CENTRE ESPECÍFIC
D´EDUCACIÓ A DISTÀNCIA DE
LA COMUNITAT VALENCIANA

UNIT 4
DIRECTORY SERVICE

Web Applications Deployment
CFGS DAW

Author: Carlos Cacho López

Reviewed by: Lionel Tarazón Alcocer

lionel.tarazon@ceedcv.es

2019/2020

License

Nomenclature

During this unit we are going to use special symbols to distinct some important elements. This symbols are:

Important

Attention

Interesting

INDEX

U04. DIRECTORY SERVICE

1. INTRODUCTION

A **directory service** is a network application specialized in containing, managing and providing information about users, systems, services and applications in a network. It is usually used to help network administrators manage network users and their rights to access network resources (computers, applications, printers, etc.).

Some features of the directories are:

- Tend to contain descriptive, attribute-based information and support sophisticated filtering capabilities.
- Generally does not support complicated transaction or roll-back schemes found in database management systems designed for handling high-volume complex updates.
- Their updates are typically simple all-or-nothing changes, if they are allowed at all.
- Generally tuned to give quick response to high-volume lookup or search operations. They may have the ability to replicate information widely in order to increase availability and reliability, while reducing response time.

There are many different ways to provide a **directory service**. Different methods allow different kinds of information to be stored in the directory, place different requirements on how that information can be referenced, queried and updated, how it's protected from unauthorized access, etc.

Some directory services are *local*, providing service to a restricted context (e.g., the finger service on a single machine).

Other services are global, providing service to a much broader context (e.g., the entire Internet). Global services are usually *distributed*, meaning that the data they contain is spread across many machines, all of which cooperate to provide the directory service. Typically a global service defines a uniform *namespace* which gives the same view of the data no matter where you are in relation to the data itself.

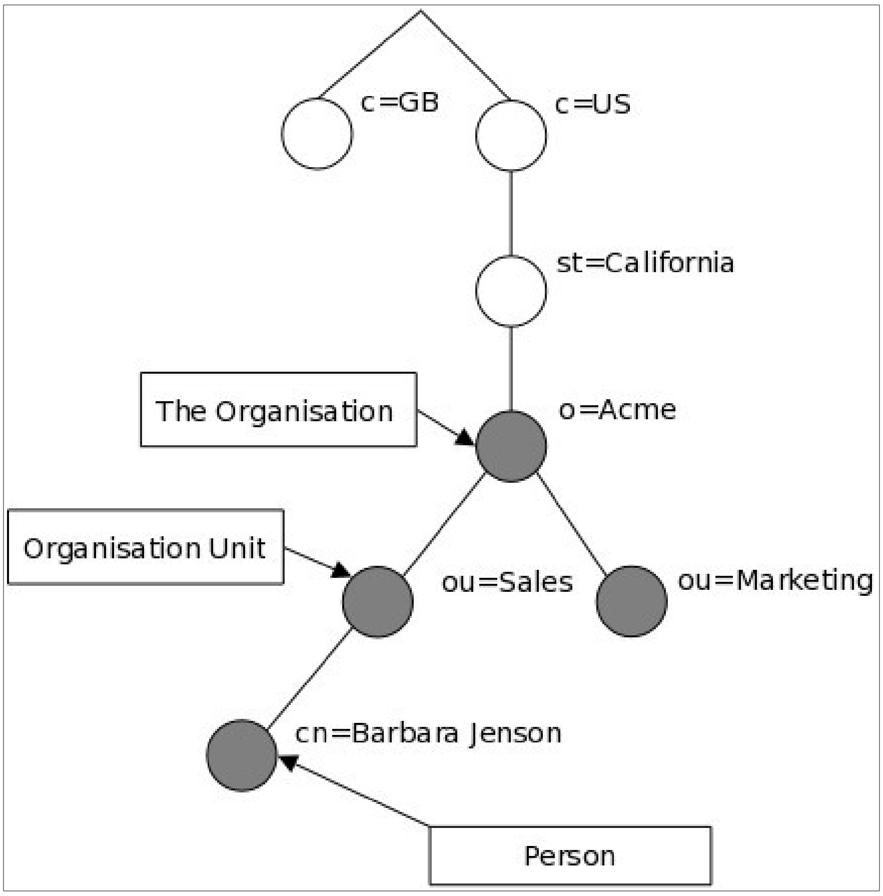
2. LDAP

LDAP stands for Lightweight Directory Access Protocol. As the name suggests, it is a lightweight protocol for accessing directory services, specifically X.500-based directory services.

The LDAP information model is based on *entries*. An entry is a collection of attributes that has a globally-unique Distinguished Name (DN). The DN is used to refer to the entry unambiguously. Each of the entry's attributes has a *type* and one or more *values*. The types are typically mnemonic strings, like "cn" for common name, or "mail" for email address. The syntax of values depend on the attribute type. For example, a cn attribute might contain the value “Babs Jensen” and a mail attribute might contain the value "babs@example.com".

LDAP uses a *client-server model*. One or more LDAP servers contain the data making up the directory information tree (**DIT**). Client can connect to servers and makes a request. The server replies with an answer and/or with a pointer to where the client can get additional information (typically, another LDAP server). No matter which LDAP server a client connects to, it sees the same view of the directory; a name presented to one LDAP server references the same entry it would at another LDAP server. This is an important feature of a global directory service.

Example of Directory Information Tree (DIT)



2.1 LDAP entries

Every entry (object) in the Directory Information Tree has a **Distinguished Name (DN)** and a **Relative Distinguished Name (RDN)**, as well the attributes (information contained in the entry).

The **RDN is the name of the entry**. Examples taken from the previous page:

- o=Acme
- ou=Sales
- ou=Marketing
- cn=Barbara Jenson

The **DN is the full name of the enry**, which is composed by adding the RDN to the whole path from the top of the tree up to the entry (in reverse order):

- o=Acme,st=California,c=US
- ou=Sales,o=Acme,st=California,c=US
- ou=Marketing,o=Acme,st=California,c=US
- cn=Barbara Jenson,ou=Sales,o=Acme,st=California,c=US

An entry can look like this when represented in LDAP Data Interchange Format (LDIF):

```
dn: cn=Barbara Jenson,ou=Sales,o=Acme,st=California,c=US
na: Barbara
sn: Jenson
tel: +1 888 555 6789
mail: barbara@sales.acme.com
manager: cn=Peter,dc=example,dc=com
objectClass: inetOrgPerson
```

The first line contains the Distinguished Name of the entry, noted with **dn:**

The other lines show the attributes of the entry. Attribute names are typically mnemonic strings such as "cn" for common name, "na" for name, “sn” for surname, etc. Attributes may also hold references to other entries, as in “manager” above which indicates the who is Barbara’s manager.

2.2 LDAP url

LDAP URLs have the following syntax:

ldap[s]://hostname:port/base_dn?attributes?scope?filter

The ldap:// protocol is used to connect to LDAP servers over unsecured connections, and the ldaps:// protocol is used to connect to LDAP servers over TLS/SSL connections (secure and encrypted).

The components used are:

- ***hostname*:** Name (or IP address in dotted format) of the LDAP server. For example, ldap.example.com or 192.202.185.90.
- ***port*:** Port number of the LDAP server (for example, 696). If no port is specified, the standard LDAP port (389) or LDAPS port (636) is used.
- ***base_dn*:** Distinguished name (DN) of an entry in the directory. This DN identifies the entry that is the starting point of the search. If no base DN is specified, the search starts at the root of the directory tree.
- ***attributes*:** The attributes to be returned. To specify more than one attribute, use commas to separate the attributes; for example, cn,mail,telephoneNumber. If no attributes are specified in the URL, all attributes are returned.
- ***scope*:** The scope of the search, which can be one of these values: (If no scope is specified, the server performs a base search.)
- ***base*** retrieves information only about the distinguished name (*base_dn*) specified in the URL.
  - ***one*** retrieves information about entries one level below the distinguished name (*base_dn*) specified in the URL. The base entry is not included in this scope.
  - ***sub*** retrieves information about entries at all levels below the distinguished name (*base_dn*) specified in the URL. The base entry is included in this scope.
- ***filter*:** Search filter to apply to entries within the specified scope of the search. If no filter is specified, the server uses the filter (objectClass=*).

3. BIBLIOGRAPHY

[1] https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

[2] *http://www.openldap.org/doc/*