Servicios de directorio

Modulo: Despliegue de aplicaciones web

Directorios

- Desde los inicios de los sistemas de ficheros, hasta llegar a los primeros sistemas operativos para ordenadores PC, la palabra **directorio** se ha **asociado al esquema con el que los distintos archivos están organizados en las unidades de almacenamiento.** Por tanto **el concepto de directorio** está estrechamente **ligado a la organización de datos**.

- Un **directorio** es una **estructura jerárquica** que **organiza y almacena datos acerca de elementos**. Podemos decir que **es un tipo concreto de base de datos**.

- En un **directorio de sistema informático en red**, la **información que se guarda** tiene que ver con los recursos del sistema (**servidores, impresoras, etc.) y con sus usuarios**.

- Es preciso que el sistema cuente con un **servidor** para poder consultar la información, almacenarla o simplemente diseñarla.

- La información puede estar almacenada de forma **distribuida y/o replicada**.

Servicios de directorio

- **Un servicio de directorio es una plataforma que proporciona métodos para gestionar y almacenar los datos que contiene el directorio**.

- Un servicio de directorio (SD) es una **aplicación o un conjunto de aplicaciones** que **almacena y organiza la información de los usuarios de una red de computadores**, permitiendo a los administradores **gestionar el acceso de usuarios a los recursos** sobre dicha red. Además, los servicios de directorio **actúan como una capa de abstracción entre los usuarios y los recursos compartidos.**

- Los **directorios tienden a contener información descriptiva basada en atributos y tienen capacidades de filtrado muy sofisticadas**. Los directorios **generalmente no soportan transacciones complicadas ni esquemas de vuelta atrás (Roll Back)** como los que se encuentran en los sistemas de bases de datos diseñados para manejar grandes y complejos volúmenes de actualizaciones. **Las actualizaciones de los directorios son normalmente cambios simples**.

- Un **servicio de directorio no debería confundirse con el repositorio de directorio**, que es la base de datos. Esta es la que contiene la información sobre los objetos, gestionados por el servicio de directorio.

Servicios de directorio

- El servicio de directorio **proporciona la interfaz de acceso a los datos** que se contienen en uno o más espacios de nombre de directorio.

- **La interfaz** del servicio de directorio es la **encargada de gestionar la autenticación de los accesos al servicio de forma segura**, actuando como autoridad central para el acceso a los recursos de sistema que manejan los datos del directorio.

- Como base de datos, un **servicio de directorio** está **altamente optimizado para lecturas y proporciona alternativas avanzadas de búsqueda** en los diferentes atributos que se puedan asociar a los objetos de un directorio.

- Los datos que se almacenan en el directorio son definidos por un **esquema extensible y modificable.**

Servicios de directorio

- El servicio de directorio puede estar **centralizado o distribuido.**
  - **Centralizado:** En este caso un único servidor ofrece todo el servicio de directorio respondiendo a todas las consultas de los clientes.
  - **Distribuido**: Si el directorio está distribuido, varios servidores proporcionan el servicio de directorio. Cuando está distribuido, los datos pueden estar fraccionados y/o replicados:
    - Cuando está fraccionado, cada servidor de directorio almacena un subconjunto único y no solapado de la información, es decir, una entrada es almacenada en un solo servidor.
    - Cuando la información está replicada, una entrada puede estar almacenada en varios servidores.
- Los servicios de directorio de las grandes organizaciones **utilizan un modelo distribuido para almacenar su información y esa información generalmente está replicada entre los servidores** que forman el directorio.

Características de los servicios de directorio

- **El Directorio es Dinámico**. Los directorios electrónicos pueden ser **consultados y/o actualizados en tiempo real** y su fiabilidad es por lo tanto mucho mayor.
- **El Directorio es Flexible**. La flexibilidad se puede contemplar desde dos aspectos
    a. En cuanto a contenido: Esto permite ampliar la información almacenada sin muchas repercusiones.
    b. En cuanto a organización: **la organización de la información permite localizarla de diferentes maneras**, incluso puede realizar búsquedas aproximadas, algo que es imposible con los directorios clásicos (ej. una guía telefónica).
- **El directorio es seguro**. Puede ser **controlado el acceso a los datos en función de diferentes criterios**.
- **El directorio es configurable**. Los directorios electrónicos permiten la personalización de los datos que se muestran a los distintos usuarios. Se puede establecer la información que recibe una persona en función de sus necesidades y qué personas pueden acceder a dicha información.

Características técnicas de los servicios de directorio

Un directorio puede verse como una base de datos especializada, **aunque las diferencias** entre una base de datos de propósito general y un directorio **son las siguientes**:

- **Relación entre lecturas y escrituras**. En un directorio se espera un número muy alto de lecturas frente a escrituras, esto se debe a que generalmente la información contenida en el directorio cambia raramente. al crear un directorio, los esfuerzos de optimización se concentran en las búsquedas y lecturas, mientras que no importa que por ello se penalicen las actualizaciones.

- **Extensibilidad**. El término *directory schema* se refiere a los tipos de información que se almacenan en el directorio, qué reglas debe cumplir dicha información y cómo se realizan las operaciones de búsqueda sobre estos datos. La ventaja que presentan los directorios frente a las bases de datos tradicionales estriba en que dicho esquema se puede modificar para cubrir las necesidades que vayan surgiendo en la organización. En las bases de datos tradicionales, esto es mas complejo, o sus repercusiones son mayores.

Características técnicas de los servicios de directorio

- **Distribución de los datos**. Fragmentación vertical frente a horizontal. Los directorios permiten que **los datos referentes a toda una unidad organizativa sean almacenados en un servidor controlado por esta unidad** (**fragmentación horizontal**). Este tipo de fragmentación simplifica las actualizaciones, ya que todos los datos referentes a una persona se encuentran en el mismo servidor y permite a su vez optimizar las búsquedas, ya que las consultas se pueden ejecutar en paralelo.

- **Replicación de la información**. Las bases de datos de propósito general que admiten replicación de datos, están preparadas para replicar los datos en un número reducido de servidores, esto se debe a que las copias deben ser consistentes y por lo tanto, las actualizaciones deben realizarse de forma sincronizada entre las diferentes sedes

  En el caso de los directorios, es aceptable una inconsistencia temporal, por lo que el protocolo de replicación/actualización es menos restrictivo.

Características técnicas de los servicios de directorio

- **Inherente a la replicación de la información**, se encuentra el aumento en la **fiabilidad del sistema**, ya que en caso de catástrofe, se puede utilizar el servidor replicado. Además también se puede obtener una mejora en el rendimiento al situar las replicas en redes cercanas a los usuarios, optimizando el camino de acceso al directorio y repartiendo la carga entre las distintas replicas.

  La fiabilidad del directorio comienza a ser crítica en el momento en el que varias aplicaciones lo utilizan para tareas como autenticación , control de accesos y gestión de configuración

- **Estándares**. El hecho de que las bases de datos de propósito general utilicen ligeras variantes del estándar SQL no suele ser un problema, ya que rara vez tienen que interactuar dos bases de datos de diferentes fabricantes, sin embargo, dado que el directorio es una base de datos accesible desde múltiples aplicaciones, el estricto cumplimiento del estándar es un requisito indispensable.

  Este aspecto es importante, ya que permite separar el desarrollo del cliente del desarrollo del servidor, permitiendo que cada desarrollo este optimizado en el sentido que sea conveniente

Para que usar un servicios de directorio

Los directorios electrónicos permiten:

- **Encontrar información**. Los directorios electrónicos permiten acceder a la información contenida en los mismos de múltiples formas. Un directorio electrónico permite realizar búsquedas, no solamente por orden alfabético, sino también por: apellido: dirección, teléfono Es más, podemos sumar campos de búsqueda, como por ejemplo: dirección y apellido.

- **Gestionar información**. En los directorios electrónicos pueden existir varios usuarios que en tiempo real estén realizando modificaciones, como agregar/editar/eliminar distintos usuarios con sus correspondientes campos. Además, esta información ya estaría visible para todas aquellas aplicaciones que accedan a dicha información.

- **La información que se almacena es aquella que permita organizar de manera jerárquica todos los usuarios de la red**. Estructurar la información de los usuarios de la red es de utilidad a la hora de restringir el acceso a los servicios y recursos de la red, permitiendo gestionar con mayor facilidad la red.

Para que usar un servicios de directorio

Los directorios electrónicos permiten:

- **Control de seguridad**. permiten delimitar el acceso a los usuarios, sino que también proporcionan una solución al problema de gestión de certificados digitales. Así, permiten:

  a. Su creación: Incorporar a los certificados los datos contenidos en el directorio.
  b. Su distribución: Tener accesibles mediante un protocolo estándar los certificados.
  c. Su destrucción: Revocar los certificados de forma sencilla simplemente borrando el certificado del directorio.
  d. Su ubicación: Los usuarios pueden acceder a través del directorio a los certificados de los restantes usuarios, de forma muy sencilla y fácil de integrar con las aplicaciones.

Diferencias entre Directorios y otros programas y/o servicios

- **Directorios vs Bases de datos (ya visto anteriormente):**
  - Directorios optimizados para accesos de lectura. BD para accesos de lectura y escritura.
  - Directorios optimizados para almacenar información relativamente estática.
  - Los directorios no soportan transacciones.
  - Mayoría de bases de datos utilizan el lenguaje de consulta SQL, que permite el desarrollo de funciones de consulta y actualización muy complejas. Por otra parte, los directorios LDAP utilizan un protocolo simplificado y optimizado.

- **Directorio vs Sistemas de ficheros:**

  Los directorios están optimizados para almacenar pequeños fragmentos de información que puede estructurarse como entradas con diferentes atributos, en cambio, los sistemas de ficheros contienen archivos, a veces de tamaños superiores al gigabyte. Además, los sistemas de ficheros permiten acceder a un fichero y posicionarse dentro de él, sin embargo, los directorios a lo sumo permiten acceder a un atributo, pero no hay forma de posicionarse dentro de dicho atributo, que por lo tanto debe ser leído por completo

Diferencias entre Directorios y otros programas y/o servicios

- **Directorios vs DNS**: Tanto un servicio de directorio como un servicio DNS proporcionan acceso a una base de datos jerárquica, pero difieren en:

    a. Los servidores de directorio no están particularizados a una acción concreta, sino orientados deforma más general, mientras que el servicio DNS está dedicado a la traducción de nombres de dominios a direcciones IP.

    b. La información almacenada en el servicio de directorio no es fija, mientras que en el servicio DNS tiene una estructura fija.

    c. Los servicios de directorio suelen utilizar protocolos orientados a conexión (TCP), mientras que el servicio DNS opera con protocolos no orientados a conexión (UDP)

LDAP

- En 1988, la CCITT (actual ITU-T) creó el **estándar X.500**, sobre servicios de directorio.
- X.500 especifica que la comunicación entre el cliente y el servidor de directorio debe emplear el **Directory Access Protocol (DAP)**. Pero DAP es un protocolo a nivel de aplicación, por lo que, tanto el cliente como el servidor debían implementar completamente la torre de protocolos OSI.
- Las iniciales **LDAP** en inglés significa **Lightweight Directory Access Protocol**; **Protocolo Ligero para Acceder al Servicio de Directorio.**
- **LDAP surge como una alternativa a DAP**. Las claves del éxito de LDAP en comparación con DAP de X.500 son:
  - LDAP utiliza TCP/IP en lugar de los protocolos OSI. TCP/IP requiere menos recursos y está más disponible, especialmente en ordenadores de sobremesa.
  - El modelo funcional de LDAP es más simple y ha eliminado opciones raramente utilizadas en X.500. LDAP es más fácil de comprender e implementar.
  - LDAP representa la información mediante cadenas de caracteres en lugar de complicadas estructuras ASN.1 (norma para representar datos independientemente de la máquina que se esté usando y sus formas de representación internas).

LDAP

- **LDAP** es un conjunto de protocolos usados para acceder a información guardada centralmente a través de la red.

- El protocolo **LDAP define** el método para acceder a datos en el servidor a nivel cliente. Es decir, LDAP define el método por el cual se accede a los datos de directorio, y necesariamente, también define y describe cómo los datos son representados en el servicio de directorio (el modelo de datos -información-).

- **También define** como los datos son cargados (importados) dentro y guardados (exportado) fuera en un servicio de directorio (utilizando archivos **LDIF**).

- **LDAP no define** la manera en la que se almacenan internamente los datos y como se manipulan.

- El protocolo LDAP actualmente se encuentra en su 3ª versión y el IETF (Grupo de Trabajo de Ingeniería de Internet) lo ha estandarizado. Por lo tanto, existe una RFC (Request for comments) para cada versión de LDAP que constituye un documento de referencia:
  - RFC 1777 para LDAP v.2
  - RFC 2251 para LDAP v.3

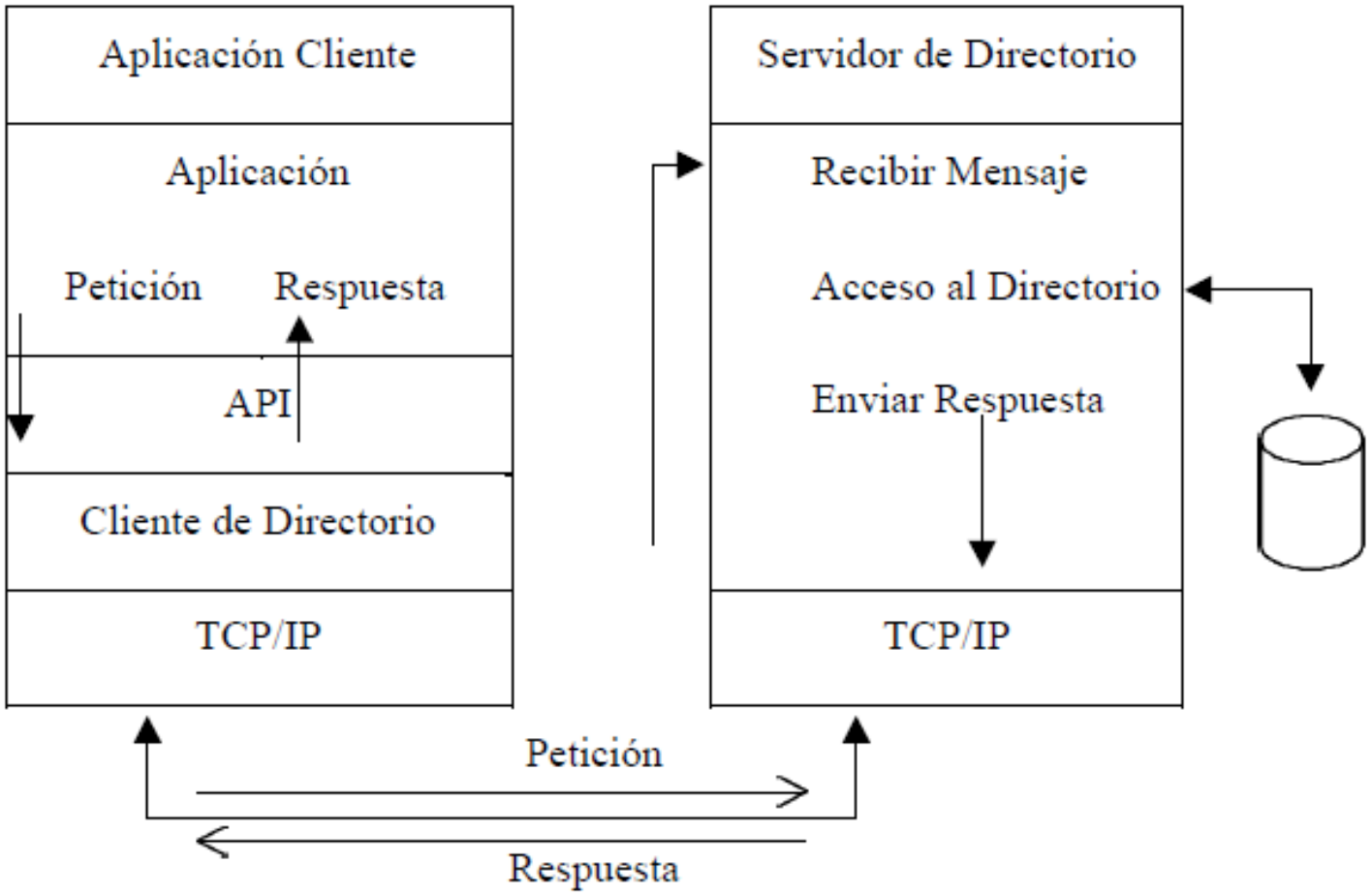
Esquema de interacción entre cliente y servidor LDAP

- El cliente establece una sesión con el servidor LDAP. El cliente indica el servidor y el puerto en el que el servidor LDAP está escuchando. El cliente puede proporcionar información de autenticación o establecer una sesión anónima con los accesos por defecto.
- El cliente efectúa las operaciones sobre los datos. LDAP proporciona capacidades de búsqueda, lectura y actualización.
- Una vez finalizadas las operaciones, el cliente cierra la sesión.

Arquitectura Cliente-Servidor del servicio de Directorio

Los servicios de directorio suelen implementarse siguiendo el modelo cliente-servidor, de modo que una aplicación que desea acceder al directorio no accede directamente a la base de datos, sino que llama a una función de la API (Application Programming Interface), que envia un mensaje a un proceso en el servidor. Dicho proceso accede al directorio y devuelve el resultado de la operación

Arquitectura Cliente-Servidor del servicio de directorio



Estructura del directorio LDAP

- Un directorio **LDAP** tiene una estructura de árbol. Todas las entradas, denominadas "objetos“ (persona, impresora, etc), del directorio tienen una posición definida en esta jerarquía. Esta jerarquía se denomina ***árbol de información del Directorio*** **(DIT)**. La vía completa a una entrada, que la identifica de forma clara, se llama ***nombre completo*** **o DN (distinguished name)**. Un nodo sencillo junto con la vía a esta entrada se denomina ***nombre completo relativo*** **o RDN**. Un **DN esta compuesto por una secuencia de RDN.**

- **Esquema de directorio LDAP**: colección de atributos definidos, clases de objetos definidas… para controlar dónde es almacenado cada dato.

  - Cualquier base de datos, sin tener en cuenta su complejidad o tecnología subyacente, tiene un esquema. En términos simples, un esquema es el modelo de los datos, el diseño en lo tocante a cómo los datos se almacenan, qué tipos de datos son rastreados, y las relaciones entre datos almacenados en varias entradas.

  - Cuando se configura un directorio LDAP, la información para cualquier entrada dada se almacena en una serie de atributos. Se pueden crear nuevos tipos de valores que serán almacenados en el directorio.

Estructura del directorio LDAP

- **Esquema de directorio LDAP (continuación)**
  - Colectivamente, a todos los atributos que pueden ser utilizados para un tipo específico de objeto se les llama **Clases de Objetos** (**Object Class, en ingles**). **Todos los objetos de LDAP deben tener el atributo objectClass**. Como con los atributos, se pueden definir nuevas clases de objetos para adecuarlas a las necesidades. Dentro de cada clase de objeto, se pueden designar que algunos atributos son requeridos, y otros que son meramente opcionales.

    Si hacemos un símil con bases de datos tradicionales: los campos son similares a los atributos, las tablas son similares a las clases de objetos.

Por tanto, **un esquema (schema) define**: qué clases de objetos se pueden almacenar en el directorio, qué atributos deben contener, qué atributos son opcionales y el formato de los atributos.

Estructura del directorio LDAP

Por lo general, existen dos tipos de objetos:

- **Contenedor**: Este tipo de objeto puede contener a su vez otros objetos. Algunos ejemplos de estos elementos son: Root (elemento raíz del árbol de directorios que no existe en realidad), c(country), ou (OrganizationalUnit) y dc (domainComponent).

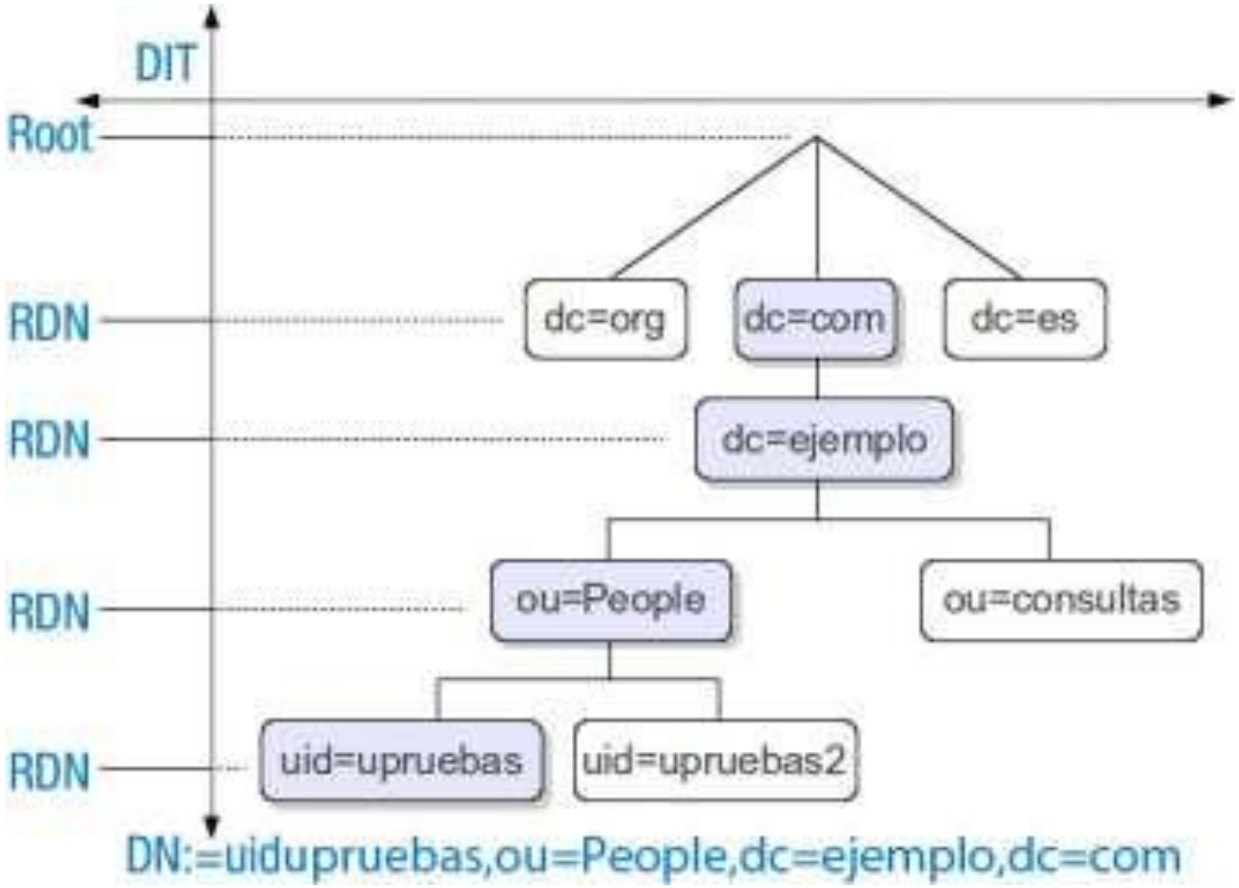
  La figura análoga al contenedor es el directorio (carpeta) de un sistema de archivos.

- **Hoja**: Este tipo de objeto se encuentra al final de una rama y carece de objetos subordinados.

  Algunos ejemplos son: Person/InetOrgPerson (Internet Organizational Person) o groupofNames**.**

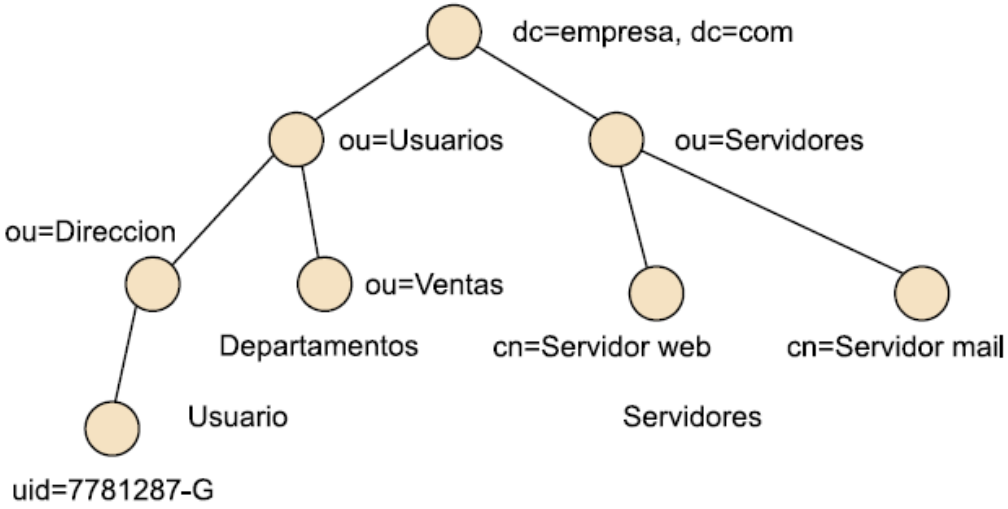
En la cúspide de la jerarquía del directorio se encuentra el elemento raíz Root. A este elemento le puede seguir en un nivel inferior **c (country), dc (domainComponent) ó o (organization)**.

Estructura del directorio LDAP



La figura representa un DIT ficticio con entradas en cuatro niveles. Cada entrada se corresponde con una casilla en la figura. En este caso, el nombre válido completo DN del empleado ficticio **upruebas es:**dn: uid=upruebas,ou=People,dc=ejemplo,dc=com .
Uid sersía user identification.

Estructura del directorio LDAP



En esta organización (*empresa.com) hay definidos dos grupos de objetos: los usuarios y* los servidores. Los usuarios se dividen en departamentos. LDAP y otras implementaciones derivadas permiten la agrupación de elementos y crear una jerarquía. LDAP no fija ninguna jerarquía ni ningún número determinado de niveles: el espacio de nombres permite dar flexibilidad para adaptarse a multitud de usuarios.

Tarea

- Elabora un pequeño documento con algunas de las implementaciones de LDAP y sus características principales.