INTRODUCCIÓN A LDAP

M1- SISTEMAS

GRUPO: AMS/AWS

¿Qué es?

(Protocolo Ligero de Acceso a Directorios) es un conjunto de protocolos usados para **acceder a información guardada de forma centralizada en una red.**

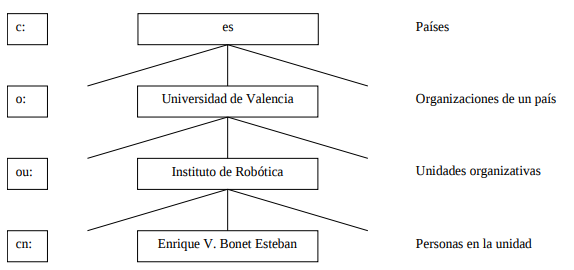
En LDAP, **un cliente se conecta a un servidor para consultar un servicio de directorio o intentar modificarlo**. En caso de una consulta, el servidor puede contestar la consulta o, si no puede contestarla localmente, puede redirigir la consulta a otro servidor LDAP que tenga la respuesta.

Si el cliente intenta modificar la información del servicio de directorio de LDAP, el servidor comprueba que el usuario tiene permiso para realizar la operación solicitada y después añade o actualiza la información.

La principal **ventaja de usar LDAP** es que la información se puede centralizarse, permitiendo una administración más sencilla y eficaz de listas de usuarios, etc. Por otra parte, y dado que LDAP soporta SSL y TLS, es posible su uso mediante protocolos seguros, lo que permite enviar y recibir información de forma segura.

¿Cómo se estructura la información?

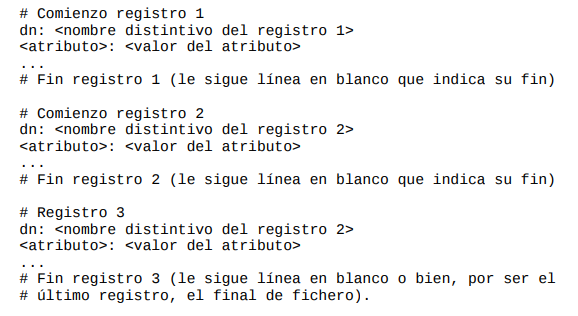
En LDAP, el servicio de directorio debe representar, mediante un modelo abstracto, la información de la empresa, etc., debiendo estar cada elemento identificado por un nombre distintivo (Distinguished Name) que debe ser único dentro de LDAP (DC).

Ejemplo:

Donde tenemos que el nombre distintivo de esta entrada (**dn**) está formado por el nombre de la persona (**Common Name**), que pertenece a una unidad organizativa (**Organization Unit**), esta a su vez a una organización de un país (**Organization**) y, por último, la organización a un país (**Country**), pudiendo haberse introducidos niveles intermedios entre, por ejemplo, la organización y el país, como pueden ser la provincia, etc.

Los ficheros de extensión LDIF

En LDAP, los ficheros de extensión LDIF corresponden a ficheros de texto UTF-8 que **permiten representar, introducir y extraer la información de las entradas de LDAP**. Además, los ficheros LDIF permiten especificar modificaciones que deben realizarse en las entradas de LDAP.



Los ficheros de extensión SCHEMA:

La información que se desea introducir en cada uno de los registros (elementos) de LDAP se debe encontrar previamente definida en unos archivos, cuya **extensión es SCHEMA**, y que son conocidos como esquemas de LDAP. Los esquemas (schemas) **contienen la información relativa a los atributos** (attributes) y a las clases de objectos (object classes) que podemos almacenar en LDAP. En la configuración de LDAP, que veremos con posterioridad, se deben incluir todos los esquemas que deseemos utilizar. Los esquemas que existen por defecto se encuentran generalmente en el directorio **/etc/openldap/schema** o sus subdirectorios.

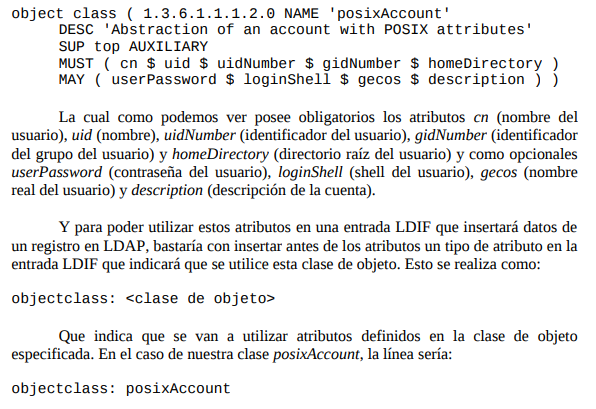
**En los esquemas**, los atributos son los elementos que forman parte de un registro de LDAP, por ejemplo, el nombre, apellidos, teléfono, dirección de correo, etc., pudiendo utilizarse cualquier atributo que exista en los esquemas incluidos.

**Las clases de objeto** describen el tipo de registro que se está intentando construir, indicando que atributos son obligatorios y que atributos son opcionales, de forma que todo atributo debe estar asociado con la clase de objeto apropiada.

**Un registro puede estar formado por atributos pertenecientes a una o varias clases de objeto.**

Los atributos de una clase de objeto pueden tener dos calificadores, MUST o MAY. Si un atributo tiene el calificador MUST, significa que esa clase de objeto obliga a que la presencia de un valor para ese atributo es obligatoria para esa clase de objeto, mientras que, si se encuentra con el calificador MAY, ese atributo puede tomar o no valor para esa clase de objeto.

Ejemplo 2:



CONFIGURACIÓN DEL SERVIDOR

El servidor de LDAP es el programa **/usr/sbin/slapd**.

En las versiones antiguas de LDAP, la configuración se realizaba en el fichero /etc/openldap/slapd.conf8, mientras que en la actualidad la configuración se realiza mediante un backend9 de **slapd** donde se almacena la configuración.

Este cambio de formato de configuración permite modificar la configuración de LDAP y aplicar los cambios sin necesidad de volver a arrancar el servidor de LDAP.

El backend de configuración se encuentra dentro del directorio **/etc/openldap/slapd.d**.

Dentro de ese directorio podemos encontrar un fichero, cn=config.ldif que contiene las opciones globales básicas de configuración del funcionamiento del servidor de LDAP (directorio de configuración, fichero de almacenamiento del identificador de proceso, tamaño de buffers, etc.), y un subdirectorio cn=config, dentro del cual se encuentran los ficheros que definen los diferentes tipos de backends existentes y un subdirectorio cn=schema que contiene los esquemas básicos de LDAP.

