LDAP

RONAK PAREKH[1] AND GREGOR VON LASZEWSKI[2]

[1] *School of Informatics and Computing, Bloomington, IN 47408, U.S.A.*
[*] *Corresponding authors: parekhr@indiana.edu*

project-001, April 2, 2017

LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network. In a network, a directory tells you where in the network something is located. On TCP/IP networks (including the Internet), the domain name system (DNS) is the directory system used to relate the domain name to a specific network address (a unique location on the network).LDAP allows you to search for an individual without knowing where they're located (although additional information will help with the search).An LDAP directory can be distributed among many servers. Each server can have a replicated version of the total directory that is synchronized periodically.

Keywords: LDAP, directory, authentication, X.500, commands, design

https://github.com/cloudmesh/sp17-i524/blob/master/paper1/S17-IR-2024/report.pdf

INTRODUCTION

LDAP (Lightweight Directory Access Protocol) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol network.[1] LDAP is based on the client/server model of distributed computing. It has evolved as a lightweight protocol for accessing information in X.500 directory services.[2] LDAP is specified in a series of Internet Engineering Task Force(IETF) Standard Track publications called Request for Comments (RFC's), using the description language ASN.1. LDAP is based on a simpler subset of the standards contained within the X.500 standard.

BACKGROUND

LDAP was a result of the X.500 series of International Telecommunication Union (ITU) recommendations. X.500 is a set of recommendations about directories. [2] Because of this relationship, the structure of X.500 and LDAP is similar. LDAP directory implementations are often X.500 compliant and gateways between the two directories are plentiful. LDAP is defined by a set of published Internet standards, commonly referenced by their Request For Comment (RFC) number. The main reason for the emergence of LDAP can be attributed to the fact that X.500 was too tied to the OSI (Open Systems Interconnection) protocols, making it out of favour for the TCP-dominated world that was emerging. LDAP and Domain Naming System solved problems in a simpler way and thus, LDAP started becoming widely used. [2]

WHY LDAP OVER X.500?

The success of LDAP has been largely due to the characteristics that makes it simpler to implement and use as compared to X.500. LDAP runs over TCP/IP rather than the OSI protocol stack. The availability of TCP/IP is more and it consumes less resources. The functional model of LDAP is simpler i.e it removes less frequently used, duplicate and esoteric features, making it easier to implement and understand. LDAP uses strings to represent data rather than Abstract Syntax Notation One (ASN.1) which is considered much more complicated.[2]

LDAP ARCHITECTURE OVERVIEW

LDAP defines the content of messages exchanged between an LDAP client and an LDAP server. There are some operations such as search, modify, delete which are specified by the messsages requested by the client or responses from the server. The messages also describe the format of the data it carries [3]. The messages are carried over a TCP/IP protocol and thus, there are operations to establish and disconnect a session between the client and the server. The factors to be considered while designing the LDAP directory are the logical model which is defined by the messages and data types, the organization structure of the directory, the possible operations to be perfomed on the directory and the security of the information carried in the messages.[1]

The general interaction between an LDAP client and LDAP server is as follows:

The first step is known as Binding step. In this step, the client establishes a session with the LDAP server. The client specifies

the host name or the IP address and the TCP/IP port number where the LDAP server is listening. The client can provide a user name and a password to properly authenticate with the server. Data encryption can also be used while establishing a session to inmprove security. The client then performs operations on directory data. LDAP offers both read and update capabilities. Thus, the directory information can be managed as well as queried. Searching is a common LDAP operation where user can specify what part of the directory to search and what information to return. When the client is finished making requests, it closes the session with the server which is known as unbinding. The LDAP directory stores and organizes data structures known as entries. A directory entry usually descibes an object such as a person or a server and so on. Each entry has a distinguished name (DN) that uniquely identifies it. The DN consists of a sequence of parts called relative distinguished names (RDNs). The entries can be arranged into a hierarchical tree-like structure based on their distinguised names. The tree of directory entries is called the Directory Information Tree. [2]

Each entry contains one or more attributes that describe the entry. Each attribute has a type and a value. A directory entry describes some object which in general is called as a template. The following operations are defined by LDAP for accessing and modifying directory entries:

- Adding an entry
- Deleting an entry
- Modifying an entry
- Comparing an entry
- Moving an entry

A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agen (DSA), by default on TCP and UDP port 389, or on port 636 for LDAPS. The client sends an operation request to the server, and the server sends responses in return. The client does not need to wait for a response before sending the next request, and the server may send the responses in any order. The client may request the following operations: StartTLS, Bind, Search, Compare, Add entry, Delete Entry, Modify Entry, Abandon, Extended Operation, Unbind. The server may send Unsolicited Notifications" that are not responses to any request.

DESIGNING AND MAINTAINING LDAP DIRECTORY

The designing of an LDAP directory are distributed into four phases [4]

- First Phase: The first phase is defining the directory content. It has two components: First component is to define the directory requirements which is to carefully analyse the main purpose of the directory and the consideration to arrive to a holistic approach for the directory plan. The second component is the designing of data which is to understand the source and nature of the data. The scope of the data within the directory is decided and its integration with external data is planned. [4]
- Second Phase: This phase is also divided into two components. First is designing the schema and determining the format in which the data is to be stored. The second component is desinging the namespace and determining the hierarchical structure of the directory.
- Third Phase: This phase involves securing the directory entries. The privacy and security of the data in the directory is the main area of focus. The applications using the directory should also be secured and their security is also considered in this phase.
- Fourth Phase: This phase involves in designing the underlying network infrastructure and designing the server. This phase involves the topology design which helps to determine the number of servers and the location of their directory services. It also considers about the distribution of data amongst the servers. Replication can also be considered in this phase, which enables multiple copies of the data to be deployed. [4]

LDAP COMMAND-LINE TOOLS

LDAP protocol operations are divided into three categories: Authentication, Interrogation, and Update and Control. The LDAP C-API provides a number of simple command-line tools that together covers all three categories [5].

- ldapbind: It authenticates to a directory server. It can also be used to check whether a particular server is running or not.
- ldapsearch: It searches for specific entries in a directory. It opens a connection to a directory, authenticates the user performing the operation, searches for the specified entry, and prints the result of the search operation.
- ldapadd: It adds an entry to the directory. It opens a connection to the directory and authenticates the user and opens the LDIF file supplied as an argument and adds each entry in the file in succession.
- ldapdelete: It removes the leaf entries from a directory. It deletes the specified entry by opening a connetion and authenticating the user.
- ldapmodify: It modifies the existing entries by opening a connection to the directory and opening the LDIF file supplied and then modifies the entry.
- ldapmoddn: It changes the RDN of an entry. It moves an entry or subtree to another location in the directory.

FUTURE OF LDAP

The future of LDAP lies in refinements to LDAPv3. The most recent improvements added include upgrades to managements GUIs that allow easier modification of users and their attributes. The greatest challenge is one shared with any other directory service which includes Active Directory. LDAP's ability to adapt to the changes in delivery of identity and access management which could be possible through new types of authentication such as biometrics or through Software as a Service (SaaS) models. The key features to LDAP's future are its ability to be flexible, scalable and adaptable with new technologies. [2]

CONCLUSION

By reviewing the features and implementation of LDAP, we can conclude that LDAP is lightweight and a Standard wire protocol. LDAP has emerged as a mature protocol for accessing directories. Its servers provide a number of security features such

as automatically encoding passwords with one-way digests, its support for extensible authentication via the SASL framework. It includes general purpose data storage which can hold information about users and groups. Alongwith a variety of features LDAP supports high availability, disaster recovery and logging options to boost its usability. Thus, making LDAP extremely effective.

REFERENCES

[1] Wikipedia, "Lightweight directory access protocol," Web Page, Feb. 2017, online; accessed 20-Feb-2017. [Online]. Available: https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

[2] S. Tuttle, A. Ehlenberger, R. Gorthi, J. Leiserson, R. Machbeth, N. Owen, S. Ranahandola, M. Storrs, and C. Yang, *Understanding LDAP*, 2nd ed. Greenwich, CT, USA: Redbooks, 2004. [Online]. Available: http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg244986.pdf

[3] Sun Microsystems, Inc., "How ldap servers organize directories," Web Page, Feb. 2006, accessed 2017-02-21. [Online]. Available: https://docs.oracle.com/cd/E19203-01/819-1160-13/ldap.html

[4] Chris Wilson, "Designing and maintaining ldap directory services," Web Page, Feb. 2012, accessed 2017-02-22. [Online]. Available: https://niccs.us-cert.gov/training/search/skillsoft/designing-and-maintaining-ldap-directory-services

[5] Sun Microsystems, Inc., "Ldap command line tools," Web Page, Feb. 2002, accessed 2017-02-21. [Online]. Available: https://docs.oracle.com/cd/B10501_01/network.920/a96579/comtools.htm