CHAPTER 7

LDAP

The following topics are covered in this chapter:

- LDAP binds
  - DN
  - Password
  - Server address and LDAP port
  - Connection method
- Understanding LDAP queries
  - LDAP filter
  - Scope
  - Base
  - Performance considerations
- Persistent Search
- Managing the LDAP objects
  - LDAP server object
  - LDAP group object
  - Creating and configuring the LDAP objects
- Walking the tree
  - Default referral
  - Conditions to use default referral
  - Referral options
- Access control
- Using ICE to bulk-load data

The Lightweight Directory Access Protocol (LDAP) is an industry-standard client-server protocol. LDAP provides a common interface in which LDAP-compliant clients can access data from within an X.509 database. Most directories on the market today are either partially or fully LDAP compliant. Because of this, developers can create LDAP clients that are capable of attaching to many LDAP directories, allowing for tremendous flexibility.

eDirectory provides an LDAP server, the purpose of which is to process LDAP requests from LDAP clients. The LDAP server does this by converting the requests into formats that the eDirectory Agent can understand and then forwarding the requests to the eDirectory Agent. The eDirectory Agent accesses the eDirectory database and retrieves or modifies the database based off of the request. The result is sent back to the LDAP server, which converts the message into an LDAP-compliant message that can be understood by the LDAP client, and then forwards the reply back to the client.

LDAP Binds

LDAP binds is an LDAP term that refers to the action of authenticating to an LDAP directory. The authentication methodology that is specific to each directory is irrelevant to the LDAP client that is making the bind request. Because the LDAP protocol is a standard protocol, the bind request packet is consistent, regardless of the LDAP directory.

Each LDAP client has its own method of collecting information from the user that is making the authentication request. Regardless of how the LDAP client gathers the information from the user, the following information needs to be sent to the LDAP server to perform a successful LDAP bind:

- *DN*: Distinguished Name of the user that is requesting the bind.
- *Password*: The user's password.
- *Server address*: The network address of the LDAP server that will complete the bind request.
- *Port*: The port that the LDAP server is listening to for LDAP requests.
- *Connection method*: There are two connection methods:
  - *Clear*: The data transmitted between the two entities that are connected is transmitted in clear text.
  - *Secure*: The data transmitted between the two entities that are connected is encrypted with an SSL encryption algorithm.
- *Path to the server certificate*: If the connection method is Secure, the location of the server certificate is necessary.

The items in the preceding list are described next in more detail.