LDAP overview

Bruce Ricard, UAA

August 20, 2018

Table of contents

LDAP

Lightweight Directory Access Protocol

What is LDAP? Basically: distributed filesystem over an IP network.

- tree structure
- read, write, search

LDAP

Lightweight Directory Access Protocol

What is LDAP? Basically: distributed filesystem over an IP network.

- tree structure
- read, write, search

Example: store usernames and passwords.

LDAP

History

Telecomunication companies created in 1992
LDAPv3 in 1997

Protocol

Interface

- StartTLS
- Bind authenticate and specify LDAP protocol version
- Unbind close the connection (not the inverse of Bind)
- Search
- Compare test if a named entry contains a given attribute value
- Add a new entry
- Delete an entry
- Modify an entry
- Extended Operation generic operation used to define other operations

Directory structure

Entries

Entry: collection of information about an entity.

- distinguished name (DN)
- collection of attributes
- collection of object classes

Entry

example

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

Directory structure

DNs and RDNs

```
dn: cn=John Doe,dc=example,dc=com
```

“cn=John Doe”: RDN (Relative distinguished name) file name
“dc=example,dc=com”: 2 RDNS, DN of the parent entry path
“cn=John Doe+telephoneNumber=+1 123-456-7890”: multi valued RDN (+) cn: common name dc: domain component

Directory structure

Attributes

Hold the data.

- attribute type
- 0+ attribute options
- set of values – actual data

Directory structure

Attributes

Hold the data.

- attribute type
- 0+ attribute options
- set of values – actual data

Attribute types: schema elements that specify how attributes should be treated by LDAP clients and servers

- object identifier (OID)
- 0+ names – used to reference attributes of that type tags
- attribute syntax
- matching rules how to compare values of this attribute type

Attribute options: rarely used

Directory structure

Object classes

Object classes are schema elements that specify collections of attribute types that may be related to a particular type of object, process, or other entity. Every entry has a structural object class, which indicates what kind of object an entry represents (e.g., whether it is information about a person, a group, a device, a service, etc.), and may also have zero or more auxiliary object classes that suggest additional characteristics for that entry.

Directory structure

Object identifiers (OID)

sequence of numbers separated by periods
e.g., 1.2.840.113556.1.4.473 OID for server-side sort request control

Directory structure

Object identifiers (OID)

sequence of numbers separated by periods
e.g., 1.2.840.113556.1.4.473 OID for server-side sort request control
identify: schema elements, controls, and extended requests and responses

LDAP schema

- Attribute Syntaxes define the types of data that can be represented in a directory server.
- Matching Rules define the kinds of comparisons that can be performed against LDAP data.
- Attribute Types define named units of information that may be stored in entries.
- Object Classes define named collections of attribute types which may be used in entries containing that class, and which of those attribute types will be required rather than optional.