

LDAP. Your e-Business Directory

Leveraging LDAP for iSeries e-business applications | By Pat Fleming

Editor's Note: Part one of this two-part series on lightweight directory access protocol (LDAP) examines some of its uses for iSeries e-business applications. Part two will follow in a future issue.

Lightweight Directory Access Protocol (LDAP) is a client/server protocol for accessing a directory service. It was initially used as a front-end to X.500 but also can be used with stand-alone and other kinds of directory servers. Many technology companies, including IBM, Novell, Netscape and Microsoft* support LDAP, which allows users to locate organizations, individuals and other resources such as files and devices in a network, whether on the Internet or an intranet. And you don't need to know the domain name, IP address or geographic whereabouts. An LDAP directory can be distributed among many servers on a network, then replicated and synchronized regularly.

The good news is that as an iSeries customer you can take advantage of a LDAP solution that already exists on your iSeries today.

LDAP, the Internet Standard for Directory Access

Implemented using the client/server model, LDAP runs over TCP/IP using non-secure or secure sockets (SSL). The



client supports an API, and the server processes requests. The initial LDAP client implementation provided a C API, which is now available on most workstations and server platforms, including iSeries and Windows*. For Java* applications, Sun* Microsystems defined Java Naming and Directory Interface (JNDI), an API for accessing directories using LDAP (and other protocols). Sun and IBM both provide implementations of JNDI.

Directories accessed using LDAP are usually referred to as LDAP directories. LDAP servers can choose to provide gateway access to existing direc-

tories or implement directories that are only accessible using an LDAP client. Examples of products providing LDAP gateway servers are Lotus Domino* and Novell Network Directory Services (NDS). An example of an LDAP standalone directory that can be accessed only by an LDAP client is the IBM SecureWay Directory implementation, which is available on all IBM @server models, Windows NT/2000 and Solaris.

LDAP on iSeries

An IBM SecureWay Directory implementation is supported on iSeries starting with OS/400* V4R3. LDAP clients and an

LDAP server are provided free with Directory Services. In V4R5, Directory Services was included with the base operating system. LDAP clients for Windows and OS/400 provide APIs for use by both C and Java applications. The OS/400 client also provides APIs for use by all Integrated Language Environment (ILE) programming languages.

LDAP utilities are provided for common administrative tasks such as searching or modifying the directory and can be run from the OS/400 Qshell command environment or a Windows command prompt. To allow mail clients to search for e-mail addresses of OS/400 users, Directory Services enables System Distribution Directory (SDD) information to be published to an LDAP directory.

All IBM SecureWay Directory LDAP server implementations use the IBM Universal Database (UDB). When implemented on iSeries, this results in an LDAP directory that is scalable, robust and easy to manage. Millions of entries can be added to the directory with little impact on performance. Backup and recovery of the LDAP directory is performed using standard OS/400 administrative procedures. Configuration is accomplished using a wizard within Operations Navigator (V4R3 or later) in the TCP/IP Servers folder for your system. Select the Directory server and select "Configure."

LDAP with Domino

Domino R5 provides support for LDAP in two ways. First, applications can use LDAP to search a Domino server's directory. For example, a Netscape mail client could locate an e-mail address of a Domino user by configuring a Domino server to search secondary



directories. Second, a Notes client can access e-mail addresses of non-Domino users from both an intranet and the Internet.

LDAP with an HTTP Server

For Web serving, the IBM HTTP Server for iSeries supports LDAP in two ways. First, HTTP configuration information can be stored in an LDAP directory and shared across HTTP server instances. Second, the HTTP server can be configured to use an LDAP directory as a user registry for authentication of Web users. Both uses of LDAP by the HTTP server provide more efficient management of resources for e-business applications because server configurations and users can be defined once and shared within the network. The user registry also can be shared with other applications enabled to use LDAP, such as Domino and WebSphere* Application Server (WAS).

LDAP with WAS

For Web-application serving, both WAS Standard Edition and Advanced Edition for iSeries support LDAP directories as a user registry for authentication of users to Web resources. Multiple Web and application servers can be configured to share a single user registry, thus reducing management while increasing consistency of information.

LDAP Functionality

A set of Internet standards defines a consistent way to search for and manage entries in a directory. Each entry is one or more groups of attributes that are associated with a distinguished name (DN). Each entry in a directory has a unique DN. For example `cn=Pat Fleming,ou=Rochester,o=IBM`. Because a DN is comprised of one or more name components, the directory is hierarchical, much like the file systems on Windows and

iSeries. Each name component consists of an attribute name, for example cn (commonName), and an attribute value, such as "Pat Fleming." Directory entries can be placed below other directory entries, thus creating containers much like a folder contains files in Windows. The hierarchical structuring of entries into a tree is important for organizing data from multiple organizations and applications. The LDAP directory tree can easily be searched and secured.

LDAP implementations provide a common set of utilities for searching and managing LDAP directories. The following is an example of the search utility as performed from the Qshell environment. (Note: This example also works from Windows or UNIX* systems) To search the LDAP directory located on "myhost.ibm.com" for all entries of type "person" starting at "o=IBM" in the directories hierarchy:

```
ldapsearch -h myhost.ibm.com -b o=IBM
objectclass=person
```


From an LDAP-enabled Web browser, such as Netscape Communicator, this same search could be performed by specifying the following URL:

```
ldap://myhost.ibm.com/o=IBM??sub?object-
class=person
```

With V4R5, it's possible to use the Directory Management Tool (DMT) to manage an LDAP directory. DMT provides a user-friendly method for users and administrators to navigate, browse and update an LDAP directory. IBM LDAP directory implementations use a common security model for authentication and authorization based on access control lists (ACLs). By default,

directory entries are owned by the user creating the entry and can be searched by everyone. To help ease administration, security properties can be configured to automatically propagate down in the directory hierarchy. If you elect to do this, you can set the security properties at one point or level of the directory tree and all directory entries lower in the directory hierarchy will share the same security properties. You won't have to set the security of each new directory entry, unless it requires a different set of security properties. Both users and groups of users are supported. Operations Navigator provides administration of the LDAP directory security.

More to Come

Part two of this series will examine more of the details behind using LDAP with your iSeries and its applications including the use of extensible markup language (XML) with LDAP directories. 

Pat Fleming is senior software engineer for the iSeries in Rochester, Minn. He is currently an IBM WebSphere Application Server for iSeries architect. Prior to that, he was an OS/400 Directory Services (LDAP) architect. He can be reached at flemingp@us.ibm.co

For Further Information

- iSeries 400 Directory Services (LDAP): www.ibm.com/eserver/series/ldap
- IBM HTTP Server for iSeries: www.ibm.com/servers/eserver/series/software/http
- IBM WebSphere Application Server for iSeries: www.ibm.com/servers/eserver/series/software/websphere/wsappserver
- Domino Server for AS/400: www.ibm.com/servers/eserver/series/domino