

LDAP

Emilio Cabo Gomis



Indice

Historia.....	3
X500.....	3
Protocolos y evolución.....	4
Objetos y atributos LDAP.....	5
Usos comerciales.....	6
Bibliografía.....	7

Historia

Denominado **protocolo ligero de acceso a directorios**, permite el acceso a un servicio de directorio. Parecido al concepto de una agenda telefónica.

Basado en la tecnología de resolución de nombres basada en dominios nos permite acceder a información como nombres de usuario, contraseñas, direcciones de correo electrónico, entre otros datos. El protocolo de red empleado para acceder a esta información es el protocolo TCP/IP.

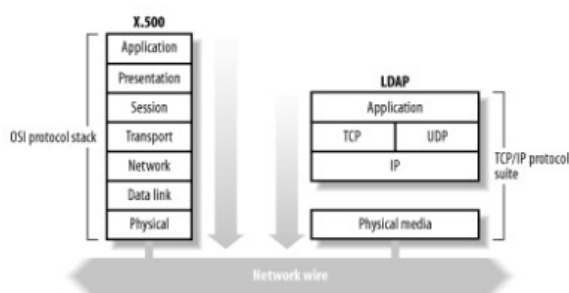
X500

Es imposible hablar de LDAP sin hablar de el estándar de telecomunicaciones X500. Este fué desarrollado por el International Telecommunication Union (ITU-T). El LDAP está basado en el protocolo de directorio del conjunto de protocolos X500.

Se dice que este protocolo es el protocolo “pesado” debido a que requería que el cliente y el servidor se comunicara empleando el Open Systems Interconnection(OSI) stack. (Este stack es el mismo que aprendimos en PAR).

El LDAP es un protocolo que omite muchos de las capas OSI no imprescindibles. Es decir, es un protocolo “más ligero” que el x500

Esta es una imagen que ilustra la estructura del stack de programación.



O'Reilly - Ldap System Administration

LDAP es un protocolo de comunicación asíncrono. Cuando hablamos de un servidor LDAP normalmente nos referimos a la vista de árbol que ofrece LDAP para visualizar los datos contenidos de una manera jerárquica.

Muchas veces, por limitaciones de la mente humana, editamos ficheros y no sabemos de dónde vienen ni porqué se hicieron de esa manera. Por ejemplo: ¿Qué son los ficheros LDIF?

Los ficheros de configuración se crearon de una manera que fuera fácil para los administradores de sistemas editar los contenidos con un editor de texto. Es por ello que desarrollaron los ficheros .ldif para ser fácilmente legibles y editables.

#sole

dn: uid=sole,ou=colaboradores,ou=usuarios,dc=lpyme10,dc=net

objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: sole
sn: Lúa
cn: Colab - sole Lúa
givenName: sole
displayName: Colab - sole Lúa
uidNumber: 10000
gidNumber: 10000
userPassword: abc123.
gecos: Colab - sole Lua
loginShell: /bin/bash
homeDirectory: /home/lpyme10/colaboradores/sole
mail: sole@lpyme10.net
initials: SL
shadowExpire: -1

Contenido de un fichero LDIF de configuración de usuarios

Funcionalidades:

LDAP esencialmente es un protocolo de comunicación bidireccional que mediante una estructura de árbol, nos permite acceder a datos almacenados de una manera rápida y eficiente. Mediante un stack de redes reducido y de bajo “peso” comunica estos datos a equipos clientes.

Si bien hay muchos tipos de atributos en los que almacenar información (Incluso podemos incorporar fotografías) LDAP no es una base de datos, y no podemos pensar que podemos almacenar mediante LDAP cualquier tipo de información en su interior. Cada atributo tiene la función de almacenar un tipo determinado de información.

Protocolos y evolución

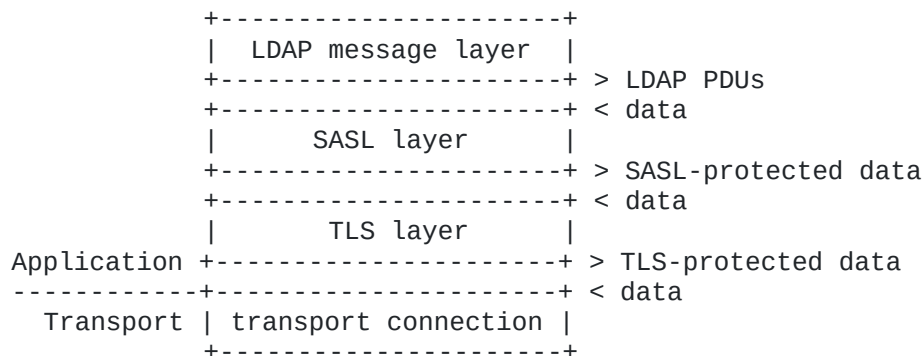
El servicio de OpenLdap es un software open-source que es compatible con LDAPv3

Es muy utilizado debido a que soporta Linux, Solaris, Mac OS 10.2, and Windows.

LDAPv2 era ampliamente utilizado con una capa de encriptación SSL, pero esto nunca fué formalizado en un protocolo. Se dejó de brindar soporte a este protocolo en el año 2003.

LDAPv3 fué desarrollado en 1997 incluyó soporte para la extensibilidad e integró autenticación mediante el protocolo Simple Authentication and Security Layer (SASL), se incorporó formalmente la autenticación mediante TLS/SSL

Este es una representación gráfica de los distintos niveles de encriptación y autenticación y como se aplican en el stack de LDAPv3. Esto difiere de el estándar IETF de LDAPv2.



En relación a la funcionalidad en red de LDAP. LDAP escucha en el puerto 389
LDAPS (versión segura) puerto 636.

Objetos y atributos LDAP

¿Que es un atributo en LDAP?

Si nos imaginamos que una lista de contactos nos encontraremos campos que rellenar como Nombre, Nombre de pila, apellidos, dirección, número de teléfono...

Podemos tambien imaginarlo como una variable en un lenguaje de programación. Existen diferentes tipos de datos que se le asignan a las variables. En función del tipo de datos asignado esa variable almacenará un contenido de cierto tipo a l queue después podremos acceder.

Esto es básicamente los atributos. Algunos de los más empleados son los siguientes:

- Dn -> Distinguished Name
- Cn -> Common Name
- Gn -> Given Name
- Gid -> Group identifier
- homeDirectory -> Directorio home del usuario

¿Qué es un objeto en LDAP?

Existen diferentes tipos de objetos. El tipo de objeto que puede ser almacenado en un directorio dependerá del “schema”.

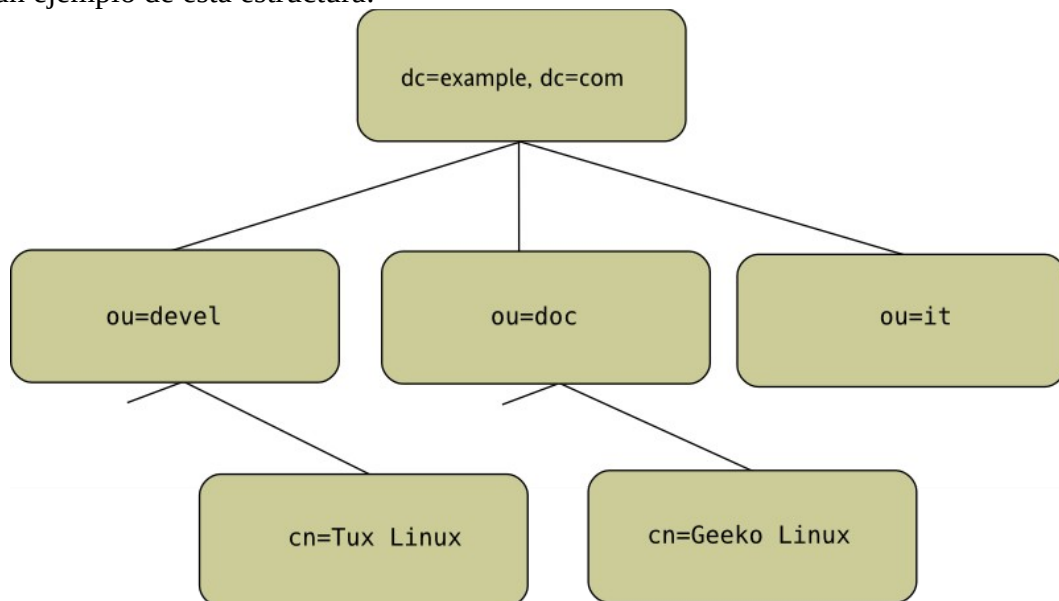
Algunos de los objetos que nos podemos encontrar son los siguientes:

- Grupos
- InetOrgPerson → Es una entrada para una persona.
 - Attr requeridos: commonName, surname, objectClass
- Organizational Unit → Es una entada para Unidades Organizationales

- Attr requeridos: ou , objectClass
- Organization → Entrada para organizaciones
 - Attr requeridos: o, objectClass
- SambaAccount
 - Attr requeridos: uid, rid

Cuando en la explicación de la progresión histórica de LDAP hablé que el “servidor” ofrece una vista de árbol jerárquico de la estructura del protocolo.

Este es un ejemplo de esta estructura:



Novell LDAP

Usos comerciales

Su implementación es común en sistemas de gestión de identidades, intranets corporativas y plataformas de software como servicio (SaaS).

Entre ellas se encuentra el uso extendido de ldap en Active Directory.

En plataformas como Microsoft Exchange o Zimbra, utilizan LDAP para almacenar y gestionar datos de contacto, listas de distribución y configuraciones de usuarios.

Este servicio también es empleado en aplicaciones de teléfono móvil para almacenar contactos.



En servicios de gestión de tickets como JIRA se pueden importar datos desde ldap para evitar la introducción manual evitando así datos incorrectos o duplicidades.

Bibliografía

Libro O'Reilly

O'Reilly - Ldap System Administration (Apuntes de ASO)

IETF

[RFC 4511 - Lightweight Directory Access Protocol \(LDAP\): The Protocol \(ietf.org\)](https://tools.ietf.org/html/rfc4511)

It pro

[What are X.500 and LDAP? \(itprotoday.com\)](https://itprotoday.com/what-are-x500-and-ldap/)

Network Encyclopedia

[X.500 - NETWORK ENCYCLOPEDIA](#)

Wikipedia

[Simple Authentication and Security Layer - Wikipedia](#)

[Lightweight Directory Access Protocol - Wikipedia](#)

[X.500 - Wikipedia](#)

REDHAT

[What is lightweight directory access protocol \(LDAP\) authentication? \(redhat.com\)](#)

Novell

[Novell Doc: Reference - Structure of an LDAP Directory Tree](#)