Enterprise Directories and Security Management: Merging Technologies for More Control

Contents

Introduction

This document provides basic information concerning enterprise directories, discussing some of the common directory servers (DS) found currently on the market and how they relate to security administration.

The focus is lightweight directory access protocol (LDAP) and how it can be implemented to support enterprise security management. Despite limited claims that directory servers can be employed alone to achieve an enterprise security management solution, it is widely accepted that CONTROL-SA® and its components are still very necessary to system-wide security administration.

Directory Services

A directory service is a simple method of managing user data via a tree structure format. Directories in the form of address and telephone lists were created and used long before computers became a standard medium. Other common types of directories today contain organizational charts and security access control lists, some actually containing a built-in proprietary directory. IT professionals have long recognized the need for a system to centrally manage these directories and now many companies are spending large portions of their IT budget on implementing directory services solutions.

A brief history of LDAP

X.500 was one of the first standard directory access protocols (DAP) used to implement a directory service. This standard breaks down the directory service model into four parts:

- Data
- Tree structure
- Data operations
- Authentication

An example of a basic directory structure in X.500 is:

- Root (typically an organization name)
- Organizational unit (a department)
- Leaf object (person, group, application, etc.)

Each branch and leaf in the directory tree can contain attributes and values. For example, the root object may contain attributes such as organization, country, locality and domain name. The one rule enforcing conformity is that each entry in the directory must be unique (using node name and attributes).

X.500 is very robust and designed to allow the directory to be spread across the network. However, in order to accomplish the task, X500 relies on the OSI communications protocol (similar to TCP/IP), which is neither widely used nor popular. Additionally, X.500 places an enormous strain on computing resources and is a major management and implementation burden.

LDAP was created by developers at the University of Michigan to serve as a gateway between different X.500 servers. Its main design objective was to be easier to use and implement than X.500. For a communications protocol, the group chose the more common TCP/IP. The end result was that LDAP retained most of the functionality of X.500, but at a fraction of the implementation cost. After LDAP version 2 was provided with its own repository and easy-to-use APIs, it drew a lot of attention quickly becoming very popular. LDAP version 3 offers even more.

Several features have been added to version 3 making LDAP more practical:

- The ability to program automatic access and change the schema of the directory structure (it was manual in version 2)
- Secured sockets layer (SSL) is used to connect the APIs and the LDAP directory server
- Native support for digital certificates in an entry

A call to an LDAP directory server on the network is done through socket services using a well-known port, as with other services like “telnet”, “rsh” and “ftp”. The LDAP protocol has also been incorporated into the Internet URL syntax (i.e., ldap://www.site.org/). All major vendors that have, or will have LDAP support built into their products, are using the LDAP version 3 protocol.

LDAP today

The LDAP data structure was modeled after X.500 and the whole schema can be displayed in a directory and object-oriented format. The objects and their attributes are actually defined in RFC2256, which is published in many RFC repositories on the Internet. Each LDAP record is known as an entry. Each entry can belong to one or more object classes. Object classes may include individuals, groups of people, applications and products. The most important part of the entry is the distinguished name (DN).

All DNs must be unique and this is achieved by having one or more attributes such as an enterprise user ID, organizational unit, and organization. Attributes are usually limited to a minimum, making the directory more manageable. Other parts of the entry include further attributes and object classes, completing the data for that entry. Additional attributes for a *person* entry (e.g., object class=people) may include the following characteristics: common name, full name, surname, name of the supervisor and building location.

LDAP implementation on a much larger scale is a subject of growing interest. This exceeds organizational and biographical data concerning an individual, but may also incorporate:

- Inaccessible security systems
- Their particular user groups
- User IDs
- Passwords
- PKI certificates

Additional data is added and managed as attributes, or object classes on an entry within the directory. Some commercial LDAP directory servers provide limited integration into the more common security systems. For now, the majority of native security systems do not have direct LDAP support, thus requiring each organization to incorporate it where needed. Everything considered, LDAP carries a heavy price and a huge development effort. Moreover, once it's developed internally, organizations must face maintenance issues.

Free and commercially available LDAP version 3 servers

The University of Michigan LDAP Directory Server and a server group called Open LDAP is free with source code at ftp://terminator.rs.itd.umich.edu/ldap and www.openldap.com respectively.

When it comes to commercially available LDAP directory servers:

- Netscape's directory server continues to be the most popular and dominant on the market.
- Novell offers Novell Directory Services (NDS), an LDAP version 3-compliant server.
- Microsoft Windows 2000 and Exchange 2000 use the active directory, which has LDAP version 3 connectors.
- Sun and Netscape teamed up to provide the *iplanet* directory server (in reality, Netscape's directory server), also LDAP version 3-compliant.

Each of the noted LDAP directory servers is LDAP version 3-compliant. Any directory server that has LDAP version 3 APIs is considered to be LDAP-compliant.

The future of LDAP

Implementing an LDAP directory server is easy, if kept simple. Many software vendors and LDAP developers are delivering LDAP directory servers that offer out-of-the-box support for specific types of applications (e.g., email, HR, e-commerce, etc.). IT organizations are ending up with multiple LDAP directory server repositories. A new technology, called "meta-directories", is emerging to meet this new challenge. A meta-directory is simply an LDAP directory server providing connections to multiple directories. On the surface it has the look and feel of an LDAP directory server with the ability to hold massive amounts of information. However, meta-directories don't contain actual data. Instead, they contain pointers indicating specific servers and where the data resides on them. Standard LDAP APIs (referred to as connectors) are called upon to pull out the

information as requested, hiding the underlying infrastructure. Sometimes the data is replicated using connectors incorporating specific rules concerning when data is propagated in or out of the meta-directory.

LDAP and CONTROL-SA

LDAP directory services and CONTROL-SA are two technologies that when integrated provide complete enterprise security administration. Since the data structure in CONTROL-SA is very similar to that of an LDAP directory server, it really comes down to three basic points of integration:

- CONTROL-SA can be engineered to use an LDAP directory server as one of its many sources.
- Another alternative is to make CONTROL-SA LDAP-compliant by integrating native LDAP APIs into the existing CONTROL-SA application.
- The most beneficial point of integration is to position an LDAP directory server as a managed resident security system, using the asynchronous capabilities of the CONTROL-SA Universal Security Administration API (USA-API).

The CONTROL-SA organizational tree and enterprise user

The Enterprise SecurityStation® manages the key repository for CONTROL-SA. It contains two entities, which together become an X.500 directory. These are the organization and enterprise user.

An enterprise user record has configurable attributes (keywords) like name, supervisor, email address, etc. The entity can be connected to an object in the organization, such as an organizational unit.

This is the basic underlying concept of X.500 directories. Since LDAP was developed using X.500 as its data structure, objects in CONTROL-SA can now be mapped directly to those found in most contemporary LDAP directory servers.

Enterprise security administration with an LDAP repository

Using an LDAP directory server as the repository for CONTROL-SA is considered a suitable alternative to the relational database management systems (RDBMS) in use today. LDAP supports the attributes necessary to:

- Identify a person in the organization
- Identify that person’s role and organizational user IDs
- Store passwords and PKI certificates

With such apparent compatibility between LDAP and CONTROL-SA, the following questions then arise:

- Why isn’t LDAP widely used as a solution for enterprise security management?

- Why doesn’t Enterprise SecurityStation bring into play LDAP?

Part of the problem is that LDAP does not store all of the access control lists (ACLs) and group access methods for each security system out-of-the box. To program these objects as additional attributes would entail a huge effort. The values of the attributes would need to be populated by the connectors, which would also require programming. Additionally, one of the few weaknesses of LDAP is that it was never designed to administer updates on the same level as an RDBMS. Consider the number of times per day that an LDAP entry would need to be updated in order to support functions such as password synchronization, creating and modifying new accounts, connections to security groups, intercepting native administration, and more.

LDAP could contain and manage such security attributes and stay in sync with outside feed sources, but this would defeat its original purpose, transforming LDAP from a “lightweight” to a “heavyweight” directory access protocol server.

CONTROL-SA developers have spent years perfecting the technology to do just this. CONTROL-SA continues to be the most comprehensive, flexible and reliable solution on the market today. CONTROL-SA role-based security access management is powered by a high performance RDBMS, better suited for this kind of business process than an LDAP directory server is. It will also remain the primary repository for the Enterprise SecurityStation, with asynchronous electronic links to other sources such as directory servers and Human Resource applications.

LDAP directory servers as authentication servers

Many applications are offering authentication to be provided by a directory server. Solaris 2.8 offers LDAP authentication And Microsoft Windows 2000 authenticates to its own Active Directory. Nevertheless, these offerings only address initial entry into the server and do not consider user access after authentication. That access must be managed by means of an interface to the security attributes.

A further issue is that the more demands placed on the LDAP directory server, the longer authentication will take. Unfortunately, the user community cannot afford the extra seconds during authentication in order to consolidate and streamline security administration.

LDAP directory servers as enterprise security servers

Nearly all LDAP directory servers can include attributes in the schema for added support with other LDAP and non-LDAP-compliant applications and security systems. The communication is done using connectors, which can be native to the directory server, or through a collection of third-party scripts. Implementation is a major undertaking. Most connectors to other LDAP directory servers use bi-directional replication, having a dramatic effect on performance. Connectors to non-LDAP security systems are typically

one-way and they do not have a means of reverse synchronization. As a result, if there is a connector to a Unix system, an account can be pushed out, but the directory server cannot know when native security changes have been made (e.g., add/delete/modify users).

CONTROL-SA, LDAP and LDIF

Although an LDAP directory server may not be an ideal primary repository for all enterprise security attributes, it still holds promise as a general look-up service (its original purpose). Many applications are using it currently, while many more will have LDAP services written in. However, CONTROL-SA must be considered the primary source for the security attributes feeding an LDAP directory server, including the various security systems and user groups a person may access. Alternatively, CONTROL-SA is best utilized when fed changes in the organization, such as new employees and their specific roles. Using role-based access controls (RBAC) automation in CONTROL-SA enables new users to be set up instantly and in some cases the data is fed directly to an LDAP directory server.

Many sites are using or considering an LDAP directory server to provide access to human resource-related data. Tight integration can be set up, requiring minimal efforts by using LDAP, CONTROL-SA command line utilities and APIs. For example, LDAP directory server information can be dumped into a flat file using freely available tools such as those published by Mark Wilcox at *www.mjwilcox.com*. Netscape also provides command line tools and PERL scripts to export and import LDAP data. Each of the tools used with non-LDAP directory servers tend to work with a file in the LDAP data interchange format or LDIF.

Any LDAP Directory Server can read an LDIF file. These files are easily parsed (Shell Script, PERL, etc.) into a set of transactions executed on the Enterprise SecurityStation. Such transactions add users to their respective organizational units and initiate any RBAC automation to create accounts on all managed resident security systems. This style of integration is popularly used in IT organizations today.

Current efforts by CONTROL-SA developers will result in an LDAP-compliant front-end into CONTROL-SA. Using the LDAP protocol, CONTROL-SA will communicate bi-directionally with other LDAP directory servers and meta-directories by using a CONTROL-SA LDAP directory server. This would mean that LDAP APIs could be used by any other LDAP-compliant application. Eventually, Enterprise SecurityStation® API could perform the required actions.

Integration can be carried out as described previously, or as part of a replication process. Many LDAP directory servers, such as Netscape's Directory Server, provide a replication server with their product in which a set of replication rules are defined. Parts of that server are replicated to another server, or come from within other LDAP directory servers.

Communicating with the enterprise via CONTROL-SA creates an LDAP front-end directory servers, leaving a back-end LDAP working as a highly efficient application for security administration with a high performance RBMS engine.

LDAP: A managed resident security system (RSS)

The LDAP directory server brings the organization yet another set of security ACLs and consequently the need to manage them. The LDAP directory server should (and usually does) require some form of authentication. The authentication process in effect validates someone in the directory. CONTROL-SA currently supports any LDAP-compliant directory server using an open LDAP version of its agent technology. This includes directory servers like Netscape, *iplanet* and PeerLogic (recently acquired by Critical Path). The agent requires a discovery process and mapping of the schema objects to objects in CONTROL-SA. CONTROL-SA provides agents for Microsoft's Exchange 5.5, the Windows 2000 active directory and Novell's NDS. These agents are pre-configured to manage LDAP directory servers, and may require some additional configurations based on site modifications to those directory schemas. With CONTROL-SA USA-API (the backbone of CONTROL-SA agent technology), it is possible to manage any of the LDAP directory servers listed in this document and any others that are LDAP version 3-compliant.

In addition to its importance in LDAP applications, the CONTROL-SA USA-API is probably the most essential aspect of integration. The USA-API also manages the legacy security systems across a multitude of platforms and applications such as OS/390, Native Unix, Windows NT, AS/400, VMS, Tandem, RDBMSs, and ERP environments.

CONTROL-SA has the ability to communicate asynchronously with itself and with another managed resident security system (RSS). Using the association facility in the Enterprise SecurityStation, the enterprise user record and organizational tree can be populated during a download of RSS data. The organizational tree and enterprise user can become a mirror image of LDAP directory server data. Since native RSS administration activity (i.e., add users, update users, etc.) is always sent to the Enterprise SecurityStation during the agent interception process, data between the RSS and Enterprise SecurityStation remains in sync.

Whether security administration is done through Enterprise SecurityStation, or locally in the RSS by another method (e.g., administrators, batch jobs, etc.) is of no consequence. The association facility will always detect new entries added locally and decide what to do with those entries in relation to the Enterprise SecurityStation organizational tree.

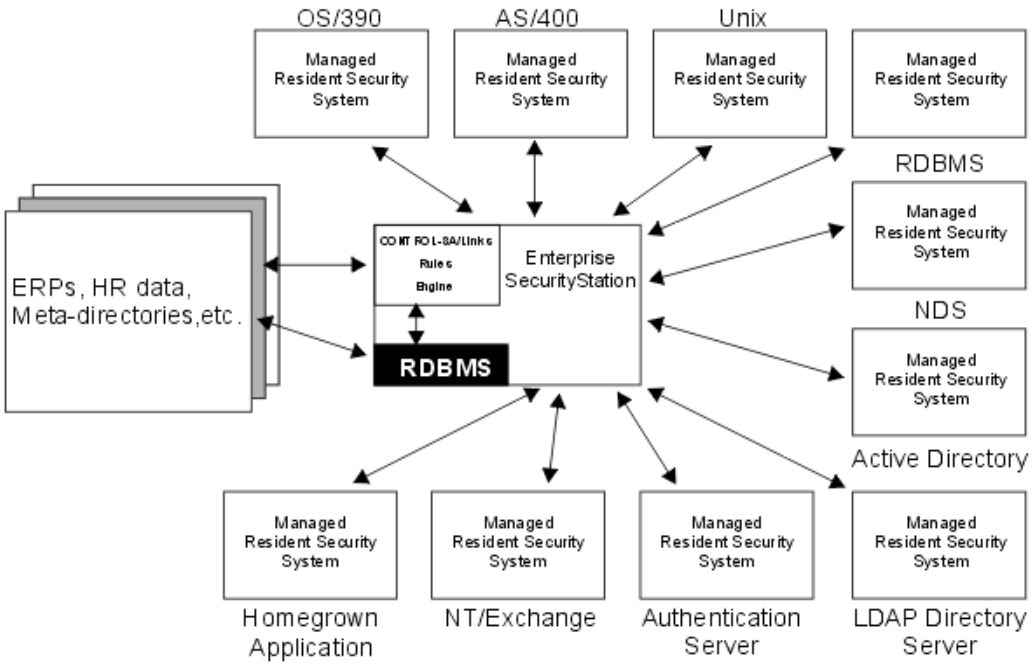
CONTROL-SA/Links offers additional capabilities. CONTROL-SA/Links is a product that supports message and rule-based automation. Both CONTROL-SA/Links and/or the download exit can apply the native changes to the enterprise user and the organizational tree using site-specific business rules and policies.

Active directory and CONTROL-SA

Today many companies are involved with the erroneous task of converting legacy NT domains to an active directory forest. There are many new features that Microsoft has added to the active directory to help manage users and their desktops. The active directory, like other directory servers allows the creation of an organizational tree, from which organizational units can be created, containing users and computers. The CONTROL-SA Windows 2000 Agent asynchronously manages the organizational tree in the active directory as well as its objects. Where an object is placed in the active directory tree can determine what logon scripts are executed, what software is delivered, desktop properties and a multitude of other security policies. All this is achieved by applying a Group Policy Object (GPO) to the organizational unit.

The CONTROL-SA organizational tree can be used as an initial source for the active directory. This tree can be a combination of several directory servers and ERP applications like PeopleSoft and SAP.

The tree can be used entirely, or partially, when objects are created and placed in the active directory. This can expedite the migration from Windows NT to the active directory, especially when Windows NT domains are also in the Enterprise SecurityStation. If the active directory is going to be maintained outside of the Enterprise Security department, the asynchronous communication in the CONTROL-SA Windows 2000 agent can detect changes to the active directory (e.g., creation of organizational units). The rules engine in CONTROL-SA/Links can propagate all or some of these changes to the organizational tree in the Enterprise SecurityStation.



This drawing illustrates how data from LDAP and non-LDAP-compliant applications and security databases can be linked and managed using CONTROL-SA .

Summary

LDAP directory servers are an important asset in information management. Software vendors continue to find new and innovative ways to incorporate LDAP into their products. It's easy to use, open-ended and simple implementations can be done rapidly.

However, tackling enterprise security using an *off-the-shelf* LDAP directory server can prove to be a major undertaking. There are many aspects of enterprise security, like role-based access controls, that are not addressed when an LDAP directory server is the only tool. Because CONTROL-SA offers multiple integration points into LDAP directory server and legacy security systems that are not LDAP-compliant, it is worthwhile to combine the two technologies.

There is no need to go through a lengthy LDAP design process to include management of all possible security attributes, since the technology in CONTROL-SA already achieves this. It does make sense to include attributes in the LDAP directory such as a common user ID, password, and/or digital certificates. By combining one or more LDAP directory servers with the CONTROL-SA Enterprise SecurityStation and asynchronous USA-API technology, the result is a more functional and higher performance enterprise security management solution.

For more information view BMC Software on the Internet at www.bmc.com.

Assuring Business Availability™

100036467 2/01