Cameron Laird and Kathryn Soraiz manage their own software consultancy, Network Engineered Solutions, from just outside Houston, TX.

LDAP Comes of Age

It's time to talk about the Lightweight Directory Access Protocol (LDAP).

We've begun writing a column on LDAP every couple of weeks since last summer, then laid it aside in favor of more urgent topics. LDAP's story is a complex one, and knowledge about it is unlikely to pay off as quickly as it does for the latest scoops on operating system reliability or a powerful new application server. The Christmastime release of *Understanding and Deploying LDAP Directory Services*, by Timothy A. Howes, Mark C. Smith and Gordon S. Good (published by Macmillan Technical Publishing, 1998, ISBN 1578700701), however, capped a succession of LDAP events in 1998 that deserve mention.

Let's take a look at what happened and why it's likely to matter to you.

What is LDAP?

Before starting in on the technical characteristics of LDAP, it's useful to get a picture of the kinds of problems it solves. Let's use a typical workday as an example: You log into your Windows NT domain, your UNIX server and the license managers for a couple of monitoring applications. You complain to Human Resources that your paychecks are *still* being routed to the old building. You curse the efficiency of the janitorial staff because you left the latest company telephone list in the trash, forgetting that Chris in Graphics has a new extension. And you think to yourself, "Can't all these computers get together and stop making me answer the same questions over and over?"

LDAP promises to come to your rescue. LDAP is a protocol, like File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP). HTTP and SMTP, for example, are designed to provide for efficient transactions of Web pages and email messages, respectively. LDAP's target is information that fits into a directory, such as names, addresses, passwords, access authorizations, native languages and so on. LDAP is designed for a client/server architecture, which manages and uses directory information.

A useful LDAP application, therefore, has several pieces. For example, Netegrity Inc.'s SiteMinder product is an authorization and policy manager for Web applications. It includes components that manage information about Web visitors and provides access to that information.

Does that sound like a job for a DBMS? It is. In several aspects LDAP is a special-purpose DBMS. SiteMinder was originally tested on a relational DBMS like Oracle from Oracle Corp. By moving to LDAP, Netegrity was able to lower licensing costs and management overhead and improve SiteMinder performance and scalability.

LDAP: Not Just a DBMS

Don't be mislead into thinking LDAP is simply an inexpensive DBMS, however. Strictly speaking, LDAP is just the networking protocol. It's possible to feed that protocol through a gateway from a conventional DBMS and, in fact, several installations do exactly this. Very often, those who work with it say "LDAP" to abbreviate the entire system, including a specific data store and query interface, as well as the networking pieces that communicate through the protocol. SiteMinder uses Netscape Communications Corp.'s Directory Server as its data store. Directory Server, now available in Version 4.0, is tuned to high-performance

information delivery (accounts, passwords and so on) typical of directories.

Another difference between LDAP and DBMSs is an emphasis on replication. It might be advantageous to, say, store directory information about a particular department's employees on that department's server. Then, most LDAP inquiries from that department can be answered locally. The LDAP standard describes how data elements can be kept on more than one host and how different hosts cooperate to retrieve information not accessible locally. Distribution and replication of LDAP data stores are part of the definition of the protocol, although the complete specification of the latter is still under discussion. Netscape Directory Architect Mark Smith offers this definition:

"LDAP is an Internet standard protocol for accessing and updating online directory information. Online directories are most commonly used to store information about people and their roles and relationships, but LDAP can be used for any kind of data. A full definition of LDAP involves discussion of four important models:

• The LDAP information model, which defines the kind of data you can put into the directory.

• The LDAP naming model, which defines how you organize and refer to your directory data.

• The LDAP functional model, which defines how you access and update the information in your directory.

• The LDAP security model, which defines how directory information can be protected from unauthorized access."

Driving Force for LDAP

Smith is uniquely qualified to speak on LDAP. He was a driving force behind the development of the University of Michigan's LDAP reference implementation and a key designer of the university's directory service. Netscape hired him in 1996, along with coauthors of *Understanding and Deploying LDAP Directory Services* Good and Howes (also of the University of Michigan), and the center of the LDAP world moved from Ann Arbor, MI, to Mountain View, CA. The following year, Smith and Howes wrote *LDAP: Programming Directory-Enabled Applications with Lightweight Directory Access Protocol*. Also published by Macmillan, this was the standard printed reference before the publication of *Understanding and Deploying LDAP Directory Services*. Throughout this time, Smith has kept up with work for the Internet Engineering Task Force (IETF), most visibly as the author of several RFCs and Internet Drafts.

With the publication of *Understanding and Deploying LDAP Directory Services*, there's finally an authoritative "LDAP Bible," as the book's preface jokes. More precisely, "anyone who wants to know more about LDAP…will find the book useful." The authors emphasize that the book is primarily intended for three types of reader: decision makers, designers and administrators. In many ways, the "why" of LDAP has been more difficult to grasp than the "how." Most early LDAP publications were technical papers written to help programmers get started. Only now does this publication make clear the business significance of directory services, particularly in the maintenance phase. Most of the life cycle of LDAP applications is in administration, of course, so this focus is both overdue and welcome.

One of the merits of the book is it's organized realistically. Readers often don't want to read a technical book from cover to cover, but pick up a volume with one or two particular questions in mind, so the best books lead readers to particular answers efficiently. The 846 pages of *Understanding and Deploying LDAP Directory Services* appear in six parts. The organization is strong and clear so readers will be able to find the answers they need (Should we be using LDAP? What steps do I take to populate my directories accurately? Where can I find out more?) without mishap.

LDAP's Limitations

So if LDAP is so great, why aren't you using it?

First, the technology is relatively young. It was largely a research project until 1996. When *LDAP: Programming Directory-Enabled Applications with Lightweight Directory Access Protocol* was published in 1997, the book was most useful to working coders who already knew what they were building. At this point, LDAP inherited much of its feel from X.500, an earlier directory protocol of most importance to big projects in large organizations. Most LDAP histories emphasize its early development as a gateway to X.500.

Perhaps the biggest hurdle to LDAP's adoption is that, like most decisions about platforms, middleware or infrastructure, use of LDAP is intrinsically strategic.

Marketplace messages since then have been confusing. For much of this time, Microsoft Corp. and Novell Inc., the two vendors that most urgently need directory solutions for their respective products, have favored proprietary technologies. While Netscape has been way ahead of the field in its LDAP implementation, the early 1.x releases of the Directory Server failed to meet customer expectations.

Perhaps the biggest hurdle to LDAP's adoption is that, like most decisions about platforms, middleware or infrastructure, use of LDAP is intrinsically *strategic*. In contrast, you might change Web servers because of a single feature, such as reliability or performance. LDAP commitments are usually more involved than this. Selection of the right bundle of LDAP

server, LDAP software development kit(s) and LDAP maintenance tools demands delicate, careful analysis. Even when technical decisions are clear, organizational dynamics often handicap LDAP deployment. Efficient LDAP usage depends on adherence to standards and high-quality data, which strains the capacity for teamwork in many departments. Many of the initial benefits of LDAP deployment have to do with a reduction in maintenance costs. Sexier and more dramatic issues such as Y2K, multimedia and teamware easily command more attention than the "internal plumbing" that LDAP often seems to represent.

Whither LDAP?

LDAP's profile has improved dramatically in the past year. Novell Directory Services (NDS) is now compatible with LDAP, and Microsoft promises the same for its Active Directory. Netscape's Smith is proud of the progress his team has made since its first product release: "I am certain that Directory Server 3.1 is an exceptionally robust product." Customers have responded by purchasing 50 million user licenses in the past six months. Netscape lowers development hurdles by binding LDAP to several languages, including Java, JavaScript, Open Database Connectivity (ODBC) and Visual Basic. Well-known open-source projects such as Apache, FreeBSD, Linux, Perl, Portable Hypertext Processor (PHP), Sendmail, Python and Tcl all expanded their LDAP connections in 1998. In addition, the OpenLDAP Project emerged as "a collaborative effort to develop a robust, commercial-grade, fully featured and open-source LDAP suite of applications and development tools," according to its Web site.

Several prospective "killer apps" dependent on LDAP have also appeared. Perhaps the most interesting of these is Sun Microsystems Inc.'s Sun.Net remote access product. Sun.Net combines Internet commodity pricing with sophisticated security and access features to allow remote workers to use corporate computing applications, internal Web sites and network services inexpensively and safely. As Dr. Stuart Wells, senior director of Sun's Network Software products, explains, "This new technology will provide a secure, cost-effective connection from the public Internet…without the costs normally associated with building a virtual private network [VPN]–it's true ubiquitous access to corporate IT resources and your virtual enterprise." LDAP's contribution is to manage an access-control scheme that's flexible enough to span the requirements of both security and efficiency.

Netscape's Smith emphasizes LDAP's ability to help administrators solve several problems at once. "LDAP directories are valuable because they can help Web administrators solve a number of difficult problems. These include authentication of users, authorization (based on users, groups, roles and so on), sharing of configuration information between multiple instances of applications, server management and a variety of problems where an inexpensive, fast database is needed," Smith says.

LDAP is emerging as a technology organizations reuse in a range of development projects. Smith told us one of his favorite success stories is Ford Motor Co.'s Supplier Network. This suite of Web-based applications running on Ford's intranet has exacting requirements for large-scale authentication and authorization. "The performance characteristics, ease of integration and standard access protocol are some of the things that made them choose an LDAP directory service instead of an RDBMS," Smith says.

Even LDAP's thorniest problems seem to be improving. Schema standardization is progressing, with heavyweights like Cisco Systems Inc. and Microsoft supporting standards such as the Desktop Management Task Force Inc.'s Directory Enabled Networks (DEN) specification. Last year saw an explosion of activity in metadirectory technologies, which promise to rationalize many of the current challenges, especially the quality of data, in maintaining LDAP information. On the key technical point of when the IETF LDAP replication standard will be approved and widely implemented, Smith says: "We will see early products sometime in 1999, but the standard itself probably won't be stable until sometime in 2000."

LDAP's a keeper. Whatever hardware and applications you use, you're likely to be connecting to LDAP within the next few years. This is a good time to read *Understanding and Deploying LDAP Directory Services* to be sure you're ready for the changes.

Acknowledgments and Disclaimer

Our thanks to Merrill Cook, Alexandre Ferrieux, Randy Kunkee, Larry Virden and Jean-Claude Wippler for their discussions on LDAP and related subjects.

One of us (Laird) occasionally does business with Macmillan Technical Publishing. Bluntly, the amounts involved are too small to threaten the integrity of our assessment of the two Macmillan books mentioned in this column.

Companies Mentioned in this Article

Cisco Systems Inc.
170 W. Tasman Drive
San Jose, CA 95134
http://www.cisco.com
Circle 171

Desktop Management Task Force Inc.
200 S.W. Market St.
Ste. 450
Portland, OR 97201
http://www.dmtf.org
Circle 172

Microsoft Corp.
1 Microsoft Way
Redmond, WA 98052
http://www.microsoft.com
Circle 173

Netegrity Inc.
245 Winter St.
Waltham, MA 02154
http://www.netegrity.com
Circle 174

Netscape Communications Corp.
501 E. Middlefield Road
Mountain View, CA 94043
http://www.netscape.com
Circle 175

Novell Inc.
2211 N. First St.
San Jose, CA 95131
http://www.novell.com
Circle 176

OpenLDAP Project
270 Redwood Shores Pwy.
Ste. 107
Redwood City, CA 94065
http://www.openldap.org
Circle 177

Sun Microsystems Inc.
901 San Antonio Road
Palo Alto, CA 94303
http://www.sun.com
Circle 178