Apuntes: Servicio de directorio.

UD 1. Servicios de red implicados en el despliegue de una aplicación.

1.6. Servicio de directorio: características y funcionalidad.

Un directorio es una base de datos preparada para navegar, leer y buscar información almacenada en ella. Los directorios permiten encontrar información de forma electrónica, a diferencia de los directorios clásicos.

Las funciones básicas de un directorio:

- ***Buscar información***. Accedida de múltiples formas, ya sea por nombre o por cualquier otro campo.
- ***Gestionar información***. Función primordial. Permite agregar, editar o borrar usuarios.
- ***Control de seguridad***. Controlar el acceso por parte de los usuarios.

1.6. Servicio de directorio: características y funcionalidad.

Las aplicaciones que acceden a los servicios de directorio son muy diversas:

- Aplicaciones web.
- Correo electrónico.
- Acceso a edificios.
- Sistemas operativos.
- Servicio de DNS es un servicio de directorio distribuido.

1.7. Organización de LDAP.

1. ***Centralizada***: Todas las consultas se canalizan a un único servidor, y todas ellas son respondidas por él.
    a. No es necesario sincronizarlo a otros servidores. (ventaja).
    b. En caso de fallo el sistema se queda sin validación. (desventaja).
2. ***Distribuido*:** Permite que la información esté dividida en varios servidores. Los datos pueden estar fraccionados o replicados:
    a. Fraccionada -> Los servidores que intervienen en el servicio de directorio no contienen toda la información.
    b. Replicada -> Toda la información del directorio forma parte de todos los servidores que componen el cluster del servicio de directorio.

1.7.Organización de LDAP.

La organización óptima para contrarrestar los inconvenientes de una y otra opción, sería la de configurar una **mezcla de ambas**, es decir, una parte de la información estaría replicada y la otra fraccionada.

LDAP (Protocolo ligero de acceso a directorio) surge como alternativa a DAP. Las funciones más llamativas son las siguientes:

- LDAP usa TCP/IP en lugar de protocolos teóricos del modelo OSI.
- LDAP representa la información mediante cadenas de caracteres en lugar de complicadas estructuras ASN1.
- El modelo funcional de LDAP es más simple y ha eliminado las opciones raras usadas en X.500.

1.7. Organización de LDAP.

La implementación de LDAP se realiza mediante Open LDAP de código abierto y posee las siguientes características:

- Es multiplataforma.
- El código es de licencia libre.
- Basado en el estándar X.500.
- Tiene estructura de árbol denominado DIT.
- Soporta IPv3, LDAPv3 y esquema distribuido.
- Internacionalización mediante el uso de caracteres UTF-8.
- En el mundo Linux tiene magnífica integración con otras aplicaciones.
- Tiene mecanismos de búsqueda avanzados.

1.7. Organización de LDAP.

Terminología importante:

- **Entrada u objeto**: Se trata de la unidad mínima en un directorio LDAP.
- **Atributos:** Estas son las piezas de información asociadas a un objeto. Por ejemplo, la dirección de email.
- **objectClass:** Determina las características del objeto. En particular, el conjunto de atributos que el objeto puede tener.
- **Esquema:** Contiene todas las definiciones de sintaxis de atributos y las definiciones de objectClass.
- **LDIF:** Siglas de LDAP Data Interchange Format (Formato de intercambio de datos LDAP).
- **DN:** Distinguished Name (Nombre Distinguido).
- **RDN:** Relative Distinguished Name (Nombre Distinguido Relativo).

1.7. Organización de LDAP.

1. ***Modelo de información***. Nos permite darle forma a la estructura de la información almacenada en LDAP. El dato básico en el directorio es una entrada que corresponde con un objeto del mundo real. Una **entrada** se compone de un conjunto de **atributos**, cada uno de ellos tiene un **tipo** con sus **valores**. El tipo define la información que se va a almacenar y los valores son la información en sí. Todos los atributos tienen un **identificador** llamado **OID** y una sintaxis que permite definir qué valores va a poseer.

dn: dc=ejemplo, dc=com

1.7. Organización de LDAP.

2. ***Modelo de referencia:*** a la hora de nombrar los datos LDAP define cómo se organizan y referencian estos, primero se definen las estructuras de cómo se organizan las entradas y posteriormente se indica cómo referenciar o acceder a las mismas.

1.8. Archivos básicos de configuración y uso.

El formato de intercambio de datos LDAP (LDIF) es una extensión de archivo de texto sin formato usada para almacenar datos del directorio LDAP como un conjunto de registros y solicitudes de actualizaciones de LDAP que incluyen agregar, eliminar, modificar y cambiar nombre.

La sintaxis que posee LDIF es de la siguiente forma:

```
dn: <nombre distinguido>

<nombre_atributo>:<valor>

<nombre_atributo>:<valor>

<nombre_atributo>:<valor>
```

1.8. Archivos básicos de configuración y uso.

Una entrada del directorio en formato de intercambio de datos LDIF consta de dos partes:

1. DN que debe figurar en la primera línea de entrada y que se compone de la cadena dn: seguida del nombre distinguido (DN) de la entrada.
2. La segunda parte son los atributos de la entrada, como se puede observar en el ejemplo anterior.

Lo ideal es colocar primero el atributo *objectclass* para mejorar la comprensión del fichero. En un archivo LDIF puede existir más de una entrada definida. Cada entrada se separa de las demás por una línea en blanco y a su vez, en cada entrada puede haber una cantidad arbitraria de los pares ***nombre_atributo -> valor***.