MIDRANGE COMPUTING
www.midrangecomputing.com
BUSINESS COMPUTING SOLUTIONS FOR AS/400 & iSERIES PROFESSIONALS

LDAP and the AS/400

by John A. McMeeking

Along with many other companies in the computer industry, **IBM** provides support for an Internet protocol called the Lightweight Directory Access Protocol (LDAP) to help you access information in a network directory. OS/400 includes a directory server, client, and other directory-related services as part of its Directory Services option. In this article I will explain what LDAP is, how it is used, and what directory capabilities are provided by OS/400. I will then show you how to set up and run the directory server on your AS/400, as well as how to use some of the other Directory Services features.

What Is LDAP?

LDAP is an industry standard that allows network clients to access information in a network directory. A directory is a listing of information about objects that gives details about the objects. Using an LDAP-enabled application, network clients can query the server to find details about specific objects or search for objects having specified characteristics.

LDAP was originally conceived as a lightweight gateway/ client to an X.500-compliant directory. The X.500 standards use the entire Open Systems Interconnection (OSI) protocol stack and define an extensive set of functions. LDAP defines a TCP/IP communication protocol that could be easily implemented using limited resources on the client, yet provides a rich set of functionality. LDAP does not define the directory itself. Subsequently, many vendors have implemented directories directly on the server. LDAP has been widely implemented and LDAP servers and clients are readily available for many platforms. Here are some of the functions that are defined by the LDAP protocol:

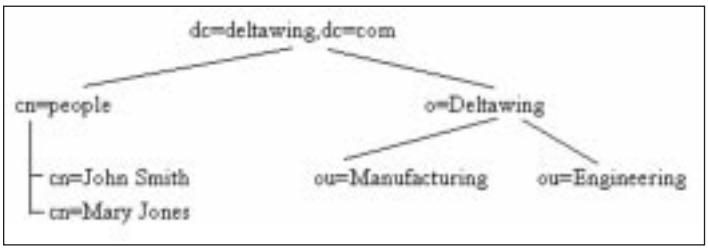

Figure 1: This figure shows the directory tree structure for the Deltawing company.

- Searching for directory entries
- Creating, modifying, and deleting directory entries
- Authentication

Additionally, LDAP V3 defines standard mechanisms for accessing a schema that describes the directory data model (the kinds of objects that the directory can contain and their attributes). It also includes support for national language-sensitive data by using UTF-8—an encoding of the Unicode character set—for string data.

The LDAP standards do not currently define an access control model for controlling access to directory data. However, most LDAP vendors, including IBM, have implemented their own access control models and work is under way to define access control model standards.

What Is a Directory?

A directory is a listing of information about objects that provides details about the objects. The information in the directory is organized as a tree. Depending on what you are using the directory for, the tree may be flat or it may have a hierarchical structure. Each object in the directory has a relative distinguished name (RDN) that identifies the object relative to its parent; each object also has a set of attributes that describe the object. Objects are uniquely identified in the directory by their distinguished name (DN), which consists of the RDNs of the object and its parents.

Directory names follow a syntax defined by the X.500 standards and are of the form *attribute-name = attribute-value*. Attribute names include *cn* (common name), *c* (country), and *o* (organization), and the attribute value is the object's common name, country, etc. **Figure 1** depicts a directory tree for the Deltawing company. The top of the tree is named after the company's Internet domain *dc=deltawing,dc=com* (dc is the attribute name for domain component). There is a container, *cn=people*, in which all of the employees are listed and a sub-tree containing organizational information. The entry for Mary Jones has a RDN of *cn=Mary Jones* and a DN of *cn=Mary Jones, cn=People, dc=deltawing, dc=com*.

Each entry also has a set of attributes defined by the directory schema. Attributes can have multiple values (multiple telephone numbers, for example). One mandatory attribute, *objectclass*, identifies the type (or types) of object. The *objectclass*, in turn, defines the set of

required and optional attributes for the object. As an example, the entry for Mary Jones might look like this:

```
dn: cn=Mary
Jones,cn=People,dc=deltawing,dc=com
objectclass: ePerson
cn: Mary Jones (where cn stands for "common
name," e.g.,. name commonly known as)
sn: Jones (where sn stands for "surname")
givenName: Mary
mail: mjones@deltawing.com
telephoneNumber: 555.555.5555
ou: manufacturing
```

Given entries like this, you can now look up Mary Jones' email address using an LDAP-enabled mail application, or perhaps use a corporate application to find Mary as one of the members of the manufacturing organization.

How Are LDAP Directories Used?

One typical use of an LDAP directory is as an address book. Most email applications support using an LDAP directory as an address book, but LDAP can be used for much more than that. Any client application that needs information about people, for example, in your network can use LDAP to obtain that information. You can store information about network-wide resources in a directory. The Internet Printing Protocol (IPP), a draft Internet standard, can use LDAP to locate printers and printer services. Network applications can use LDAP functions to authenticate a user to an LDAP server, and if successful, grant access to non-LDAP resources. An LDAP directory can be used to manage network-wide resources. Some systems management applications support using LDAP for functions such as network quality of service. **Figure 2** illustrates some of the products and services on the AS/400 that can use LDAP. So, even if you don't need LDAP for your own purposes, applications like these may make it desirable to have an AS/400 LDAP server in your network.

LDAP on the AS/400

IBM provides two cross-platform LDAP directories: the IBM SecureWay Directory and the Domino server. The IBM SecureWay Directory Web site (*www-4.ibm.com/software/network/directory/*) is supported on several platforms, including System/390, the AS/400, AIX, Solaris, and **Microsoft** Windows NT. The server included with AS/400 Directory Services is the AS/400 version of the SecureWay Directory Server. The AS/400 directory server is included free with OS/400 as part of AS/400 Directory Services (option number 32 of 5769-SS1). Also, an LDAP server is part of the Domino server product (including Domino for AS/400), which is a licensed product. The remainder of this article focuses on AS/400 Directory Services.

AS/400 Directory Services has been available since OS/400 V4R3. It includes a server, command line utilities, client APIs, and a Windows 95/98/NT client software development kit. AS/400 Directory Services also includes support for publishing information—for example, the System Distribution Directory (SDD)—to an LDAP server in your network. The server uses DB2 for OS/400 (DB2/400) for storing the directory information and the server is configured using AS/400 Operations Navigator. Note: Passwords are not stored in the DB2/400 database; they are kept in a secure store elsewhere on your AS/400.

New in V4R5 is support for the LDAP version 3 standards. These add national language support and a standard mechanism for viewing and extending the schema, which defines the object classes and attributes that can be used for directory objects.

Features of the AS/400 directory server include a large, scalable directory; Secure Sockets Layer (SSL) support for secure communication between clients and the AS/400 directory server; national language support using UTF-8; and directory replication to provide increased availability and improved search performance

Application	Use of LDAP
WebSphere Application Server	Authentication
HTTP Server	Authentication and configuration
WebSphere Commerce Suite (formerly known as Net.Commerce)	Required for authentication
Management Central	Hardware and software inventory

Figure 2: Several products and services on the AS/400 that can use LDAP.

Getting an LDAP Server Up and Running on Your AS/400

Getting the server configured and started on your AS/400 is simple. Before you start, you'll need these things:

- AS/400 Operations Navigator (OpsNav). All directory server configuration tasks are performed using OpsNav. There are no green-screen commands.
- A user profile with *ALLOBJ and *IOSYSCFG special authorities.
- A suffix (or naming context). This is a DN that defines the name space for your directory. Suggestions for this DN include your organization's name and country, for example: *o=deltawing, c=us* or your TCP/IP domain name (*dc=deltawing, dc=com* for the deltawing.com domain). Be careful to remember, however, that defining a suffix to the AS/400 LDAP server does not create a directory entry. A suffix simply identifies to the server that DNs in this namespace can be handled by the AS/400 LDAP server. Other DNs will result in a referral to another server or in a no such object error.

One typical use of an LDAP directory is as an address book.

- The administrator DN and password. A client authenticated to the server using the administrator DN and password can create, delete, modify, and read all data in the directory.
- For V4R3 and V4R4, you also need to identify a library that will contain the database files and specify the name for the local relational database directory entry (typically the system name). When using V4R5 OpsNav with a V4R5 AS/400 system, a new user library, QUSRDIRDB, is automatically configured as the database library.

To configure the server, launch OpsNav and open the TCP/IP servers folder (which is accessed through the Network-Servers-TCP/IP node in the OpsNav tree). Right- click on the Directory option that appears in the TCP/IP pane on the right-hand side of the OpsNav window; this brings up a pop-up context menu from which you should select the Configure menu option **Figure 3**. This brings you to the Configure Directory Server wizard **Figure 4**. In the wizard, you enter the name and password for your LDAP administrator (the default name is *cn=Administrator*) and the directory suffixes you want to add to this server. When you get to the final configuration screen, click Finish and your server is configured. You can now start the server.

Figure 3: You perform most of the LDAP configuration tasks from the AS/400 Directory pop-up context menu.

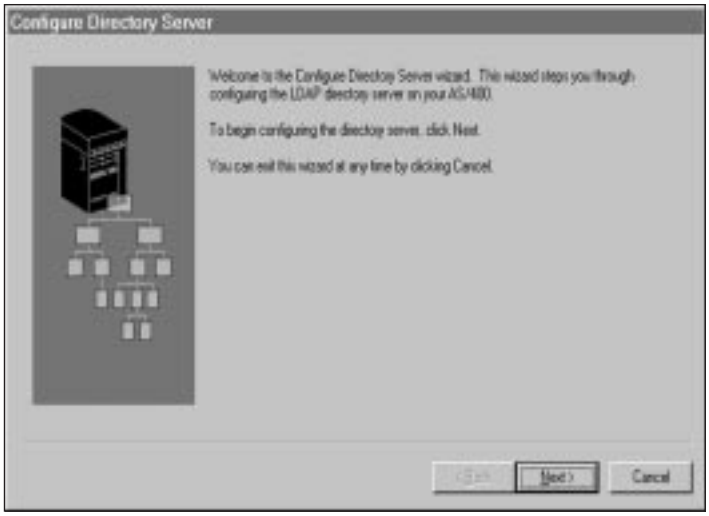

Figure 4: The OpsNav Configure Directory wizard is the only place where you can configure your AS/400 LDAP Directory server.

Starting and Stopping the LDAP Server

The LDAP server can be started in three different ways. First, when you configure the LDAP server using the OpsNav Configure Directory Server wizard, there is a check-box option to start your Directory Server automatically whenever TCP/IP is started. If you checked that option, your LDAP server will automatically be started whenever TCP/IP is started on your AS/400. You can also specify an automatic start for your Directory server and any other TCP/IP server by using the Servers to Start option on the TCP/IP properties screen in OpsNav (which is accessed by right-clicking on the Network-Protocols-TCP/IP node in OpsNav and selecting Properties from the pop-up context menu). For more information about using OpsNav to specify which servers should be automatically started whenever TCP/IP is started, see "The Fine Art of Starting TCP/IP on the AS/400," Joe Hertvik, *AS/400 Network Expert*, May/June 2000.

If you prefer to start your AS/400 LDAP directory server manually, you can start the server either from the green-screen or from OpsNav. To start the LDAP server from a green-screen, type in the Start TCP/IP Server (STRTCPSVR) command:

```
STRTCPSVR SERVER(*DIRSRV)
```

To stop the server from the green-screen, use the End TCP/IP Server (ENDTCPSVR) command:

```
ENDTCPSVR SERVER(*DIRSRV)
```

The *DIRSRV variable tells OS/400 to start or stop the AS/400 directory server. These commands can also be run from within CL programs.

To start or stop the server from OpsNav, right click on the Directory entry in the Network-Servers-TCP/IP pane (the same Window you used to configure the server as shown in Figure 3) and select the Start or Stop options from the pop-up context menu.

When the server is first started, several database tables are created in the database library (which is QUSRDIRDB for V4R5; for OS/400 V4R3 and V4R4, you define the DB2/400 database library to use). To backup the directory contents, you'll want to save everything in this library.

In some cases you may want to view the directory server job log. To do this directly from OpsNav, select Server Jobs from the Directory server context menu. Or, from a 5250 session, use the Work with Active Jobs (WRKACTJOB) command for the QDIRSRV job:

```
WRKACTJOB JOB(QDIRSRV)
```

This brings you to the Work with Job display where you can find messages such as failed bind attempts and various directory errors. The job log can be useful when debugging LDAP applications and the LDAP return code doesn't give you enough information to determine what is wrong.

If you want to set up your server to use SSL or configure a server as a replica, use OpsNav to select Properties from the Directory server context menu, which brings up the Directory server Properties pane **Figure 5**. Inside this pane, you would select the Network tab to configure SSL for your server or the Replicas tab to designate a server to contain a replica of your configuration. While these options are outside the scope of this article, you can obtain more information on the features by visiting the AS/400 Information Center Web site: (*http://publib.boulder.ibm.com/pubs/html/as400/v4r5/ic2924/info/index.htm*).

Administering Directory Data

Directory content administration falls broadly into two categories: managing the actual directory data and controlling access to the directory.

Managing directory content is application-dependent. AS/400 Directory Services provides two sets of tools that you can use. A set of AS/400 shell utilities provides the capability to view, change, delete, and rename directory objects. To access the QSH shell interpreter, use the AS/400-based Start QSH (QSH) command:

```
QSH
```

You can find more information on the LDAP shell utilities in AS/400 Information Center Web site (*http://publib.boulder.ibm.com/pubs/html/as400/infocenter.htm*) under the Networking drop-down, choose TCP/IP, choose TCP/IP Services and Applications, choose Directory Services (LDAP), and choose the LDAP command line utilities topic. You can also develop your own application using the C LDAP APIs that are provided as part of AS/400 Directory Services. The C APIs are widely portable, based on a draft Internet standard.

Documentation for these APIs is located in AS/400 Information Center under the Programming dropdown, choose CL and APIs, choose OS/400 APIs, choose APIs by category topic. Select the Directory Services category.

LDAP clients are available for many platforms from IBM and other sources. For IBM clients, see the IBM SecureWay Directory home page, *www.ibm.com/software/network/directory*.

In V4R5, the IBM SecureWay Directory Client SDK for Windows 95/98 and NT is included with your AS/400 Directory Services install, and it can be installed on your PC from your AS/400 IFS. Using AS/400

NetServer, map a network drive to the QDIRSRV share (/QIBM/ProdData/OS400/DirSrv, the QDIRSRV share is automatically set up when you install AS/400 Directory Services), and run the setup.exe program from the UserTools\Windows directory. This SDK includes command line utilities, C and Java client APIs, online documentation, and the Directory Management Tool (DMT). DMT is a GUI for managing directory data. It can be used to create, delete, and modify directory entries, edit the ACL for directory entries, and view/modify the directory schema. DMT can only be used with IBM SecureWay directories that support LDAP V3 (AS/400 V4R5 or later).

The LDAP standards (RFC 2849) define a standard data interchange format, the LDAP Data Interchange Format (LDIF). This defines a format for a text file that can be used to import data into the directory. For example, to add a new directory entry, you could create an LDIF containing these lines:

```
dn: cn=Mary Jones, cn=users, o=Deltawing,
dc=deltawing, dc=com
objectclass: ePerson
cn: Mary Jones
sn: Jones
givenName: Mary
mail: mjones@deltawing.com
telephoneNumber: 555.555.5555
ou: manufacturing
```

You can write an application that creates such a file from an existing database or creates a file containing periodic updates. Refer to the AS/400 Information Center Web site at *http://publib.boulder.ibm.com/pubs/html/as400/infocenter.htm* for more information on LDIF files.

You can also import an LDIF file into the directory using the AS/400 QgldImportLdif APIs or by using Operations Navigator. In OpsNav, IBM provides tools to import and export LDIF files from the AS/400 LDAP Directory. These tools can be found in the Directory pop-up context menu (accessed by right-clicking on the Network-Servers-TCP/IP-Directory node, Figure 3) and selecting the Tools option off that menu. The LDIF import utility can be used only to create new entries. It will not update existing entries.

The LDIF format is also understood by the ldapadd and ldapmodify shell utilities provided with the AS/400 Directory Services product. When used by the ldapmodify utility, LDIF files can be used to modify existing entries. LDIF files are a convenient tool for modifying the directory schema. By adding a changetype directive, LDIF files can be used to add, delete, modify, and rename entries. When used to modify entries, LDIF files can add, delete, or replace attribute values. This example shows how you might add a new objectclass, sampleObject, to the schema by using the changetype and add directives:

```
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: (
 oc-sampleObject-oid NAME 'sampleObject'
 DESC 'Used to store information about sample
objects.'
 SUP 'top' Auxiliary
 MUST ( sampleAttribute1 $ sampleAttribute2 )
 MAY ( description )
 )
```

ACL Model

Since the directory server is a network directory, access to the directory is not based on AS/400 authority and authentication mechanisms. Instead, the directory server defines its own authority model. Access to directory data is determined by the DN used to connect to the server. A DN can be a member of a group (an accessgroup or accessrole directory object) and the group DN used to grant authority to directory objects.

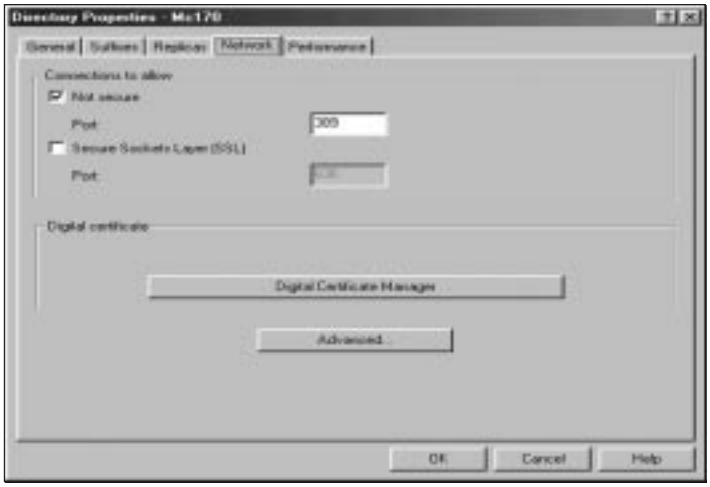

Figure 5: The Directory Server properties allow you to configure SSL and specify a server where your LDAP data is replicated, as well as some other configuration functions.

The authority model uses a sparse representation, meaning that objects that do not have an access control list (ACL) defined inherit the ACL of an ancestor object. The ACL identifies the owner, object authority, and attribute authority. The owner has all access to an object. Object authority specifies the authority other DNs have to create lower level objects, and to delete this object. Attribute authority defines the authority of other DNs to access the attribute values (e.g., email address). Attributes are classified into access classes (this is defined in the schema). You define authority to attributes based on the attributes' access class, and the operations that the user can perform on attributes in an access class.

These "pseudo DNs" are useful when defining ACLs:

- *cn=anybody*—Any LDAP client, including anonymous connections
- *cn=this*—The authority granted to cn=this applies to a client authenticated using the DN of the object being accessed
- *cn=authenticated*—All authenticated clients (those not using anonymous connections)

From Operations Navigator, you can work with groups or object authority. Select Authority from the Directory server pop-up context menu to view or edit the ACL. Select ACL groups to view, create, delete, or change accessgroup objects. The Directory's ACL is managed via server-defined attributes, so you can also use LDAP APIs, or some other LDAP application to modify the ACL-related attributes.

Using LDAP for Authentication

Using LDAP for authentication is straightforward. You simply use LDAP APIs to connect to an LDAP server using credentials provided by the user. If the authentication (bind) operation is successful, the user is considered authenticated. The credentials provided by the user could take the form of an LDAP DN and password. Or, rather than providing a DN, the application may be given the user's name or user ID. The application can perform an LDAP search to find the DN to use on the bind request. For example, given the user name *Mary Jones*, a search for *cn=Mary Jones* would provide the entry used in the examples. The application then binds as *cn=Mary Jones*, *cn=users*, etc. with the password the user entered.

Tip: If you are creating an LDAP entry for a person that also has an AS/400 user profile, you can set up the entry so that it uses the user's AS/400 password. You do this by creating an entry with a UID attribute

that contains the user profile name, but which does not have a userPassword attribute. In this case, the server verifies that the password used to authenticate is correct for the AS/400 user profile identified in the uid attribute. For our Mary Jones example, we can create your entry in this manner:

```
dn: cn=Mary Jones, cn=users, o=Deltawing,
dc=deltawing, dc=com
...
uid: MJONES
```

Publishing to LDAP from the AS/400

AS/400 Directory Services provides additional support for storing and retrieving information in an LDAP directory. A set of publishing APIs is provided that allows an application to send data to an LDAP server without the application needing to manage information like the server address, how to connect to the server, and where in the directory to put the information. These APIs also will retry operations that fail due to errors such as the server being down. The publishing APIs are documented in the AS/400 Information Center in the Directory Services topic.

To use these APIs, you first configure a publishing agent with the information necessary to connect and authenticate to a server (such as server, port, bind DN) and the location of your data in the directory (parent DN). The remaining APIs are used to publish objects under one of these agents. From AS/400 Operations Navigator, you can modify the publishing agent configuration from the Directory Services property page of the AS/400 system you wish to configure. Note that you reach this option by right-clicking on your AS/400 system in OpsNav, not the Directory server node under Network-Servers-TCP/IP that I referred to in the earlier part of this article. To reach the Directory Services Properties Panel, right-click on your AS/400 system and select Properties from the pop-up context menu. On the AS/400 Properties panel, select the Directory Services tab and that will bring up the panel where you can modify your publishing agent configuration. Tip: Be sure to use the Verify button when you're adding publishing agent information. In addition to verifying that the server and connection information is correct, it will also verify that the parent DN exists, and if not, optionally create it for you.

Two agents are predefined by AS/400 Directory Services for you to use. The Users agent will publish users from the system distribution directory to an LDAP server. The computer's agent will publish information about your AS/400 hardware and software.

The User's agent publishes users from the system distribution directory to an LDAP server and keeps the LDAP directory synchronized with changes made in the system distribution directory. You can then use the information that you publish in LDAP from applications like the **Netscape** Communicator address book using the Search directory function or from other LDAP applications that access address book information. Changes made in LDAP are not published back to the system distribution directory.

The Computers agent publishes information about your AS/400 to the directory. Directory Services will publish limited information identifying your AS/400 and the operating system. However, the Computers agent is also used by other products. Management Central publishes detailed information about your AS/400 hardware and software configuration. Netfinity for AS/400 can publish information about workstation and server inventory.

Quick Evolution, Important Results

LDAP and LDAP directories have quickly evolved from being viewed as a network address book to become an important part of network applications and operating systems. The AS/400 provides you with a directory server and the APIs and services needed to use LDAP on your AS/400 system. **Expert**

John A. McMeeking is a staff programmer in the IBM Enterprise Server Group in Rochester, Minnesota, where he has worked since 1992. John works on directory architecture and GUI design as a member of the AS/400 Directory Services team.

References and Related Material

AS/400 Directory Services LDAP Web page: *www.as400.ibm.com/ldap*

AS/400 Information Center Web site:

http://publib.boulder.ibm.com/html/as400/ and select Information Center. (You'll find AS/400 Directory Services under the Networking topic. Information about programming using LDAP is under the Programming topic; look in the Directory Services category.)