LDAP

Sergio Acevedo, Ruben Garcia, Sergio Díaz

Por sus siglas Lightweight Directory Access Protocol o Protocolo Ligero de Acceso de Directorio en español, se trata de un protocolo cliente/servidor seguro y ligero de acceso a directorios. Dicho de otro modo, es una manera organizada y jerárquica de guardar datos dentro de una carpeta. Se utiliza en forma de aplicación.

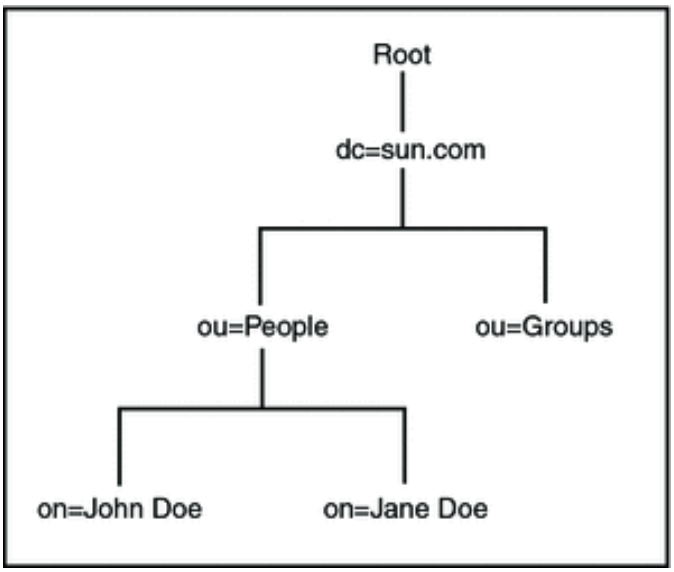
Antes de profundizar sobre LDAP debemos entender qué es un servicio de directorios. Un servicio de directorios es una base de datos optimizada para lectura, navegación y búsqueda.
Hay muchas formas de proveer un servicio de directorio. Algunos servicios de directorio son locales y otros son globales. El DNS es un ejemplo de un sistema de directorio globalmente distribuido.

LDAP se basa en el protocolo X.500. Es un servicio global de directorio. Sus componentes cooperan para manejar la información pedida por el usuario. La información se lleva a cabo en una base de la información del directorio (DIB) y los usuarios pueden (conforme al control de acceso) modificarlo. X.500 incluye los siguientes protocolos:

- De acceso al directorio.
- De sistema de directorio.
- De ocultación de información de directorio.
- De gestión de enlaces operativos de directorio.

(Para más información sobre el protocolo X.500 visitar: http://sec.cs.kent.ac.uk/x500book/)

LDAP se basa en entradas, que son colecciones y atributos con nombre único (DN). Para hacernos a la idea, gracias a su organización de directorios y ficheros somos capaces de clasificar la información haciéndola muy intuitiva para su acceso. Resumiendo, organiza la información en forma de árbol. Ejemplo:



Normalmente, la sintaxis utilizada para los atributos se basa en palabras sencillas y fáciles de recordar. Por ejemplo, para referirnos al correo electrónico

podríamos mencionarlo cómo mail. No obstante, cada atributo tiene su tipo, por lo que es algo que debemos tener en cuenta para su correcta sintaxis. Al final y al cabo no debemos olvidar que LDAP debe ser organizado, entendible e intuitivo para poder acceder bien a los datos.

LDAP es capaz de comunicarse de forma remota con otros directorios LDAP situados en distintos servidores. Esto es una gran ventaja, pues es como tener una base de datos descentralizada.

Antes de comenzar entendamos bien los atributos.

- **dn** (*domain name*): nombre de entrada, pero no forma parte de la propia entrada.
- **dc**: componente de dominio para identificar las partes del dominio donde se almacena el directorio LDAP.
- **cn** (*common name*): nombre de atributo para identificar el nombre de usuario.
- **sn** (*surname*): apellido.
- **objectClass**: distintas entradas para identificar las propiedades de los atributos.

En cuanto a manipular la información podemos añadir, eliminar, actualizar una entrada existente, editar el nombre… Bueno, era de esperar. Obviamente LDAP también sirve para hacer búsquedas en nuestros directorios, al fin y al cabo su función es extremadamente parecida a la de una base de datos. Este sistema cuenta con operaciones de búsqueda basadas en filtros, recalcando una vez más que LDAP no da una muy buena accesibilidad a los datos.

¿Cómo podemos *acceder a la información*? Sencillo, a través de una URL de este tipo:
ldap://servidor:puerto/DN?atributos?ambito?filtros?extensiones

- **Servidor** (*host*): es la dirección IP o nombre del dominio del servidor LDAP
- **Puerto**: el que conecta con el servidor (*389 por defecto*).
- **DN**: nombre distinguido para usar en la búsqueda.
- **Atributos**: es una lista de campos a devolver separados por comas.
- **Ámbito** (*scope*): especifica el ámbito de búsqueda, puede ser *base* (por defecto), *one* o *sub*.
- **Filtros**: para una búsqueda más específica.
- **Extensiones**.

Ejemplo de acceso (encontrado en internet, fuente: https://www.profesionalreview.com/2019/01/05/ldap/):
ldap://ldap.profesionalreview.com/cn=Jose%20Castillo,dc=profesionalreview,cd=com
Cito textualmente:

> “ *Estamos buscando todos los usuarios que haya en la entrada Jose Castillo en profesionalreview.com.*
> *Además de esta notación, también tendremos una versión de LADP con certificado de seguridad SSL, cuyo identificador para la URL será “ldaps:”*. “

Es peligroso no asegurar nuestros datos y dejarlos al libre acceso de cualquiera. Para ello LDAP cuenta con un sistema de autentificación de acceso, además de soportar servicios de privacidad e integridad.

¿Cómo funciona LDAP?
Simplificando mucho, los clientes envían consultas y LDAP los contesta. Este sistema puede enviar una respuesta clara y concisa, o puede enviar punteros que indican donde puede encontrar tal información. Recordemos que las entradas son únicas en LDAP por lo que no importa desde qué servidor se conecte el cliente.
Cabe resaltar que LDAP utiliza la representación en texto ASCII, por lo que si escribes una línea en blanco finalizas una entrada.

Hay una serie de comandos para las *consultas de datos* en LDAP para el cliente:

- **Abandon**: cancelar la operación previa enviada al servidor.
- **Add**: agrega una entrada en el directorio.
- **Bind**: Iniciar una nueva sesión en el servidor LDAP.
- **Compare**: compara las entradas en un directorio según los criterios.
- **Delete**: eliminar una entrada de un directorio.
- **Extended**: Realiza operaciones extendidas.
- **Rename**: cambia el nombre de una entrada.
- **Search**: busca entradas en un directorio.
- **Unbind**: finaliza una sesión en el servidor LDAP.

Ventajas LDAP:
La mayor ventaja de LDAP es que se puede consolidar información para toda una organización entorno a un repositorio central.
LDAP también soporta un número de bases de datos backend (bases de datos de lado servidor) en las que se pueden guardar directorios. Esto permite que los administradores tengan la flexibilidad para desplegar la base de datos más indicada para el tipo de información que el servidor tiene que diseminar.

Características OpenLDAP:
Soporte LDAPv3: soporta la capa de autenticación y seguridad (SASL), la seguridad de la capa de transporte (TLS) y la capa de conexión segura (SSL),es decir, es más seguro que la versión anterior.
Soporte IPv6: soporta la próxima generación del protocolo de Internet versión 6.
LDAP sobre IPC: se puede comunicar dentro de un sistema usando comunicación interproceso (IPC). Esto mejora la seguridad al eliminar la necesidad de comunicarse a través de la red.
API de C actualizada: mejora la forma en que los programadores se conectan para usar servidores de directorio LDAP.
Soporte LDIFv1: provee compatibilidad completa con el formato de intercambio de datos.
Servidor Stand-Alone mejorado: incluye un sistema de control de acceso actualizado, conjunto de hilos, herramientas mejoradas y mucho más.

Características que implementa LDAPv3 sobre LDAPv2:
Autentificación fuerte haciendo uso de SASL (framework para autenticación y autorización en protocolos de Internet.).
Protección de integridad y confidencialidad haciendo uso de TLS (SSL).
Internacionalización gracias al uso de Unicode.

Remisiones y continuaciones.
Descubrimiento de esquemas.
Extensibilidad (controles, operaciones extendidas …).

Backends, objetos y atributos en LDAP:
Slapd (Stand-Alone LDAP daemon)se suministra con tres diferentes bases de datos de backends (bases de datos de segundo plano) entre las que se pueden elegir: LDBM (base de datos de gran rendimiento basada en disco, SHELL(interfaz de base de datos para órdenes de UNIX o scripts del intérprete de órdenes (shell)) y PASSWD (sencilla base de datos de contraseñas).
Para explicarlo vamos a tomar como referencia la bases de datos LDBM.
La base de datos LDBM asigna un identificador de 4 bytes, único para cada entrada de la base de datos. La BDD utiliza ese identificador para hacer referencia a entradas en los índices. La BDD está compuesta de un fichero índice principal, llamado “id2entry”, que mapea el identificador único de una entrada en la representación en texto de esa misma entrada.

Para importar y exportar información de directorio entre servidores de directorios basados en LDAP o hacer una serie de cambios en el directorio, se usa en general un fichero llamado LDIF (“LDAP interchange format”). El archivo LDIF almacena información en jerarquías de entradas orientadas a objetos y el paquete de software LDAP convierte el fichero LDIF a formato LDBM (que es la base de datos que hemos elegido).
Ejemplo fichero LDIF:

```
dn: o=Insflug, c=ES
o: Insflug
objectclass: organization
dn: cn=Luiz Malere, o=Insflug, c=ES
cn: Luiz Malere
sn: Malere
mail: malere@yahoo.com
objectclass: person
```

El DN (distinguished name) está compuesto por el nombre que tiene que ser diferente al resto, más las ruta de nombres que permiten rastrear la entrada hacia atrás hasta la parte superior de la jerarquía del directorio.
En LDAP, una clase de objetos define la colección de atributos que pueden usarse para una entrada.
Una entrada determinada puede pertenecer a más de una clase de objetos.
Los datos del directorio se representan mediante pares de atributo y su valor. Hay atributos que son obligatorios para crear el directorio y otros atributos se permiten pero no son obligatorios. Cada atributo tiene una definición de sintaxis que le corresponde. Por ejemplo en persona hay un atributo que es “teléfono” y tiene una sintaxis numérica.
HISTORIA DE LDAP:

En la década de los 80, las compañías telefónicas introducen una agrupación de protocolos. Esta se llama X.500. Los servicios de directorio de X.500 se accedían vía DAP (directory access protocol). Con la aparición de TCP/IP el acceso a los servicios de X.500 se denominó LDAP (lightweight directory access protocol).