style-type: none"> 0 Successful completion. 1 An error occurred. <p>On error, verbose error messages are output to standard output.</p>
ATTRIBUTES	See <code>attributes(5)</code> for descriptions of the following attributes:

ns-inactivate.pl(1)

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `ns-inactivate.pl(1)`, `account-activate(1)`,
`account-status(1)`

NAME	pwdhash – print the encrypted form of a password using one of the server’s encryption algorithms
SYNOPSIS	<pre>directoryserver pwdhash -D instance_dir [-H] [-c comparepwd -s scheme] password ServerRoot/bin/slapd/server/pwdhash -D instance_dir [-H] [-c comparepwd -s scheme] password</pre>
DESCRIPTION	The pwdhash command prints the encrypted form of a password using one of the server’s encryption algorithms. If a user cannot log in, you can use this command to compare the user’s password with the password stored in the directory.
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none"> -c Specifies the encrypted password with which the user password is to be compared. The result of this comparison is either OK or password does not match -D Instance Directory Server. -H Specifies that the passwords are hex-encoded. <i>password</i> The clear password/s from which the encrypted form should be generated (or against which the password in the directory should be compared). -s Generates the encrypted passwords according to the scheme’s algorithm. The available schemes are SSHA, SHA, CRYPT, and CLEAR.
EXAMPLES	<p>EXAMPLE 1 Comparing two passwords</p> <pre>#directoryserver pwdhash -D ServerRoot/slapd-serverID -s SSHA mypassword " {SSHA}mtHyZSHfhOZ4FHmvQe09FQjvLZpnW1wbmW05cw==" #directoryserver pwdhash -D ServerRoot/slapd-serverID -c " {SSHA}mtHyZSHfhOZ4FHmvQe09FQjvLZpnW1wbmW05cw==" aPassword /usr/ds/v5.2/slapd/server/pwdhash: password does not match</pre>
EXIT STATUS	<p>The following exit values are returned:</p> <ul style="list-style-type: none"> 0 Successful completion. 1 An error occurred.
ATTRIBUTES	See attributes(5) for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu

pwdhash(1)

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `account-activate(1)`, `account-inactivate(1)`, `account-status(1)`

NAME	repldisc – discover a replication topology
SYNOPSIS	<pre>ServerRoot/shared/bin/repldisc [-D bindDN] [-w password] [-j file] [-t] [-n] [-a] [-p port] [-T timeout] [-J file] [-W keypassword] [-K keydbpath] [-N certname] [-P certdbpath] [-e SSL port] [-b ReplicaRoot] -s -S HostSpec</pre>
DESCRIPTION	The <code>repldisc</code> command enables the discovery of a replication topology. Topology discovery starts with one server and constructs a graph of all known servers (using the RUVs and Replication Agreements). <code>repldisc</code> then prints an adjacency matrix describing the topology.
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none"> -a Specifies that only the arcs between pairs of connected hosts are printed. For more information, see the EXAMPLES. Note: If the total line length of the output exceeds 80 characters, symbolic host names are used, accompanied by a legend. Otherwise, full host names are printed. Using the <code>-a</code> option ensures that symbolic host names are not used. -b The suffix (replica root) that has been specified for replication. If <code>-b</code> is not specified, the delay for all suffixes is printed. -D Distinguished name with which to bind to the server. This parameter is optional if the server is configured to support anonymous access. If a DN is specified in the <i>HostSpec</i> option, this overrides the <code>-D</code> option. -j If specifying the default password at the command-line poses a security risk, the password can be stored in a file. The <code>-j</code> option specifies this file. -n Specifies that <code>repldisc</code> should not run in interactive mode. Running in interactive mode allows you to re-enter the bindDN, password, host and port, if a bind error occurs. -p The TCP port used by the Directory Server. The default port is 389. If a port is specified in the <i>HostSpec</i>, this overrides the <code>-p</code> option. -t Prints the mode of transport (SSL or CLEAR). -T Specifies the number of seconds after which <code>repldisc</code> will time out if the server connection goes down. -w Password associated with the distinguished name specified by the <code>-D</code> option. If a password is specified in the <i>HostSpec</i>, this overrides the <code>-w</code> option.

repldisc(1)

Host Spec

Host specification, which takes the form [bindDN[:[password]]@]host[:port]

Example: "**cn=directory manager**":mypword@myserver:5201. If you are using SSL, use -S in the server specification. In this case, *HostSpec* specifies the certificate name and key password, rather than the bindDN and password.

SSL OPTIONS

You can use the following options to specify that *repldisc* uses LDAPS when communicating with Directory Server. You can also use these options if you want to use certificate-based authentication. These options are valid only when LDAPS has been turned on and configured. For more information on certificate-based authentication and how to create a certificate database for use with LDAP clients, see the *Directory Server Administration Guide*.

-e

Default SSL port

-J

This option has the same function as the -j option, for the key password.

-K

Specifies the name of the certificate key used for certificate-based client authentication. For example, -K *Server-Key*.

-N

Specifies the certificate name to use for certificate-based client authentication. For example, -N *Server-Cert*. If this option is specified, the -W option is required.

-P

Specifies the location of the certificate database.

-W

Specifies the password for the certificate database identified by the -P option. For example, -W *serverpassword*.

EXAMPLES

EXAMPLE 1 Sample output in a single replication scenario

```
# repldisc -D "cn=directory manager" -w mypword -b o=rtest \\  
-s myserver:1389
```

Topology for suffix: o=rtest

Legend:

```
^ : Host on row sends to host on column.  
v : Host on row receives from host on column.  
x : Host on row and host on column are in MM mode.  
H1 : france.example.com:1389  
H2 : spain:1389  
H3 : portugal:389
```

```
    | H1 | H2 | H3 |  
====+=====
```

EXAMPLE 1 Sample output in a single replication scenario (Continued)

```
H1 |   | ^ |   |
---+-----
H2 | v |   | ^ |
---+-----
H3 |   | v |   |
---+-----
```

EXAMPLE 2 Sample output using the -a option

Topology for suffix: o=rtest

Legend:

The direction of the replication is indicated with arrows.

Single-master: suppliers appear on left, consumers on right (->).

Multi-master : servers are shown linked by a double arrow (<->).

france.example.com:1389 -> spain:1389

spain:1389 -> portugal:389

EXIT STATUS The following exit values are returned:

0 Successful completion.

1 An error occurred.

ATTRIBUTES See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `insync(1)`, `entrycmp(1)`

NOTES The node on which you are running the `entrycmp`, `insync`, and `repldisc` tools must be able to reach all the specified hosts. If these hosts are unavailable due to a firewall, VPN, or other network setup reasons, you will encounter difficulties using these tools. For the same reason ensure that all servers are up and running before using these tools.

When identifying hosts, you must use either symbolic names or IP addresses for all hosts since the replication monitoring commands do not address resolution between symbolic names and IP addresses. Using a combination of the two can cause problems, especially on multi-homed hosts.

When SSL is enabled, the directory server on which you are running the tools must have a copy of all the certificates used by the other servers in the topology.

repldisc(1)

`repldisc` takes the host specification from the replication agreement, unless otherwise specified at the command line.

The replication monitoring tools rely on access to `cn=config` to obtain the replication status. This should be taken into account particularly when replication is configured over SSL.

DS 1m

bak2db(1M)

NAME	bak2db – restore the database from the most recent archived backup
SYNOPSIS	directoryserver [{-s -server} server-instance] bak2db backup_directory ServerRoot/ slapd -serverID/ bak2db backup_directory
DESCRIPTION	The bak2db command restores the database from the most recent archived backup. Directory Server must be stopped for this tool to work.
OPTIONS	There are no options for the bak2db command.
EXIT STATUS	The following exit values are returned: 0 Successful completion. non-zero An error occurred.
ATTRIBUTES	See <code>attributes(5)</code> for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `bak2db.pl(1M)`, `bak2db-task(1M)`, `db2bak(1M)`

NAME bak2db-task, bak2db.pl – restore the database from the most recent archived backup

SYNOPSIS **directoryserver** [{-s|-server} **server-instance**] **bak2db-task** -D *rootDN* {-w *password* | -w - | -j *filename*} -a *backup_directory* [-t *databasetype*]

ServerRoot/slapd-serverID/bak2db.pl [-v] -D *rootDN* {*wpassword-w -* | -j *filename*} -a *backup_directory* [-t *databasetype*]

DESCRIPTION The bak2db-task command creates an entry in the directory that launches the dynamic task of restoring the database from the most recent archived backup. An entry is generated based upon the values you provide for each option. Directory Server must be running for this tool to work.

OPTIONS The following options are supported:

- a Directory of the backup files.
- D User DN with root permissions, such as Directory Manager. The default is the DN of the directory manager, which is read from the nsslapd-root attribute under cn=config.
- j Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified, the -w must not be specified.
- t Database type. Currently, “ldb database” is the only possible type and the default value.
- v Verbose mode.
- w Password associated with the user DN. If you do not specify this option anonymous access is used. If you specify -w -, the utility prompts for the password. If either -w option is specified, the -j option must not be specified. For example, -wdiner892.

EXIT STATUS The following exit values are returned:

- 0 Successful completion.
- 1 An error occurred.

On error, verbose error messages are output to standard output.

ATTRIBUTES See attributes(5) for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO directoryserver(1M), bak2db(1M), bak2db.pl(1M), db2bak(1M), stop-slapd(1M), start-slapd(1M), restart-slapd(1M)

bak2db-task(1M)

NAME	bak2db-task, bak2db.pl – restore the database from the most recent archived backup						
SYNOPSIS	<pre>directoryserver [{-s -server} server-instance] bak2db-task -D rootDN {-w password -w - -j filename} -a backup_directory [-t databasetype] ServerRoot/slapd-serverID/bak2db.pl [-v] -D rootDN {wpassword-w - -j filename} -a backup_directory [-t databasetype]</pre>						
DESCRIPTION	The bak2db-task command creates an entry in the directory that launches the dynamic task of restoring the database from the most recent archived backup. An entry is generated based upon the values you provide for each option. Directory Server must be running for this tool to work.						
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none">-a Directory of the backup files.-D User DN with root permissions, such as Directory Manager. The default is the DN of the directory manager, which is read from the nsslapd-root attribute under cn=config.-j Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified, the -w must not be specified.-t Database type. Currently, "ldbm database" is the only possible type and the default value.-v Verbose mode.-w Password associated with the user DN. If you do not specify this option anonymous access is used. If you specify -w -, the utility prompts for the password. If either -w option is specified, the -j option must not be specified. For example, -wdiner892.						
EXIT STATUS	<p>The following exit values are returned:</p> <ul style="list-style-type: none">0 Successful completion.1 An error occurred. <p>On error, verbose error messages are output to standard output.</p>						
ATTRIBUTES	<p>See attributes(5) for descriptions of the following attributes:</p> <table border="1"><thead><tr><th>ATTRIBUTE TYPE</th><th>ATTRIBUTE VALUE</th></tr></thead><tbody><tr><td>Availability</td><td>SUNWdsvu</td></tr><tr><td>Stability Level</td><td>Committed Private</td></tr></tbody></table>	ATTRIBUTE TYPE	ATTRIBUTE VALUE	Availability	SUNWdsvu	Stability Level	Committed Private
ATTRIBUTE TYPE	ATTRIBUTE VALUE						
Availability	SUNWdsvu						
Stability Level	Committed Private						
SEE ALSO	directoryserver(1M), bak2db(1M), bak2db.pl(1M), db2bak(1M), stop-slapd(1M), start-slapd(1M), restart-slapd(1M)						

- NAME** db2bak – create a backup of the current database contents
- SYNOPSIS** **directoryserver** [{-s|-server} **server-instance**] **db2bak**
[backup_directory]
ServerRoot/slapd-serverID/db2bak backup_directory
- DESCRIPTION** The db2bak command creates a backup of the current database contents. This command can be executed with the server either running or not. The default backup directory is *ServerRoot/slapd-serverID/bak*. The backup file is named according to the year_month_day_hour_minute_second format (*YYYY_MM_DD_hh_mm_ss*).
- OPTIONS** There are no options for the db2bak command.
- EXIT STATUS** The following exit values are returned:
 0 Successful completion.
 non-zero An error occurred.
- ATTRIBUTES** See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `db2bak.pl(1M)`, `db2bak-task(1M)`, `bak2db(1M)`

db2bak.pl(1M)

NAME db2bak-task, db2bak.pl – create a backup of the current database contents

SYNOPSIS `directoryserver [{-s|-server} server-instance] db2bak-task [-v] -D rootDN {-w password | -w - | -j filename} -a backup_directory [-t databasetype]`

`ServerRoot/slaped-serverID/db2bak.pl [-v] -D rootDN {-w password | -w - | -j filename} -a backup_directory [-t databasetype]`

DESCRIPTION The db2bak-task command creates an entry in the directory that launches the dynamic task of creating a backup of the current database contents. An entry is generated based upon the values you provide for each option. Directory Server must be running to execute this command.

OPTIONS The following options are supported:

- a Directory where the backup files will be stored. By default it is under `ServerRoot/slaped-serverID/bak`. The backup file is named according to the year_month_day_hour_minute_second format (`YYYY_MM_DD_hh_mm_ss`).
- D User DN with root permissions, such as Directory Manager. The default is the DN of the directory manager, which is read from the `nsslapd-root` attribute under `cn=config`.
- j Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified, the `-w` must not be specified.
- t Database type. Currently, “ldb database” is the only possible type and the default value.
- v Verbose mode.
- w Password associated with the user DN. If you do not specify this option anonymous access is used. If you specify `-w -`, the utility prompts for the password. If either `-w` option is specified, the `-j` option must not be specified. For example, `-wdiner892`.

EXIT STATUS The following exit values are returned:

- 0 Successful completion.
- 1 An error occurred.

On error, verbose error messages are output to standard output.

ATTRIBUTES See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu

db2bak.pl(1M)

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Stability Level	Committed Private

SEE ALSO directoryserver(1M), db2bak(1M), db2bak.pl(1M), bak2db(1M), start-slapd(1M), stop-slapd(1M), restart-slapd(1M)

db2bak-task(1M)

NAME db2bak-task, db2bak.pl – create a backup of the current database contents

SYNOPSIS **directoryserver** [{-s|-server} **server-instance**] **db2bak-task** [-v]
 -D *rootDN* {-w *password* | -w - | -j *filename*} -a *backup_directory* [-t
databasetype]
ServerRoot/slaped-serverID/db2bak.pl [-v] -D *rootDN*
 {-w *password* | -w - | -j *filename*} -a *backup_directory* [-t *databasetype*]

DESCRIPTION The db2bak-task command creates an entry in the directory that launches the dynamic task of creating a backup of the current database contents. An entry is generated based upon the values you provide for each option. Directory Server must be running to execute this command.

OPTIONS The following options are supported:

- a Directory where the backup files will be stored. By default it is under *ServerRoot/slaped-serverID/bak*. The backup file is named according to the year_month_day_hour_minute_second format (*YYYY_MM_DD_hh_mm_ss*).
- D User DN with root permissions, such as Directory Manager. The default is the DN of the directory manager, which is read from the *nsslapd-root* attribute under *cn=config*.
- j Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified, the -w mut not be specified.
- t Database type. Currently, “ldb database” is the only possible type and the default value.
- v Verbose mode.
- w Password associated with the user DN. If you do not specify this option anonymous access is used. If you specify -w -, the utility prompts for the password. If either -w option is specified, the -j option must not be specified. For example, -wdiner892.

EXIT STATUS The following exit values are returned:

- 0 Successful completion.
- 1 An error occurred.

On error, verbose error messages are output to standard output.

ATTRIBUTES See *attributes(5)* for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu

db2bak-task(1M)

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `db2bak(1M)`, `db2bak.pl(1M)`, `bak2db(1M)`,
`start-slapd(1M)`, `stop-slapd(1M)`, `restart-slapd(1M)`

db2ldif(1M)

NAME	db2ldif – export the contents of a database to LDIF
SYNOPSIS	<pre> directoryserver [{-s -server} server-instance] db2ldif {-n <i>backend_instance</i>}* {-s <i>includesuffix</i>}* [{-x <i>excludesuffix</i>}*] [-r] [-C] [-u] [-U] [-m] [-M] [-a <i>outfile</i>] [-1] [-N] [-Y <i>keydb-pwd</i>] [-y <i>keydb-pwd-file</i>] <i>ServerRoot</i>/slapd-serverID db2ldif {-n <i>backend_instance</i>}* {-s <i>includesuffix</i>}* [{-x <i>excludesuffix</i>}*] [-r] [-C] [-u] [-U] [-m] [-M] [-a <i>outfile</i>] [-1] [-N] [-Y <i>keydb-pwd</i>] [-y <i>keydb-pwd-file</i>] </pre>
DESCRIPTION	The db2ldif command exports the contents of the database to LDIF. The * indicates that multiple occurrences are allowed. This tool can be executed while the server is still running.
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none"> -a File name of the output LDIF file. -C Only the main database file is used. -1 For reasons of backward compatibility, omits leading <code>version: 1</code> indication in LDIF output. -m Minimal base64 encoding. -M Use of several files for storing the output LDIF, with each instance stored in <code>instance_outfile</code> (where <code>outfile</code> is the file name specified for the <code>-a</code> option). -n Name of database to be exported. -N Specifies that entry IDs are not to be included in the LDIF output. -r Exports replication information. Use this option when replication is configured and the generated LDIF will be used to initialize another replica or as a backup. Note that <code>db2ldif -r</code> cannot be used if another <code>slapd</code> process is running. To export the database while a <code>slapd</code> process is running, use <code>db2ldif-task -r</code> instead. -s Suffix(es) to be included. If used in conjunction with the <code>-n</code> option, this option specifies the subtree(s) to be included. When exported suffixes split across multiple backends, you must export each subsuffix separately. With the <code>-s suffix</code> option, Directory Server exports only those entries in the backend containing the <code>suffix</code> entry. -u Request that the unique id is not exported. -U Request that the output LDIF is not folded. -x Suffix(es) to be excluded. -y Specifies the file in which the password for the key database is held, also used when handling encrypted attributes.

-Y Specifies the password for the key database, providing a means of authentication required by Directory Server when handling encrypted attributes.

EXIT STATUS The following exit values are returned:

0 Successful completion.

Otherwise check logs for further information.

ATTRIBUTES See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `db2ldif-task(1M)`, `db2ldif.pl(1M)`, `stop-slapd(1M)`, `start-slapd(1M)`, `restart-slapd(1M)`

NOTES You must specify either the `-n` or the `-s` option (or both). The output LDIF will be stored in one file by default. Should you want to specify the use of several files, then use the `-M` option.

db2ldif.pl(1M)

NAME	db2ldif-task, db2ldif.pl – export the contents of a database to LDIF
SYNOPSIS	<pre> directoryserver [{-s -server} server-instance] db2ldif-task [-v] -D <i>rootDN</i> {-w <i>password</i> -w - -j <i>filename</i>} {-n <i>backend_instance</i>}* {-s <i>includesuffix</i>}* [{-x <i>excludesuffix</i>}*] [-a <i>outfile</i>] [-N] [-r] [-C] [-u] [-U] [-m] [-o] [-1] [-M] [-Y <i>keydb-pwd</i>] [-Y <i>keydb-pwd-file</i>] <i>ServerRoot</i>/slapd-serverID/db2ldif.pl [-v] -D <i>rootDN</i> {-w <i>password</i> -w - -j <i>filename</i>} {-n <i>backend_instance</i>}* {-s <i>includesuffix</i>}* [{-x <i>excludesuffix</i>}*] [-a <i>outfile</i>] [-N] [-r] [-C] [-u] [-U] [-m] [-o] [-1] [-M] [-Y <i>keydb-pwd</i>] [-Y <i>keydb-pwd-file</i>] </pre>
DESCRIPTION	<p>The <code>db2ldif-task</code> command creates an entry in the directory that launches the dynamic task of exporting the contents of a database to LDIF. The entry is generated based upon the values you provide for each option. The * indicates that multiple occurrences are allowed. Directory Server must be running for this tool to work and you must specify either <code>-n backend_instance</code> or <code>-s includesuffix</code> for this tool to work.</p>
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none"> -a File name of the output LDIF file. -C Only the main database file is used. -D User DN with root permissions, such as Directory Manager -j Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified the <code>-w</code> option must not be specified. -1 For reasons of backward compatibility, omits leading version: 1 indication in LDIF output. -m Minimal base64 encoding. -M Output LDIF is stored in multiple files. -n Name of database to be exported. -N Specifies that entry IDs are not to be included in the LDIF output. -o Output LDIF to be stored in one file by default with each <i>instance</i> in <i>instance_outfile</i>. -r Exports replication information. Use this option when replication is configured and the generated LDIF will be used to initialize another replica or as a backup. Use <code>db2ldif-task</code> as opposed to <code>db2ldif</code> if you have another <code>slapd</code> process running. -s Suffix(es) to be included. If used in conjunction with the <code>-n</code> option, this option specifies the subtree(s) to be included. When exporting suffixes split across multiple backends, you must export each subsuffix separately. With the <code>-s suffix</code> option, Directory Server exports only those entries in the backend containing the <i>suffix</i> entry.

- u Request that the unique id is not exported.
- U Request that the output LDIF is not folded.
- v Verbose mode
- w Password associated with the user DN. If you do not specify this option anonymous access is used. If you specify -w -, the utility prompts for the password. If either -w option is specified, the -j option must not be specified. For example, -wdiner892.
- x Suffix(es) to be excluded.
- Y Specifies the file in which the password for the key database is held, also used when handling encrypted attributes.
- Y Specifies the password for the key database, providing a means of authentication required by Directory Server when handling encrypted attributes.

EXIT STATUS The following exit values are returned:

- 0 Successful completion.
- 1 An error occurred.

Otherwise check logs for further information.

db2ldif-task(1M)

NAME	db2ldif-task, db2ldif.pl – export the contents of a database to LDIF
SYNOPSIS	<pre>directoryserver [{-s -server} server-instance] db2ldif-task [-v] -D <i>rootDN</i> {-w <i>password</i> -w - -j <i>filename</i>} {-n <i>backend_instance</i>}* {-s <i>includesuffix</i>}* [{-x <i>excludesuffix</i>}*] [-a <i>outfile</i>] [-N] [-r] [-C] [-u] [-U] [-m] [-o] [-1] [-M] [-Y <i>keydb-pwd</i>] [-Y <i>keydb-pwd-file</i>] <i>ServerRoot</i>/slapd-serverID/db2ldif.pl [-v] -D <i>rootDN</i> {-w <i>password</i> -w - -j <i>filename</i>} {-n <i>backend_instance</i>}* {-s <i>includesuffix</i>}* [{-x <i>excludesuffix</i>}*] [-a <i>outfile</i>] [-N] [-r] [-C] [-u] [-U] [-m] [-o] [-1] [-M] [-Y <i>keydb-pwd</i>] [-Y <i>keydb-pwd-file</i>]</pre>
DESCRIPTION	The db2ldif-task command creates an entry in the directory that launches the dynamic task of exporting the contents of a database to LDIF. The entry is generated based upon the values you provide for each option. The * indicates that multiple occurrences are allowed. Directory Server must be running for this tool to work and you must specify either -n backend_instance or -s includesuffix for this tool to work.
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none">-a File name of the output LDIF file.-C Only the main database file is used.-D User DN with root permissions, such as Directory Manager-j Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified the -w option must not be specified.-1 For reasons of backward compatibility, omits leading version: 1 indication in LDIF output.-m Minimal base64 encoding.-M Output LDIF is stored in multiple files.-n Name of database to be exported.-N Specifies that entry IDs are not to be included in the LDIF output.-o Output LDIF to be stored in one file by default with each instance in instance_outfile.-r Exports replication information. Use this option when replication is configured and the generated LDIF will be used to initialize another replica or as a backup. Use db2ldif-task as opposed to db2ldif if you have another slapd process running.

- s Suffix(es) to be included. If used in conjunction with the -n option, this option specifies the subtree(s) to be included. When exporting suffixes split across multiple backends, you must export each subsuffix separately. With the -s *suffix* option, Directory Server exports only those entries in the backend containing the *suffix* entry.
- u Request that the unique id is not exported.
- U Request that the output LDIF is not folded.
- v Verbose mode
- w Password associated with the user DN. If you do not specify this option anonymous access is used. If you specify -w -, the utility prompts for the password. If either -w option is specified, the -j option must not be specified. For example, -wdiner892.
- x Suffix(es) to be excluded.
- Y Specifies the file in which the password for the key database is held, also used when handling encrypted attributes.
- Y Specifies the password for the key database, providing a means of authentication required by Directory Server when handling encrypted attributes.

EXIT STATUS The following exit values are returned:

- 0 Successful completion.
- 1 An error occurred.

Otherwise check logs for further information.

directoryserver(1M)

NAME	directoryserver – front end for Directory Server (DS)
SYNOPSIS	<pre>/usr/sbin/directoryserver { -getdefaultversion -g } /usr/sbin/directoryserver { -listversions -l } /usr/sbin/directoryserver { -setdefaultversion -d } <i>version</i> /usr/sbin/directoryserver { -useversion -u } <i>version subcommand</i> {...} /usr/sbin/directoryserver help [<i>subcommand</i>] /usr/sbin/directoryserver [configure] [-<i>fconfiguration_file</i>] /usr/sbin/directoryserver [unconfigure] [-<i>fconfiguration_file</i>] /usr/sbin/directoryserver [{-s -server} <i>server-instance</i>] {start stop restart} /usr/sbin/directoryserver { start-admin stop-admin restart-admin startconsole } /usr/sbin/directoryserver { magt sagt } {...} /usr/sbin/directoryserver { -s -server } <i>server-instance</i> { monitor saveconfig restoreconfig db2index-task ldif2db-task ldif2db ldif2ldap vlvindex db2ldif db2ldif-task db2bak db2bak-task bak2db bak2db-task suffix2instance account-status account-activate account-inactivate } {...} /usr/sbin/directoryserver <i>nativetoascii</i> <i>admin_ip</i> <i>ldif</i> <i>pwdhash</i> <i>idsktune</i> <i>mmldif</i> {...}</pre>
DESCRIPTION	<p>The <code>directoryserver</code> command is a comprehensive, front end to the utility programs provided by the Solaris Directory Server (DS).</p> <p>Options for the <code>directoryserver</code> command itself must appear before the subcommand. Arguments for a subcommand must appear after the subcommand. Subcommands have specific arguments. See SUBCOMMANDS.</p> <p>When managing multiple versions of Directory Server, use the appropriate option to identify the version to which the command applies. By default Directory Server operates using the most recent version. The <code>-useversion</code> option allows you to select which version you wish to use. When multiple versions of Directory Server are installed, the initial default version is the first version installed.</p>
SUBCOMMANDS	<p>The following subcommands are supported:</p> <p><code>account-inactivate</code> <i>args</i> Inactivates and locks an entry or group of entries.</p> <p><code>account-activate</code> <i>args</i> Activates an entry or group of entries.</p>

account-status *args*

Provides account status information to establish whether an entry or group of entries is inactivated or not.

admin_ip *args*

Deprecated subcommand. Use the Server Console to update the local Administration Server configuration file and configuration directory instead. When your computer system's IP address changes, you must change to the new IP address, as failing to do so would prevent you from being able to start Administration Server.

bak2db *args*

Restore the database from the most recent archived backup. Directory Server must be stopped for this tool to work.

bak2db-task *args*

Restore the data to the database.

configure *args*

Configure an instance of Directory Server.

The `configure` subcommand has two modes of operation. You can invoke it with a curses-based interaction to gather input. Alternatively, you can provide input in a configuration file using the `-f` option, which requires the `DISPLAY` environment variable to be set.

The `configure` subcommand supports the following arguments:

`-f` *configuration_file*

Specifies the configuration file for silent installation.

db2bak *args*

Create a backup of the current database contents. This command can be executed with the server either running or not.

db2bak-task *args*

Create a backup of the current database contents. Directory Server must be running to execute this command.

db2index-task *args*

Create and generate the new set of indexes to be maintained following the modification of indexing entries in the `cn=config` configuration file.

db2ldif *args*

Export the contents of the database to LDIF. You must specify either the `-n` or the `-s` option or both. This tool can be executed while the server is still running.

db2ldif-task *args*

Export the contents of the database to LDIF. To run this subcommand the server must be running and either the `-n` *backend_instance* or the `-s` *includesuffix* option is required.

directoryserver(1M)

help [*subcommand*]

Display `directoryserver` usage message or subcommand specific usage message. To obtain a usage message for the `directoryserver` command itself, type `directoryserver help` and to obtain a usage message for a `directoryserver` subcommand, type `directoryserver subcommand help`.

idsktune *args*

Provide an easy and reliable way of checking the patch levels and kernel parameter settings for your system. You must install Directory Server before you can run `idsktune`. It gathers information about the operating system, kernel, and TCP stack to make tuning recommendations.

For information regarding the arguments supported by the `idsktune` command see: `idsktune(1)`.

ldif2db *args*

Import directory contents from LDIF. To run this tool Directory Server must be stopped.

ldif2db-task *args*

Import data to the directory. The server must be running when you run this subcommand.

ldif *args*

Format LDIF files, and create base 64 encoded attribute values. With base 64 encoding you can represent binary data, such as a JPEG image, in LDIF. You identify base 64 encoded data by using the `::` symbol. The `ldif` subcommand takes any input and formats it with the correct line continuation and appropriate attribute information. The subcommand also senses whether the input requires base 64 encoding.

ldif2ldap *args*

Perform an import operation over LDAP to Directory Server. To run the `ldif2ldap` subcommand the server must be running.

magt

Deprecated subcommand. See/use the `mpsadmserver(1m)` `magt` subcommand instead.

monitor

Retrieve performance monitoring information using the `ldapsearch` command-line utility.

mmldif *args*

Combine multiple LDIF files into a single authoritative set of entries. Typically each LDIF file is from a master server cooperating in a multi master replication agreement (e.g. masters that refuse to sync up for whatever reason). Optionally, it can generate LDIF change files that could be applied to the original to bring it up to date with the authoritative. At least two input files must be specified.

nativetoascii

Subcommand is no longer supported. Use `iconv(1M)` instead.

pwdhash *args*

Print the encrypted form of a password using one of the server's encryption algorithms. If a user cannot log in, you can use this script to compare the user's password to the password stored in the directory.

restart

Restart Directory Server. All instances are started by default. With the *-s* option, you can specify the instance to be restarted.

restart-admin

Deprecated subcommand. See/use the `mpsadmserver(1m)` `restart-admin` subcommand instead.

restoreconfig

Restore the most recently saved Directory Server configuration information. This subcommand overrides the content under `/ServerRoot/slapd-serverID/config` with the data from `/ServerRoot/slapd-serverID/confbak`

sagt

Deprecated subcommand. See/use the `mpsadmserver(1m)` `sagt` subcommand instead.

saveconfig

Save the Directory Server configuration information to the `/ServerRoot/slapd-serverID/confbak` directory. Directory Server must be running for this tool to work.

start

Start Directory Server. All instances are started by default. With the *-s* option, you can specify the instance to be restarted.

start-admin

Deprecated subcommand. See/use the `mpsadmserver(1m)` `start-admin` subcommand instead.

startconsole

Deprecated subcommand. See/use the `mpsconsole(1m)` `startconsole` subcommand instead.

stop

Stop Directory Server.

With the *-s* option, you can specify the instance to be stopped.

stop-admin

Deprecated subcommand. See/use the `mpsadmserver(1m)` `stop-admin` subcommand instead.

suffix2instance *{-s suffix}*

Map a suffix to a database.

Specify *-s suffix* as the suffix to be mapped to the database.

directoryserver(1M)

unconfigure *args*

Removes all Directory Server instances and configuration, including any changes made following configuration.

The `unconfigure` subcommand has two modes of operation. You can invoke it with a GUI-based interaction to gather input. Alternatively, you can provide input in a configuration file using the `-f` option.

The `unconfigure` subcommand supports the following arguments:

`-f configuration_file`

Specifies the configuration file for silent installation.

vlvindex *args*

Create virtual list view (VLV) indexes, known in the Directory Server Console as Browsing Indexes. The server must be stopped beforehand.

OPTIONS

Options for the `directoryserver` command itself must appear before the subcommand argument.

The following options are supported:

`-getdefaultversion`

`-g`

Display the version of Directory Server managed and the path to the `directoryserver` command used when no version is specified.

`-listversions`

`-l`

Display all versions of Directory Server that can be managed with the `directoryserver`.

`-setdefaultversion version`

`-d version`

Set the version of Directory Server managed when no version is specified. *version* must be of the form displayed when the `-listversions` option is used.

`-s server-instance`

`-server server-instance`

The server instance name. Specify the Directory Server instance to process the command against. For some of the listed subcommands the server instance is optional and for other sub commands it is a required option.

`-useversion version subcommand {...}`

`-u version subcommand {...}`

Use the version of Directory Server specified to perform the subcommand using the arguments specified. *version* must be of the form displayed when the `-listversions` option is used.

EXAMPLES

EXAMPLE 1 Starting All Instances of Directory Server

The following command starts all the instances of Directory Server:

```
example% directoryserver start
```

EXAMPLE 2 Starting the Instances of myhost of Directory Server

The following command starts the instances of myhost of Directory Server.

```
example% directoryserver -s myhost start
```

EXAMPLE 3 Running the Monitor Tool and Outputting the Current Status

The following command runs the monitor tool and outputs the current status of the ephesus directory instance.

```
example% directoryserver -s ephesus monitor
```

EXAMPLE 4 Running the idsktune Tool and Outputting Performance Tuning Information

The following command runs the idsktune tool and outputs performance tuning information:

```
example% directoryserver idsktune
```

EXAMPLE 5 Configuring a Specific Version

Configure Directory Server 5.2 when 5.1 is also installed.

```
example% directoryserver -u 5.2 configure
```

EXAMPLE 6 Identifying the Default Version

Check the version managed and `directoryserver` command used when no version is specified.

```
example% directoryserver -g
Default is: 5.2:/usr/ds/v5.2/sbin/directoryserver
```

The path to the command used is provided for debugging purposes only. Do not use such paths in your scripts.

EXAMPLE 7 Setting the Default Version

Make Directory Server 5.2 the version managed when no version information is specified.

```
example% directoryserver -d 5.2
```

EXAMPLE 8 Stop a 5.1 Instance When 5.2 Is the Default Version

This example shows that when 5.2 is the default version, you can still manage Directory Server 5.1 instances. The 5.1 instance in this example is named `dirserv`.

```
example% directoryserver -g
Default is: 5.2:/usr/ds/v5.2/sbin/directoryserver
example% directoryserver -u 5.1 stop -s dirserv
```

directoryserver(1M)

EXIT STATUS The following exit values are returned:

0 Successful completion.

non-zero An error occurred.

ATTRIBUTES See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Stable

SEE ALSO `mpsadmserver(1M)`

Directory Server Administration Guide

Directory Server Administration Reference

NAME	ldif2db – import directory contents from an LDIF file
SYNOPSIS	<pre> directoryserver [{-s -server} server-instance] ldif2db -n <i>backend_instance</i> {-s <i>includesuffix</i>}* [{-x <i>excludesuffix</i>}*] {-i <i>ldif-file</i>}* [-O] [-Y <i>keydb-pwd</i>] [-Y <i>keydb-pwd-file</i>] <i>ServerRoot</i>/slapd-serverID ldif2db -n <i>backend_instance</i> {-s <i>includesuffix</i>}* [{-x <i>excludesuffix</i>}*] {-i <i>ldif-file</i>}* [-O] [-Y <i>keydb-pwd</i>] [-Y <i>keydb-pwd-file</i>] </pre>
DESCRIPTION	The <code>ldif2db</code> command imports directory contents from LDIF. To run this tool Directory Server must be stopped.
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none"> -i File name of the input ldif file(s). When you import multiple files, they are imported in the order in which you specify them on the command line. -n Name of database to be imported. Ensure that you specify a database name that corresponds to the suffix contained by the LDIF file. Otherwise the data contained by the database is deleted and the import fails. -O Requests that only the core database is created without attribute indexes. -s Suffixes to be included. If used in conjunction with the -n option, this option specifies the subtree(s) to be included. When importing suffixes split across multiple backends, you must import each subsuffix separately. With the -s <i>suffix</i> option, Directory Server imports only those entries in the backend containing the <i>suffix</i> entry. -x Suffix(es) to be excluded. -Y Specifies the file in which the password for the key database is held, also used when handling encrypted attributes. -Y Specifies the password for the key database, providing a means of authentication required by Directory Server when handling encrypted attributes.
NOTES	<ol style="list-style-type: none"> 1. <code>ldif2db</code> supports LDIF version 1 specifications. You can load an attribute using the <code><URL</code> specifier notation. For example: <pre>jpegphoto:< file:///tmp/myphoto.jpg</pre> Although the official notation requires three <code>///</code>, the use of one <code>/</code> is tolerated. 2. The default behavior of a read-write replica that has been initialized either online or offline from a backup or an LDIF file, is NOT to accept client update requests. The replica will remain in read-only mode and refer any updated operations to other suppliers in the topology until the administrator does one of the following:

ldif2db(1M)

- changes the duration of the read-only mode default period using the `ds5referralDelayAfterInit` attribute
- manually resets the server to read-write mode using the `ds5BeginReplicaAcceptUpdates` attribute (once the replica has completely converged with the other supplier in the topology)

The second option is advised because it does not present non-convergence risks.

You must specify either the `-n` or the `-s` option (or both), and the `-i` option. When identifying hosts, you must use either symbolic names or IP addresses for all hosts. Using a combination of the two can cause problems.

EXIT STATUS The following exit values are returned:

0 Successful completion.

Otherwise check logs for further information.

ATTRIBUTES See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `ldif2db-task(1M)`, `ldif2db.pl(1M)`, `db2ldif(1M)`, `mmldif(1)`, `start-slapd(1M)`, `stop-slapd(1M)`, `restart-slapd(1M)`

NAME	ldif2db-task, ldif2db.pl – import directory contents from LDIF
SYNOPSIS	<pre> directoryserver [{-s -server} <i>server-instance</i>] ldif2db-task [-v] -D <i>rootDN</i> {-w <i>password</i> -w - -j <i>filename</i>} -n <i>backend_instance*</i> {-s <i>includesuffix</i>}* [{-x <i>excludesuffix</i>}*] [-c <i>size</i>] [-O] [-g [<i>string</i>]] [-G <i>namespace_id</i>] [{-i <i>filename</i>}*] <i>ServerRoot</i>/slapd-serverID/ldif2db.pl [-v] -D <i>rootDN</i> {-w <i>password</i> -w - -j <i>filename</i>} -n <i>backend_instance*</i> {-s <i>includesuffix</i>}* [{-x <i>excludesuffix</i>}*] [-c <i>size</i>] [-g [<i>string</i>]] [-G <i>namespace_id</i>] [{-i <i>filename</i>}*] </pre>
DESCRIPTION	<p>The <code>ldif2db-task</code> command creates an entry in the directory that launches the dynamic task of importing the directory from LDIF. The entry is generated based upon the values you provide for each option. Directory Server must be running for this tool to work.</p>
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none"> -c Merge chunk size. -D User DN with root permissions, such as Directory Manager. -g Generation of a unique ID. Type <code>none</code> for no unique ID to be generated and <code>deterministic</code> for the generated unique ID to be name-based. By default a time-based unique ID is generated. <p>If you use the <code>deterministic</code> generation to have a name-based unique ID, you can also specify the namespace you want the server to use as follows:</p> <pre>-g deterministic <i>namespace_id</i></pre> <p>Use this option if you want to import the same LDIF file into two different Directory Servers, and if you want the contents of both directories to have the same set of unique IDs. If unique IDs already exist in the LDIF file you are importing, then the existing IDs are imported to the server regardless of the options you have specified.</p> <ul style="list-style-type: none"> -G Specify the namespace you want the server to use. -i File name of the input ldif file(s). When you import multiple files, they are imported in the order in which you specify them on the command line. -j Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified the <code>-w</code> option must not be specified. -n Database backend to be exported.

ldif2db.pl(1M)

- O Request that only the core database is created without attribute indexes.
- s Suffix(es) to be included. If used in conjunction with the -n option, this option specifies the subtree(s) to be included.

When exporting suffixes split across multiple backends, you must export each subsuffix separately. With the -s *suffix* option, Directory Server exports only those entries in the backend containing the *suffix* entry.
- v Verbose mode.
- w Password associated with the user DN. If you do not specify this option anonymous access is used. If you specify -w -, the utility prompts for the password. If either -w option is specified, the -j option must not be specified. For example, -wdiner892.
- x Suffix(es) to be excluded.

EXIT STATUS The following exit values are returned:

- 0 Successful completion.
- 1 An error occurred.

Otherwise check logs for further information.

ATTRIBUTES See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `ldif2db(1M)`, `(1M)`, `mmldif(1)`, `db2ldif(1M)`, `start-slapd(1M)`, `stop-slapd(1M)`, `restart-slapd(1M)`

NAME	ldif2db-task, ldif2db.pl – import directory contents from LDIF
SYNOPSIS	<pre> directoryserver [{-s -server} <i>server-instance</i>] ldif2db-task [-v] -D <i>rootDN</i> {-w <i>password</i> -w - -j <i>filename</i>} -n <i>backend_instance*</i> {-s <i>includesuffix</i>}* [{-x <i>excludesuffix</i>}*] [-c <i>size</i>] [-O] [-g [<i>string</i>]] [-G <i>namespace_id</i>] [{-i <i>filename</i>}*] <i>ServerRoot</i>/slapd-serverID/ldif2db.pl [-v] -D <i>rootDN</i> {-w <i>password</i> -w - -j <i>filename</i>} -n <i>backend_instance*</i> {-s <i>includesuffix</i>}* [{-x <i>excludesuffix</i>}*] [-c <i>size</i>] [-g [<i>string</i>]] [-G <i>namespace_id</i>] [{-i <i>filename</i>}*] </pre>
DESCRIPTION	<p>The <code>ldif2db-task</code> command creates an entry in the directory that launches the dynamic task of importing the directory from LDIF. The entry is generated based upon the values you provide for each option. Directory Server must be running for this tool to work.</p>
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none"> -c Merge chunk size. -D User DN with root permissions, such as Directory Manager. -g Generation of a unique ID. Type <code>none</code> for no unique ID to be generated and <code>deterministic</code> for the generated unique ID to be name-based. By default a time-based unique ID is generated. <p>If you use the <code>deterministic</code> generation to have a name-based unique ID, you can also specify the namespace you want the server to use as follows:</p> <pre>-g deterministic <i>namespace_id</i></pre> <p>Use this option if you want to import the same LDIF file into two different Directory Servers, and if you want the contents of both directories to have the same set of unique IDs. If unique IDs already exist in the LDIF file you are importing, then the existing IDs are imported to the server regardless of the options you have specified.</p> <ul style="list-style-type: none"> -G Specify the namespace you want the server to use. -i File name of the input ldif file(s). When you import multiple files, they are imported in the order in which you specify them on the command line. -j Specifies the file from which the bind password is read. Used for simple authentication. If this option is specified the <code>-w</code> option must not be specified. -n Database backend to be exported.

ldif2db-task(1M)

- O Request that only the core database is created without attribute indexes.
- s Suffix(es) to be included. If used in conjunction with the -n option, this option specifies the subtree(s) to be included.

When exporting suffixes split across multiple backends, you must export each subsuffix separately. With the -s *suffix* option, Directory Server exports only those entries in the backend containing the *suffix* entry.
- v Verbose mode.
- w Password associated with the user DN. If you do not specify this option anonymous access is used. If you specify -w -, the utility prompts for the password. If either -w option is specified, the -j option must not be specified. For example, -wdiner892.
- x Suffix(es) to be excluded.

EXIT STATUS The following exit values are returned:

- 0 Successful completion.
- 1 An error occurred.

Otherwise check logs for further information.

ATTRIBUTES See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `ldif2db(1M)`, `(1M)`, `mmldif(1)`, `db2ldif(1M)`, `start-slapd(1M)`, `stop-slapd(1M)`, `restart-slapd(1M)`

NAME	ldif2ldap – perform an import operation over LDAP to Directory Server
SYNOPSIS	<pre> directoryserver [{-s -server} server-instance] ldif2ldap -D <i>rootDN</i> -w <i>password</i> -f <i>filename</i> <i>ServerRoot/slaped-serverID/ldif2ldap</i> -D <i>rootDN</i> -w <i>password</i> -f <i>filename</i> </pre>
DESCRIPTION	The ldif2ldap command performs an import operation over LDAP to Directory Server. Directory Server must be running for this tool to work.
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none"> -D User DN with root permissions such as Directory Manager. -f File name of the file to be imported. -w Password associated with the user DN.
EXIT STATUS	<p>The exit status returned reflects the return values of the underlying functions used, which may depend on return values sent by the server. The return values are defined through <ldap.h> files both on the client side and on the server side. Common exit status codes follow:</p> <ul style="list-style-type: none"> 0 Successful completion; LDAP_OPERATIONS_ERROR; 0x00. 1 Server encountered errors while processing the request; LDAP_OPERATIONS_ERROR; 0x01. 2 Server encountered errors, such as a BER-decoding error, while processing the request; LDAP_PROTOCOL_ERROR; 0x02. 10 Base DN belongs to an entry handled by neither server, and the referral URL identifies another server that handles the entry; LDAP_REFERRAL; 0x0a. 16 Attribute to be modified does not exist; LDAP_NO_SUCH_ATTRIBUTE; 0x10. 19 Attribute modification requested is not a proper modification. For example, a requested change to userpassword would result in a user password shorter than the minimum length allowed; LDAP_CONSTRAINT_VIOLATION; 0x13. 20 Attribute to add already exists with the specified value; LDAP_TYPE_OR_VALUE_EXISTS; 0x14. 21 In response to a request to modify directory schema, the requested modification includes no object class or attribute type specification; LDAP_INVALID_SYNTAX; 0x15. 32 Base DN belongs to an entry handled by neither server, and no referral URL is available for the entry; LDAP_NO_SUCH_OBJECT; 0x20. 50 Bind DN user does not have permission to read the entry from the directory; LDAP_INSUFFICIENT_ACCESS; 0x32.

ldif2ldap(1M)

- 53 Directory is read-only; LDAP_UNWILLING_TO_PERFORM; 0x35.
- 65 Requested modification would cause the entry not to comply with the directory schema; LDAP_OBJECT_CLASS_VIOLATION; 0x41.
- 67 Requested modification would cause the entry to be missing attributes that are components of the entry DN; LDAP_NOT_ALLOWED_ON_RDN; 0x43.
- 68 An entry already exists with the same DN as the entry to add; LDAP_ALREADY_EXISTS; 0x44.
- 81 One of the directories did not respond to the request, or the connection was lost; LDAP_SERVER_DOWN; 0x51.
- 82 An error occurred while receiving results; LDAP_LOCAL_ERROR; 0x52.
- 83 The request could not be BER-encoded; LDAP_ENCODING_ERROR; 0x53.
- 84 A result could not be decoded; LDAP_DECODING_ERROR; 0x54.
- 89 An option or argument is not valid; LDAP_PARAM_ERROR; 0x59.
- 90 Needed memory could not be allocated; LDAP_NO_MEMORY; 0x5a.
- 91 A specified host name or port is not valid; LDAP_CONNECT_ERROR; 0x5b.
- 92 At least one server supports only LDAPv2, and the -v 2 option was not used; LDAP_NOT_SUPPORTED; 0x5c.

ATTRIBUTES See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `ldif2db(1M)`, `ldif2db-task(1M)`, `ldapmodify(1)`

NAME	migrateinstance5 – migrates data, configuration, and schema to a new Directory Server instance
SYNOPSIS	migrateinstance5 -D <i>rootDN</i> { -w <i>password</i> -w - -j <i>filename</i> } -p <i>port</i> -o <i>oldInstancePath</i> -n <i>newInstancePath</i> [-t <i>tracelevel</i>] [-L <i>logfile</i>] [-noinput]
DESCRIPTION	The migrateInstance5 command migrates database content, configuration data, and schema from a Directory Server instance created using an earlier version of the product to a Directory Server instance using the current version of the product. Both instances must be installed on the same host system. For further information regarding the migration process, see <i>Directory Server Installation and Migration Guide</i> .
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none"> -D New 5.x Directory Server user DN with root permissions, such as Directory Manager. -j Specifies the file from which the new 5.x bind password is read. Used for simple authentication. If this option is specified, the -w option must not be specified. -L File in which to log the migration report. By default the migration report is stored under <i>ServerRoot/slapd-serverID/logs/Migration_ddmmyyyy_hhmmss.log</i> A sample log might contain: <i>ServerRoot/slapd-serverID/logs/Migration_20022004_153604.log</i> for a log created on 20 February 2004 at 15:36:04. -n Path to the new Directory Server instance. -noinput No user interventions during migration processing to solve conflicts. -o Path to the old Directory Server instance. -p New 5.x Directory Server port. -t Trace level of either 0 (no trace) or 1 (trace). The default level is 1. -w New 5.x password associated with the user DN. If you do not specify this option anonymous access is used. If you specify -w -, the utility prompts for the password. If either -w option is specified, the -j option must not be specified. For example, -wdiner892.
EXIT STATUS	<p>The following exit values are returned:</p> <ul style="list-style-type: none"> 0 Successful completion. 1 An error occurred.

migrateinstance5(1M)

ATTRIBUTES See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

NOTES `migrateInstance5` is implemented as a perl script, despite the fact that it does not have the `.pl` extension.

Before performing the migration, check that the user-defined variables contain the following associated values:

```
PERL5LIB ServerRoot/bin/slapd/admin/bin
```

```
PATH ServerRoot/bin/slapd/admin/bin
```


NAME	ns-ldapagt – starts a Directory Server SNMP subagent						
SYNOPSIS	<code>/usr/ds/v5.2/bin/slapd/server/ns-ldapagt -d run-dir [-v] [-V] [-D]</code>						
DESCRIPTION	The <code>ns-ldapagt</code> command is used to start a Directory Server SNMP subagent. For more information on configuring an SNMP subagent, refer to the <i>Directory Server Administration Guide</i> .						
OPTIONS	The following options are supported: <ul style="list-style-type: none"> -d <i>run-dir</i> The path to the Directory Server instance. -D Specifies that the subagent should be started in debug mode. -v Indicates the version of Directory Server that is installed. -V Provides additional version information on the Directory Server, including system information and plug-in versions. 						
EXAMPLES	<p>EXAMPLE 1 Start the SNMP subagent in debug mode</p> <pre>% cd /usr/ds/v5.2/bin/slapd/server % ./ns-ldapagt -d /var/ds/v5.2/slapd-serverID/ -D</pre>						
EXIT STATUS	The following exit values are returned: <ul style="list-style-type: none"> 0 Successful completion. 1 An error occurred. 						
ATTRIBUTES	See <code>attributes(5)</code> for descriptions of the following attributes:						
	<table border="1"> <thead> <tr> <th>ATTRIBUTE TYPE</th> <th>ATTRIBUTE VALUE</th> </tr> </thead> <tbody> <tr> <td>Availability</td> <td>SUNWdsvu</td> </tr> <tr> <td>Stability Level</td> <td>Committed Private</td> </tr> </tbody> </table>	ATTRIBUTE TYPE	ATTRIBUTE VALUE	Availability	SUNWdsvu	Stability Level	Committed Private
ATTRIBUTE TYPE	ATTRIBUTE VALUE						
Availability	SUNWdsvu						
Stability Level	Committed Private						
SEE ALSO	<code>magt(1M)</code> , <code>sagt(1M)</code> , <code>mpsadmserver(1M)</code>						
NOTES	Before the <code>ns-ldapagt</code> command can be run, the SNMP master agent must be configured and running.						

restart(1M)

NAME restart – restart Directory Server

SYNOPSIS `directoryserver [{-s|-server} server-instance] restart`
`ServerRoot/slaped-serverID/restart-slaped`

DESCRIPTION The restart command restarts Directory Server.

OPTIONS There are no options for the restart command.

EXIT STATUS The following exit values are returned:

0 Server restarted successfully.

1 Server could not be restarted.

ATTRIBUTES See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `restart-slaped(1M)`, `stop(1M)`, `start(1M)`, `scswitch(1M)`

NOTES The exit status information returned in a cluster-enabled environment is managed by the Sun Cluster `scswitch` command, and not by the Directory Server `restart` command. If the server does not restart successfully in a cluster-enabled environment, see the Sun Cluster `scswitch(1M)` man page to obtain non-zero exit status information.

NAME restart-slapd – restart Directory Server

SYNOPSIS *ServerRoot*/**slapd-serverID**/**restart-slapd**

DESCRIPTION The `restart-slapd` command restarts Directory Server.

OPTIONS There are no options for the `restart-slapd` command.

EXIT STATUS The following exit values are returned:

0 Server restarted successfully.

1 Server could not be restarted.

ATTRIBUTES See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `restart(1M)`, `stop(1M)`, `start(1M)`, `scswitch(1M)`

NOTES The exit status information returned in a cluster-enabled environment is managed by the Sun Cluster `scswitch` command, and not by the Directory Server `restart-slapd` command. If the server does not restart successfully in a cluster-enabled environment, see the Sun Cluster `scswitch(1M)` man page to obtain non-zero exit status information.

restoreconfig(1M)

NAME restoreconfig – restore the most recently saved Directory Server configuration

SYNOPSIS **directoryserver** [{-s|-server} *server-instance*] **restoreconfig**
ServerRoot/**slapd-serverID**/**restoreconfig**

DESCRIPTION The restoreconfig command restores the most recently saved Directory Server configuration information. This command overrides the content stored under:
ServerRoot/*slapd-serverID*/*config* with the data under
ServerRoot/*slapd-serverID*/*confbak*

To restore the configuration:

1. Stop Directory Server
2. Run `directoryserver restoreconfig`
3. Restart Directory Server
4. Restart Administration Server for the changes to be taken into account.

OPTIONS There are no options for the restoreconfig command.

EXIT STATUS The following exit values are returned:

0 Successful completion.

1 An error occurred.

ATTRIBUTES See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `saveconfig(1M)`, `directoryserver(1M)`, `stop(1M)`, `start(1M)`, `restart-admin(1M)`

- NAME** | saveconfig – save the Directory Server configuration information
- SYNOPSIS** | **directoryserver** [{-s|-server} server-instance] **saveconfig**
ServerRoot/**slapd-serverID**/**saveconfig**
- DESCRIPTION** | The **saveconfig** command saves the Directory Server configuration information to the following directory:
ServerRoot/*slapd-serverID*/*confbak*
 Directory Server must be running for this tool to work.
- OPTIONS** | There are no options for the **saveconfig** command.
- ATTRIBUTES** | See **attributes(5)** for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

- SEE ALSO** | **restoreconfig(1M)**, **directoryserver(1M)**, **start(1M)**, **restart(1M)**

schema_push.pl(1M)

- NAME** | schema_push.pl – ensure manually modified schema are replicated to consumers
- SYNOPSIS** | *ServerRoot*/**slapd-serverID**/**schema_push.pl**
- DESCRIPTION** | When schema modifications are made manually (by editing the .ldif files directly), the `schema_push.pl` command should be run to update the modification time used by replication. This ensures that the modified schema are replicated to the consumers. Once the script has been run, you must restart the server to trigger the schema replication.
- OPTIONS** | There are no options for the `schema_push.pl` command.
- ATTRIBUTES** | See `attributes(5)` for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

- SEE ALSO** | `directoryserver(1M)`, `restart(1M)`

NAME	start – start Directory Server
SYNOPSIS	directoryserver [{-s -server} server-instance] start ServerRoot/slapd-serverID/start-slapd
DESCRIPTION	The <code>start</code> command starts Directory Server.
OPTIONS	There are no options for the <code>start</code> command.
EXIT STATUS	The following exit values are returned: 0 Server started successfully. 1 Server could not be started. 2 Server was already started.
ATTRIBUTES	See <code>attributes(5)</code> for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `start-slapd(1M)`, `stop(1M)`, `restart(1M)`, `scswitch(1M)`

NOTES The exit status information returned in a cluster-enabled environment is managed by the Sun Cluster `scswitch` command, and not by the Directory Server `start` command. If the server does not start successfully in a cluster-enabled environment, see the Sun Cluster `scswitch(1M)` man page to obtain non-zero exit status information.

start-slapd(1M)

NAME	start-slapd – start Directory Server
SYNOPSIS	ServerRoot/slapd-serverID/start-slapd
DESCRIPTION	The <code>start-slapd</code> command starts Directory Server.
OPTIONS	There are no options for the <code>start-slapd</code> command.
EXIT STATUS	The following exit values are returned: 0 Server started successfully. 1 Server could not be started. 2 Server was already started.
ATTRIBUTES	See <code>attributes(5)</code> for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO `directoryserver(1M)`, `start(1M)`, `stop(1M)`, `restart(1M)`, `scswitch(1M)`

NOTES The exit status information returned in a cluster-enabled environment is managed by the Sun Cluster `scswitch` command, and not by the Directory Server `start-slapd` command. If the server does not start successfully in a cluster-enabled environment, see the Sun Cluster `scswitch(1M)` man page to obtain non-zero exit status information.

NAME	stop – stop Directory Server
SYNOPSIS	directoryserver [{-s -server} server-instance] stop ServerRoot/slapd-serverID/stop-slapd
DESCRIPTION	The stop command stops Directory Server.
OPTIONS	There are no options for the stop command.
EXIT STATUS	The following exit values are returned: 0 Server stopped successfully. 1 Server could not be stopped. 2 Server was already stopped.
ATTRIBUTES	See attributes(5) for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO [directoryserver\(1M\)](#), [stop-slapd\(1M\)](#), [start\(1M\)](#), [restart\(1M\)](#), [scswitch\(1M\)](#)

NOTES The exit status information returned in a cluster-enabled environment is managed by the Sun Cluster `scswitch` command, and not by the Directory Server `stop` command. If the server does not stop successfully in a cluster-enabled environment, see the Sun Cluster `scswitch(1M)` man page to obtain non-zero exit status information.

stop-slapd(1M)

NAME	stop-slapd – stop Directory Server
SYNOPSIS	directoryserver [{-s -server} server-instance] stop ServerRoot/slapd-serverID/stop-slapd
DESCRIPTION	The stop-slapd command stops Directory Server.
OPTIONS	There are no options for the stop-slapd command.
EXIT STATUS	The following exit values are returned: 0 Server stopped successfully. 1 Server could not be stopped. 2 Server was already stopped.
ATTRIBUTES	See attributes(5) for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

SEE ALSO directoryserver(1M), stop(1M), start(1M), restart(1M), scswitch(1M)

NOTES The exit status information returned in a cluster-enabled environment is managed by the Sun Cluster scswitch command, and not by the Directory Server stop-slapd command. If the server does not stop successfully in a cluster-enabled environment, see the Sun Cluster scswitch(1M) man page to obtain non-zero exit status information.

NAME suffix2instance – map a suffix to a database

SYNOPSIS **directoryserver** [{-s|-server} server-instance] **suffix2instance**
 {-s suffix}
 ServerRoot/**slapd-serverID/suffix2instance** {-s suffix}

DESCRIPTION The **suffix2instance** command maps a suffix to a database.

OPTIONS The following options are supported:
 -s *suffix* The suffix to be mapped to the database.

EXIT STATUS The following exit values are returned:
 0 Successful completion.
 Otherwise check logs for further information.

SEE ALSO **directoryserver(1M)**

ATTRIBUTES See **attributes(5)** for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWdsvu
Stability Level	Committed Private

sync-cds(1M)

NAME	sync-cds – synchronize the Directory Server product version information with the configuration directory server after upgrade						
SYNOPSIS	directoryserver sync-cds [5.2] [-f {credfile}] [-l [logfile]]						
DESCRIPTION	The <code>sync-cds</code> command synchronizes the Directory Server product version with the configuration directory server after upgrade.						
OPTIONS	<p>The following options are supported:</p> <p>-f Absolute path to the file containing bind credentials on two lines:</p> <p> Admin ID:<i>uid</i></p> <p> Admin Password:<i>password</i></p> <p> Here, <i>uid</i> is the user ID for the configuration directory server administrator user, and <i>password</i> is the corresponding password.</p> <p>5.2 Specifies 5.2. based synchronization.</p> <p>-l Absolute path to the file in which to log the synchronization operation results.</p>						
EXIT STATUS	<p>The following exit values are returned:</p> <p>0 Successful completion.</p> <p>1 Error occurred.</p>						
ATTRIBUTES	See <code>attributes(5)</code> for descriptions of the following attributes:						
	<table border="1"><thead><tr><th>ATTRIBUTE TYPE</th><th>ATTRIBUTE VALUE</th></tr></thead><tbody><tr><td>Availability</td><td>SUNWdsvu</td></tr><tr><td>Stability Level</td><td>Committed Private</td></tr></tbody></table>	ATTRIBUTE TYPE	ATTRIBUTE VALUE	Availability	SUNWdsvu	Stability Level	Committed Private
ATTRIBUTE TYPE	ATTRIBUTE VALUE						
Availability	SUNWdsvu						
Stability Level	Committed Private						
SEE ALSO	<code>directoryserver(1M)</code>						

NAME	vlvindex – create virtual list view indexes						
SYNOPSIS	<pre>directoryserver [{-s -server} server-instance] vlvindex -n backend_instance {-s suffix }* -T attribute ServerRoot/slapd-serverID/vlvindex -n backend_instance {-s suffix }* -T attribute</pre>						
DESCRIPTION	<p>The vlvindex command creates virtual list view (VLV) indexes, known in the Directory Server console as Browsing Indexes. VLV indexes introduce flexibility in the way you can view search results. Using VLV indexes, you can organize search results alphabetically or in reverse alphabetical order, and you can scroll through the list of results. VLV index configuration must already exist prior to running this tool. Directory Server must be stopped for the vlvindex command to work. For further information on configuring indexes see the <i>Directory Server Administration Guide</i>.</p>						
OPTIONS	<p>The following options are supported:</p> <ul style="list-style-type: none"> -n Name of the database containing the entries to index. -s Name of the suffix containing the entries to index -T VLV index identifier to use to create VLV indexes. You can use the console to specify a VLV index identifier for each database supporting your directory tree, as described in the <i>Sun Java(TM) System Directory Server 5.2 2004Q4 Administration Guide</i>. 						
EXIT STATUS	<p>The following exit values are returned:</p> <ul style="list-style-type: none"> 0 Successful completion. 1 An error occurred. Check logs for further information. 						
ATTRIBUTES	<p>See attributes(5) for descriptions of the following attributes:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">ATTRIBUTE TYPE</th> <th style="text-align: center;">ATTRIBUTE VALUE</th> </tr> </thead> <tbody> <tr> <td>Availability</td> <td>SUNWdsvu</td> </tr> <tr> <td>Stability Level</td> <td>Committed Private</td> </tr> </tbody> </table>	ATTRIBUTE TYPE	ATTRIBUTE VALUE	Availability	SUNWdsvu	Stability Level	Committed Private
ATTRIBUTE TYPE	ATTRIBUTE VALUE						
Availability	SUNWdsvu						
Stability Level	Committed Private						
SEE ALSO	directoryserver(1M), ldapsearch(1)						
NOTES	Either the -n backend_instance option or the -s includesuffix option must be specified.						

vlvindex(1M)
