TEORÍA LDAP

Servicio de directorio: características y funcionalidad

Un directorio en cualquier Sistema Operativo es una base de datos preparada para navegar, leer y buscar información almacenada en ella.

Estos directorios electrónicos no contemplan transacciones complicadas, ni opción de vuelta atrás. La actualización en esos directorios es mediante cambios simples. Los directorios están preparados para dar respuesta a grandes solicitudes de búsqueda: también tienen la capacidad de incrementar la disponibilidad y la fiabilidad cuando se replica la información.

Las funciones básicas de un directorio son las siguientes:

a) Buscar información: es su función principal.
b) Gestionar información: agregar, editar o barrar usuarios por distintos campos. Normalmente se centraliza la información en un directorio. En caso de que exista más de un directorio, habría que sincronizar todos los directorios para que posean la misma información.
c) Control de seguridad: controlar el acceso por parte de los usuarios. El servicio de directorio gestiona los certificados digitales de los usuarios del directorio, cuyas funciones serían:
   - Creación
   - Distribución
   - Destrucción
   - Ubicación

Las aplicaciones que acceden a los servicios de directorio son muy diversas. El servicio de DNS es un servicio de directorio distribuido.

Organización de LDAP

La organización de este tipo de directorios puede estar centralizada o distribuida.

1. Centralizada: todas las consultas se canalizan a un único servidor, y todas ellas son respondidas por él.
   * Ventajas: no es necesario sincronizarlo a los demás servidores.
   * Inconvenientes: en caso de fallo el sistema se queda sin validación. Como mínimo sería necesario un backup (copia de seguridad) del servicio de directorio.
2. Distribuida: la información está dividida en varios servidores. Los datos pueden estar fraccionados o replicados.
   - Fraccionados: los servidores no contienen toda la información, sino un subconjunto de ella.
   - Replicada: toda la información del directorio forma parte de todos los servidores que forman el servicio de directorio.
   La opción más viable es una mezcla de las anteriores opciones. Una parte estaría replicada y otra fraccionada.

<u>LDAP (Lightweight Directory Access Protocol)</u>

Se trata de una serie de estándares definidos por IETF qu podemos observar en varios RFC.

Las funciones más llamativas y que llevaron al éxito de LDAP son las siguientes:

- ✔ LDAP usa TCP/IP en lugar de los protocolos teóricos OSI
- ✔ LDAP representa la información mediante cadenas de caracteres.
- ✔ El modelo funcional de LDAP es más simple y ha eliminado las funciones raras.

LDAP define un protocolo para el contenido de los mensajes entre un cliente y el servidor propiamente dicho. Este protocolo permite acceder a las operaciones definidas por el cliente, las respuestas del servidor y los datos transportados en el mensaje.

La implementación de LDAP se realiza mediante Open LDAP. Sus principales características son:

- Es multiplataforma.
- El código es de licencia libre.
- Tiene estructura de árbol (denominado DIT)
- Internacionalización mediante el uso de caracteres UTF-8
- En el mundo Linux tiene una magnífica integración con otras aplicaciones.
- Tiene mecanismos de búsqueda avanzados.

Vamos a analizar LDAP desde diferentes puntos de vista:

1. Modo de información: nos permite darle forma a la estructura de la información almacenada en LDAP. El dato básico es una entrada que corresponde con un objeto del mundo real. Un entrada se compone de un conjunto de atributos, cada uno de ellos tiene un tipo de valores. El tipo define la información que se va a almacenar y los valores son la información en sí. Los atributos tienen un identificador llamado OID y una sintaxis que permite definir qué valores va a poseer.
   Ejemplo: dn:dc=ejemplo,dc=com
   Cada servidor puede definir su estructura o esquema, aunque se tiende a que el esquema sea estándar.
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 misma.

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 (Lightweight Directory Access Protocol) como un conjunto de registros y solicitudes de actualizaciones de LDAP que incluyen agregar, eliminar, modificar y cambiar nombre. LDAP es un protocolo de software que determina la ubicación de los archivos, dispositivos, organización a través de la red TCP/IP

La sintaxis que posee LDIF es la siguiente.

Dn: <nombre distinguido>
<nombre_atributo>: <valor>
<nombre_atributo>: <valor>
<nombre_atributo>: <valor>

Por lo tanto, 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.

No existe ningún orden prestablecido, pero sería ideal colocar primero el atributo object-class 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 pares nombre_atributo → valor.

Es conveniente realizar copias de seguridad para poder regresar al punto de partida en caso de fallo o de introducción de datos erróneos.

Tareas

1. Busca en Internet los siguientes conceptos:
   - IETF
   - RFC
2. ¿Qué es el modelo OSI? ¿Y el protocolo TCP/IP?

Soluciones:

1)
IETF: Organización internacional que desarrolla estándares abiertos para que Internet funcione mejor.
RFC: Request For Comment: Documento numérico que define y describe protocolos

2)
OSI: Es un modelo teórico, que no se usa en la práctica, que describe cómo un ordenador puede enviar mensajes a otro ordenador. La transmisión del mensaje está dividida en capas.
Cada capa recibe información de la capa anterior, procesa esta información, y la envía a la capa siguiente.

TCP/IP: Es un protocolo real, que sí se usa en la práctica, y sirve para enviar un mensaje de un ordenador a otro ordenador.
Cuando un ordenador A envía un mensaje a un ordenador B, el mensaje atraviesa varias capas y es transmitido a través de la red. Al llegar al ordenador B, atraviesa las misma capas en sentido inverso.
Este protocolo es lento pero seguro.