Isode's email and directory server products are used around the world by ISPs, Multinational Corporations, Governments, and Universities.

Whitepapers

LDAP and X.500

First Published in Messaging Magazine, September 1996

Introduction

The need for an industry standard directory has been articulated for many years. Many in the industry have promoted and continue to promote the ISO/ITU X.500 standard as the basis for this directory. Netscape, along with a number of other companies, recently announced that they would be supporting LDAP (Lightweight Directory Access Protocol) based directory services. This has led to a rapid growth of interest in LDAP, and has also led to substantial confusion as to what LDAP is and what it might become.

This paper describes X.500 and LDAP, including recent developments of both standards, and explaining the relationship between the two. It then looks at various scenarios for the evolution of both protocols, and then expresses views as to how X.500 and LDAP will be deployed. Finally, the paper considers some issues relating to the deployment of an Internet Directory.

What is Common to X.500 and LDAP

The most important thing to understand about X.500 and LDAP is that they have more in common than different. The things that they have in common relate to the information model and standard services, which are absolutely central to both X.500 and LDAP. This section describes the common core:

1. Hierarchical Names. LDAP and X.500 both define a hierarchical directory with hierarchical names. An example name is as follows: CN=Marshall T. Rose; O=Dover Beach Consulting; C=US This name represents the person with Common Name (CN) 'Marshall T. Rose', within the organization (O) 'Dover Beach Consulting', within country 'US'.

2. Typed Name Components. Name components are typed (Common Name, Organization, and Country in the example above). This contrasts with other schemes which have typeless names, such as the domain name scheme. As discussed later, it is straightforward to represent typeless names in a typed naming scheme.

3. Typed Objects. Objects are represented as Entries in an X.500/LDAP directory. These entries are given a type (or types), known as the object class, by use of an Object Class attribute. Typical object classes are People, Organizations, and Computers. X.500 and LDAP share object class definitions.

4. Typed Attributes. Information within objects is held as a set of typed attributes. For example there may be a 'telephone number' attribute with one or more values. Many attributes are encoded as strings. Other attributes have an encoding which is inferred from the attribute type. This can be used for non-string data such as pictures or to handled structured information. X.500 and LDAP share attribute type definitions.

5. Directory Operations. X.500 and LDAP share a common set of operations to access and manage data in the directory. These are: read; compare; search; add; delete; modify entry; modify rdn.

The rest of this paper will focus on differences, but the common core is important.

Core Services: X.500 (1988)

X.500 and LDAP both have their origins in the ISO/ITU X.500(1988) specifications, which were the result of work started in 1982. This section reviews the core concepts of this specification, which are not common to LDAP, or are needed to help understand the relationship between X.500 and LDAP:

1. Directory System Agent (DSA). The DSA is the core directory server. A single DSA will typically hold only a part of the data available in the total directory.
2. Directory User Agent (DUA). A DUA is the client process that accesses information in the directory. This could be a (human) user interface or embedded in another application.
3. Directory Access Protocol (DAP). DAP is the protocol which a DUA uses to access one or more DSAs. Thus it is the protocol which allows the client/server model of the X.500 directory.
4. Directory System Protocol (DSP). DSP is the protocol that DSAs use to talk to each other, and it carries the same operations as DAP, along with some DSA control information. These interactions are governed by a set of procedures for distributed operations, which enable a set of DSAs to provide a coherent service, with the DUA unaware of how the directory data is distributed between DSAs.

LDAP

LDAP (Lightweight Directory Access Protocol) arose from initial experience with deploying X.500 directory services on the Internet in 1989-91. Two DUA implementers (Marshall Rose and Tim Howes) developed lightweight protocols to communicate between a DUA and a gateway which mapped from LDAP onto X.500 DAP. It was clear that this was a more general requirement, which led three people (Wengyik Yeong, Steve Kille, and Tim Howes) to develop the LDAP standard under the aegis of the IETF OSI-DS working group. This resulted in RFC 1487, subsequently updated as RFC 1777.

The goal of the original LDAP was to give simple lightweight access to an X.500 directory, to facilitate the development of X.500 DUAs and use of X.500 for a wide variety of applications.

LDAP usage grew, and became a core component of X.500 activity on the Internet. There were several implementations, but by far the most significant and popular was the free implementation by University of Michigan Implementation, written by Tim Howes, Mark Smith and others. This package included a number of free LDAP DUAs. Following on from this, most suppliers of X.500 DSAs started to provide gateways to provide LDAP access by LDAP to DAP conversion.

Recently, there has been a substantial interest in LDAP, following the announcement by Netscape in conjunction with forty other companies that it will be adopting LDAP. This has led to a number of other companies announcing that they are “adopting LDAP”, and an increasing view that LDAP is synonymous with the Internet Directory.

Before looking further at the role of LDAP in relationship to X.500, it is useful to consider why LDAP is ‘simple’, relative to X.500:

1. Simple protocol encoding. While the LDAP PDUs are based on those from X.500, elements of the protocol have been modified to produce...
a protocol that is significantly simpler.

2. Names and attributes use text encoding. Names and attributes are pervasive in the protocol. In X.500, these have a complex ASN.1 encoding, whereas in LDAP they are given a simple string encoding. This is particularly helpful for applications that do not need to handle the detailed structure of names or attributes.

3. Mapping directly onto TCP/IP. LDAP maps directly onto TCP/IP (the Internet transport layer), and removes the need for a non-trivial amount of OSI protocol.

4. Simple API. The University of Michigan implementation has set a de facto API standard, published as RFC 1823. This is arguably the most important benefit, as it enables easy implementation of directory enabled applications. The X/Open XDS interface, which is the preferred API onto X.500, is much more complex.

5. LDAP relies on X.500 for the service definition and distributed operations. Because LDAP is defined as an access protocol to X.500 and not as a complete directory service, it is possible to specify LDAP very concisely. The detailed service definitions, while often intuitive from the protocol, are formally specified in X.500. Where the directory service is provided by more than one Directory Server, the procedures for doing this are not defined by LDAP.

The original LDAP was very clearly a lightweight access protocol to an X.500 directory. It is important to understand this clearly, when looking at the issues of providing a large scale directory service.

X.500 Evolution: X.500 (1993)

X.500 has evolved significantly, to encompass features not in the original X.500(1988) version. This has led to significant updates in the X.500 (1993) specification. Some smaller additions are also planned for X.500(1997). The major changes for X.500(1993) are:

1. Sophisticated replication using Directory Information Shadowing Protocol (DISP). Replication of data is critical for providing a robust directory service. X.500 DISP provides this service, and gives a lot of flexibility for different replication configurations.

2. Access Control. There is a standard and flexible mechanism for specifying access control. This is important to allow open and controlled management of data in the directory, especially when the data is replicated.

3. Improvements to information model. There are a number of improvements to the X.500 data model, based on experience with X.500 (1988). These include attribute subtyping, which allows related attributes to be handled in a clean manner and operational attributes, which allow directory management attributes to be distinguished from user data.

4. Administrative area model to help management. A mechanism is added whereby data can be grouped into administrative areas, and data (including access control) shared over this area by use of collective attributes. This is an important change for many operational environments.

5. A number of small changes to the overall directory service.

On the outside, the X.500(1993) directory has not changed a great deal. There has been significant change to the internal operations and management features, which address serious service and deployment issues.

LDAP Evolution
LDAP is also moving forward based on experience with the first version. Mark Wahl, Tim Howes, and Steve Kille started work in 1996 on a new version of LDAP under the aegis of the IETF ASID working group. This new work is known as LDAP version 3. The key elements of this new protocol are:

1. Access to X.500(1993) features. This allows an LDAPv3 client to access the new directory services defined in X.500(1993). In effect, LDAP is tracking X.500.
2. Security features. This includes access to the X.500 DUA/DSA peer authentication services and data confidentiality by use of the Internet Secure Socket Layer (SSL) protocol. It does not include access to X.500 signed operations.
3. Extensibility mechanisms. These allow new operations to be added without changing the core protocol.
4. Referrals. The original LDAP connected an LDAP client to a single server. The new LDAP allows an LDAP server to redirect an LDAP client to contact a different LDAP server.

An important, but frequently misunderstood, change is that LDAP version 3 does not require X.500 to be used as the back end. Many have interpreted this change as "the light and simple LDAP is now free of the complex and heavy X.500 baggage". This is not true, as LDAP relies on X.500 for much of its specification, and in particular for the service definitions. The change is that LDAP may be used in two distinct ways:

1. As a lightweight access mechanism to an X.500 directory.
2. As a lightweight mechanism to a server which is not X.500, but which provides the LDAP service. The server does not have to be X.500, but it does have to look like the LDAP abstraction of X.500.

In summary, LDAP version 3 has added a number of useful services to LDAP, and has increased the generality of LDAP's usage as a directory access protocol.

Directory Access and the Future of LDAP

This paper has described the history and state of the art of X.500 and LDAP. The rest of this paper will now consider and give views as to how this will move forward. This section considers directory access.

LDAP has an excellent future as a directory access protocol, and will become the access mechanism for directory service in the Internet, and the leading open directory access protocol. Reasons for this are:

1. It is simple and easy to implement.
2. It has good functionality.
3. LDAP access will be provided by all major directory vendors, because it can be mapped onto proprietary services or X.500.

LDAP version 3 will be the version adopted, because security and referral support are essential for many applications. Peer authentication is necessary for access control in the directory to be effective, and this is needed for effective management. Referrals will be needed to link Intranet directories, and to allow reference to other information services. These requirements will ensure rapid migration from the current LDAP standard.

The major alternatives to LDAP as an access protocol will be:

1. Proprietary, closed, access protocols. Because many environments...
will be able to operate without open protocols, there will still be a significant role for proprietary access.

2. X.500 DAP will have a role, particularly in environments that are using X.500 servers and require access to the signed operation services of X.500.

The increasing use of LDAP in applications will lead to a movement from proprietary to LDAP access. Because LDAP is easy to provide in an X.500 environment, this pressure will not affect X.500 DAP usage.

**Intranet Directories and the Future of X.500**

Moving on from access, the next level is to consider how a typical enterprise will provide a directory, usually in the enterprise Intranet environment. For most organizations, provision of directory is primarily an internal service, and so Intranet provision is the most important service issue. Where access is proprietary, provision will be proprietary. Similarly, where access is by X.500, provision will be by X.500. The interesting case to consider is the common case where access is by LDAP. There are three possible scenarios:

1. Proprietary provision. This is straightforward, and has the commercial (vendor) advantages of achieving vendor lock in, and allowing vendors to offer proprietary value add for this service provision. Many major vendors are likely to follow this path.

2. Provision by X.500. X.500(1993) has a range of features that make it well suited for providing an Intranet directory service. It is also directly aligned to LDAP. For this reason, many vendors will choose X.500 as the mechanism for providing an Intranet directory.

3. Provision by new protocols in the LDAP family. It would be possible to specify a set of open protocols in the LDAP family for replication, distributed operations, access control, and other features needed for providing an Intranet directory service.

The effort associated with driving a new set of open specifications, and the presence of options 1 and 2, will be strong factors to prevent 3 from happening. There will be strong market players pursuing both options 1 and 2. While there is a clear benefit to open provision of an Intranet directory, the requirement is not over riding. For this reason, the battle between proprietary and X.500 provision of Intranet directory is likely to be determined by the price and quality of the products on offer.

**The Future Internet Directory**

The spectacular success of the Internet now makes it certain that an Internet Directory and a Global Directory would be one and the same thing. There are two key problems to solve.

The first problem is that Internet Objects are named by domain names and mailboxes. For example:

www.netscape.com

S.Kille@Isode.com

An Internet Directory must provide mechanisms to allow objects to be named in this way. This will probably need to be in addition to the more general X.500 naming, as there are directory applications that will need to use a more general form of naming. A key challenge is to define the integration of domain names within X.500. A number of proposals have been made here and there is clearly not an industry consensus as to the best solution. Hierarchical encoding, with each domain component represented as
an X.500 Relative Distinguished name, as proposed in RFC 1279, is probably the best way forward. This X.500 encoding can be hidden from the end user. While the solution is not clear, the user requirement for the directory to operate with domain names is crystal clear.

The second problem is how to connect all of the Intranet directories into a single global directory. There are a number of solutions:

1. Don't do this. There is a clear view that a global directory is not really needed, and even if it was, most organizations would not be prepared to make available their data for it.
2. Use LDAP cross references. Where organizations wish to share data, they can simply managing cross references by manually adding them. This is only a partial solution, as it allows directories to connect, but does not create a global directory.
3. Use X.500 as the interconnect. This is the approach being advocated by many vendors and users. It is attractive in that X.500 was designed to solve this problem, and there are a number of commercial implementations, and significant deployment which demonstrates the potential of this solution. The demonstration of X.500 at the EMA Directory Challenge in 1997 will be a key test of this approach.
4. Use the Internet Domain Name System (DNS) as the interconnect. This makes sense in the context of domain names being used in an Internet directory service. An approach to do this has been proposed by Netscape (use of DX records). This has the advantage of simplicity, although even very small changes such as this to the DNS infrastructure have proved hard in the past.
5. Use of new protocols in the LDAP family. This would mean defining X.500 like system protocols and procedures for distributed operation, in order to use LDAP like protocols as the glue for an Internet directory. This is not easy to do, and it is not clear that it gives sufficient advantage over use of X.500 to be worth the effort.

Both of these problems will need to be resolved, with an approach which has broad industry consensus, before a global Internet directory can be achieved.

Conclusions

In summary, the following evolution of X.500 and LDAP is expected:

1. LDAP version 3 will be the most widely use Directory access mechanism, with X.500 DAP and proprietary mechanisms having some role.
2. Some Intranet Directories will be provided using X.500, and others using proprietary mechanisms. X.500 will only be a small factor in determining the most successful products.
3. To build a global (Internet) directory, industry consensus must be reached on two key problems:
   ○ How to integrate the domain name space into LDAP/X.500 based directory services.
   ○ How to interconnect Intranet directories. X.500 is a possible solution for this.

LDAP will have a key role to play as the preferred Directory Access Mechanism, although it will not become the Internet directory. X.500 will have a role, and possibly a very significant role in the provision of directory services.