Red Hat Directory Server 12

Managing directory attributes and values

Using command-line utilities to add, update, and delete values

Red Hat Directory Server 12 Managing directory attributes and values

Using command-line utilities to add, update, and delete values

Legal Notice

Abstract

This documentation describes how to use utilities from the openldap-clients package to manage entries in Directory Server.

Table of Contents

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so:

- For simple comments on specific passages:

    1. Make sure you are viewing the documentation in the *Multi-page HTML* format. In addition, ensure you see the **Feedback** button in the upper right corner of the document.

    2. Use your mouse cursor to highlight the part of text that you want to comment on.

    3. Click the **Add Feedback** pop-up that appears below the highlighted text.

    4. Follow the displayed instructions.

- For submitting more complex feedback, create a Bugzilla ticket:

    1. Go to the Bugzilla website.

    2. As the Component, use **Documentation**.

    3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.

    4. Click **Submit Bug**.

CHAPTER 1. PROVIDING INPUT TO THE LDAPADD, LDAPMODIFY, AND LDAPDELETE UTILITIES

When you add, update, or delete entries or attributes in the directory, you can either use the interactive mode of the utilities to enter LDAP Data Interchange Format (LDIF) statements or pass an LDIF file to them.

1.1. THE INTERACTIVE MODE OF OPENLDAP CLIENT UTILITIES

In the interactive mode, the **ldapadd**, **ldapmodify**, and **ldapdelete** utilities read the input from the command line. To exit the interactive mode, press the **Ctrl**+**D** (^D) key combination to send the end-of-file (EOF) escape sequence.

In interactive mode, the utility sends the statements to the LDAP server when you press **Enter** twice or when you send the EOF sequence.

Use the interactive mode:

- To enter LDAP Data Interchange Format (LDIF) statements without creating a file.

  Example 1.1. Using the ldapmodify interactive mode to enter LDIF statements

  The following example runs **ldapmodify** in interactive mode, deletes the **telephoneNumber** attribute, and adds the **manager** attribute with the **cn=manager_name,ou=people,dc=example,dc=com** value to the **uid=user,ou=people,dc=example,dc=com** entry. Press **Ctrl+D** after the last statement to exit the interactive mode.

  ```
  # ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

  dn: uid=user,ou=people,dc=example,dc=com
  changetype: modify
  delete: telephoneNumber
  -
  add: manager
  manager: cn=manager_name,ou=people,dc=example,dc=com

  modifying entry "uid=user,ou=people,dc=example,dc=com"

  ^D
  ```

- To redirect LDIF statements, outputted by an another command, to the server:

  Example 1.2. Using the ldapmodify interactive mode with redirected content

  The following example redirects the output of the **command_that_outputs_LDIF** command to **ldapmodify**. The interactive mode exits automatically after the redirected command exits.

  ```
  # command_that_outputs_LDIF | ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x
  ```

Additional resources

- **ldif(5)** man page

1.2. THE FILE MODE OF OPENLDAP CLIENT UTILITIES

In the interactive mode, the **ldapadd**, **ldapmodify**, and **ldapdelete** utilities read the LDAP Data Interchange Format (LDIF) statements from a file. Use this mode to send a larger number of LDIF statements to the server.

> **Example 1.3. Passing a File with LDIF Statements to ldapmodify**
>
> 1. Create a file with the LDIF statements. For example, create the ~/**example.ldif** file with the following statements:
>
>    ```
>    dn: uid=user,ou=people,dc=example,dc=com
>    changetype: modify
>    delete: telephoneNumber
>    -
>    add: manager
>    manager: cn=manager_name,ou=people,dc=example,dc=com
>    ```
>
>   This example deletes the **telephoneNumber** attribute and to adds the **manager** attribute with the **cn=manager_name,ou=people,dc=example,dc=com** value to the **uid=user,ou=people,dc=example,dc=com** entry.
>
> 2. Pass the file to the **ldapmodify** command using the **-f** parameter:
>
>    ```
>    # ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x -f ~/example.ldif
>    ```

Additional resources

- **ldif(5)** man page

1.3. THE CONTINUOUS OPERATION MODE OF OPENLDAP CLIENT UTILITIES

By default, if you send multiple LDAP Data Interchange Format (LDIF) statements to the server and one operation fails, the process stops. However, entries processed before the error occurred were successfully added, modified, or deleted.

To ignore errors and continue processing further LDIF statements in a batch, pass the **-c** parameter to **ldapadd** and **ldapmodify**:

```
# ldpamodify -c -D "cn=Directory Manager" -W -H ldap://server.example.com -x
```

CHAPTER 2. ADDING AN LDAP ENTRY

To add a new entry to the directory, use the **ldapadd** or **ldapmodify** utility. Note that /**bin/ldapadd** is a symbolic link to **/bin/ldapmodify**. Therefore, **ldapadd** performs the same operation as **ldapmodify -a**.

> **NOTE**
>
> You can only add a new directory entry if the parent entry already exists. For example, you cannot add **cn=user,ou=people,dc=example,dc=com**, if the **ou=people,dc=example,dc=com** parent entry does not exist.

2.1. ADDING AN ENTRY USING LDAPADD

To use the **ldapadd** utility to add, for example, the **cn=user,ou=people,dc=example,dc=com** user entry, enter:

```
# ldapadd -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
uid: user
givenName: given_name
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetorgperson
sn: surname
cn: user
```

> **NOTE**
>
> Running **ldapadd** automatically performs a **changetype: add** operation. Therefore, you do not need to specify **changetype: add** in the LDIF statement.

Additional resources

- **ldapadd(1)** man page

2.2. ADDING AN ENTRY USING LDAPMODIFY

To use the **ldapmodify** utility to add, for example, the **cn=user,ou=people,dc=example,dc=com** user entry, enter:

```
# ldapmodify -a -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
uid: user
givenName: given_name
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetorgperson
sn: surname
cn: user
```

‒

> **NOTE**
>
> When passing the **-a** parameter to the **ldapmodify** command, the utility automatically performs a **changetype: add** operation. Therefore, you do not need to specify **changetype: add** in the LDIF statement.

Additional resources

- **ldapmodify(1)** man page

2.3. CREATING A ROOT ENTRY OF A DATABASE SUFFIX

To create the root entry of a database suffix, such as **dc=example,dc=com**, bind as the **cn=Directory Manager** user and add the entry. The distinguished name (DN) corresponds to the DN of the root or sub-suffix of the database.

For example, to add the **dc=example,dc=com** suffix, enter:

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: dc=example,dc=com
changetype: add
objectClass: top
objectClass: domain
dc: example
```

> **NOTE**
>
> You can add root objects only if you have one database per suffix. If you create a suffix that is stored in several databases, you must use the **dsctl ldif2db** command to set the database that will hold the new entries.

Additional resources

- Importing data using the command line while the server is offline

CHAPTER 3. UPDATING AN LDAP ENTRY

When you modify a directory entry, use the **changetype: modify** statement. Depending on the change operation, you can add, change, or delete attributes from the entry.

3.1. ADDING ATTRIBUTES TO AN LDAP ENTRY

To add an attribute to an LDAP entry, use the **add** operation.

For example, to add the **telephoneNumber** attribute with the **555-1234567** value to the **uid=user,ou=People,dc=example,dc=com** entry, enter:

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
changetype: modify
add: telephoneNumber
telephoneNumber: 555-1234567
```

If an attribute is multi-valued, you can specify the attribute name multiple times to add all the values in a single operation. For example, to add two **telephoneNumber** attributes at once to the **uid=user,ou=People,dc=example,dc=com**, enter:

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
changetype: modify
add: telephoneNumber
telephoneNumber: 555-1234567
telephoneNumber: 555-7654321
```

3.2. UPDATING THE VALUE OF AN ATTRIBUTE

The procedure for updating an attribute's value depends on whether the attribute is single-valued or multi-valued:

- Updating a single-value attribute:
  When updating a single-value attribute, use the **replace** operation to override the existing value. The following command updates the **manager** attribute of the **uid=user,ou=People,dc=example,dc=com** entry:

  ```
  # ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

  dn: uid=user,ou=People,dc=example,dc=com
  changetype: modify
  replace: manager
  manager: uid=manager_name,ou=People,dc=example,dc=com
  ```

- Updating a specific value of a multi-value attribute:
  To update a specific value of a multi-value attribute, first delete the entry you want to replace, and then add the new value. The following command updates only the **telephoneNumber** attribute that is currently set to **555-1234567** in the **uid=user,ou=People,dc=example,dc=com** entry:

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
changetype: modify
delete: telephoneNumber
telephoneNumber: 555-1234567
-
add: telephoneNumber
telephoneNumber: 555-9876543
```

3.3. DELETING ATTRIBUTES FROM AN ENTRY

To delete an attribute from an entry, use the **delete** operation:

- Deleting an attribute:
  For example, to delete the **manager** attribute from the
  uid=user,ou=People,dc=example,dc=com entry, enter:

  ```
  # ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

  dn: uid=user,ou=People,dc=example,dc=com
  changetype: modify
  delete: manager
  ```


  IMPORTANT

  If the attribute contains multiple values, this operation deletes all of them.

- Deleting a specific value of a multi-value attribute:
  If you want to delete a specific value from a multi-value attribute, list the attribute and its value in the LDAP Data Interchange Format (LDIF) statement. For example, to delete only the **telephoneNumber** attribute that is set to **555-1234567** from the **uid=user,ou=People,dc=example,dc=com** entry, enter:

  ```
  # ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

  dn: uid=user,ou=People,dc=example,dc=com
  changetype: modify
  delete: telephoneNumber
  telephoneNumber: 555-1234567
  ```

CHAPTER 4. DELETING AN LDAP ENTRY

You can remove entries from an LDAP directory, but you can only delete entries that have no child entries. For example, you cannot delete **ou=People,dc=example,dc=com**, if the **uid=user,ou=People,dc=example,dc=com** entry still exists.

4.1. DELETING AN ENTRY USING LDAPDELETE

The **ldapdelete** utility enables you to delete one or multiple entries. For example, to delete the **uid=user,ou=People,dc=example,dc=com** entry, enter:

```
# ldapdelete -D "cn=Directory Manager" -W -H ldap://server.example.com -x
"uid=user,ou=People,dc=example,dc=com"
```

To delete multiple entries in one operation, append them to the command:

```
# ldapdelete -D "cn=Directory Manager" -W -H ldap://server.example.com -x
"uid=user1,ou=People,dc=example,dc=com" "uid=user2,ou=People,dc=example,dc=com"
```

Additional resources

- **ldapdelete(1)** man page

4.2. DELETING AN ENTRY USING LDAPMODIFY

To delete an entry using the **ldapmodify** utility, use the **changetype: delete** operation. For example, to delete the **uid=user,ou=People,dc=example,dc=com** entry, enter:
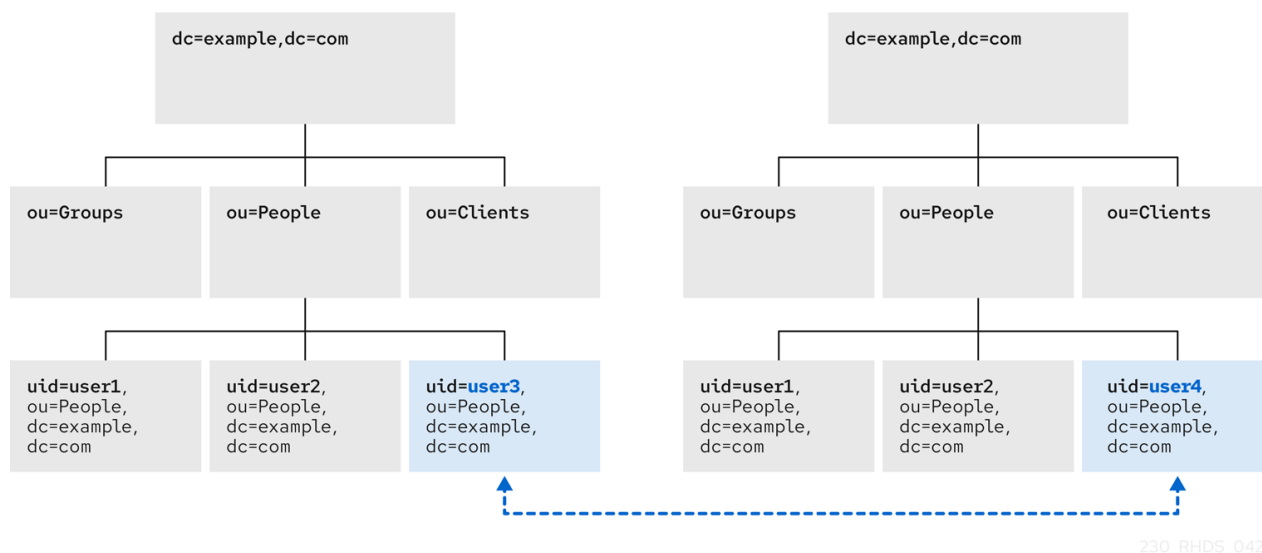
```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
changetype: delete
```

CHAPTER 5. RENAMING AND MOVING AN LDAP ENTRY

The following rename operations exist:

Renaming an entry

If you rename an entry, the **modrdn** operation changes the relative distinguished name (RDN) of the entry:

```
dc=example,dc=com                          dc=example,dc=com

ou=Groups   ou=People   ou=Clients          ou=Groups   ou=People   ou=Clients

uid=user1,  uid=user2,  uid=user3,          uid=user1,  uid=user2,  uid=user4,
ou=People,  ou=People,  ou=People,          ou=People,  ou=People,  ou=People,
dc=example, dc=example, dc=example,         dc=example, dc=example, dc=example,
dc=com      dc=com      dc=com              dc=com      dc=com      dc=com
```

230_RHDS_0422

Renaming a subentry

For subtree entries, the **modrdn** operation renames the subtree and also the DN components of child entries:

```
dc=example,dc=com                          dc=example,dc=com

ou=Groups   ou=People   ou=Clients          ou=Groups   ou=New People   ou=Clients

uid=user1,  uid=user2,  uid=user3,          uid=user1,      uid=user2,      uid=user3,
ou=People,  ou=People,  ou=People,          ou=New People,  ou=New People,  ou=New People,
dc=example, dc=example, dc=example,         dc=example,     dc=example,     dc=example,
dc=com      dc=com      dc=com              dc=com          dc=com          dc=com
```

230_RHDS_0422
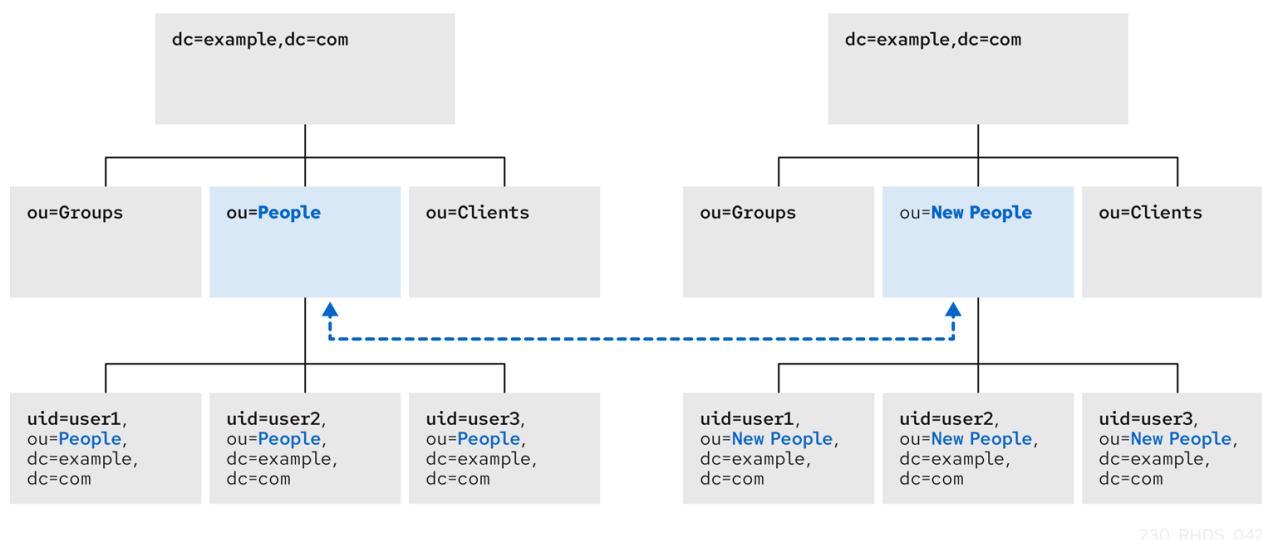
Note that for large subtrees, this process can take a lot of time and resources.

Moving an entry to a new parent

A similar action to renaming a subtree is moving an entry from one subtree to another. This is an expanded type of the **modrdn** operation, which simultaneously renames the entry and sets a **newSuperior** attribute which moves the entry from one parent to another:

230_RHDS_0422
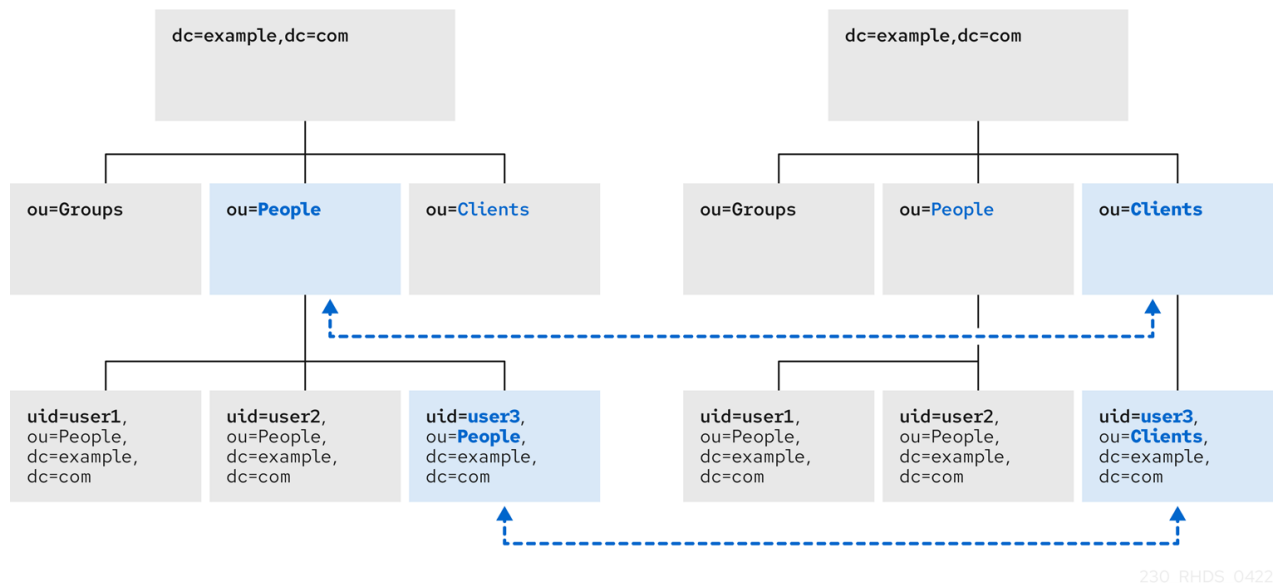
5.1. CONSIDERATIONS FOR RENAMING LDAP ENTRIES

Keep the following in mind when performing rename operations:

- You cannot rename the root suffix.

- Subtree rename operations have minimal effect on replication. Replication agreements are applied to an entire database, not to a subtree within the database. Therefore, a subtree rename operation does not require re-configuring a replication agreement. All name changes after a subtree rename operation are replicated as normal.

- Renaming a subtree might require any synchronization agreements to be reconfigured. Synchronization agreements are set at the suffix or subtree level. Therefore, renaming a subtree can break synchronization.

- Renaming a subtree requires that any subtree-level access control instructions (ACI) set for the subtree be reconfigured manually, as well as any entry-level ACIs set for child entries of the subtree.

- Trying to change the component of a subtree, such as moving from **ou** to **dc**, might fail with a schema violation. For example, the **organizationalUnit** object class requires the **ou** attribute. If that attribute is removed as part of renaming the subtree, the operation fails.

- If you move a group, the **MemberOf** plug-in automatically updates the **memberOf** attributes. However, if you move a subtree that contain groups, you must manually create a task in the **cn=memberof** task entry or use the **dsconf memberof fixup** command to update the related **memberOf** attributes.

5.2. CONTROLLING THE RELATIVE DISTINGUISHED NAME BEHAVIOR WHEN RENAMING ENTRIES

When you rename an entry, the **deleteOldRDN** attribute controls whether the old relative distinguished name (RDN) will be deleted or retained:

deleteOldRDN: 0

The existing RDN is retained as a value in the new entry. The resulting entry contains two **cn** attributes: one with the old and one with the new common name (CN).

For example, the following attributes belong to a group that was renamed from **cn=old_group,dc=example,dc=com** to **cn=new_group,dc=example,dc=com** with the **deleteOldRDN** attribute set to **0**:

```
dn: cn=new_group,ou=Groups,dc=example,dc=com
objectClass: top
objectClass: groupOfUniqueNames
cn: old_group
cn: new_group
```

deleteOldRDN: 1

Directory Server deletes the old entry and creates a new entry using the new RDN. The new entry only contains the **cn** attribute of the new entry.

For example, the following group was renamed to **cn=new_group,dc=example,dc=com** with the **deleteOldRDN** attribute set to **1**:

```
dn: cn=new_group,ou=Groups,dc=example,dc=com
objectClass: top
objectClass: groupofuniquenames
cn: new_group
```

Additional resources

- Renaming an LDAP entry or subtree

5.3. RENAMING AN LDAP ENTRY OR SUBTREE

To rename an entry or subtree, use the **changetype: modrdn** operation, and set the new relative distinguished name (RDN) in the **newrdn** attribute.

For example, to rename the **cn=demo1,dc=example,dc=com** entry to **cn=demo2,dc=example,dc=com**, enter:

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: cn=demo1,dc=example,dc=com
changetype: modrdn
newrdn: cn=demo2
deleteOldRDN: 1
```

Additional resources

- Controlling the relative distinguished name behavior when renaming entries

5.4. MOVING AN LDAP ENTRY TO A NEW PARENT

To move an entry to a new parent, use the **changetype: modrdn** operation, and set the following to attributes:

- **newrdn**: Sets the relative distinguished name (RDN) of the moved entry. You must set this entry, even if the RDN remains the same.

- **newSuperior**: Sets the distinguished name (DN) of the new parent entry.

For example, to move the **cn=demo** entry from **ou=Germany,dc=example,dc=com** to **ou=France,dc=example,dc=com**, enter:

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: cn=demo,ou=Germany,dc=example,dc=com
changetype: modrdn
newrdn: cn=demo
newSuperior: ou=France,dc=example,dc=com
deleteOldRDN: 1
```

Additional resources

- Controlling the relative distinguished name behavior when renaming entries

CHAPTER 6. USING SPECIAL CHARACTERS IN OPENLDAP CLIENT UTILITIES

When using the command line, enclose characters that have a special meaning to the command-line interpreter, such as space ( ), asterisk (*), or backslash (\), with quotation marks. Depending on the command-line interpreter, use single or double quotation marks. For example, to authenticate as the **cn=Directory Manager** user, enclose the user's distinguished name (DN) in quotation marks:

> # **ldapmodify -a -D "*cn=Directory Manager*" -W -H *ldap://server.example.com* -x**

Additionally, if a DN contains a comma in a component, escape it using a backslash. For example, to authenticate as the **uid=user,ou=People,dc=example.com Chicago, IL** user, enter:

> # **ldapmodify -a -D "*cn=uid=user,ou=People,dc=example.com Chicago\, IL*" -W -H *ldap://server.example.com* -x**

CHAPTER 7. USING BINARY ATTRIBUTES IN LDIF STATEMENTS

Certain attributes support binary values, such as the **jpegPhoto** attribute. When you add or update such an attribute, the utility reads the value for the attribute from a file. To add or update such an attribute, you can use the **ldapmodify** utility.

For example, to add the **jpegPhoto** attribute to the **uid=user,ou=People,dc=example,dc=com** entry, and read the value for the attribute from the **/home/user_name/photo.jpg** file, enter:

> **# ldapmodify -D "*cn=Directory Manager*" -W -H *ldap://server.example.com* -x**
>
> **dn:** *uid=user,ou=People,dc=example,dc=com*
> **changetype: modify**
> **add: jpegPhoto**
> **jpegPhoto:< file:*///home/user_name/photo.jpg***

IMPORTANT

Note that there is no space between **:** and **<**.

CHAPTER 8. UPDATING AN LDAP ENTRY IN AN INTERNATIONALIZED DIRECTORY

To use attribute values with languages other than English, associate the attribute's value with a language tag.

When using **ldapmodify** to update an attribute that has a language tag set, you must match the value and language tag exactly or the operation will fail.

For example, to modify an attribute value that has the **lang-fr** language tag set, include the tag in the modify operation:

```
# ldapmodify -D "cn=Directory Manager" -W -H ldap://server.example.com -x

dn: uid=user,ou=People,dc=example,dc=com
changetype: modify
replace: homePostalAddress;lang-fr
homePostalAddress;lang-fr: 34 rue de Seine
```