

LDAP

What is LDAP (Lightweight Directory Access Protocol)?

LDAP (Lightweight Directory Access Protocol) is a widely used Internet protocol for accessing online directory information. LDAP is an open industry standard.

A directory such as a telephone directory is a listing of entries (objects) and information about these entries. LDAP directories are used to store data like white pages, user profiles, and devices available on the company network. LDAP facilitates the management of company policies regarding the different kinds of privileges employees are allowed and their access rights to different kinds of equipment. The data stored in LDAP directories can be shared by a variety of applications.

An LDAP directory is a limited and specialized database. Unlike databases, LDAP directories do not, for example, support concurrency control or transactions, and they do not have active database capabilities (triggers). In case of directory replication, there is no notion of simultaneous updates of the replicas.

LDAP Directory Specifics

Directory entries are like the tuples in a relational database. Entries have fields whose values are attribute-value pairs. Some entries can be specified to be required while others can be declared to be optional. Each entry has at least one type, `objectclass`, associated with it. An entry can have multiple types, and types can be added to or deleted from an entry at run time.

A directory schema is typically (but not always) hierarchical, similar to schemas found in object databases. In case of a white page enterprise directory, the directory hierarchy should reflect the enterprise hierarchy.

LDAP provides simple operations for adding, deleting and updating entries and querying (searching) the directory. Queries can be specified to search all or part of a directory. The results of a query can be narrowed by specifying “filters” which are similar to WHERE clauses in SQL. Filters are not as general as the WHERE clause since they are limited to examining the fields of a single entry. Like the SELECT clause in SQL, LDAP also allows queries to specify which field values are to be returned in the result.

Each directory entry is updated separately. Consequently, data in the replicas may temporarily not be synchronized with each other. Also, since there are no transactions, a directory update involving multiple entries can make a directory temporarily inconsistent since each entry must be updated separately.

Directories are typically queried far more often than they are updated. Consequently, LDAP directories are optimized for querying.

LDAP Directory Services

LDAP runs over TCP/IP. LDAP directory services are implemented using the client-server model. A single directory can be spread over multiple servers and/or may be replicated on multiple servers. Regardless of the directory data distribution, each client gets the same view of the directory – except for temporary periods when multiple servers are being updated to make a directory update.

What is the Advantage of LDAP?

LDAP is an open industry standard. LDAP directories are limited but specialized databases. They have been designed for storing relatively simple information such as white pages for organizations and enterprises, and devices in networks.

Compared to databases, LDAP directories are

- o flexible,
- o easier to scale,
- o handle heterogeneity well,
- o facilitate replication (for availability and reliability),
- o support distributed data management while giving clients a unified view of the stored data,
- o optimized for queries, and
- o simpler and cheaper to maintain.

Where will LDAP be used?

Some examples where LDAP is being used are

- o enterprise directories,
- o web user profiles,
- o Directory Enabled Networks (DEN) — intelligent networks where information about network components is stored and available in directories,
- o library catalogs,
- o access control and authentication, and
- o messaging.

Where Can I Find More Information?

- o [Internet Engineering Task Force](http://www.ietf.org) (<http://www.ietf.org>)
- o [An LDAP Roadmap & FAQ](http://www.kingsmountain.com/ldapRoadmap.shtml) (<http://www.kingsmountain.com/ldapRoadmap.shtml>)
- o [Introductory LDAP Articles & Papers](http://www.rage.net/ldap/links.shtml) (<http://www.rage.net/ldap/links.shtml>)