Tru64 UNIX

OpenLDAP Directory Server Installation and Administration

December 2002

Product Version: OpenLDAP Version 2.0.33

Operating System and Version: Tru64 UNIX Version 5.1B or higher

This manual describes how to install and configure the Lightweight Directory Access Protocol (LDAP) Directory Server in a Tru64 UNIX environment.

Hewlett-Packard Company
Palo Alto, California

Contents

Tables

About This Manual

This manual describes how to install and configure the Lightweight Directory Access Protocol (LDAP) Directory Server in a Tru64 UNIX environment.

In particular, it explains how to install and configure the default LDAP server for Tru64 UNIX, OpenLDAP, which is available on the *Associated Products, Volume 1*, CD-ROM for Tru64 UNIX Version 5.1B or higher. It also describes how to use the Tru64 UNIX LDAP Browser application.

Audience

This manual is intended for system and network adminstrators responsible for configuring and managing network services. Administrators are expected to have knowledge of operating system concepts, commands, and configuration. It is also helpful to have knowledge of Transmission Control Protocol/Internet Protocol (TCP/IP) networking concepts and network configuration.

Organization

This manual is divided into several chapters, each of which contains information about configuring a different service or application.

Chapter 1	Gives an overview of LDAP directory services.
Chapter 2	Describes how to install the OpenLDAP Directory Server and the LDAP Browser.
Chapter 3	Describes how to use the OpenLDAP configuration scripts.
Chapter 4	Describes how to use the Tru64 UNIX LDAP Browser

Related Documents

For more information about Tru64 UNIX networking and communications, see the following books:

- *Network Administration: Connections*

  Describes how to configure and manage network interfaces and network transports, and also how to solve problems associated with these interfaces and transports.

- *Network Administration: Services*

Describes how to configure and manage network applications and services, and also how to solve problems associated with these applications and services. Includes information about Network Information Service (NIS), which is similar in some ways to LDAP.

- *Security Administration*

  Describes security concepts and administration including authentication, securing resources, and auditing. This manual also describes how to configure LDAP User Authentication.

Reader's Comments

HP welcomes any comments and suggestions you have on this and other Tru64 UNIX manuals.

You can send your comments in the following ways:

- Fax: 603-884-0120 Attn: UBPG Publications, ZKO3-3/Y32
- Internet electronic mail: `readers_comment@zk3.dec.com`

  A Reader's Comment form is located on your system in the following location:

  `/usr/doc/readers_comment.txt`

Please include the following information along with your comments:

- The full title of the manual and the order number. (The order number appears on the title page of printed and PDF versions of a manual.)
- The section numbers and page numbers of the information on which you are commenting.
- The version of Tru64 UNIX that you are using.
- If known, the type of processor that is running the Tru64 UNIX software.

The Tru64 UNIX Publications group cannot respond to system problems or technical support inquiries. Please address technical questions to your local system vendor or to the appropriate HP technical support office. Information provided with the software media explains how to send problem reports to HP.

Conventions

This manual uses the following typographic conventions:

%	A percent sign represents the C shell system prompt.
$	A dollar sign represents the system prompt for the Bourne, Korn, and POSIX shells.

`#`	A number sign represents the superuser prompt.
`% cat`	Boldface type in interactive examples indicates typed user input.
file	Italic (slanted) type indicates variable values, placeholders, and function argument names.
[|] { | }	In syntax definitions, brackets indicate items that are optional and braces indicate items that are required. Vertical bars separating items inside brackets or braces indicate that you choose one item from among those listed.
. . .	In syntax definitions, a horizontal ellipsis indicates that the preceding item can be repeated one or more times.
`cat`(1)	A cross-reference to a reference page includes the appropriate section number in parentheses. For example, `cat`(1) indicates that you can find information on the `cat` command in Section 1 of the reference pages.
Return	In an example, a key name enclosed in a box indicates that you press that key.
Ctrl/*x*	This symbol indicates that you hold down the first named key while pressing the key or mouse button that follows the slash. In examples, this key combination is enclosed in a box (for example, Ctrl/C).

1

Overview of LDAP

The Lightweight Directory Access Protocol (LDAP) is an Internet standard directory service protocol that runs over TCP/IP. LDAP evolved as a less complex version of the Directory Access Protocol (DAP), which is designed to work with the X.500 international networking standard. You can use an LDAP server to manage entries in a director and make the information available to users and applications across the network.

The OpenLDAP Project (**http://www.openldap.org**) is a collaborative effort with contributors word-wide. The OpenLDAP Project provides OpenLDAP, an Open Source implementation of the LDAP technology. HP provides the same OpenLDAP software with the Tru64 UNIX operating system.

The LDAP information model is based on entries. An entry is a collection of attributes that has a globally unique Distinguished Name (DN). Each of the entry's attributes has a type and one or more values. The types are typically strings such as:

- *cn* for common name
- *mail* for e-mail address
- *uid* for user ID

The syntax of values depend on the attribute type.

In LDAP, directory entries are arranged in a hierarchical tree-like structure. This structure often reflects the geographic or organizational boundaries of the information being referenced.

An LDAP server can be used as a central repository of user information to identify and authenticate individuals. When used in this way, an LDAP server is similar to Network Information Services (NIS), also known as yellow pages. Compared to NIS, an LDAP server offers the following advantages:

- An LDAP directory is highly scalable.
- LDAP directories are dynamically updated. Administrators do not have to rebuild maps and push them onto the network. Also, changes are available virtually immediately.
- An LDAP directory database can be used to centralize management of user-related information

- An attribute can be modified at the attribute level. Users can be allowed to modify noncritical information (such as their preferred login shell or mail forwarding address). Modifications to more sensitive information (such as UID, GID, or a user's home directory) can be restricted to authorized directory managers only.
- You can set up multiple LDAP servers to make the data in the directory highly available. Through a process called replication, you can ensure that all LDAP servers have identical copies of the directory. The LDAP servers bind to one another and, through standard LDAP commands, propagate changes to the directory.

The *OpenLDAP 2.0 Administrator's Guide* provides an introduction to the LDAP model. It is available from the following URL:

http://www.openldap.org/doc/admin20/

2

Installing the OpenLDAP Server

This chapter describes how to install the OpenLDAP server.

The OpenLDAP Server software is provided in the software subset `IAEOLDAP590` located in the `/OpenLDAP` directory on the Tru64 UNIX Associated Products, Volume 1, CD–ROM. This subset can be installed on Tru64 UNIX using the software subset management utility `setld`. You can follow this `setld` installation procedure to install the software or use the `dusetup` installation tool provided on the Tru64 UNIX Associated Products CD–ROM to install the software.

2.1 System Requirements

Before installing the subsets using `setld`, you must determine if your AlphaServer system meets the minimum hardware and software requirements necessary to complete the install successfully. Table 2–1 lists the minimum requirements to verify on your system before proceeding with the installation.

Table 2–1: Minimum System Requirements

Name	Requirement
System Type	AlphaServer
Disk Space	50 MB
Main Memory	128 MB recommended (or greater, depending on system load)
Swap Space	It is generally recommended that you create swap space equal to twice the size of physical memory
Operating System	Tru64 UNIX Version 5.1B or later

2.2 OpenLDAP Installation Procedure

To install the OpenLDAP Server:

1. Place the Tru64 UNIX Associated Products, Volume 1, CD–ROM into your system's CD–ROM drive.
2. Log in as root at the console device or from a terminal emulator.

3. Mount the CD–ROM on the file system using the following command:

   ```
   $ /sbin/mount /dev/disk/cdrom0c mount point
   ```

   The OpenLDAP Server software is located in the *mount point*/OpenLDAP directory on the CD–ROM.

4. Use the `setld` command, specifying the directory containing the OpenLDAP server software :

   ```
   $ setld -l mount point/OpenLDAP
   ```

After the `setld` installation has completed, the OpenLDAP server will be located in the `/usr/internet/openldap/admin` directory.

For addition information on installing software using the `setld` command, refer to `setld`(8).

2.3 Accessing the LDAP Browser

The Tru64 UNIX LDAP Browser is a Java (jar) file named `ldap-browser.jar`. When you install the Open LDAP server subset, the `ldapbrowser.jar` file is installed in the `/usr/internet/openldap/admin` directory. Ensure that the permissions of the jar file are set to be executable.

If you want to run the LDAP Browser on the same system where OpenLDAP is installed, you do not need to do any additional installation tasks. If you want to run the LDAP Browser on other systems, you can copy the `ldapbrowser.jar` file to the desired system.

Chapter 4 describes how to use the LDAP browser.

3

Configuring the OpenLDAP Directory Server

This chapter describes how to configure and start an OpenLDAP server and where to get additional information.

3.1 Using the Configuration Scripts

The `slapd.conf` configuration file is used to configure the OpenLDAP server. Use the `/usr/internet/openldap/config_openldap.sh` script to configure the `/usr/internet/openldap/etc/slapd.conf` file and to initialize an LDAP database. You will need to provide an Organization Name, used as the search base, a Distinguished Name, used for connections to the server, and an Administrative password.

Once this script has run, use the `/sbin/init.d/openldap start` command to start the OpenLDAP `slapd` daemon on your system.

You can run the `config_openldap.sh` script more than once. However the script will attempt to reinitialize the database each time it is run and you will lose the existing data. To preserve existing data before reinitializing, either use the provided script, `/usr/internet/openldap/sbin/dump_db.sh`, or the `/usr/internet/openldap/sbin/slapcat` utility. See the `slapcat`(8) reference page for more information.

3.2 Accessing OpenLDAP Documentation

The OpenLDAP Directory Server is an implementation of the OpenLDAP project. LDAP Directory Server concepts and options are described in detail in the *OpenLDAP 2.0 Administration Guide*, available from the following URL:

`http://www.openldap.org/doc/admin20/`

Everything in this Administration Guide is applicable to the OpenLDAP Directory Server on Tru64 UNIX, with the following exception:

- You can ignore the chapter entitled “Building and Installing OpenLDAP Software”. The installation procedure specific to Tru64 UNIX is described in Chapter 2 of this manual.

The *OpenLDAP 2.0 Administration Guide* provides guidelines for planning your server deployment strategy, and setting access control.

For troubleshooting information, refer to the following URL:

http://www.openldap.org/faq/data/cache/1.html

4

Using the Tru64 UNIX LDAP Browser

The Tru64 UNIX LDAP Browser allows any LDAP V3 directory server to be browsed, searched, and modified using a graphical user interface. The LDAP Browser can be run on any platform that has the Java Runtime Engine (JRE) Version 1.3 or higher installed.

4.1 Managing Frequently Used Connections

The connection management window allows you to manage the configuration information for frequently accessed LDAP servers. The following functions can be performed:

- Establish a connection by selecting it in the list and clicking the Connect button.
- Establish a connection by selecting it in the list and clicking the Connect button.
- Edit a connection entry by selecting it in the list and clicking the Edit button
- Delete a connection entry by selecting it in the list and clicking the Delete button.
- Rename a connection entry by selecting it in the list, clicking the Rename button, and entering a new name when prompted.
- Make a copy of a connection entry by selecting it in the list, clicking the Copy button, and entering a name for the new entry when prompted.

4.1.1 Connecting to an LDAP Server

To connect to an LDAP server, select the Connect from the File menu to access the connection management window.

4.1.2 Creating or Editing Frequently Used Connections

The form used for adding or editing connection entries prompts for the following connection configuration information:

Field	Description
Connection nickname	Enter a short nickname to represent this connection in the list of frequently accessed connections
Hostname	Enter the hostname of an LDAP v3-compliant directory server
Port	Enter the port number on which the LDAP server is listening. The default LDAP port is 389.
Base DN	Enter the base distinguished name for this connection. The base distinguished name defines the top of the directory tree. To obtain a list of base distinguished names for a particular directory, make sure the hostname and port fields have been filled in correctly and then click the *Fetch* button. If the directory server has been set up to require authentication for this operation, the Bind DN and Password fields will have to be filled in correctly as well. The LDAP Browser will attempt to connect to the specified LDAP server, obtain the list of supported base distinguished names, and populate the Base DN option menu with those names.
Secure connection	Choose whether to communicate with the LDAP server using the Secure Sockets Layer (SSL). Such communication is only possible if the LDAP server has been configured to accept SSL connections and if the certificate presented by the server during SSL communication is signed by a trusted certificate authority. See Section 4.1.3 for more information on how to create a trusted certificate store.
Bind DN	Enter the distinguished name to use for authentication when binding to the LDAP server. To bind to a directory anonymously, simply leave this field blank. Many directories allow anonymous clients to perform read-only operations like searching, but will require authentication information for clients that attempt to write to the directory.
Password	Enter the password that corresponds to the Bind DN that was entered. Leave this field blank if anonymous binding is desired.
Bind information prompting	When BIND information is entered for a connection entry, this information is stored in the LDAP Browser configuration file in the user's home directory. If the security of the user's home directory is compromised, that bind information could potentially be obtained from the configuration file by an intruder. If this is a concern, or if you will not always be binding to the directory as the same user, leave the Bind DN and Password fields blank and click this toggle to cause the LDAP browser to prompt for BIND information each time the connection is established.
Referral strategy	Indicate if you want to automatically follow referrals to entries residing on other LDAP servers. Check either *Follow* or *Don't Follow*.

Field	Description
Alias dereferencing	Pick a strategy for dereferencing LDAP aliases. Check one of the following: *Never*, *Finding*, *Searching* or *Always*.
Search limit	You can limit the number of entries that will be returned by any LDAP search operation. Check either *None* for no search limit; or give a specific limit by checking Limit to and then entering a value in the results field. This limit can be useful when dealing with very large directories, because searches that return very large numbers of entries can take a considerable amount of time to complete and the search results can consume a large amount of memory.
Operation time limit	Allows you to enter a time limit (in milliseconds) for any LDAP operation to complete. Check *None* to specify no time limit. To specify a time limit, check *Limit to*, and then enter a value in milliseconds in the ms field. This option is useful when dealing with slow or unreliable connections.

4.1.3 Connecting to an LDAP Server Using SSL

The form for adding or modifying connections provides an option to use the Secure Sockets Layer (SSL) when communicating with the LDAP Server. SSL allows for verification of the LDAP server's identity as well as for encryption of the data that passes between the browser and server. In order for an SSL connection to successfully be established, the following conditions must be satisfied:

- The LDAP server must be configured by its administrator to accept SSL connections. The default port for LDAP over SSL is port 636. Many servers are not configured by default to accept SSL connections, so check with the server administrator if there is any doubt.
- The authentication certificate presented to the LDAP Browser by the server must be signed by a trusted certificate authority.

The LDAP Browser will automatically recognize and trust server certificates that are signed by any one of a group of well-known certificate authorities. However, if the LDAP server presents a certificate that is not signed by one of these well-known certificate authorities, the connection attempt will fail. This will typically be the case when attempting to connect to LDAP servers that have been configured with self-signed certificates or certificates issued by a certificate authority internal to a company or organization. In cases such as this, the server's certificate must be manually added to a certificate store that the LDAP Browser will use as a source of trusted certificates. Perform the following steps to accomplish this:

1. Obtain the LDAP server's digital certificate from the server's administrator. Some administrators provide access to this certificate by posting a link to it on an associated web site or by storing it in a

publicly-accessible entry in the LDAP directory. Either the binary form of the certificate or the printable Base64-encoded form defined by the Internet RFC 1421 standard is acceptable

2. Import the certificate into a trusted certificate store file called `.keystore` in the user's home directory. To accomplish this, use the `keytool` utility that ships as part of the Java installation. For example, on a UNIX system a command like the following would be used:

```
# keytool -import -alias someserver -file \
someserver.cer -keystore ~/.keystore -storepass mypassword
```

   where *someserver* is an alias that will be used to refer to this certificate, someserver.cer is a file containing the certificate, and *mypassword* is a password used to access the keystore.

3. Restart the LDAP Browser to load the new keystore and try connecting to the server.

If all of the above steps have been performed and the connection still cannot be made, verify that the host name, port, base distinguished name, and bind authentication information are all configured correctly. If the problem still remains, the LDAP Browser can be run from the command line with a special switch that turns on SSL debugging, this can sometimes reveal the problem. To use the switch, run the LDAP Browser with a command line like the following from the directory where the `ldapbrowser.jar` file resides:

```
# java -jar ldapbrowser.jar -Djavax.net.debug=all
```

4.1.4 Disconnecting from an LDAP Server

To terminate the currently established LDAP connection, choose Disconnect from the File menu.

4.1.5 Reconnecting to an LDAP Server

Choose Reconnect from the File menu to disconnect and then reconnect from an established connection, or to reestablish a connection which was terminated.

4.1.6 Using the Main Browsing Window

Once a connection has been established, the main browsing window allows you to view and manage the information in the directory. The directory is graphically represented in tree form, with each directory entry identified by its relative distinguished name (RDN). From the main browsing window, you can perform the following functions:

- Operate upon an entry — Click on an entry in the tree and then choose any of the appropriate operations from the Edit or View menus, or from the entry's context-sensitive popup menu.
- View an entry — Click on an entry in the tree to select it and see a list of its attributes in the adjoining table. The attributes of an entry can also be viewed in a separate window by selecting the entry and using the View entry item in the appropriate menus, or by double-clicking on an entry that has no descendants.
- View an entry's descendants — Double-click on an entry in the tree or click on the tree node expansion icon for that entry. The tree node expansion icon will graphically indicate that an entry has descendants until this operation is actually performed for the entry and the existence of descendants is either confirmed or disproved.
- Operate upon an attribute — Select an entry in the tree, select one or more attributes from the attribute table, and then choose any of the appropriate operations from the Edit menu or from the attribute's context-sensitive popup menu. Alternately, double-click an attribute in the table to modify it.
- Sort the attribute table — Click on either column header in the attribute table to sort by the data in that column. Click on the header again to reverse the sort order.

4.1.7 Opening a New Main Window

To create a new main window, choose the New Window option from the File menu. A newly created main window can be connected to the same directory server as any other main window, or to an entirely different directory server

4.1.8 Closing a Main Window

To close a main window without affecting any other main windows that are currently open, choose the Close Window option from the File menu.

4.1.9 Viewing an Entry in a Separate Window

Select an entry in the main window and choose View entry from the View menu or from the entry's context-sensitive popup menu. Alternately, double-click on an entry that has no descendants.

4.1.10 Refreshing an Entry

Select an entry in the main window and choose Refresh entry from the View menu. This will cause the LDAP Browser to reload the information for the selected entry from the LDAP server and to set the state of the

entry's descendants such that their information will also be refreshed the next time they are selected.

4.1.11 Controlling Client-Side Schema Checking

Client-side schema checking allows the LDAP Browser to adapt to and enforce the rules imposed by an LDAP directory's schema when entries are being created or modified. As a result, the process of creating and modifying entries becomes much less mistake-prone, and vague Object class violation errors that result from server-side schema checking can often be prevented. Client-side schema checking can be enabled and disabled through an Edit menu checkbox item in either the main browsing window or the add/modify entry forms. When schema checking is turned on, the following behavior is introduced:

- In the add and modify entry forms, required attributes are marked with an asterisk (*).
- Deletion of required attributes is disallowed.
- The add attribute dialog only presents choices allowed by the schema
- Multiple values are not allowed to be added for attributes defined as single-valued by the schema
- When `objectClass` attribute values are removed or modified, attributes that are no longer allowed as a result of the change are removed, after warning the user first.
- When `objectClass` attribute values are added or modified, newly required attributes that do not already exist in the entry are automatically added.

Client-side schema checking is enabled by default.

4.1.12 Adding New Entries

To add new entries, follow these steps:

1. Select the parent for the new entry in the main window
2. Choose a template to use for the new entry from the Add Entry submenu beneath the Edit menu.

Entry templates define which object classes a new entry will belong to and which attributes will be included in the entry creation form by default. Several default templates are provided, see Section 4.1.22 for information on how to create more.

Once a template is selected, a form will appear that allows the new entry's parent and attributes to be defined. Use the + and - buttons next to the

attributes to add additional values or to remove existing values for the attribute. Attributes not present in the form can also be added through an option in the form's Edit menu. Another option in the form's Edit menu determines whether attribute values left blank are ignored (the default) or are communicated to the LDAP server. Attributes can have either string or binary values. The binary value editor allows binary attribute values (such as JPEG files, certificates, and so on) to be loaded from a file. The current value can also be saved to a file.

4.1.13 Modifying Entries

To modify entries, follow these steps:

1. Select an entry in the main window.
2. Choose Modify entry from the Edit menu or from the entry's context-sensitive popup menu.

   A form similar to the one used for adding entries will appear, allowing the entry's attributes to be modified or deleted, and new attributes to be added.

4.1.14 Deleting Entries

To delete entries, follow these steps:

1. Select one or more entries in the main window.
2. Choose Delete entry from the Edit menu.
3. Respond to the confirmation prompt.

Deleting an entry will delete not just the entry but all of its descendants, so use with care.

4.1.15 Copying Entries

To copy entries, follow these steps:

1. Select an entry in the main window.
2. Choose Copy entry from the Edit menu or from the entry's context-sensitive popup menu.
3. Fill in the copy parameters in the resulting dialog. The entry can be copied to either the same parent or to a new one. If the entry is copied to the same parent, a different RDN value for the new entry should be specified — otherwise, an underscore and a sequence number will be appended to the RDN attribute to distinguish it from the original entry.

Multiple copies of an entry can also be made. By default, an underscore and a sequence number will be appended to the RDN of each copy to distinguish them from each other. Alternately, if a pound sign (#) is included in the new RDN value, the new RDN value will be generated by replacing the pound sign with a sequence number.

The copy entry dialog also offers the choice of whether or not to copy an entry's descendants along with the entry itself.

4.1.16 Renaming Entries

Renaming an entry refers to modifying the entry's RDN value while the entry's parent remains unchanged. To rename an entry, follow these steps:

1. Select the entry in the main window.
2. Choose Rename entry from the Edit menu or from the entry's context-sensitive popup menu.
3. Enter the entry's new RDN value when prompted.

4.1.17 Moving Entries

Moving an entry refers to reparenting the entry while the entry's RDN remains unchanged. To move an entry, follow these steps:

1. Select the entry in the main window.
2. Choose Move entry from the Edit menu or from the entry's context-sensitive popup menu.
3. Enter the distinguished name of the entry's new parent when prompted.

Note that moving an entry is actually a two part operation consisting of making a copy of the entry under the new parent followed by deletion of the old entry. This operation may fail under some circumstances, for example when a directory server enforces that two entries in the same directory can not have the same value for a particular attribute, such as a UID.

4.1.18 Adding Attributes

To add an atrribute, follow these steps:

1. Select an entry in the main window.
2. Choose Add attribute from the Edit menu or from the attribute list's context-sensitive popup menu.
3. Specify the name and type of the attribute to be added and then specify one or more values for the attribute in the resulting form.

4.1.19 Modifying Attributes

To modify an atrribute, follow these steps:

1. Select an entry in the main window.
2. Choose Modify attribute from the Edit menu or from the attribute list's context-sensitive popup menu.
3. Modify the values for the attribute in the resulting form.

4.1.20 Deleting Attributes

To delete an atrribute, follow these steps:

1. Select an entry in the main window.
2. Choose Delete attribute from the Edit menu or from the attribute list's context-sensitive popup menu.
3. Choose whether to delete only the selected values for the attributes, or whether to delete all values for the selected attributes.

4.1.21 Managing Entry Templates

Entry templates define which object classes a newly created entry will belong to and which attributes and attribute values will be included in entry creation forms by default. Entry templates can be added, modified, deleted, copied and renamed by choosing Manage entry templates from the Edit menu and performing those operations in the resulting dialog window.

4.1.22 Creating Entry Templates

An entry template can be created either from scratch or from an existing entry in the directory that is similar to some new entries that you plan to create.

To create an entry template, follow these steps:

1. Optionally selecting a model entry in the main window.
2. Click the New button in the template management directory.
3. Enter a template name and then define the template in the resulting template definition form.

The template definition form allows you to add the attributes and default values that will appear in future entry creation forms based upon this template. The Edit menu provides an option for adding new attributes to the form, and buttons next to each attribute value allow those values to be deleted or additional values to be added. Use the arrow buttons in the

form to change the ordering of attributes. The attribute in the top row will be used as the RDN value for new entries created with this template, so be sure to adjust the attribute ordering accordingly.

4.1.23 Editing Entry Templates

To edit entry templates, follow these steps:

1. Select the template to be edited from the list in the template management dialog.
2. Click the Edit button.
3. Edit the template in the resulting template definition form.

4.1.24 Deleting Entry Templates

To delete an entry template, follow these steps:

1. Select the template to be deleted from the list in the template management dialog.
2. Click the Delete button.
3. Confirm your choice when prompted.

4.1.25 Renaming Entry Templates

To rename an entry template, follow these steps:

1. Select the template to be renamed from the list in the template management dialog.
2. Click the Rename button.
3. Enter a new name for the template when prompted.

4.1.26 Copying Entry Templates

To copy an entry template, follow these steps:

1. Select the template to be copied from the list in the template management dialog.
2. Click the Copy button.
3. Enter a new name for the template copy when prompted.

4.2 Searching the Directory

To search the directory, follow these steps:

1. Select an entry in the main window to serve as the search base. Then, select Search from the View menu. The resulting search form prompts for the following information
   - Base DN — The base node for the search
   - Search filter — A standard LDAP search filter. The default of (objectclass=*) will match any entry.
   - Attributes — A list of attributes that the search should return. These attributes will be displayed in columns that can be used as the basis for sorting the search results. A list of attribute names separated by spaces or commas should be provided, for example, `cn uid description`.
   - Search scope — Select whether the search will match only entries a single level below the search base, or match entries at any depth below the search base.
2. Initiate the search by clicking the Search button, or alternately by pressing the RETURN key when focus is in any of the text fields. Once the search results have been obtained, the following operations can be performed:
   - Sort the results — Click on any column header to sort the results based upon the data in that column. Click on the column header again to perform a reverse sort based upon the column data. Column data is treated as text strings for sorting purposes, so attributes that contain numerical data may not sort in the expected manner.
   - View a full entry — Select an entry and then choose View entry from the search window's View menu or from the entry's context-sensitive popup menu. Alternately, double-click on the entry to view it.
   - Modify an entry — Select an entry and then choose Modify entry from the search window's Edit menu or from the entry's context-sensitive popup menu.
   - Delete an entry — Select an entry and then choose Delete entry from the search window's Edit menu or from the entry's context-sensitive popup menu.

4.3 Viewing the Object Class Schema

To view information about the list of object classes defined by a directory server's schema, follow these steps:

1. Select Browse object class schema from the View menu.

   The resulting dialog presents a list of defined object classes.

2. Click on an object class in the list to view the OID, parent object class, description, and lists of required and optional attributes for that object class.

4.4 Viewing the Attribute Schema

To view information about the attributes defined by a directory server's schema, follow these steps:

1. Select Browse attribute schema from the View menu.

   The resulting dialog presents a list of defined attributes.

2. Click on an attribute in the list to view the OID, description, syntax, and value type for that attribute.

4.5 User Configuration File

The LDAP Browser stores its configuration information in the file `.ldapbrowser.xml` in the user's home directory. The contents of this file should not be edited directly. If the LDAP Browser encounters startup errors, one possible cause is that this file has been hand-edited incorrectly or otherwise corrupted. If there are startup errors, you can attempt to fix the problem by removing or renaming the file and restarting the LDAP Browser