

NAME

slapd – Stand-alone LDAP Daemon

SYNOPSIS

```
/usr/sbin/slapd [-[4|6]] [-T {acl|add|auth|cat|dn|index|passwd|test}] [-d debug-level] [-f slapd-config-file] [-F slapd-config-directory] [-h URLs] [-n service-name] [-s syslog-level] [-l syslog-local-user] [-r directory] [-u user] [-g group] [-c cookie]
```

DESCRIPTION

Slapd is the stand-alone LDAP daemon. It listens for LDAP connections on any number of ports (default 389), responding to the LDAP operations it receives over these connections. **slapd** is typically invoked at boot time, usually out of **/etc/rc.local**. Upon startup, **slapd** normally forks and disassociates itself from the invoking tty. If configured in the config file (or config directory), the **slapd** process will print its process ID (see **getpid(2)**) to a **.pid** file, as well as the command line options during invocation to an **.args** file (see **slapd.conf(5)**). If the **-d** flag is given, even with a zero argument, **slapd** will not fork and disassociate from the invoking tty.

Slapd can be configured to provide replicated service for a database with the help of **slurpd**, the standalone LDAP update replication daemon. See **slurpd(8)** for details.

See the "OpenLDAP Administrator's Guide" for more details on **slapd**.

OPTIONS

-4 Listen on IPv4 addresses only.

-6 Listen on IPv6 addresses only.

-T {a|c|d|i|p|t|acl|auth}

Run in Tool mode. The additional argument selects whether to run as slapadd, slapcat, slapdn, slapindex, slappasswd, or slaptest (slapacl and slapauth need the entire "acl" and "auth" option value to be spelled out, as "a" is reserved to **slapadd**). This option should be the first option specified when it is used; any remaining options will be interpreted by the corresponding slap tool program, according to the respective man pages. Note that these tool programs will usually be symbolic links to slapd. This option is provided for situations where symbolic links are not provided or not usable.

-d debug-level

Turn on debugging as defined by *debug-level*. If this option is specified, even with a zero argument, **slapd** will not fork or disassociate from the invoking terminal. Some general operation and status messages are printed for any value of *debug-level*. *debug-level* is taken as a bit string, with each bit corresponding to a different kind of debugging information. The meaning is the same as for the **loglevel** configuration option documented in **slapd.conf(5)**. Remember that if you turn on packet logging, packets containing bind passwords will be output, so if you redirect the log to a logfile, that file should be read-protected.

-s syslog-level

This option tells **slapd** at what level debugging statements should be logged to the **syslog(8)** facility.

-n service-name

Specifies the service name for logging and other purposes. Defaults to basename of argv[0], i.e.: "slapd".

-l syslog-local-user

Selects the local user of the **syslog(8)** facility. Value can be **LOCAL0**, through **LOCAL7**, as well as **USER** and **DAEMON**. The default is **LOCAL4**. However, this option is only permitted on systems that support local users with the **syslog(8)** facility.

-f slapd-config-file

Specifies the slapd configuration file. The default is **/etc/ldap/slapd.conf**.

-F *slapd-config-directory*

Specifies the slapd configuration directory. The default is `/etc/ldap/slapd.d`. If both **-f** and **-F** are specified, the config file will be read and converted to config directory format and written to the specified directory. If neither option is specified, slapd will attempt to read the default config directory before trying to use the default config file. If a valid config directory exists then the default config file is ignored. All of the slap tools that use the config options observe this same behavior.

-h *URLlist*

slapd will by default serve `ldap:///` (LDAP over TCP on all interfaces on default LDAP port). That is, it will bind using `INADDR_ANY` and port 389. The **-h** option may be used to specify LDAP (and other scheme) URLs to serve. For example, if slapd is given **-h "ldap://127.0.0.1:9009/ ldaps:/// ldapi://"**, it will listen on 127.0.0.1:9009 for LDAP, 0.0.0.0:636 for LDAP over TLS, and LDAP over IPC (Unix domain sockets). Host 0.0.0.0 represents `INADDR_ANY` (any interface). A space separated list of URLs is expected. The URLs should be of the LDAP, LDAPS, or LDAPI schemes, and generally without a DN or other optional parameters (excepting as discussed below). Support for the latter two schemes depends on selected configuration options. Hosts may be specified by name or IPv4 and IPv6 address formats. Ports, if specified, must be numeric. The default `ldap://` port is 389 and the default `ldaps://` port is 636.

The listener permissions are indicated by "x-mod=-rwxrwxrwx", "x-mod=0777" or "x-mod=777", where any of the "rwx" can be "-" to suppress the related permission, while any of the "7" can be any legal octal digit, according to `chmod(1)`. The listeners can take advantage of the "x-mod" extension to apply rough limitations to operations, e.g. allow read operations ("r", which applies to search and compare), write operations ("w", which applies to add, delete, modify and `modrdn`), and execute operations ("x", which means bind is required). "User" permissions apply to authenticated users, while "other" apply to anonymous users; "group" permissions are ignored. For example, "ldap:///???x-mod=-rw-----" means that read and write is only allowed for authenticated connections, and bind is required for all operations. This feature is experimental, and requires to be manually enabled at configure time.

-r *directory*

Specifies a directory to become the root directory. **slapd** will change the current working directory to this directory and then `chroot(2)` to this directory. This is done after opening listeners but before reading any configuration file or initializing any backend. When used as a security mechanism, it should be used in conjunction with **-u** and **-g** options.

-u user **slapd** will run slapd with the specified user name or id, and that user's supplementary group access list as set with `initgroups(3)`. The group ID is also changed to this user's gid, unless the **-g** option is used to override. Note when used with **-r**, slapd will use the user database in the change root environment.

Note that on some systems, running as a non-privileged user will prevent passwd back-ends from accessing the encrypted passwords. Note also that any shell back-ends will run as the specified non-privileged user.

-g *group*

slapd will run with the specified group name or id. Note when used with **-r**, slapd will use the group database in the change root environment.

-c *cookie*

This option provides a cookie for the syncrepl replication consumer. The cookie is a comma separated list of name=value pairs. Currently supported syncrepl cookie fields are **rid** and **csn**. **rid** identifies a replication thread within the consumer server and is used to find the syncrepl specification in `slapd.conf(5)` having the matching replication identifier in its definition. The **rid** must be provided in order for any other specified values to be used. **csn** is the commit sequence number received by a previous synchronization and represents the state of the consumer replica content

which the syncrepl engine will synchronize to the current provider content.

EXAMPLES

To start *slapd* and have it fork and detach from the terminal and start serving the LDAP databases defined in the default config file, just type:

```
/usr/sbin/slapd
```

To start **slapd** with an alternate configuration file, and turn on voluminous debugging which will be printed on standard error, type:

```
/usr/sbin/slapd -f /var/tmp/slapd.conf -d 255
```

To test whether the configuration file is correct or not, type:

```
/usr/sbin/slapd -Tt
```

SEE ALSO

ldap(3), **slapd.conf(5)**, **slapd.access(5)**, **slapacl(8)**, **slapadd(8)**, **slapauth(8)**, **slapcat(8)**, **slapdn(8)**, **slapindex(8)**, **slappasswd(8)**, **slaptest(8)**, **slurpd(8)**

"OpenLDAP Administrator's Guide" (<http://www.OpenLDAP.org/doc/admin/>)

BUGS

See <http://www.openldap.org/its/>

ACKNOWLEDGEMENTS

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