UD08
Servicio de Directorio Linux

Índice

Introducción

Introducción

- **Recuerda** que un **servicio de Directorio** es un **conjunto de aplicaciones** utilizadas en los **sistemas cliente/servidor**, que sirven **para organizar y centralizar la información** de todos los:
  - Usuarios.
  - Equipos.
  - Grupos (usuarios o equipos).
  - Dominios.
  - Recursos compartidos.
  - Políticas de seguridad.
  - ...
- La gran **ventaja** de contar con estas herramientas es que, al centralizar toda esta información, **facilita a los administradores**:
  - El control de acceso de los **usuarios**.
  - La gestión de los **recursos** de la red, es decir, **quién tiene acceso** a qué recurso y **qué puede hacer** con ellos.

Introducción

- En **Windows Server** se utiliza **Active Directory Domain Services (AD DS)** como Servicio de Directorio.
- Por tanto, **AD DS** proporciona un **repositorio central de información** para toda la infraestructura, permitiendo:
  - Un **inicio de sesión** para los usuarios.
  - El **acceso** de los usuarios a **recursos del sistema**.
- Esto **simplifica**, en los **entornos Windows, la administración** de **usuarios** y **equipos** y el acceso a los **recursos** en red.

Introducción

- Pero, **¿Cómo se presta un servicio de este tipo en Linux?**
- La **respuesta** es que este tipo de servicio se presta en el entorno de Linux Server utilizando **LDAP**.
- **LDAP** son las siglas de Lightweight Directory Access Protocol (Protocolo Ligero de Acceso a Directorio).
- LDAP es un **protocolo** basado en la **arquitectura cliente/servidor**, utilizado para **acceder a un servicio de Directorio remoto** que se encuentre **centralizado en una red**.
- **Recuerda** que una de las **ventajas de AD DS es que utiliza el protocolo LDAP** para la consulta de información contenida en el Directorio Activo.

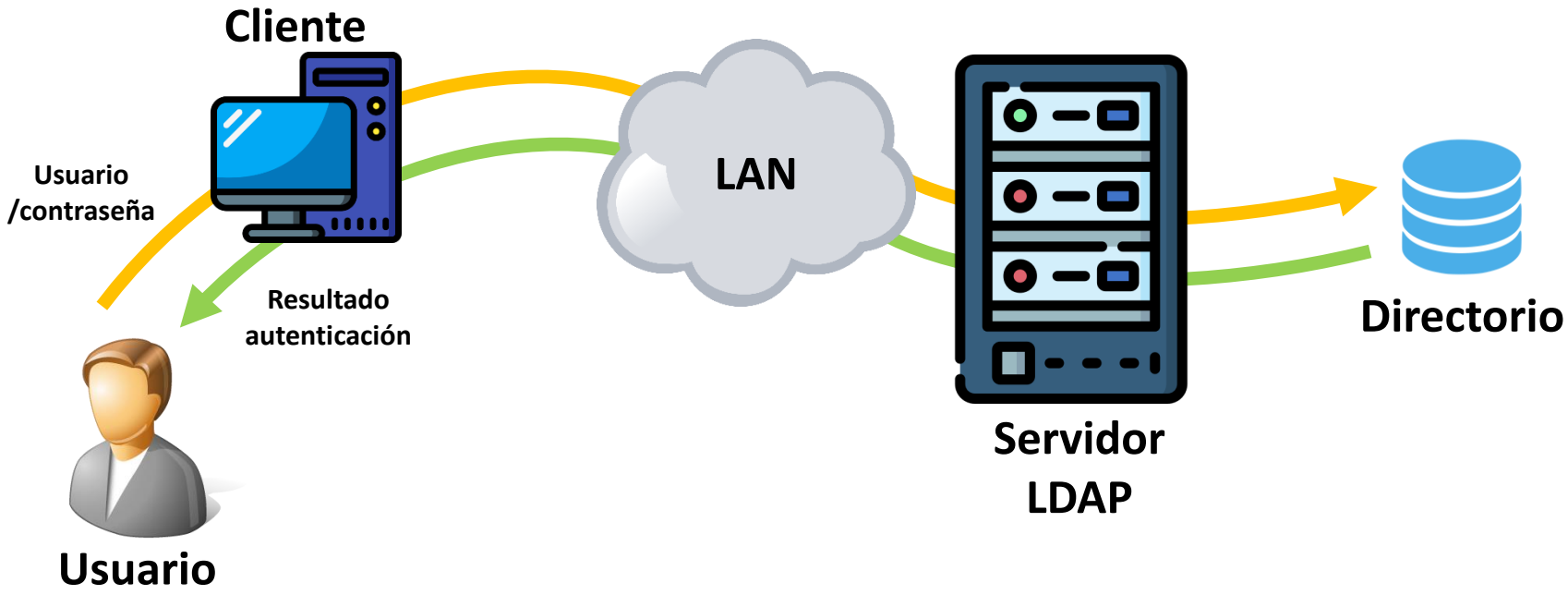
Servicio de Directorio Linux

LDAP

LDAP

- **LDAP** es un **protocolo** para el acceso a un **servicio de Directorio** implementado sobre un **entorno de red,** normalmente construido como una **base de datos jerárquica**, sobre la que se pueden realizar **consultas**.
- Puede ejecutarse sobre **TCP/IP o sobre cualquier otro servicio de trasferencia orientado a conexión**.
- También es frecuente que el servicio de Directorio almacene la **información de autenticación para los usuarios y/o recursos**.
- De esta forma, se **facilita el control de acceso** sobre los datos contenidos en el servidor.
- Esto podríamos representarlo de **modo esquemático con el siguiente dibujo**:

LDAP


Cliente
Usuario
/contraseña
Resultado
autenticación
LAN
Directorio
Servidor
LDAP
Usuario

Autenticación de usuarios en Server Linux

Autenticación de usuarios en Server Linux

- Existen **distintas formas de autenticación** de usuarios en una red Linux. No obstante, la **forma más usada** suele ser la combinación de tres herramientas diferentes: **LDAP, PAM y NSS**.
- La idea consiste en disponer de un **servidor** que facilite la **autenticación** de los usuarios, de modo que los **equipos clientes recurran al servidor** cada vez que una cuenta de **usuario necesite identificarse**.
- De esta forma, la **cuenta de usuario no es específica de un equipo cliente**, sino que será **válida en cualquier equipo** de la red que haya sido debidamente configurado.
- Éste es el **método** que suele utilizarse en **Linux** para obtener una **gestión de usuarios global, similar** a la que ofrecen los **Servidores Windows** con un controlador de dominio **AD DS**.
- Ya sabemos que LDAP es el **protocolo** para el acceso al **servicio de Directorio**. Vamos a ver cuál es la **función del servidor NSS y PAM.**

Autenticación de usuarios en Server Linux
NSS

- **NSS** (Name Service Switch) es un **servicio** que permite la **resolución de nombres de usuario y contraseñas** (o grupos) mediante el acceso a **diferentes orígenes de información**:
  - En **sistemas locales**: esta información se encuentra en los archivos locales del sistema operativo, en concreto en **/etc/passwd, /etc/shadow y /etc/group**
  - En **sistemas en red**: esta información puede proceder de otras fuentes:
    - **DNS** (Domain Name System).
    - **NIS** (Network Information Service).
    - **WINS** (Windows Internet Name Service).
    - **LDAP** (Lightweight Directory Access Protocol).

Autenticación de usuarios en Server Linux
NSS

- El **objetivo de NSS** es que los **programas o los comandos** del sistema operativo **puedan manejar información administrativa** relacionada con los **usuarios**, las **contraseñas** y los **grupos** (incluidos aspectos como la caducidad de una contraseña o su nivel de complejidad) sin **tener que conocer el lugar donde se encuentra almacenada**.
- Es decir, cuando una **aplicación**, o un **comando**, necesita información referente a una cuenta de usuario, **no consulta el fichero /etc/passwd**. En su lugar:
  - Realiza una **petición al servidor NSS**.
  - El **servidor NSS le responde** con la información solicitada.
- El servidor **NSS se encarga de localizar esta información**, que puede estar almacenada en distintas **bases de datos, locales o en red.**

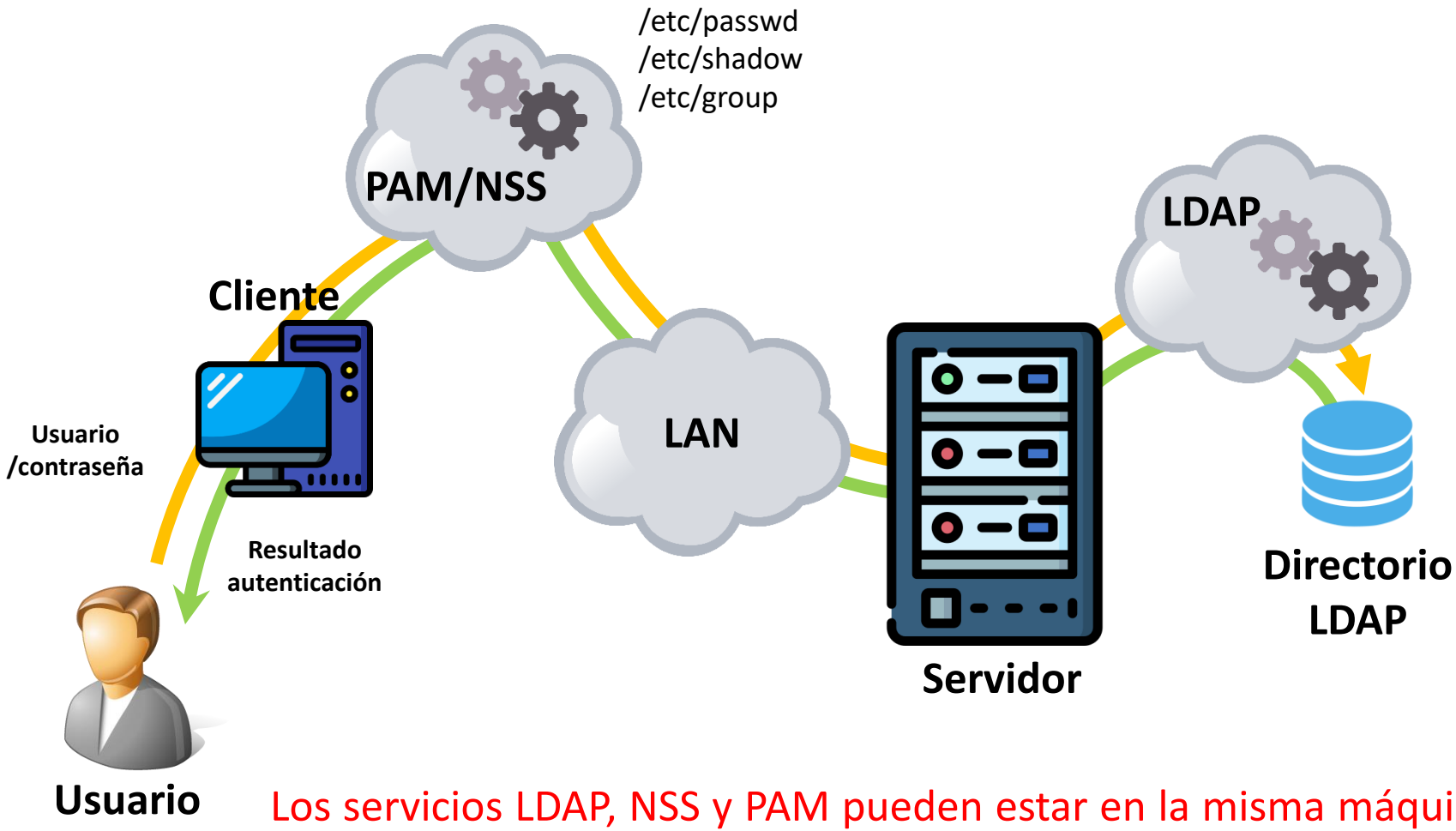
Autenticación de usuarios con LDAP
PAM

- **PAM** (Pluggable Authentication Modules) establece una **interfaz entre los programas** de usuario y distintos **métodos de autenticación**.
- La idea se basa en la **creación de módulos de autenticación**, de forma que sea **transparente** para el sistema el uso de **distintos métodos de autenticación**:
  - **Nombre de usuario** y una **contraseña**.
  - Dispositivos que faciliten la **identificación biométrica** de los usuarios (lectores de huellas, de voz, de imagen, ...).
  - **Lector de tarjetas**.
  - ...
- Gracias a ello, conseguimos que el **método de autenticación** sea **transparente para los programas**, es decir, los programas no tienen que incluir en su código el procedimiento de autenticación. El **procedimiento de autenticación se convierte en una petición de servicio al servidor PAM**.

Autenticación de usuarios con LDAP
PAM

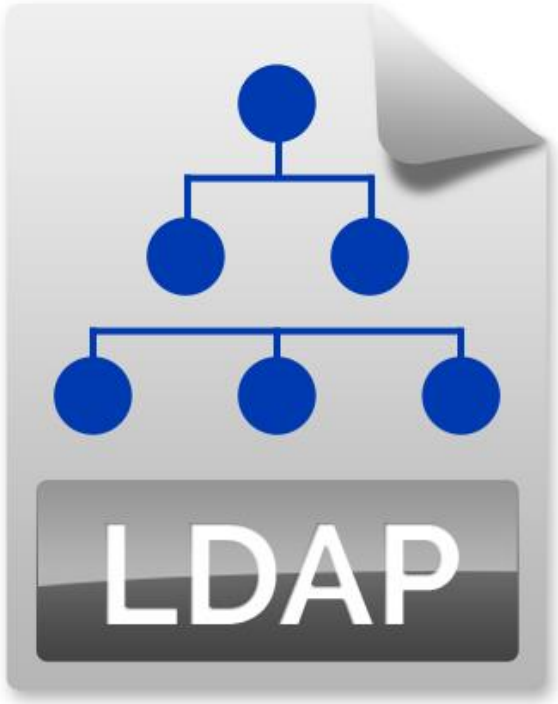
- **PAM y NSS se complementas** para la autenticación de los usuarios:
  - **NSS** se centra en **buscar**, localmente o en red, la **información** referente a los **usuarios**.
  - **PAM** controla la **autenticación, el inicio de sesión y su configuración**.
- En la actualidad, **PAM es el método que utilizan la mayoría de las aplicaciones y herramientas** de Linux que necesitan relacionarse, de algún modo, con la **autenticación de los usuarios**.

Autenticación de usuarios con LDAP



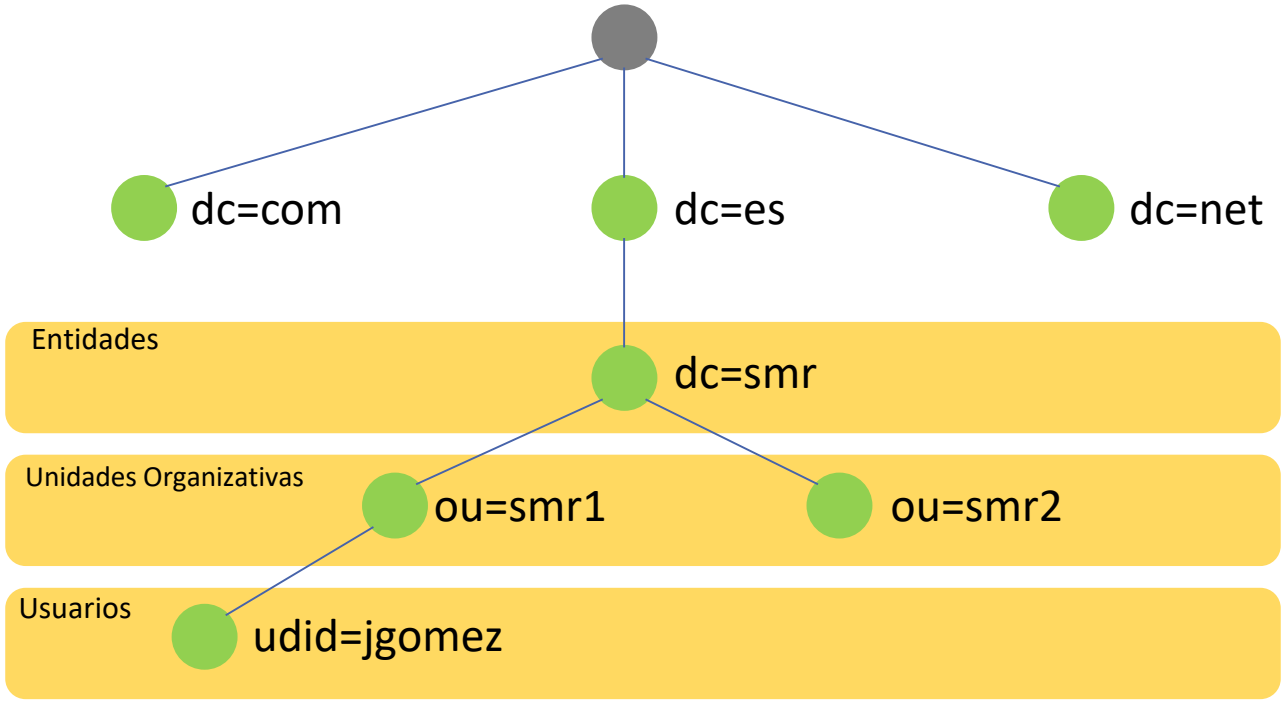
Los servicios LDAP, NSS y PAM pueden estar en la misma máquina o estar ofreciéndose desde distintos servidores de la red.

Modelo de datos de LDAP



Modelo de datos de LDAP

- El **modelo de datos de un Directorio basado en LDAP** es una **base de datos jerárquica** con forma de **árbol de nodos** llamado **Directory Information Tree** (DIT).



Árbol de directorio LDAP

Modelo de datos de LDAP

- **Cada nodo** del árbol es lo que denominamos **una entrada del Directorio** y representa un **objeto**. Este objeto puede ser **abstracto o real**:
  - Una persona.
  - Un mesa.
  - Una función en la estructura de una empresa.
  - …
- **Cada una de las entradas** está compuesta por una colección de **atributos**.
- Los **atributos** de un objeto **pueden ser diferentes** a los de otro objeto. **Cada objeto esta asociado a una o varias clases y es la clase lo que determinará los atributos** que tendrá dicho objeto.
- Es decir, los **objetos** asociados a la **misma clase** tendrán los **mismos atributos**. Lo que **variará será el valor** de los atributos en cada objeto.

Modelo de datos de LDAP

- Veamos un **ejemplo**.
- Tenemos **dos clase** de objeto:
  - Clase **mueble**, que se caracteriza por los siguientes **atributos: alto**, **ancho** y l**argo**.
  - Clase **persona**, que se caracteriza por los siguientes **atributos: edad** y **domicilio**.
- Tenemos **dos objetos** asociados a la **clase mueble**, que son **mesa1** y **mesa2**. Estos objetos tendrá los **mismos atributos** (alto, ancho y largo) pero estos atributos tendrán **distinto valor**:
  - **Mesa1**: alto=90 cm., ancho=70 cm., largo=130 cm.
  - **Mesa2**: alto=87 cm., ancho=80 cm., largo=140 cm.
- Como es lógico, **mesa1** y **mesa2 no tienen los atributos edad y domicilio**, porque no son propios de la clase a la que están asociados.

Modelo de datos de LDAP

- Los **atributos tienen nombres** que hacen referencia a su contenido y **pueden ser de dos tipos**:
  - **Atributos normales**: son los atributos que **identifican** al objeto (nombre, apellidos, …).
  - **Atributos operativos**: son los atributos que utiliza el servidor para **administrar el directorio** (fecha de creación, tamaño, …)
- Algunos **atributos** serán **obligatorios y** otros podrán ser **opcionales**.
- El **listado completo de atributos y clases de LDAP** los puedes consultar en el enlace: https://oav.net/mirrors/LDAP-ObjectClasses.html

Modelo de datos de LDAP

- Por **ejemplo**, aunque existe muchos más, los siguientes son **atributos** habituales de una **entrada asociada a la clase persona** en el Directorio LDAP ((*) comunes a todas las clases):
  - **dn** (distinguished name): nombre distintivo de una entrada, contiene un conjunto de atributos y es de carácter único (*).
  - **dc** (domain component): se refiere al componente del dominio, ya sea un componente, una etiqueta o un nombre de dominio DNS (*).
  - **ou** (organizational unit): unidad organizativa (*).
  - **uid** (user id): Identificación única de la entrada en el árbol.
  - **objectClass**: Indica el tipo de objeto al que pertenece la entrada (*).
  - **cn** (common name): Nombre de la persona representada en el objeto.
  - **givenname**: Nombre de pila.
  - **sn** (surname): Apellido de la persona.
  - **o** (organization): Entidad a la que pertenece la persona.
  - **u** (organizational unit): El departamento en el que trabaja la persona.
  - **mail**: dirección de correo electrónico de la persona.

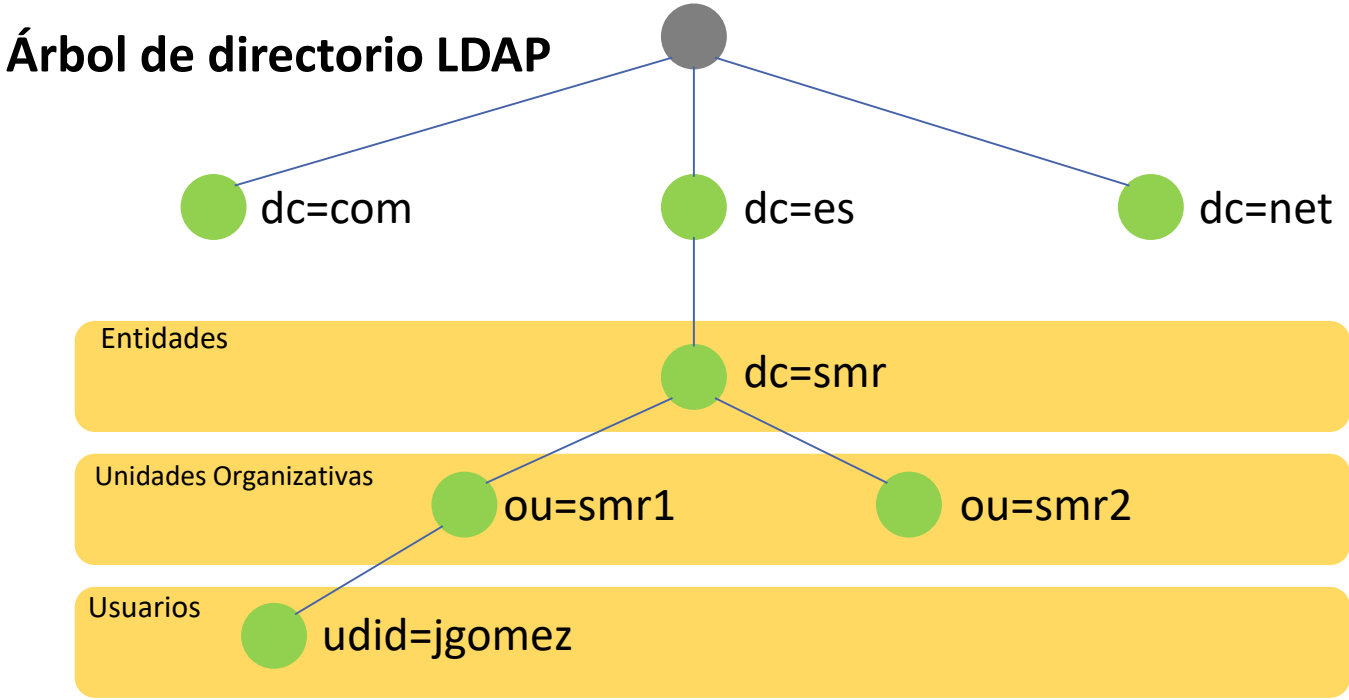
Modelo de datos de LDAP

- Para **identificar cada entrada** dentro del árbol del Directorio, se utiliza un **identificador global y único** que denominamos **nombre completo, dn (Distinguished Name)**.
- El nombre completo **dn** se formará con una serie de **pares atributo/valor, separados por comas, que reflejan la ruta** desde la posición lógica del **objeto hasta la raíz** del árbol.

  dn: **uid**=jgomez, **ou**=smr1, **dc**=smr, **dc**=es
- Como se puede **observar**:
  - **dn** está compuesto por **componentes separados por “,”**.
  - Cada **componente** es un **par “atributo=valor”**, donde el **atributo es una abreviatura** usada por LDAP.
- En el ejemplo anterior, la **estructura representada** es:

  dc=smr, **dc**=es (Componente de dominio)
  ou=smr1 (Unidad organizativa)
  uid=jgomez (Usuario)

Modelo de datos de LDAP



dn: **uid**=jgomez, **ou**=smr1, **dc**=smr, **dc**=es
objectClass: person
cn: Juan Gomez
givenname: Juan
sn: Gomez
o: smr
u: smr1
mail: jgomez@ggg.es

Ejemplo de una entrada almacenada en el directorio **LDAP**.
El atributo especial llamado **objectClass** determina qué **atributos son válidos y cuáles son obligatorios** en una entrada asociada a esa clase en particular.

Modelo de datos de LDAP

- Como hemos dicho antes, las diferentes **entradas** se organizan a modo de **árbol jerárquico** que suele **representar** una **estructura organizativa o geográfica** en particular.
- De este modo:
  - Las entradas que representan **comunidades autónomas aparecerán en la parte superior** del árbol.
  - **Debajo** estarán las que representan **provincias**.
  - **Después** las **ciudades**, los **departamentos**, los **usuarios**, etc.
- En la **actualidad**, las implementaciones de **LDAP suelen utilizar DNS** (Domain Name Service) para la estructura de los **niveles superiores** del árbol.

Modelo de datos de LDAP

- **LDAP** establece **operaciones** para:
  - **Consultar** información en el Directorio.
  - **Actualizar** información en el Directorio:
    - **Crear** entradas.
    - **Modificar** entradas existentes.
    - **Eliminar** entradas.
- La **mayor parte del tiempo**, LDAP se utiliza para realizar **consultas** sobre la información que contiene, por lo que es común que la **estructura** de su base de datos se encuentre **optimizada para la lectura (consulta) en detrimento de la escritura (modificación)**.

OpenLDAP

OpenLDAP

- **OpenLDAP** es un desarrollo del **protocolo LDAP**, implementado con la filosofía del **software libre y código abierto**.
- Igual que LDAP, **OpenLDAP** está muy **optimizado** para ofrecer buenos resultados en situaciones que requieran **operaciones de lectura intensivas**.
- Debido a esto:
  - Directorio **OpenLDAP** arrojará **resultados muy superiores a** los que ofrece una **base de datos relacional**, cuando realicemos operaciones de **consulta intensivas** sobre ambas.
  - Por contra, si utilizáramos un directorio **OpenLDAP** para guardar **datos que son actualizados de manera frecuente**, los **resultados** obtenidos serán **muy inferiores** a los ofrecidos por una **base de datos relacional**.
- No sólo **podemos encontrar OpenLDAP** en la mayoría de las distribuciones **Linux**, sino que también lo encontramos para **Microsoft Windows**, **Apple** OSX, **Solaris**, **HP UX**, **BSD**, etc.