1.1. Descripción de LDAP

Enviado por admin el 30 Noviembre, 2004 - 20:02.

**LDAP** ("Lightweight Directory Acces Protocol", en español Protocolo Ligero de Acceso a Directorios) es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio.

Se usó inicialmente como un Front-end o interfaz final para x.500, pero también puede usarse con servidores de directorio únicos y con otros tipos de servidores de directorio.

**¿Qué es un directorio?**

Un directorio es una base de datos, pero en general contiene información más descriptiva y más basada en atributos.

La información contenida en un directorio normalmente se lee mucho más de lo que se escribe. Como consecuencia los directorios no implementan normalmente los complicados esquemas para transacciones o esquemas de reducción que las bases de datos utilizan para llevar a cabo actualizaciones complejas de grandes volúmenes de datos, Las actualizaciones en un directorio son usualmente cambios sencillos de todo o nada, si es que permiten algo.

**Los directorios están para proporcionar una respuesta rápida a operaciones de búsqueda o consulta.**

Pueden tener capacidad de replicar información de forma amplia, con el fin de aumentar la disponibilidad y fiabilidad, y a la vez reducir tiempo de respuesta. Cuando se duplica la información de un directorio, pueden aceptarse inconsistencias temporales entre la información que hay en las réplicas, siempre que finalmente exista una sincronización.

Hay muchas formas de proporcionar un servicio de directorio. Los diferentes métodos permiten almacenar en el directorio diferentes tipos de información, establecer requisitos diferentes para hacer referencias a la información, consultarla y actualizarla, la forma en que protege al directorio de accesos no autorizados. Algunos servicios de directorios son locales, proporcionando servicios a un contexto restringido. Otros servicios son globales, proporcionando servicio en un contexto mucho más amplio.

**¿Un directorio LDAP es una base de datos?**

El sistema gestor de una base de datos (Database Management System ó DBMS) de Sybase, Oracle, Informix ó Microsoft es usado para procesar peticiones (queries) ó actualizaciones a una base de datos relacional. Estas bases de datos pueden recibir cientos o miles de órdenes de inserción, modificación o borrado por segundo.

Un servidor LDAP es usado para procesar peticiones (queries) a un directorio LDAP. Pero LDAP procesa las órdenes de borrado y actualización de un modo muy lento.  
En otras palabras, LDAP es un tipo de base de datos, pero no es una base de datos relacional. No está diseñada para procesar cientos o miles de cambios por minuto como los sistemas relacionales, sino para realizar lecturas de datos de forma muy eficiente.

**Funcionamiento de LDAP**

El servicio de directorio LDAP se basa en un modelo cliente-servidor.

Uno o más servidores LDAP contienen los datos que conforman el árbol de directorio LDAP o base de datos troncal, el cliente LDAP se conecta con el servidor LDAP y le hace una consulta. El servidor contesta con la respuesta correspondiente, o bien con una indicación de donde puede el cliente hallar más información. No importa con que servidor LDAP se conecte el cliente ya que siempre observará la misma vista del directorio; el nombre que se le presenta a un servidor LDAP hace referencia a la misma entrada a la que haría referencia en otro servidor LDAP.

1.2. Ventajas en el uso de LDAP

Enviado por admin el 19 Noviembre, 2004 - 13:40.

Un directorio LDAP destaca sobre los demás tipos de bases de datos por las siguientes características:

- es muy rápido en la lectura de registros

- permite replicar el servidor de forma muy sencilla y económica

- muchas aplicaciones de todo tipo tienen interfaces de conexión a LDAP y se pueden integrar fácilmente

- Dispone de un modelo de nombres globales que asegura que todas las entradas son únicas

- Usa un sistema jerárquico de almacenamiento de información.

- Permite múltiples directorios independientes

- Funciona sobre TCP/IP y SSL

- La mayoría de aplicaciones disponen de soporte para LDAP

- La mayoría de servidores LDAP son fáciles de instalar, mantener y optimizar.

1.3. Usos prácticos de LDAP

Enviado por admin el 10 Diciembre, 2004 - 19:12.

Dadas las características de LDAP sus usos más comunes son:

- **Directorios de información.** Por ejemplo bases de datos de empleados organizados por departamentos (siguiendo la estructura organizativa de la empresa) ó cualquier tipo de páginas amarillas.

- **Sistemas de autenticación/autorización centralizada.** Grandes sistemas donde se guarda gran cantidad de registros y se requiere un uso constante de los mismos.  
Por ejemplo:

o Active Directory Server de Microsoft, para gestionar todas las cuentas de acceso  
a una red corporativa y mantener centralizada la gestión del acceso a los  
recursos.

o Sistemas de autenticación para páginas Web, algunos de los gestores de  
contenidos más conocidos disponen de sistemas de autenticación a través de LDAP.

o Sistemas de control de entradas a edificios, oficinas….

- **Sistemas de correo electrónico**. Grandes sistemas formados por más de un servidor que accedan a un repositorio de datos común.

- **Sistemas de alojamiento de páginas web y FTP**, con el repositorio de datos de usuario compartido.

- **Grandes sistemas de autenticación basados en RADIUS**, para el control de accesos de los usuarios a una red de conexión o ISP.

- **Servidores de certificados públicos y llaves de seguridad.**

- **Autenticación única ó “single sign-on” para la personalización de aplicaciones.**

- **Perfiles de usuarios centralizados, para permitir itinerancia ó “Roaming”**

- **Libretas de direcciones compartidas.**

1.4. ¿cuando resulta interesante usar LDAP?

Enviado por admin el 19 Noviembre, 2004 - 13:47.

Como hemos visto LDAP es una base de datos optimizada para entornos donde se realizan muchas lecturas de datos y pocas modificaciones o borrados.

Por lo tanto es muy importante saber elegir dónde es conveniente usarlo. No será conveniente como base de datos para sitios que realicen constantes modificaciones de datos (por ejemplo en entornos de e-commerce)

Normalmente el tipo de preguntas que debes hacerte para saber si LDAP es conveniente para tus aplicaciones son:

• ¿Me gustaría que los datos fueran disponibles desde distintos tipos de plataforma?

• ¿necesito acceso a estos datos desde un número muy elevado de servidores y/o aplicaciones?

• Los datos que almaceno ¿son actualizados muchas veces?, o por el contrario ¿son sólo actualizados unas pocas veces?

• ¿tiene sentido almacenar este tipo de datos en una base de datos relacional? Si no tiene sentido, ¿puedo almacenar todos los datos necesarios en un solo registro?

Pongamos algunos ejemplos:

**Sistema de correo electrónico**

Cada usuario se identifica por su dirección de correo electrónico, los atributos que se guardan de cada usuario son su contraseña, su límite de almacenamiento (quota), la ruta del disco duro donde se almacenan los mensajes (buzón) y posiblemente atributos adicionales para activar sistemas anti-spam o anti-virus.

Como se puede ver este sistema LDAP recibirá cientos de consultas cada día (una por cada email recibido y una cada vez que el usuario se conecta mediante POP3 o webmail). No obstante el número de modificaciones diarias es muy bajo, ya que solo se puede cambiar la contraseña o dar de baja al usuario, operaciones ambas que no se realizan de forma frecuente.

**Sistema de autenticación a una red**

Cada usuario se identifica por un nombre de usuario y los atributos asignados son la contraseña, los permisos de acceso, los grupos de trabajo a los que pertenece, la fecha de caducidad de la contraseña…

Este sistema recibirá una consulta cada vez que el usuario acceda a la red y una más cada vez que acceda a los recursos del grupo de trabajo (directorios compartidos, impresoras…) para comprobar los permisos del usuario.

Frente a estos cientos de consultas solo unas pocas veces se cambia la contraseña de un usuario o se le incluye en un nuevo grupo de trabajo.

1.5. Diferencias con una base de datos relacional

Enviado por admin el 19 Noviembre, 2004 - 13:49.

Las **características de una base de datos relacional** (RDBMS o Relation Database Management Systems) son:

- Realizan **operaciones de escritura intensivas**: las bases de datos relacionales estás preparadas para hacer un uso constante de operaciones orientadas a transacciones, que implican la modificación o borrado constante de los datos almacenados.

- **Esquema específico** para cada aplicación: las bases de datos relacionales son creadas para cada aplicación específica, siendo complicado adaptar los esquemas a nuevas aplicaciones.

- **Modelo de datos complejo**: permiten manejar complejos modelos de datos que requieren muchas tablas, foreign keys, operaciones de unión (join) complejas…

- **Integridad de datos**: todos sus componentes están desarrollados para mantener la consistencia de la información en todo momento. Esto incluye operaciones de rollback, integridad referencial y operaciones orientadas a transacciones.

- Además las **transacciones se efectúan siempre aisladas** de otras transacciones. De tal forma que si dos transacciones están ejecutándose de forma concurrente los efectos de la transacción A son invisibles a la transacción B y viceversa, hasta que ambas transacciones han sido completadas.

- Disponen de **operaciones de roll-back** (vuelta atrás). Hasta el final de la transacción ninguna de las acciones llevadas a cabo pasa a un estado final. Si el sistema falla antes de finalizar una transacción todos los cambios realizados son eliminados (roll-back)

Las **características de un servidor LDAP** son:

- **Operaciones de lectura muy rápidas**. Debido a la naturaleza de los datos almacenados en los directorios las lecturas son más comunes que las escrituras.

- **Datos relativamente estáticos**. Los datos almacenados en los directorios no suelen actualizarse con mucha frecuencia.

- **Entorno distribuido**, fácil replicación

- **Estructura jerárquica**. Los directorios almacenan la información de forma jerárquica de forma nativa.

- **Orientadas a objetos**. El directorio representa a elementos y a objetos. Los objetos son creados como entradas, que representan a una colección de atributos.

- **Esquema Standard**. Los directorios utilizan un sistema standard que pueden usar fácilmente diversas aplicaciones.

- **Atributos multi-valor**. Los atributos pueden almacenar un valor único o varios.

- **Replicación multi-master**. Muchos de los servidores LDAP permiten que se realicen escrituras o actualizaciones en múltiples servidores.

1.6. Historia de LDAP

Enviado por admin el 30 Noviembre, 2004 - 19:56.

**LDAP** aparece con el estándar de los directorios de servicios. La versión original fue desarrollada por la Universidad de Michigan. La primera versión no se usó y fue en 1995 cuando se publicaron los RFC (Request For Comments) de la versión LDAPv2. Los RFC para la versión LDAPv3 fueron publicados en 1997. La versión 3 incluía características como las listas de acceso (control access lists) y replicación de directorios.

**LDAP RFCs**

Los RFCs asociados con LDAP son:

RFC1777 - Lightweight Directory Access Protocol. (Obsoletes RFC1487)  
RFC1778 - The String Representation of Standard Attribute Syntaxes  
RFC1779 - A String Representation of Distinguished Names (Obsoletes RFC1485)  
RFC1823 - The LDAP Application Program Interface  
RFC1960 - A String Representation of LDAP Search Filters (Obsoletes RFC1558)  
RFC 2251 - Lightweight Directory Access Protocol (v3)  
RFC 2252 - LDAPv3 Attribute Syntax Definitions  
RFC 2253 - UTF-8 String Representation of Distinguished Names  
RFC 2254 - The String Representation of LDAP Search Filters  
RFC 2255 - The LDAP URL Format  
RFC 2256 - A Summary of the X.500(96) User Schema for use with LDAPv3  
RFC2829 Authentication Methods for LDAP.  
RFC2830 - Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security.

RFCs relacionados

RFC1274 - The COSINE and Internet X.500 Schema  
RFC1279 - X.500 and Domains  
RFC1308 - Executive Introduction to Directory Services Using the X.500 Protocol  
RFC1309 - Technical Overview of Directory Services Using the X.500 Protocol  
RFC1617 - Naming and Structuring Guidelines for X.500 Directory Pilots (Obsoletes RFC1384)  
RFC1684 - Introduction to White Pages services based on X.500  
RFC2079 - Definition of an X.500 Attribute Type and an Object Class to Hold Uniform

1.7. Servidores LDAP disponibles en el mercado

Enviado por admin el 10 Diciembre, 2004 - 19:21.

Los más usados son:

- OpenLDAP – <http://www.openldap.org>

- Sun SunONE 5.2 – <http://www.sun.com/software/products/directory_srvr/home_directory.html>

- Siemens DirX Server 6.0 – <http://www.siemens.com/directory>

- Syntegra Intrastore Server 2000 - <http://www.syntegra.com/us/directory_messaging/>

- Computer Associates eTrust Directory 3.6 - <http://www3.ca.com/Solutions/Product.asp?ID=160>

- Novell NDS Corporate Edition 8.7.1 - <http://www.novell.com/coolsolutions/nds/>

-Microsoft ADS - Windows 2000 server edition - [http://www.microsoft.com/windows2000/technologies/directory/ad/default.a...](http://www.microsoft.com/windows2000/technologies/directory/ad/default.asp)

Comparativa

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Requirements** | **OpenLDAP** | **SunONE** | **DirX Server** | **Intrastore** | **eTrust** | **NDS** | **ADS** |
| K4 (UMich) bind | yes | no | ? | ? | ? | no | no |
| LDAPv2 protocol | yes | yes | ? | ? | ? | ? | maybe |
| LDAPv3 protocol | yes | yes | yes | yes | yes | ? | yes |
| K5 bind | yes | no | ? | ? | ? | no | yes |
| SASL GSSAPI (Krb5)  Auth | yes | yes | ? | ? | ? | ? | yes |
| Scalable >  200K entries | yes | yes | yes | ? | yes | ? | ? |
| Solaris 8 | yes | yes | yes | yes | yes | yes | no |
| Search limit tied  to binddn | yes | ? | ? | ? | ? | ? | ? |
| Multi-Master | yes | yes | ? | ? | ? | ? | ? |
| Supports "<text>  \*(space)<text>"  search | no | ? | ? | ? | ? | ? | ? |
| Support avail. | yes\* | yes | yes | yes | yes | yes | yes |

\* Se realiza a través de listas de correo, se puede contratar soporte técnico con empresas como Symas Corp., Mind NV, or Inter7.