Inventions on Extending LDAP functionality- A TRIZ based Analysis

Umakant Mishra
Inventions on Extending LDAP Functionality
-A TRIZ based analysis of US Patents

By- Umakant Mishra, Bangalore, India

http://umakantm.blogspot.in

Contents

Contents ..................................................................................................................1
1. Introduction ......................................................................................................2
2. Study on Extending LDAP Functionality ........................................................2
   2.1 Objectives of the study .............................................................................2
   2.2 Major areas of Invention ........................................................................2
   2.3 Patents analyzed for the study ................................................................2
3. The mechanism of LDAP Extended Operation ..............................................3
4. Major Concerns in LDAP Extended Operations ............................................4
5. IFR for LDAP extended functionality ............................................................4
6. Inventions on extending functionality of LDAP .............................................5
   6.1 Providing extendible Access Control for LDAP Protocol ........................5
   6.2 Framework for LDAP operation extensibility .......................................6
6.3 Bulk import to LDAP directory server .....................................................7
   6.4 Exchanging data between a java system database and LDAP directory ...9
7. Other related inventions ................................................................................10
   7.1 Using LDAP to interface Directory Assistance (DA) systems ............10
   7.2 Data security in LDAP service using a client and/or server control ....10
8. Summary and Findings of the study .................................................................10
   8.1 Distribution of patents ..........................................................................10
   8.2 Hot areas in LDAP extended functionality .........................................11
   8.3 Trends of evolution in LDAP extended functionality ........................11
Reference to patents: .........................................................................................11
Other references: ............................................................................................12
1. Introduction

Lightweight Directory Access Protocol (LDAP) is an IETF open standard to provide directory services in the network. LDAP was initially developed at the University of Michigan with an objective to include most of the features of X.500, while eliminating the burdens and difficulties of the same.

The current Version of LDAP is LDAP V.3 released in December 1997 (RFC 2251). Other specifications of LDAP can be found in different RFCs on the IETF (Internet Engineering Task Force) website.

With the growing use of Internet, LDAP is becoming more and more popular to provide directory services to a wide range of applications. This led to patenting several inventions relating to LDAP operation and application. This study on LDAP data storage is a part of the main study on LDAP based on 60 selected patents on LDAP from US Patent database.

2. Study on Extending LDAP Functionality

This study on extending functionality of LDAP is a part of the above-mentioned study on LDAP. The study is mainly based on the analysis of US patents. The methodology followed is the same as the above.

2.1 Objectives of the study

- What are the inventions made on extending functionality of LDAP Directory Services and on which aspects of it?

- What is the Ideal Final Result (IFR) in extending functionality of LDAP? Is there any trend in the series of inventions?

- Which problems on extending functionality of LDAP are not solved yet? In other words which problems need to be addressed in future?

- Which aspects of LDAP extensions are yet unexplored? What are the possible areas of improvements in future inventions?

- Can we use TRIZ to analyze the patents? Which Inventive principles or other techniques can help us solving the problems?
2.2 Major areas of Invention

- One major area that attracts the inventors is to recognize external data and create a framework for exchanging data between LDAP and other systems.

- Another area is to add external security mechanism and interface with external environment.

- In many cases the functionality of LDAP is extended to interface plug-ins for various purposes.

2.3 Patents analyzed for the study

- US Patent 6633872, “Extendible access control for lightweight directory access protocol”,


- US Patent 6366954, “Method and data format for exchanging data between a Java system database entry and an LDAP directory service”,

3. The mechanism of LDAP Extended Operation

The LDAP server stores the directory information in a database. The client makes a TCP/IP connection and sends requests to an LDAP server. The LDAP server executes the client requests and returns a response to the client. LDAP offers nine basic functional operations, viz., add, delete, modify, bind, unbind, search, compare, modify distinguished name and abandon.

Apart from the above basic operations, LDAP v3 includes new mechanism called Extended Operations, which allows additional operations to be defined for services not available in this protocol, for instance digitally signed operations and results. Using this feature it is possible to provide new operations and extend the functionality of existing operations.

This is also called a “plug-in” architecture using which a third party provider can integrate services into an LDAP server and consequently obtain processing control when a user of the LDAP server specifies the node of the plug-in in the LDAP tree. The LDAP server plug-in is a shared library containing functions external to LDAP server.
The extended operation allows clients to make requests and receive responses with predefined syntaxes and semantics. These may be defined in RFCs or be private to particular implementations. Each request must have a unique object identifier assigned to it (RFC 2251, www.ietf.org/rfc/rfc2251.txt). The server will respond to this with a message called ExtendedResponse. If the server does not recognize the request name, it will return an error.

4. Major Concerns in LDAP Extended Operations

- The protocol specifications just allow extended operations. As it does not limit the scope of operations, it leaves a space for the vendors to implement and improve their extended functionalities.

- The rules of extended operations are vender specific. The extended operations of one LDAP server may not be understood by another LDAP server.

- LDAP syntax provides two different data types for the extended operations, viz., ExtendedRequest and ExtendedResponse. But the format of these two data types depends on the specific extended operation.

- The changes to the protocol specifications are published in RFCs. The changes to extended operations are not specified as part of the specifications.

- By and large, the extended operations feature of LDAP leaves unlimited scope for additions and extensions to the protocol features.

5. IFR for LDAP extended functionality

According to TRIZ, ideality is a function of its benefits and costs. \( \text{Ideality} = \frac{\Sigma \text{Benefits}}{\left( \Sigma \text{Costs} + \Sigma \text{Harm} \right)} \). So the Ideal Final Result in LDAP extended functionality can be achieved by increasing all useful functions of the LDAP extended operations and decreasing all harmful functions of the same. An analysis of the LDAP system may find the following as IFR for LDAP extended operations.

<table>
<thead>
<tr>
<th>Should have (Positive features)</th>
<th>Should not have (Negative features)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The LDAP protocols should support all kinds of extended operations that may be useful or add value to the directory operations.</td>
<td>• The support for extended operations should not make the system complicated.</td>
</tr>
</tbody>
</table>
• The extended operations should supplement all limitations of the LDAP functionalities.

• Each vendor should be capable of implementing the extended operations on his own way.

• The extended operations should include functionalities like security, data conversion, filtration and other such operations.

• Different implementations of extended operations should understand each other and communicate between themselves.

6. Inventions on extending functionality of LDAP

There are inventions on various aspects of LDAP extended operations. Some of the selected inventions are analyzed in the following pages.

6.1 Providing extendible Access Control for LDAP Protocol

Background problem:
The LDAP protocol does not provide any security mechanism to restrict sensitive data to only to specific users or groups. Although Access Control Lists (ACL) have been used with LDAP they provide only a limited number of security classifications. They can lack security features as they are not tailored for Directory Services. The ACLs link a user to a particular access group. The access group has specific access to the directory depending on its classification whether normal, sensitive or critical. The ACLs can lack the number of security levels that may be required for controlling access to LDAP.

There is another security mechanism, which utilizes an attribute based security classifications. For example, the attribute telephone is classified as sensitive and all telephone numbers are protected from being available in public. This method although works well, it assigns a security classification to an entire attribute which does not provide necessary granularity to define access control for LDAP.

Solution provided by Patent 6633872

US Patent 6633872 provides a method of providing extendible access control to LDAP protocol. According to the method, after the LDAP server authenticates the user, the user is associated to a particular access control group. Based on the access control group, some application specific parameters will be attached to the LDAP operation specified by the user. After the application specific parameters are included in the users operation, the reformatted LDAP operation is provided to the search engine for execution.
The mechanism thus associates the user to a specific access control group and reformats the LDAP operation by including the parameters for that specific access control group. This makes the results of the operation filtered by the parameters of that access control group. The extendible ACL can be implemented as a plug-in within the scope of LDAP server.

TRIZ based analysis

According to the invention, the user, on authentication, is associated with an access control group (Principle-35: Parameter change).

The LDAP operation is reformatted based on the parameters in the access control group and provided to the search engine (Principle-28: Mechanics Substitution).

6.2 Framework for LDAP operation extensibility

Background problem

LDAP protocol specifications provide extensions to enable vendor specific schema and an Application Program Interface (API) to access the vendor specific schema. Various vendors use this feature to develop their LDAP schema for their equipments and provide an API to their customers to operate the schema. But the problem arises when the information is centrally stored but provided by multiple directory servers by different vendors. In such situation each vendor will need different client application making the situation complex.

There is therefore a need to provide a framework for open directory extensibility that permits directory independent information access such that directory servers and client applications may be independently developed and maintained.
Solution provided by patent 6665674

Patent 6665674 provides a framework for open directory extensibility that permits directory-independent information access. A Lightweight Directory Access Protocol (LDAP) Validation Proxy (LVP) is used to intercept and validate LDAP request messages from the clients intended for the directory. The LVP has the capability of generating LDAP requests in processing LDAP messages. The LVP also intercepts and processes LDAP responses issued by a directory and intended for clients.

This process of schema validation and LDAP message processing (by LVP) is modularized according to object classes representing the data stored in the directory and according to services provided. The schema is enforced by validating LDAP messages. This modularization provides a controlled message processing granularity and enables multi-threaded concurrent processing of multiple LDAP messages.

TRIZ based analysis

The invention provides for a framework for open directory extensibility that permits directory independent information access (Principle-5: Universality).

The framework uses a LDAP Validation Proxy (LVP), which processes the messages between an LDAP client and an LDAP directory (Principle-24: Intermediary).

6.3 Bulk import to LDAP directory server

Background problem

The LDAP protocol is a message-oriented protocol. The client constructs an LDAP message containing a request and sends the message to the server. The server processes the request and sends the result back to the client as a series of LDAP messages. In order to add an entry into the LDAP database, a client first opens a TCP connection to the LDAP server and submits the credentials for authentication such as passwords, digital certificates and similar. After the client is authenticated, the client issues a request to add or modify the data. This process is slow for adding a series of records, as the whole cycle of operation has to take place for each record to be added. There is a need for an improved method for importing large number of records into an LDAP database.
Solution provided by patent 6877026

US Patent 6877026 discloses a method of bulk import into LDAP server. According to the invention, the client will first send a request for an extended operation to the server. Then the client will perform the extended operation after receiving the extended operation request from the server. The client will send the object identifier of the extended operation and perform a series of LDAP add operations framed by extended operations to import an entry into the server.

During bulk import, all LDAP operations within the iDS are suspended except the operations necessary to accomplish the bulk import. The bulk Import feature of the iDS imports data using several different methods, such as, a Fast Replica Initialization method, a Wire Import method and a Direct Transfer method. This invention on bulk import provides increased reliability and performance of the directory service and can be used to import data to populate directories, merge directories, perform replication activities etc.

TRIZ based analysis

The bulk import executes faster because it eliminates unwanted activities like authentication, binding etc. for executing every add operation (Principle-21: Skipping).

During bulk import, all LDAP operations within the Server are suspended except the operations necessary to accomplish the bulk import (Principle-20: Continuity of useful action).

The invention describes several different methods of bulk import, such as, a Fast Replica Initialization method, Wire Import method and Direct Transfer method, each having advantages in different situations (Principle-3: Local Quality).
6.4 Exchanging data between a java system database and LDAP directory

Background problem
In a conventional network configuration, the process of installing new software or new applications is a static process. In such cases the network administrator statically defines each configuration on each client. The configuration information for each particular client is hard-coded in the particular client. When a major upgrade is installed it requires the network to bring down to perform that operation.

It is desirable to have a system that supports distributed management of client and user configurations by storing such configuration information at a central repository. This would allow a network administrator to manage subsystem configuration from the server. He can also propagate all kinds of changes to applications at client computers from the server.

Solution provided by US Patent 6366954
The invention discloses an extension to a directory service, which supports exchanging configuration data between a configuration server schema residing on a configuration server and a network directory service. The method involves mapping between a directory attribute and a configuration server property. The directory service entry includes multiple shadow attributes where each shadow attribute corresponds to a particular directory service attribute. The particular directory service attribute, in turn, has a corresponding property in the configuration server.

According to the invention, the configuration server is a Java System database server containing configuration data for multiple clients and network users. The exchange of data is significantly enhanced through the use of an extension to a network directory service enabling a rapid mapping between a directory service attribute and a configuration server property. The directory service entry includes multiple shadow attributes where each shadow attribute corresponds to a particular directory service attribute. The particular directory service attribute, in turn, has a corresponding property in the configuration server. The extension also includes a correspondence or path-matching file that contains matches between directory service addresses and configuration server location identifier or paths.

TRIZ based analysis
The invention addresses configuration of client systems remotely from the server. (Principle-17: Another Dimension).
The invention proposes an extension to the LDAP service (Principle-37: Expansion), which enhances the exchange of data by enabling a rapid mapping between a directory service attribute and a configuration server property (Principle-10: Prior Action).

7. Other related inventions

7.1 Using LDAP to interface Directory Assistance (DA) systems

US Patent 6609121 finds a method of mapping an LDAP interface to a DA (Directory Assistance) system. According to the invention the client will send LDAP compatible search arguments, which will be converted to DA compatible search arguments. The DA will be queried using this DA compatible search arguments. The results of the query will be converted to a result set compatible with LDAP and served to the client. All these steps of conversion are done by a plug-in to the LDAP server and make use of the extended operation features.

Patent 6732160 (by the same inventors) also provides a similar mechanism consisting of five steps as above. Both inventions use plug-ins which are loaded on startup of LDAP server.

7.2 Data security in LDAP service using a client and/or server control

US Patent 6339827 discloses a method of maintaining security in a directory service by extending the lightweight directory access protocol (LDAP). The invention includes two security controls, i.e., one client-control to be implemented on the client machine and one server-control to be implemented on a server machine (Principle-1: Segmentation). However, the invention presents a flexible model as it is not required to have both client and server controls to be implemented together. A client machine may implement the client control irrespective of whether a server involved in the directory operation is running the server control (Principle-15: Dynamize).

8. Summary and Findings of the study

8.1 Distribution of patents

- A total of six patents are presented in the article. Out of them four are more relevant to the context and analyzed in detail. Two other patents are presented in brief.

- Out of the four selected patents, two are assigned by Sun Microsystems, one by IBM and one by Nortel Networks.
8.2 Hot areas in LDAP extended functionality

Unlike other aspects of LDAP it is not easy to identify the hot areas of LDAP extended functionality. There are unlimited number of functionalities which can be added to LDAP using extended functionality. However, some of the hot areas to extend and expand LDAP functionalities are as below.

- Recognizing and interacting with unknown data types.
- Adding functionalities through application interfaces or plug-ins.
- Implementing all such things, which are not included in the protocol specifications.

8.3 Trends of evolution in LDAP extended functionality

As the inventions on extended functionality are not on any specific area, it is very difficult to find any trend in the evolution. However, keeping in mind the inventions on other aspects of LDAP, one may find the following trends in LDAP extended functionality.

- Increasing speed in LDAP data searching, updating and other directory operations.
- Increasing easiness to “configure and implement” and increasing easiness to “maintain and administer” are two common trends in any field of LDAP.
- Increasing Dynamization- defining roles, policies, improving flexibility in filtering the objects in the directory.
- Reducing Human Involvement- and automating LDAP operations
- Boundary breakdown- integrating one LDAP directory with another LDAP directory having a different schema, and integrating with different other databases having unknown structure.
- Increasing controllability in LDAP service- increasing control on data selection, data protection, data integrity etc.
- Increasing standardization- to create compatibility with new hardware, software and protocol specifications.

Reference to patents:


Other references:


