IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 7.301

Volume 3, Issue 2, January 2023

Review Paper on the Light Weight Directory Access Protocol

Sharan L Pais[1], Madhu M[2], Madhushree[3], Meghana K[4], Mohammed Firoz[5]

Faculty, Department of Information Science and Engineering[1]

Students, Department of Information Science and Engineering[2,3,4,5]

Alva's Institute of Engineering and Technology, Mijar, Mangalore, Karnataka, India

Abstract: *External LDAP directories currently use directory servers such as MS Active Directory, OpenLDAP, OpenDJ, etc. to store user, group, and authorization information and then provide that information organization's enterprise applications. This is considered a standard technique. Most organizations prefer external LDAP because the authentication protocol is very simple. The proposed system uses an external Lightweight Directory Access Protocol (LDAP) to manage and authenticate user information inside and outside the organization. This external LDAP directory stores various user information. This information can be later retrieved by other users, depending on their access level. Various applications also use this technology to ensure that authenticated users provide correct authentication data. This data must match the information stored on your LDAP server.*

Keywords: LDAP; client; server; authentication; database; synchronization

I. INTRODUCTION

External LDAP is designed in such a way that it should provide a directory where it can store all the information related to users or groups or permissions which will be the sameas a telephone directory. In the same way that a telephone directory functions, external LDAP is created to offer a directory where all user, group, and permission-related data can be stored. It resembles a file system hierarchy and functions as a database that can store all user-related data in a tree-structured format. External LDAP offers a strong layer of services, including looking for sophisticated filters that demonstrate robustness Entity with characteristics that permit limited data access. Several programs rely on external LDAP for authentication. In External LDAP, processes like queries perform very quickly, and a large, complicated system can use LDAP for a variety of write and update actions. The flexibility is provided through external LDAP.

II. THE LDAP FRAMEWORK

LDAP operations are based on a client-server model. Each LDAP client uses the LDAP protocol running over TCP/IP to retrieve data stored in the directory server database. LDAP clients are either directly controlled by servers installed on LDAP or managed by applications that interact with LDAP. on figs.

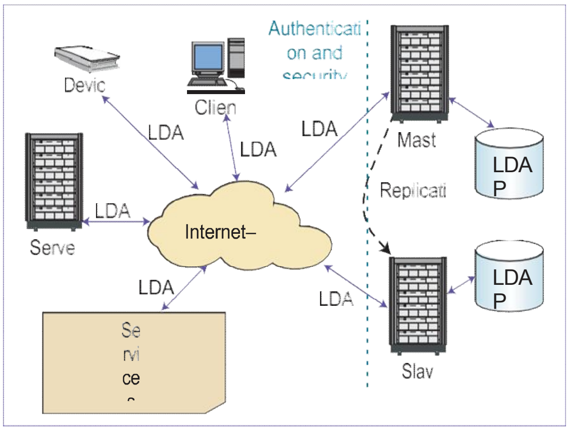


Figure 1. The LDAP framework. Devices and servers use the LDAP protocol to access a stored in LDAP server databases.

DOI: 10.48175/IJARSCT-8036

Figure 1 provides an overview of the LDAP architecture where many devices (such as printers and routers) and servers (such as mail servers) can access data stored in a database on a given LDAP server.

LDAP clients accessing the LDAP server must be authorized using an authentication mechanism that can implement a variety of security protocols. as pictured. 1, Replication is distributed among cooperating LDAP servers, with the primary LDAP server (master) sending updates to read-only replica servers (slaves).

Two components are important to the LDAP structure. An LDAP-adapted database or directory and an XML- based data representation format

III. TECHNICAL OVERVIEW OF EXTERNAL LDAP

An easy-to-use protocol called External LDAP is used to communicate with a directory database that handles query operations such as adding or changing user information. The information exposed by external LDAP depends on the relationship between structural elements. This section describes some of the components of external LDAP.

- **Attributes:** Elements also called attributes, are used to store all data stored in an external LDAP system.
- **Entry:** The Attributes that are not linked to anything in the external LDAP are meaningless. So, this is a set of properties under a name that can be used to describe something. Attributes are meaningless unless they are linked to an external LDAP. So, a group of properties grouped under a name is something you can use to define something.
- **Data Information Trees:** All entries are added to the external LDAP server as branches of a tree known as the Data Information Tree or DIT.

There are a few External LDAP protocol variations:-

1. ldap://: This is the underlying external LDAP protocol that provides structured access to external LDAP directory services.
2. ldaps://: Again, encryption is highly recommended when using external LDAP on an insecure network.
3. This type is used to specify external LDAP over SSL/TLS.
4. ldapi://: LDAP is often used for administrative purposes to securely connect to local networks. This means external LDAP over IPC.

Instead of using open network ports, they communicate through internal sockets. LDAP is just a protocol that defines a mechanism for interacting with directory services. We should have a fairly clear understanding of the external LDAP protocol and how the external LDAP implementation interprets user data.

From Fig 1 we can see there are 2 groups of users

- **Administrator or Support Staff:** These people keep external LDAP entries like users, groups, etc.
- **Internal and External Users:** They can manage data in an external LDAP directory and change information in an external LDAP directory using the LDAP Account Manager (LAM) self-service.

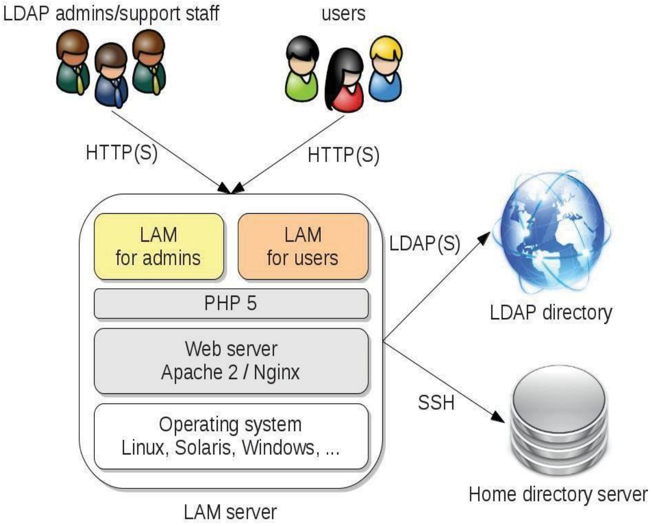


Fig. 1. Architecture of External LDAP

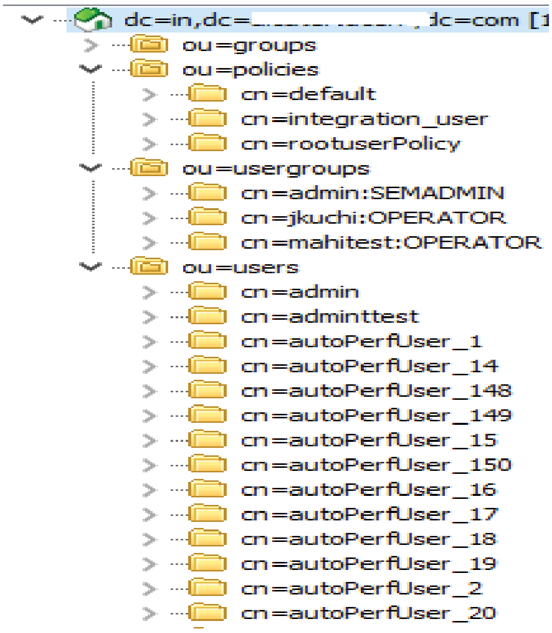
DOI: 10.48175/IJARSCT-8036

There are 2 types of LDAP Account Managers [LAM]

1. **Admins:** LAM for admins allows the management of various users, hosts, groups, etc. It can also include tools for bulk uploading users and maintaining account profiles.
2. **Users:** LAM for users allows users to change their personal information in the directory server. This external LDAP account manager runs on PHP and is operating system independent.
3. **Home directory server:** It can be managed inside LAM and resides on the server where LAM is installed. Home directory server commands are protected by SSH. LAM uses the LAM administrator username and password for authentication.
4. **LDAP Directory:** This external LDAP directory connects to the LDAP server using standard protocols and also supports encrypted connections such as SSL and TLS.

IV. STRUCTURE OF EXTERNAL

4.1 LDAP Directory



```
dc=in,dc=[redacted],dc=com [1
    ou=groups
    ou=policies
        cn=default
        cn=integration_user
        cn=rootuserPolicy
    ou=usergroups
        cn=admin:SEMADMIN
        cn=jkuchi:OPERATOR
        cn=mahitest:OPERATOR
    ou=users
        cn=admin
        cn=adminttest
        cn=autoPerfUser_1
        cn=autoPerfUser_14
        cn=autoPerfUser_148
        cn=autoPerfUser_149
        cn=autoPerfUser_15
        cn=autoPerfUser_150
        cn=autoPerfUser_16
        cn=autoPerfUser_17
        cn=autoPerfUser_18
        cn=autoPerfUser_19
        cn=autoPerfUser_2
        cn=autoPerfUser_20
```

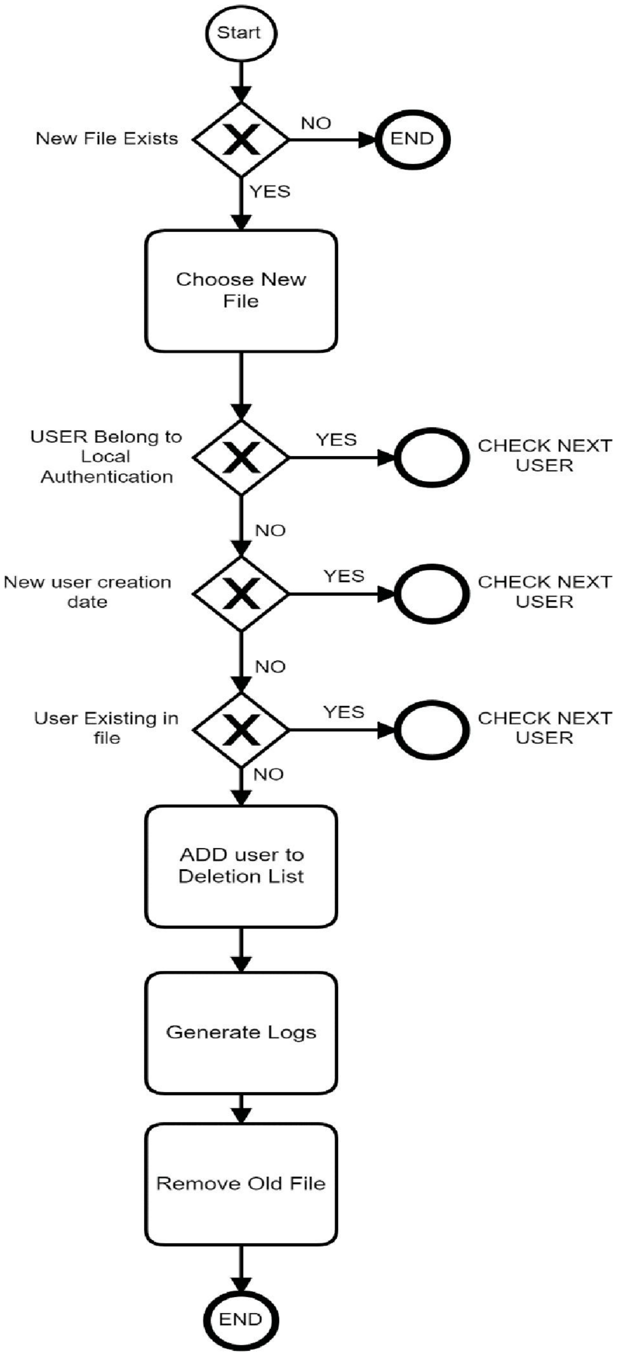
Fig. 2. Structure of LDAP Directory

As shown in the Figure 2 the structure of an external LDAP directory is like a tree.

The structure has three levels: dc, ou, and cn. These are the three object classes in an external LDAP directory. where ou stands for Organizational Unit, dc stands for Domain Component, and cn stands for InetOrgPerson (Personal Data for Intranet or Internet).

DOI: 10.48175/IJARSCT-8036

V. USER SYNCHRONIZATION PROCESS INEXTERNAL LDAP



As shown in figure 3 User synchronization happens both internally and externally on the external Ldap , checks for new files, checks for entry in external LDAP directory server, if not, completes the operation, if yes, gets the new file. Then it enters the now loop. If a user belongs to local authentication check the next user else check the creation date if yes then check the next user otherwise check the existing file. If so, check the next user in the directory, if not, add the user to the delete list, break out of the loop, create a log, and delete the previous file.

A synchronization procedure that automatically removes from the internal database users who have previously been removed from the client LDAP or who have not been granted access to applications in the client LDAP.

To know which user to delete. The LDAP client sends a file containing the full list of users belonging to the application. The application then deletes all users that exist in the internal database but do not exist in the resulting file. This synchronization procedure is performed periodically.

The synchronization procedure will consist of the following steps:

- Check if a new file has been received from ExternalLDAP
- According to this External LDAP file, check if anyuser in DB has to be deleted
- Delete the discovered users from DB if any
- Generate logs of deleted users if any

VI. EXTERNAL LDAP SERVER CONFIGURATION

1. Install OpenLDAP-servers, OpenLDAP, and clients RPMs OpenLDAP these 3 are required for the configuration of external LDAP.
2. Then you need to edit the slapd.conf file to specify the external LDAP domain and the server details in the path /etc/openldap/
3. Then you need to start the slapd service with the command /sbin/service ldap start
4. After configuring external LDAP, use the Services Configuration Tool to configure external LDAP to start at the boot process.
5. Add entries to an external LDAP directory with LDAP add.
6. Use LDAP search to check whether if slapd is accessing the information correctly or not.
7. After that, the LDAP directory should be functioning properly and can be configured with external LDAP-enabled applications used in the organizations.

VII. OPERATIONS SUPPORTED IN EXTERNAL LDAP

There are six operations that are supported by External LDAP

- Bind :- It involves logging in to the Server by the customer, after authentication as an efficiently registered customer.
- Add:- Adds the user records into the directory server of your choice.
- Search:- It can Perform search operations with or without filters.
- Modify:- Users in external LDAP can change the records according to their convenience. Different Characteristics can also be added.
- Delete:- It can Delete one or more records of users in the LDAP Directory.
- Unbind:- It requires logging in From the server and closes the Synchronization of the user’s information.

VIII. LDAP IN PRACTICE

Developers have long articulated the need for an industry-standard directory, and their need has been reinforced by numerous (and continuously evolv- ing) applications that operate under the Directory Enabled Network (DEN) framework, including net- work- management applications that communicate with existing network devices, system-configuration files, voice-over-IP, videoconferencing, and so on.

The DEN specification concentrates on building a robust and extensible infrastructure that can model different network elements and services for easy storage and retrieval from LDAP-based directories and data stores. Interesting DEN initiatives include DEN-enabled switches (http://carol.science.uva.nl/ ~handree/DEN/D1/index_en.html) and directory ser- vices middleware for multimedia conferencing (http://metric.it.uab.edu/vnet/cookbook/v1.0).

8.1 Operational Benefits and Costs

In relational data- bases, write transactions and reading performance are critical, whereas LDAP directories are used mostly for reads.

In addition:

- Most LDAP servers are simple to install and maintain, whereas RDBMS support demands considerable administrative effort;
- LDAP directories can be highly distributed, whereas relational databases are typically cen- tralized; and
- LDAP servers can replicate some or all of their data using a built-in and easily configuredreplication

DOI: 10.48175/IJARSCT-8036

technology. Many RDBMS vendors consider such functionality “extra” and charge accordingly.

- Finally, although relational databases efficiently support complex relationships between objects, in LDAP directories, it can be difficult to represent nonhierarchical relationships between objects.

X. CONCLUSION

There are few limitations in the proposed system since it is simple Due to this the write operation is slow and it won’t be suitable for complex systems.

Synchronization with External LDAP users is an important research material in the Current network security environment, and this is a pressing concern in how to ensure the synchronization process can work Fast, and healthy. In this proposed system we present the technology of managing user information and authentication of both internal and external users in the organization using external LDAP (Lightweight directory access protocol). After External LDAP has improved its performance and protection The next phase of the study is server synchronization On simplifying the authentication of the External LDAP application. We want to Research and design of a single sign-on protocol that is used in the Authentication under External LDAP. External LDAP is the only independent public network Protocol to Authenticate. Expecting open-source VPN security, more and more users will choose this one.

LDAP-based external authentication enhances Power's security, efficiency, and performance. While this support strengthens authentication methods, we believe it could introduce more security through improved communication between client and server and better authentication and protocol encryption choices. Because the proposed system is simple, it has several limitations. Because of this, write operations are slow and unsuitable for complex systems.

REFERENCES

[1]. C.R. Ey, Managing Content with Directory Servers, diplo- ma thesis, Dept. Business Info. Systems, Karlsruhe Univ. ofApplied Sciences, 2000.

[2]. L. Ahmedi and G. Lausen, “Ontology-Based Querying of Linked XML Documents,” Proc. Semantic Web Workshop, 11th World Wide Web Conf., 2002; http://semanticweb2002.aifb.uni-karlsruhe.de/proceedings/research/ahmedi.pdf.

[3]. K.L.E. Law, “XML on LDAP Network Database,” Proc. IEEE Canadian Conf. Electrical and Computer Eng. (CCECE ‘00), IEEE Press, 2000, pp. 469–473.

[4]. Isode, Comparative Performance Benchmarking of Isode M- Vault R10.1, white paper, Oct. 2003, www.isode.com/ whitepapers/m-vault-benchmarking.htm.

[5]. E.J. Thornton, D.P. Mundy, and D.W. Chadwick, “A Com- parative Performance Analysis of Seven LDAP Directories,”Proc. Conf. Terena Networking, 2003; www.terena.nl/ conferences/tnc2003/programme/ papers/p1d1.pdf.

[6]. N. Klasen, Directory Services for Linux, in Comparison with Novell NDS and Microsoft Active Directory, master’s the- sis, Dept. Computer Science, RWTH Aachen Univ., 2001.

[7]. W. Dixon et al., An Analysis of LDAP Performance Char- acteristics, tech. report TR-2002GRC154, GE GlobalResearch, 2002.

[8]. Matt Butcher, Mastering OpenLDAP, first ed., Packt Publishing Ltd., 32 Lincoln Road, Olton, Birmingham, UK

[9]. Vassiliki Koutsonikola., Athena Vakali., LDAP: Framework, Practices, and Trends &quot;, Aristotle University, IEEE Computer Society, October 2004.

[10]. Riri Fitri Sari, Syarif Hidayat, “ Integrating Web Server Applications With LDAP Authentication: Case Study on Human Resources Information System of Ul”, IEEE,2006

[11]. Edgard Jamhour., Distributed Security Management Using LDAP Directories, PPGIA, PUCPR – Pontificia, Universidade Catolica do Parana, 2001.

[12]. Xin Wang, Schulzrinne H. Kandlur D. Verma D(2008). Measurement and Analysis of LDAP Performance. Networking, IEEE/ACM Transactions on, Vol.16, No.1, pp.232 - 243.

[13]. Koutsonikola V, Vakali A.(2004) LDAP: framework, practices, and trends. Internet Computing, Vol. 8, No. 5, pp.66 - 72.

DOI: 10.48175/IJARSCT-8036

[14]. J.Sermersheim,"lightweight directory access protocol", RFC 29.4511(June 2006).

[15]. K. Zeilenga, Ed.," Lightweight Directory Access Protocol (LDAP):.Technical Specification Road Map".RFC 4510 (June 2006).

DOI: 10.48175/IJARSCT-8036