

Integración de sistemas y servicios distribuidos con LDAP

Javier Sánchez Monedero
jsanchezm en uco.es

Grupo de investigación Aprendizaje y Redes Neuronales Artificiales AYRNA
Universidad de Córdoba

12 de abril de 2012

Sistemas Operativos Distribuidos
4º Ingeniería Informática



<http://creativecommons.org/licenses/by-sa/3.0/deed.es>

Índice



- 1 **Introducción**
- 2 **Soluciones al problema**
- 3 **Directorios LDAP**
 - El protocolo LDAP
 - Organización de la información
 - Representación de la información
 - Implementaciones LDAP
- 4 **Diseño del directorio**
- 5 **Optimización de OpenLDAP**
- 6 **Demostración práctica**
- 7 **Configuración del servidor y clientes
OpenLDAP, PAM-LDAP y
NSS-LDAP**
- 8 **Referencias**

Índice



- 1 **Introducción**
- 2 Soluciones al problema
- 3 Directorios LDAP
 - El protocolo LDAP
 - Organización de la información
 - Representación de la información
 - Implementaciones LDAP
- 4 Diseño del directorio
- 5 Optimización de OpenLDAP
- 6 Demostración práctica
- 7 Configuración del servidor y clientes OpenLDAP, PAM-LDAP y NSS-LDAP
- 8 Referencias

Servicios para una comunidad

Servicios para usuarios corporativos

- Sistema de ficheros
- Correo electrónico
- Acceso a sistemas operativos diversos
- Autenticación en redes: VPN e inalámbrica
- Servicios web:
 - Implementación de restricción de accesos
 - Integración de portales diversos
 - Páginas blancas
- Otros: acceso al parking

corporación = universidad, empresa, organismo, partido político. . .

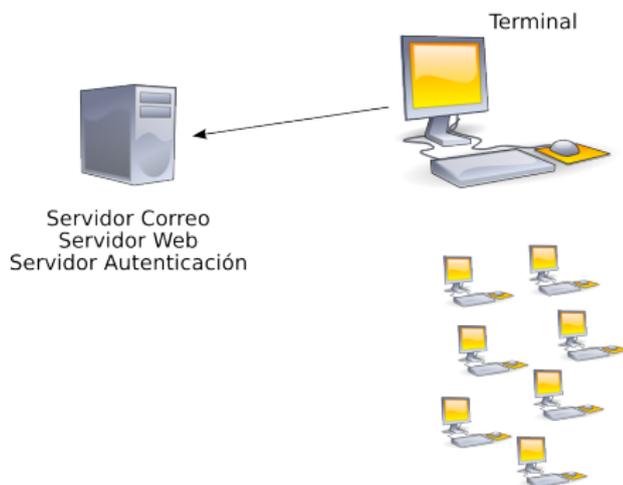
Enfoques para ofrecer servicios

Gran servidor central (mainframes) que gestiona todo: usuarios, correo, web... y terminales

Problemas

Todos los de sistemas centralizados:

- No escala en número de usuarios
- No escala a otras redes
- ...



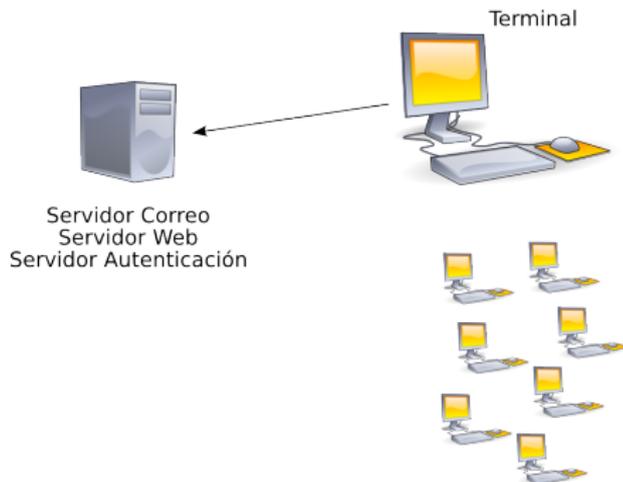
Enfoques para ofrecer servicios

Gran servidor central (mainframes) que gestiona todo: usuarios, correo, web... y terminales

Problemas

Todos los de sistemas centralizados:

- No escala en número de usuarios
- No escala a otras redes
- ...



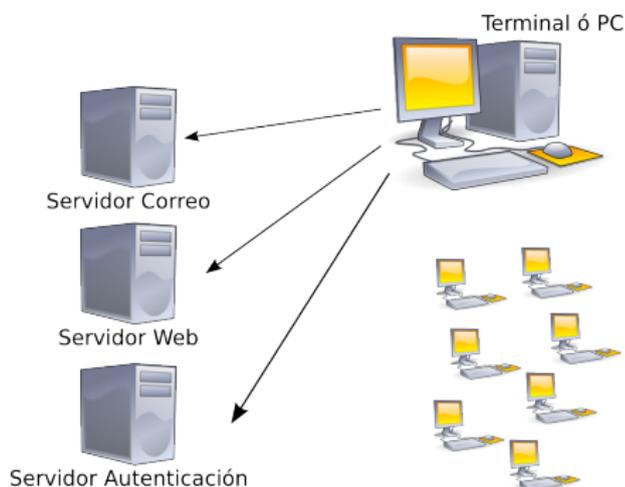
Enfoques para ofrecer servicios

Descentralización de servicios en pequeños servidores

Factores para la descentralización

El uso de grandes servidores centrales es cada vez menor:

- Coste
- Fiabilidad y capacidad de replicación de servicios
- Aumento de la variedad de servicios



Problema...

Los servicios están dispersos mientras se necesita información común de coordinación \Rightarrow integración

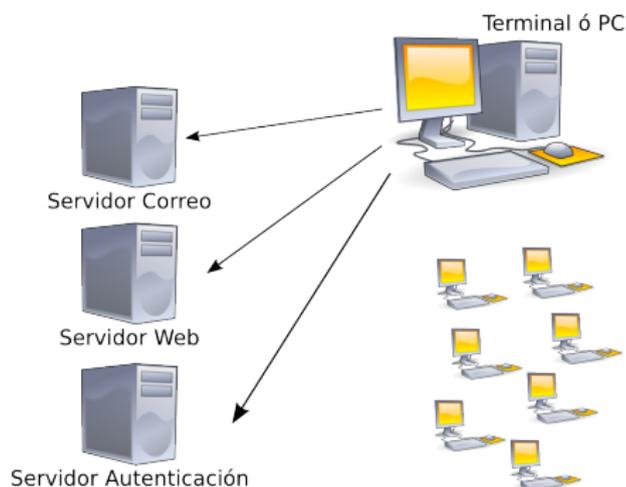
Enfoques para ofrecer servicios

Descentralización de servicios en pequeños servidores

Factores para la descentralización

El uso de grandes servidores centrales es cada vez menor:

- Coste
- Fiabilidad y capacidad de replicación de servicios
- Aumento de la variedad de servicios



Problema...

Los servicios están dispersos mientras se necesita información común de coordinación \Rightarrow integración

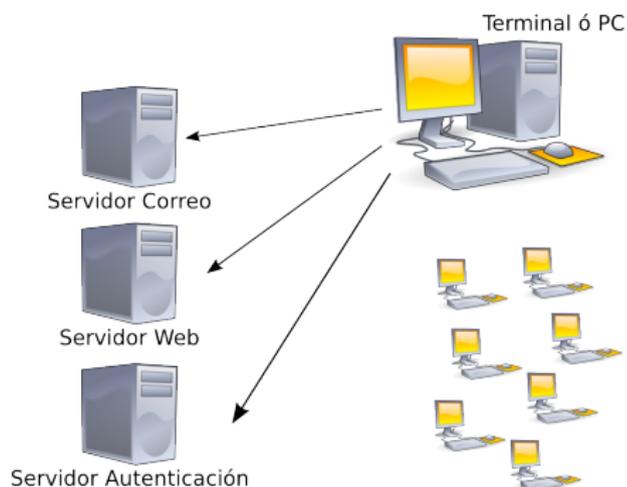
Enfoques para ofrecer servicios

Descentralización de servicios en pequeños servidores

Factores para la descentralización

El uso de grandes servidores centrales es cada vez menor:

- Coste
- Fiabilidad y capacidad de replicación de servicios
- Aumento de la variedad de servicios

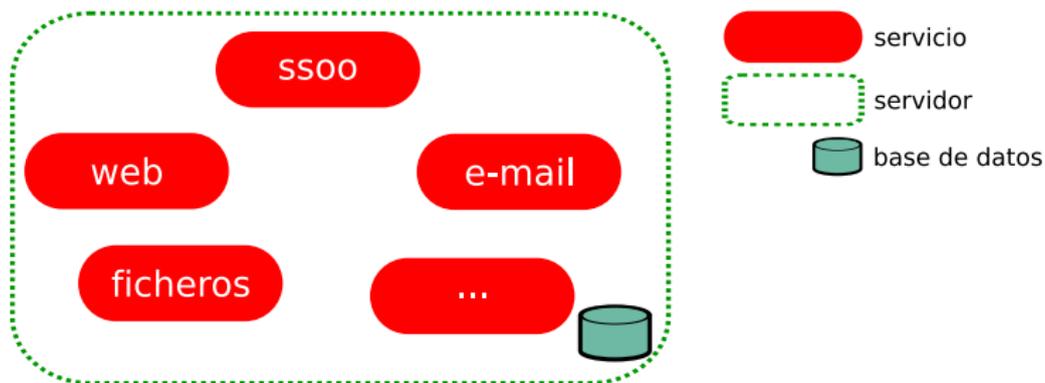


Problema...

Los servicios están **dispersos** mientras se necesita información común de **coordinación** ⇒ integración

Motivación para integración de servicios

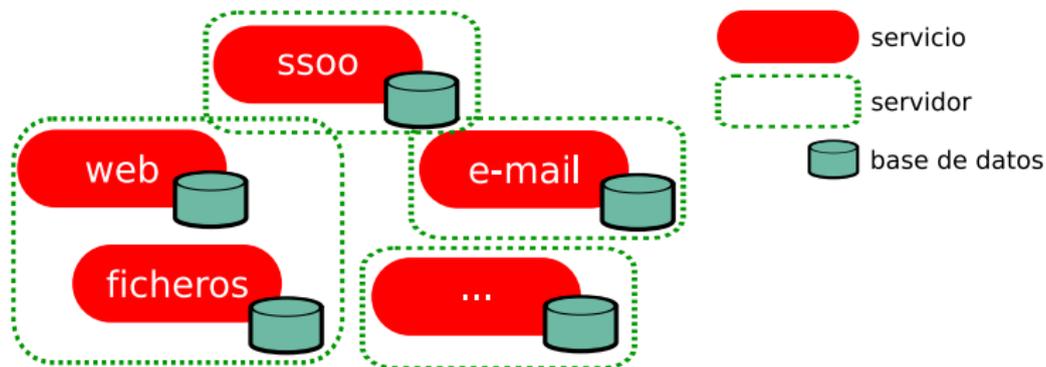
Solución de un gran servidor



No había nada que integrar al estar todo en una máquina... pero no escala

Motivación para integración de servicios

Solución de **varios servidores**



Para escalar los servicios se distribuyen en máquinas y surge el problema de manejar la autenticación, configuración, etc. **¿cómo integrarlos?**

Motivación para integración de servicios

Entorno no integrado

- Descentralización de la autenticación de usuarios
- La autenticación se hace en el servidor de cada servicio
- La configuración de los servicios se almacena en cada servidor

Motivación para integración de servicios

Problemas derivados de la descentralización de información

- Usuarios y contraseñas distintos para cada servicio
- Administración de cuentas de usuario tediosa. Cada administrador aplica soluciones “propias”, a menudo poco elegantes:
 - Ej.: copiar algunos de los ficheros de configuración y usuarios a las estaciones de trabajo ⇒ problemas de seguridad
- No sincronización de ficheros de configuración de servicios
 - Ej.: se programan guiones que sincronizan ficheros de configuración cada día, semana, etc.
- Dificultad para implementar balanceo de carga en servicios que requieren autenticación:
 - Ej.: el correo electrónico

Motivación para integración de servicios

Problemas derivados de la descentralización de información

- Usuarios y contraseñas distintos para cada servicio
- Administración de cuentas de usuario tediosa. Cada administrador aplica soluciones “propias”, a menudo poco elegantes:
 - Ej.: copiar algunos de los ficheros de configuración y usuarios a las estaciones de trabajo ⇒ problemas de seguridad
- No sincronización de ficheros de configuración de servicios
 - Ej.: se programan guiones que sincronizan ficheros de configuración cada día, semana, etc.
- Dificultad para implementar balanceo de carga en servicios que requieren autenticación:
 - Ej.: el correo electrónico

Motivación para integración de servicios

Problemas derivados de la descentralización de información

- Usuarios y contraseñas distintos para cada servicio
- Administración de cuentas de usuario tediosa. Cada administrador aplica soluciones “propias”, a menudo poco elegantes:
 - Ej.: copiar algunos de los ficheros de configuración y usuarios a las estaciones de trabajo ⇒ problemas de seguridad
- No sincronización de ficheros de configuración de servicios
 - Ej.: se programan guiones que sincronizan ficheros de configuración cada día, semana, etc.
- Dificultad para implementar balanceo de carga en servicios que requieren autenticación:
 - Ej.: el correo electrónico

Motivación para integración de servicios

Problemas derivados de la descentralización de información

- Usuarios y contraseñas distintos para cada servicio
- Administración de cuentas de usuario tediosa. Cada administrador aplica soluciones “propias”, a menudo poco elegantes:
 - Ej.: copiar algunos de los ficheros de configuración y usuarios a las estaciones de trabajo ⇒ problemas de seguridad
- No sincronización de ficheros de configuración de servicios
 - Ej.: se programan guiones que sincronizan ficheros de configuración cada día, semana, etc.
- Dificultad para implementar balanceo de carga en servicios que requieren autenticación:
 - Ej.: el correo electrónico

Índice



- 1 Introducción
- 2 Soluciones al problema**
- 3 Directorios LDAP
 - El protocolo LDAP
 - Organización de la información
 - Representación de la información
 - Implementaciones LDAP
- 4 Diseño del directorio
- 5 Optimización de OpenLDAP
- 6 Demostración práctica
- 7 Configuración del servidor y clientes
OpenLDAP, PAM-LDAP y
NSS-LDAP
- 8 Referencias

Antecedentes en integración de servicios

Network Information Service (NIS)

Los sistemas basados en NIS/NIS+ solucionan en parte el problema de la descentralización de la autenticación

- Sólo para una subred
- No cifra los datos
- No permite establecer jerarquías de usuarios complejas
- Un cambio implica reconstruir todas las bases de datos... y distribuirlas
- Un usuario del servicio = usuario sistema operativo

NIS+ supera algunas limitaciones de NIS pero es complejo de manejar

Antecedentes en integración de servicios

Bases de datos relacionales

- MySQL, PostGres, Oracle. . .
- No optimizadas para lecturas masivas
- Soluciones propias del administrador

Los servicios de directorio y LDAP

Servicios de directorio

Son bases de datos especializadas en atender lecturas masivas sobre tipos de datos simples

El protocolo LDAP

- Es un protocolo de acceso a directorios
- LDAP, *Lightweight Directory Access Protocol* o protocolo ligero de acceso a directorios, será el protocolo que utilicen todos los clientes que necesiten información de autenticación.

Los servidores de directorios implementan LDAP y los clientes de directorios implementan el protocolo de cliente LDAP.

Los servidores de directorios implementan LDAP y los clientes de directorios implementan el protocolo de cliente LDAP.

Los servicios de directorio y LDAP

Servicios de directorio

Son bases de datos especializadas en atender lecturas masivas sobre tipos de datos simples

El protocolo LDAP

- Es un protocolo de acceso a directorios
- LDAP, *Lightweight Directory Access Protocol* o protocolo ligero de acceso a directorios, será el protocolo que utilicen todos los clientes que necesiten información de autenticación.
- Cualquier cliente puede utilizar bibliotecas LDAP para autenticar usuarios o buscar otro tipo de información
- Funciona sobre TCP/IP ⇒ supera el entorno local
- Soporta TLS/SSL

Los servicios de directorio y LDAP

Servicios de directorio

Son bases de datos especializadas en atender lecturas masivas sobre tipos de datos simples

El protocolo LDAP

- Es un protocolo de acceso a directorios
- LDAP, *Lightweight Directory Access Protocol* o protocolo ligero de acceso a directorios, será el protocolo que utilicen todos los clientes que necesiten información de autenticación.
- Cualquier cliente puede utilizar bibliotecas LDAP para autenticar usuarios o buscar otro tipo de información
- Funciona sobre TCP/IP ⇒ supera el entorno local
- Soporta TLS/SSL

Los servicios de directorio y LDAP

Servicios de directorio

Son bases de datos especializadas en atender lecturas masivas sobre tipos de datos simples

El protocolo LDAP

- Es un protocolo de acceso a directorios
- LDAP, *Lightweight Directory Access Protocol* o protocolo ligero de acceso a directorios, será el protocolo que utilicen todos los clientes que necesiten información de autenticación.
- Cualquier cliente puede utilizar bibliotecas LDAP para autenticar usuarios o buscar otro tipo de información
- Funciona sobre TCP/IP ⇒ supera el entorno local
- Soporta TLS/SSL

Los servicios de directorio y LDAP

Servicios de directorio

Son bases de datos especializadas en atender lecturas masivas sobre tipos de datos simples

El protocolo LDAP

- Es un protocolo de acceso a directorios
- LDAP, *Lightweight Directory Access Protocol* o protocolo ligero de acceso a directorios, será el protocolo que utilicen todos los clientes que necesiten información de autenticación.
- Cualquier cliente puede utilizar bibliotecas LDAP para autenticar usuarios o buscar otro tipo de información
- Funciona sobre TCP/IP ⇒ supera el entorno local
- Soporta TLS/SSL

Los servicios de directorio y LDAP

Servicios de directorio

Son bases de datos especializadas en atender lecturas masivas sobre tipos de datos simples

El protocolo LDAP

- Es un protocolo de acceso a directorios
- LDAP, *Lightweight Directory Access Protocol* o protocolo ligero de acceso a directorios, será el protocolo que utilicen todos los clientes que necesiten información de autenticación.
- Cualquier cliente puede utilizar bibliotecas LDAP para autenticar usuarios o buscar otro tipo de información
- Funciona sobre TCP/IP ⇒ supera el entorno local
- Soporta TLS/SSL

Los servicios de directorio y LDAP

¿Cómo funciona la autenticación si LDAP sólo es un protocolo?

PAM (Pluggable Authentication Modules)

- Proporciona una interfaz de programación de alto nivel para programas que necesiten autenticar usuarios.
- `pam_ldap`: traduce las peticiones de autenticación a LDAP y permite el cambio de contraseñas.

NSS (Name Service Switch)

- Permite indicar los orígenes de datos necesarios para el sistema operativo (ficheros tradicionales UNIX o bases de datos)
- `nss_ldap`: resuelve peticiones de llamadas como `getpwnam()`

Los servicios de directorio y LDAP

¿Cómo funciona la autenticación si LDAP sólo es un protocolo?

PAM (Pluggable Authentication Modules)

- Proporciona una interfaz de programación de alto nivel para programas que necesiten autenticar usuarios.
- `pam_ldap`: traduce las peticiones de autenticación a LDAP y permite el cambio de contraseñas.

NSS (Name Service Switch)

- Permite indicar los orígenes de datos necesarios para el sistema operativo (ficheros tradicionales UNIX o bases de datos)
- `nss_ldap`: resuelve peticiones de llamadas como `getpwnam()`

Los servicios de directorio y LDAP

¿Cómo funciona la autenticación si LDAP sólo es un protocolo?

Módulo `mod_auth_ldap` Apache

- Implementa autenticación HTTP utilizando un directorio LDAP como base de datos
- Compatible con OpenLDAP, Novell LDAP e iPlanet (Netscape/SUN)
- Módulo adicional `mod_ldap` para optimizaciones

Soporte en casi todos los lenguajes:

- C, Java, Perl, Python...
- Por ejemplo, desde PHP:
 - `ldap_connect()`
 - `ldap_bind()`

Los servicios de directorio y LDAP

¿Cómo funciona la autenticación si LDAP sólo es un protocolo?

Módulo `mod_auth_ldap` Apache

- Implementa autenticación HTTP utilizando un directorio LDAP como base de datos
- Compatible con OpenLDAP, Novell LDAP e iPlanet (Netscape/SUN)
- Módulo adicional `mod_ldap` para optimizaciones

Soporte en casi todos los lenguajes:

- C, Java, Perl, Python...
- Por ejemplo, desde PHP:
 - `ldap_connect()`
 - `ldap_bind()`

Los servicios de directorio y LDAP

RESULTADO

La combinación LDAP+NSS+PAM permite ¡separar usuarios del sistema operativo de los usuarios de servicios que se ejecutan sobre él! ⇒ incremento de seguridad, flexibilidad, etc.

Índice



- 1 Introducción
- 2 Soluciones al problema
- 3 Directorios LDAP**
 - El protocolo LDAP
 - Organización de la información
 - Representación de la información
 - Implementaciones LDAP
- 4 Diseño del directorio
- 5 Optimización de OpenLDAP
- 6 Demostración práctica
- 7 Configuración del servidor y clientes
OpenLDAP, PAM-LDAP y
NSS-LDAP
- 8 Referencias

Operaciones del protocolo LDAP

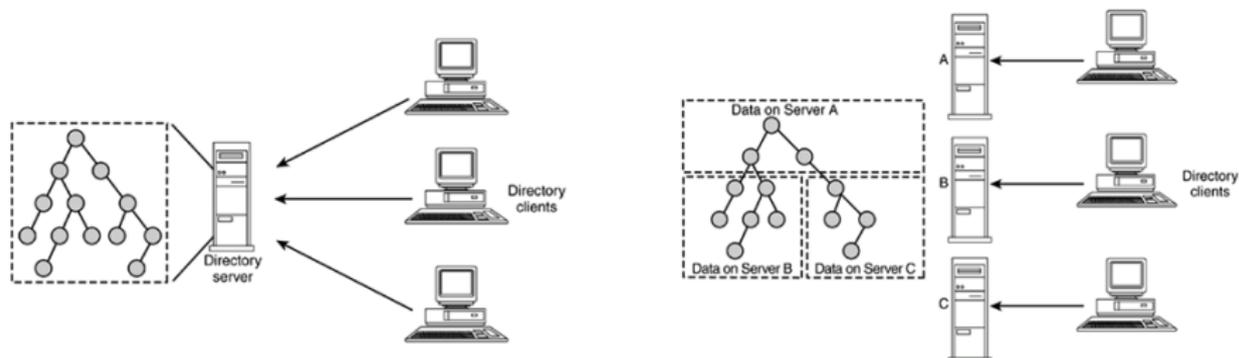
LDAP es un protocolo cliente-servidor que permite:

- Bind/Unbind: autenticación
- Search: búsqueda y filtrado de resultados
- Update Data: modificación de entradas en la base de datos
- StartTLS: establece un canal TLS (Transport Layer Security) seguro
- Abandon: cancelar una operación en marcha

Organización de la información

Estructura de datos

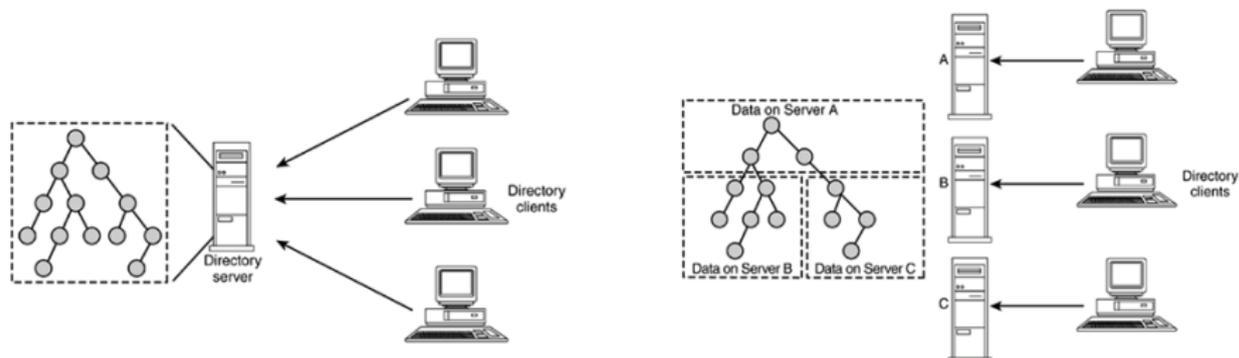
- Los directorios LDAP organizan la información en árboles jerárquicamente
- El árbol puede estar distribuido entre diferentes servidores



Organización de la información

Estructura de datos

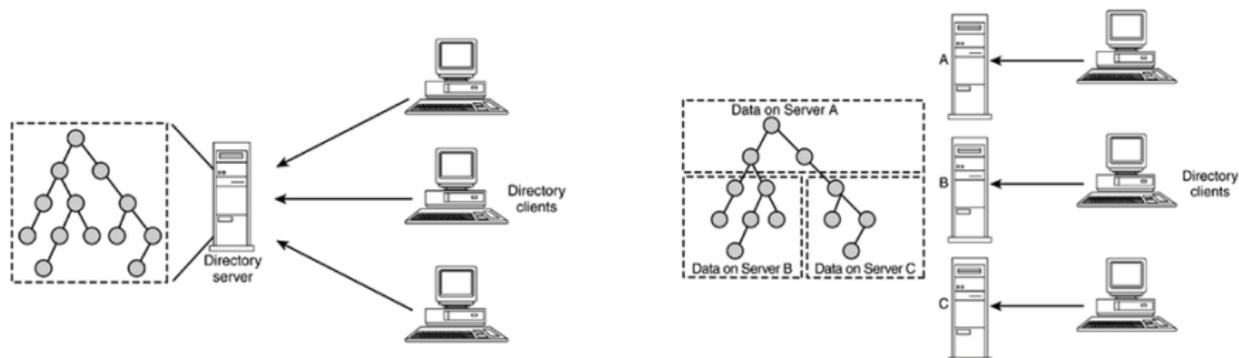
- Los directorios LDAP organizan la información en árboles jerárquicamente
- El árbol puede estar distribuido entre diferentes servidores



Organización de la información

Estructura de datos

- Los directorios LDAP organizan la información en árboles jerárquicamente
- El árbol puede estar distribuido entre diferentes servidores



Organización de la información

Directory Information Tree

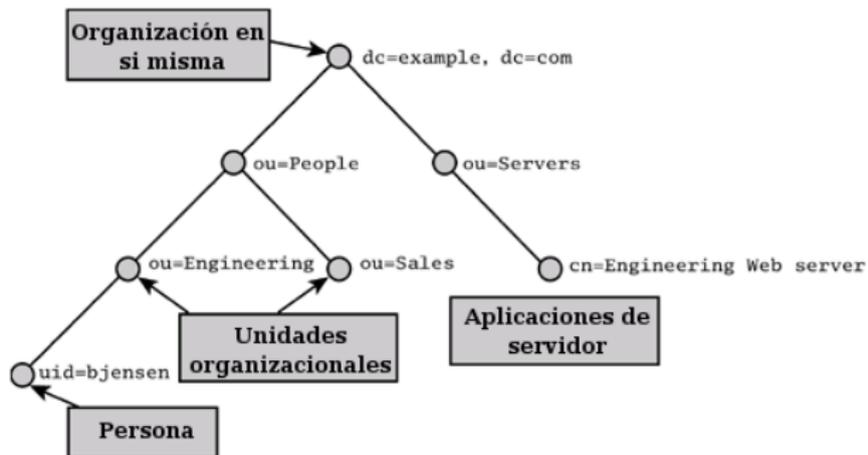
- Es el árbol de información del directorio
- Todas las entradas se identifican con un DN único
- DN = nombre distinguido (Distinguished Name)
- DN base = raíz del árbol
- RDN = nombre relativo distinguido (Relative Distinguished Name)
 - RDN es una entrada hoja o rama
- $DN = RDN + rama(s) + base$

Organización de la información

Directory Information Tree

- Es el árbol de información del directorio
- Todas las entradas se identifican con un DN único
- DN = nombre distinguido (Distinguished Name)
- DN base = raíz del árbol
- RDN = nombre relativo distinguido (Relative Distinguished Name)
 - RDN es una entrada hoja o rama
- $DN = RDN + rama(s) + base$

Organización de la información



Ejemplos de entradas del directorio LDAP

DN base → `dc=example, dc=com`

DN → `ou=People, dc=example, dc=com`

DN → `uid=bjensen, ou=Engineering, ou=People, dc=example, dc=com`

RDN → `uid=bjensen`

Entradas del directorio

Entrada de directorio LDAP

- **Unidad básica de información**
- Se compone de un conjunto de atributos, cada uno de ellos tiene un tipo y uno o varios valores
- Los esquemas (*schemas*) definen cómo son los objetos del directorio y dónde pueden ubicarse
- Existen esquemas predefinidos según la labor del directorio.
- RFC 2307: An Approach for Using LDAP as a Network Information Service

Entradas del directorio

Entrada de directorio LDAP

- Unidad básica de información
- Se compone de un conjunto de atributos, cada uno de ellos tiene un tipo y uno o varios valores
- Los esquemas (*schemas*) definen cómo son los objetos del directorio y dónde pueden ubicarse
- Existen esquemas predefinidos según la labor del directorio.
- RFC 2307: An Approach for Using LDAP as a Network Information Service

Entradas del directorio

Entrada de directorio LDAP

- Unidad básica de información
- Se compone de un conjunto de atributos, cada uno de ellos tiene un tipo y uno o varios valores
- Los esquemas (*schemas*) definen cómo son los objetos del directorio y dónde pueden ubicarse
- Existen esquemas predefinidos según la labor del directorio.
- RFC 2307: An Approach for Using LDAP as a Network Information Service

Entradas del directorio

Entrada de directorio LDAP

- Unidad básica de información
- Se compone de un conjunto de atributos, cada uno de ellos tiene un tipo y uno o varios valores
- Los esquemas (*schemas*) definen cómo son los objetos del directorio y dónde pueden ubicarse
- Existen esquemas predefinidos según la labor del directorio.
- RFC 2307: An Approach for Using LDAP as a Network Information Service

Entradas del directorio

Entrada de directorio LDAP

- Unidad básica de información
- Se compone de un conjunto de atributos, cada uno de ellos tiene un tipo y uno o varios valores
- Los esquemas (*schemas*) definen cómo son los objetos del directorio y dónde pueden ubicarse
- Existen esquemas predefinidos según la labor del directorio.
- RFC 2307: An Approach for Using LDAP as a Network Information Service

El formato LDIF

Formato de intercambio de datos LDAP

- LDAP es un protocolo binario
- *RFC 2849 The LDAP Data Interchange Format (LDIF)*
- Representación en texto plano de:
 - Contenido total o parcial del directorio
 - Actualizaciones (masivas) del directorio

Ejemplos de uso de LDIF

- Migración a LDAP (con *migration tools*)
- Copia de seguridad del directorio
- Didáctico

Entradas del directorio

Ejemplo de entrada LDAP para cuentas POSIX

```
dn: uid=usuarioldap,ou=People,dc=foo,dc=net
uid: usuarioldap
cn: Pepito Grillo
objectClass: account
objectClass: posixAccount
objectClass: top
userPassword:: {crypt}eONSWVBuFUQwdHJWRmhXVHUybGs=
loginShell: /bin/bash
uidNumber: 1006
homeDirectory: /home/usuarioldap
gecos: Pepito Grillo
structuralObjectClass: account
gidNumber: 2000
```

Equivalente en /etc/passwd

```
usuarioldap:eONSWVBuFUQwdHJWRmhXVHUybGs=:1006:2000:...
...Pepito Grillo:/home/usuarioldap:/bin/sh
```

Servidores y clientes LDAP

Libres o de código abierto

- **Servidores:** OpenLDAP, Apache Directory Server, Fedora Directory Server. . .
- **Navegadores y administración:** phpLDAPadmin, Ldap Account Manager, JXplorer. . .
- **Programas que integran LDAP:**
 - **Escritorio:** Mozilla Thunderbird, Evolution, KAddressBook. . .
 - **Servicios:** Apache, Proftpd, Subversion. . .
 - **Portales web:** Joomla, Drupal, Wordpress, Mediawiki. . .

Privativos

- **Servidores:** Microsoft Active Directory, Novell eDirectory. . .
- **Navegadores y administración:** Softerra LDAP Administrator

Servidores y clientes LDAP

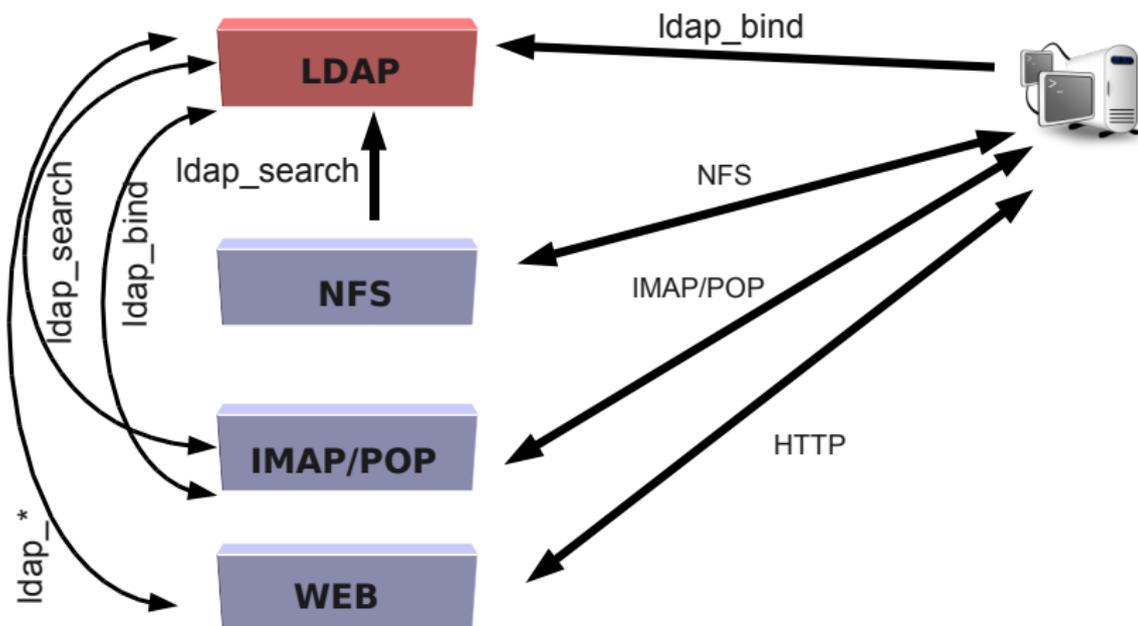
Libres o de código abierto

- **Servidores:** OpenLDAP, Apache Directory Server, Fedora Directory Server. . .
- **Navegadores y administración:** phpLDAPadmin, Ldap Account Manager, JXplorer. . .
- **Programas que integran LDAP:**
 - **Escritorio:** Mozilla Thunderbird, Evolution, KAddressBook. . .
 - **Servicios:** Apache, Proftpd, Subversion. . .
 - **Portales web:** Joomla, Drupal, Wordpress, Mediawiki. . .

Privativos

- **Servidores:** Microsoft Active Directory, Novell eDirectory. . .
- **Navegadores y administración:** Softerra LDAP Administrator

Resumen de funcionamiento de la autenticación de servicios



Índice



- 1 Introducción
- 2 Soluciones al problema
- 3 Directorios LDAP
 - El protocolo LDAP
 - Organización de la información
 - Representación de la información
 - Implementaciones LDAP
- 4 Diseño del directorio**
- 5 Optimización de OpenLDAP
- 6 Demostración práctica
- 7 Configuración del servidor y clientes OpenLDAP, PAM-LDAP y NSS-LDAP
- 8 Referencias

¿Cómo se diseña un directorio?

Diseño del directorio

- El directorio debe diseñarse cuidadosamente
- Se debe analizar el entorno actual y futuro
- El rendimiento, integridad y seguridad de datos suelen ser prioritarios

Metodología

El libro "Understanding and Deploying LDAP Directory Services" de Timothy A. Et. al. propone 6 pasos:

- 1 Aplicaciones
- 2 Datos
- 3 Esquemas LDAP
- 4 Espacio de nombres
- 5 Topología de red y replicación
- 6 Seguridad

¿Cómo se diseña un directorio?

Diseño del directorio

- El directorio debe diseñarse cuidadosamente
- Se debe analizar el entorno actual y futuro
- El rendimiento, integridad y seguridad de datos suelen ser prioritarios

Metodología

El libro "Understanding and Deploying LDAP Directory Services" de Timothy A. Et. al. propone 6 pasos:

- 1 Aplicaciones
- 2 Datos
- 3 Esquemas LDAP
- 4 Espacio de nombres
- 5 Topología de red y replicación
- 6 Seguridad

Aplicaciones y datos

1. ¿Qué aplicaciones accederán al directorio?

Ejemplos de aplicaciones son:

- Bibliotecas de sistemas operativos (ficheros tradicionales UNIX en etc o mapas NIS)
- Servidores de Telnet, SSH, FTP, Web, Correo electrónico, NFS...
- Aplicaciones de escritorio o Web

2. ¿Qué datos se almacenarán?

Cada aplicación en red necesita una serie de datos:

- Ficheros de /etc: passwd, aliases, group...
- Aplicaciones Web: rama de usuarios y grupos
- Servicios: el correo electrónico necesita usuarios y alias

Aplicaciones y datos

1. ¿Qué aplicaciones accederán al directorio?

Ejemplos de aplicaciones son:

- Bibliotecas de sistemas operativos (ficheros tradicionales UNIX en etc o mapas NIS)
- Servidores de Telnet, SSH, FTP, Web, Correo electrónico, NFS...
- Aplicaciones de escritorio o Web

2. ¿Qué datos se almacenarán?

Cada aplicación en red necesita una serie de datos:

- Ficheros de /etc: passwd, aliases, group...
- Aplicaciones Web: rama de usuarios y grupos
- Servicios: el correo electrónico necesita usuarios y alias

Objetos y atributos

3. Esquemas LDAP necesarios

Al conocer aplicaciones y tipos de datos podemos:

- Buscar esquemas LDAP para las aplicaciones
 - Muchos están descritos en RFCs: autenticación POSIX, servicios Web. . .
- Crear un esquema propio (**¡Sólo si es necesario!**)

Espacio de nombres

4. Espacio de nombres

Se refiere a la estructura en árbol del directorio

- La base o raíz se suele construir a partir de dominio:
 - Por ejemplo para `foo.net` es `dc=foo,dc=net`
- Para autenticar, se siguen nombres parecidos a los ficheros UNIX (recomendaciones RFC 2307)
 - `dn: ou=People,dc=foo,dc=net` equivale a `/etc/passwd`
 - `dn: ou=Group,dc=foo,dc=net` equivale a `/etc/group`
 - `dn: ou=Mounts,dc=foo,dc=net` equivale a `/etc/mount`

Precauciones

- Los usuarios de administración del directorio suelen situarse en ramas independientes
- Los usuarios de administración del sistema operativo no deben autenticarse contra el directorio: **si el servidor cae no tendremos acceso a la máquina**

Espacio de nombres

4. Espacio de nombres

Se refiere a la estructura en árbol del directorio

- La base o raíz se suele construir a partir de dominio:
 - Por ejemplo para `foo.net` es `dc=foo,dc=net`
- Para autenticar, se siguen nombres parecidos a los ficheros UNIX (recomendaciones RFC 2307)
 - `dn: ou=People,dc=foo,dc=net` equivale a `/etc/passwd`
 - `dn: ou=Group,dc=foo,dc=net` equivale a `/etc/group`
 - `dn: ou=Mounts,dc=foo,dc=net` equivale a `/etc/mount`

Precauciones

- Los usuarios de administración del directorio suelen situarse en ramas independientes
- Los usuarios de administración del sistema operativo no deben autenticarse contra el directorio: **si el servidor cae no tendremos acceso a la máquina**

Jerarquía de información

5. Topología de red y replicación

- LDAP está diseñado para escalar fácilmente
- OpenLDAP soporta replicación *single-master* y *multi-master* ($\geq v2.4$)

Figura: Replicación single-master



Seguridad (I)

Sensibilidad de los datos

Los datos almacenados en el directorio son **especialmente sensibles** (contraseñas, correo electrónico. . .)

6. Seguridad del directorio

- Seguridad en las comunicaciones con TLS/SSL
- Diseño y prueba de las ACLs
- Acceso restringido al directorio

- Mecanismos para proteger tanto a los usuarios que en algunos puntos pueden ser atacados
- Diseño seguro de los servidores
- Seguridad de los datos almacenados en el directorio

Seguridad (I)

Sensibilidad de los datos

Los datos almacenados en el directorio son **especialmente sensibles** (contraseñas, correo electrónico. . .)

6. Seguridad del directorio

- Seguridad en las comunicaciones con TLS/SSL
- Diseño y prueba de las ACLs
- Acceso autenticado al directorio
- Ataques DoS: poner límite a las entradas que un usuario puede obtener (directiva `sizelimit`)
- Restricción de acceso a los ficheros del directorio en el SO

Seguridad (I)

Sensibilidad de los datos

Los datos almacenados en el directorio son **especialmente sensibles** (contraseñas, correo electrónico. . .)

6. Seguridad del directorio

- Seguridad en las comunicaciones con TLS/SSL
- Diseño y prueba de las ACLs
- Acceso autenticado al directorio
- Ataques DoS: poner límite a las entradas que un usuario puede obtener (directiva `sizelimit`)
- Restricción de acceso a los ficheros del directorio en el SO

Seguridad (I)

Sensibilidad de los datos

Los datos almacenados en el directorio son **especialmente sensibles** (contraseñas, correo electrónico. . .)

6. Seguridad del directorio

- Seguridad en las comunicaciones con TLS/SSL
- Diseño y prueba de las ACLs
- Acceso autenticado al directorio
- Ataques DoS: poner límite a las entradas que un usuario puede obtener (directiva `sizelimit`)
- Restricción de acceso a los ficheros del directorio en el SO

Seguridad (I)

Sensibilidad de los datos

Los datos almacenados en el directorio son **especialmente sensibles** (contraseñas, correo electrónico. . .)

6. Seguridad del directorio

- Seguridad en las comunicaciones con TLS/SSL
- Diseño y prueba de las ACLs
- Acceso autenticado al directorio
- Ataques DoS: poner límite a las entradas que un usuario puede obtener (directiva `sizelimit`)
- Restricción de acceso a los ficheros del directorio en el SO

Seguridad (I)

Sensibilidad de los datos

Los datos almacenados en el directorio son **especialmente sensibles** (contraseñas, correo electrónico. . .)

6. Seguridad del directorio

- Seguridad en las comunicaciones con TLS/SSL
- Diseño y prueba de las ACLs
- Acceso autenticado al directorio
- Ataques DoS: poner límite a las entradas que un usuario puede obtener (directiva `sizelimit`)
- Restricción de acceso a los ficheros del directorio en el SO

Seguridad (II)

Listas de control de accesos

- Listas de control de accesos (ACL) para filtrar accesos:
 - a ramas del árbol
 - a qué atributos y con qué permisos se accede
- Las ACLs y filtros pueden utilizarse para filtrar en el directorio o en las aplicaciones
- **Demasiadas ACLs pueden ralentizar las consultas**

Ejemplo de ACL en /etc/ldap/slapd.conf

```
access to attrs=userPassword,shadowLastChange
  by dn="cn=admin,dc=foo,dc=net" write
  by anonymous auth
  by self write
  by * none
```

Seguridad (II)

Listas de control de accesos

- Listas de control de accesos (ACL) para filtrar accesos:
 - a ramas del árbol
 - a qué atributos y con qué permisos se accede
- Las ACLs y filtros pueden utilizarse para filtrar en el directorio o en las aplicaciones
- Demasiadas ACLs pueden ralentizar las consultas

Ejemplo de ACL en /etc/ldap/slapd.conf

```
access to attrs=userPassword,shadowLastChange
  by dn="cn=admin,dc=foo,dc=net" write
  by anonymous auth
  by self write
  by * none
```

Índice



- 1 Introducción
- 2 Soluciones al problema
- 3 Directorios LDAP
 - El protocolo LDAP
 - Organización de la información
 - Representación de la información
 - Implementaciones LDAP
- 4 Diseño del directorio
- 5 Optimización de OpenLDAP**
- 6 Demostración práctica
- 7 Configuración del servidor y clientes
OpenLDAP, PAM-LDAP y
NSS-LDAP
- 8 Referencias

¿Por qué optimizar?

Los servidores LDAP:

- Son una pieza clave en los sistemas operativos en red
- Su rendimiento no debe condicionar los servicios asociados
- Los servidores de directorio soportarán mucha carga de trabajo
- Problema multiobjetivo: rendimiento vs. seguridad vs. integridad

Ejemplo

Los servidores LDAP de la una universidad pequeña atienden una media 4.5 millones de operaciones de autenticación (BIND) y búsqueda (SEARCH) al día cada uno

¿Cómo optimizar?

Optimización de OpenLDAP:

- Indexación de la base de datos:
 - Un **índice** es una estructura de datos que optimiza los accesos por un atributo a entradas. Por ejemplo, `uid`
- Elección y configuración del sistema de gestión de datos (*backend*) de OpenLDAP
- Otros: Replicación, ACLs, NSCD

Indexación de la base de datos

Compromiso

Los índices:

- Aceleran notablemente el tiempo de acceso a una entrada del directorio. . .
- . . . **pero hay que construirlos y mantenerlos** ⇒ penalización sobre:
 - modificaciones sobre atributos indexados
 - tiempo de construcción de una base de datos nueva
- Conclusión: los índices deben crearse inteligentemente

Recomendaciones

Indexar sólo lo necesario:

- Seguir recomendaciones de RFCs
- Conocer qué atributos demandan las aplicaciones que se apoyan en el directorio
- OpenLDAP alerta sobre búsquedas por atributos no indexados

Indexación de la base de datos

Compromiso

Los índices:

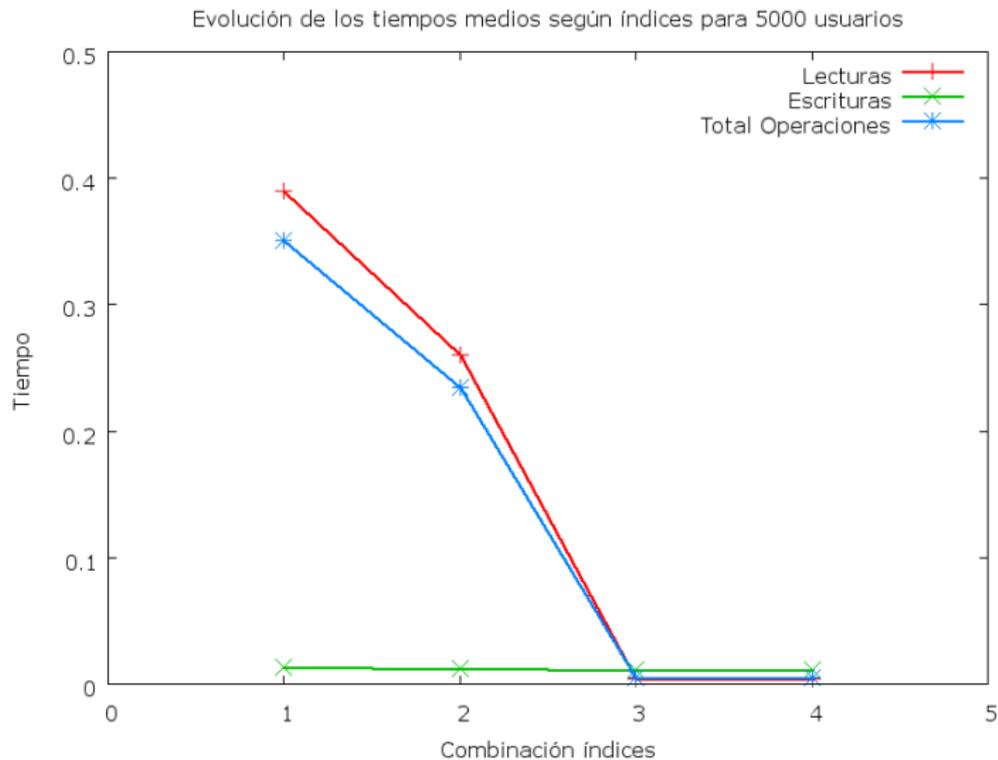
- Aceleran notablemente el tiempo de acceso a una entrada del directorio. . .
- . . . **pero hay que construirlos y mantenerlos** ⇒ penalización sobre:
 - modificaciones sobre atributos indexados
 - tiempo de construcción de una base de datos nueva
- Conclusión: los índices deben crearse inteligentemente

Recomendaciones

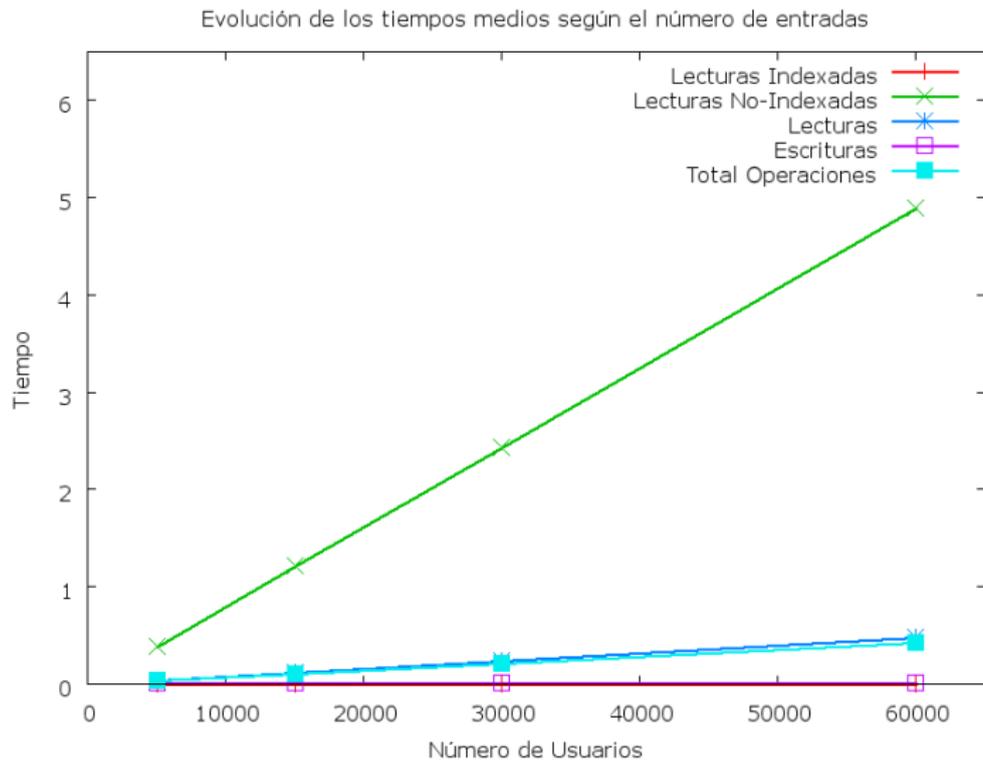
Indexar sólo lo necesario:

- Seguir recomendaciones de RFCs
- Conocer qué atributos demandan las aplicaciones que se apoyan en el directorio
- OpenLDAP alerta sobre búsquedas por atributos no indexados

Rendimiento indexación OpenLDAP-bdb (I)



Rendimiento indexación OpenLDAP-bdb (II)



Elección del backend de datos

Backend de base de datos

Arquitectónicamente OpenLDAP se divide entre:

- el *frontend* que maneja las cuestiones del protocolo
- el *backend* que maneja el almacenamiento de datos

backends disponibles

OpenLDAP soporta más de 20 *backends* con diferentes enfoques:

Almacenamiento de datos : *back-bdb*, *back-hdb*, *back-ldif* y *back-ndb*

Proxy LDAP : *back-ldap*, *back-passwd*...

Backends dinámicos : *back-config*, *back-monitor*...

Parámetros de optimización OpenLDAP con back-bdb (I)

/etc/ldap/slapd.conf en Debian

Selección del *backend*

- backend y database: selección del sistema de base de datos

Parámetros de bases de datos transaccionales:

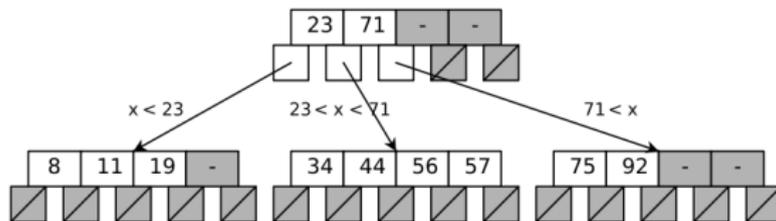
- checkpoint: frecuencia con que se vacían los búfers de los ficheros de transacciones
- dirtyread: lecturas sobre transacciones no confirmadas
- dbnosync ó DB_TXN_NOSYNC: sincronización de transacciones confirmadas y registros no inmediata
- DB_TXN_NOT_DURABLE en DB_CONFIG: supresión de registros de transacciones
- set lg regionmax, set lg bsize, set lg dir: opciones de ficheros de transacciones.

Parámetros de optimización OpenLDAP con back-bdb (II)

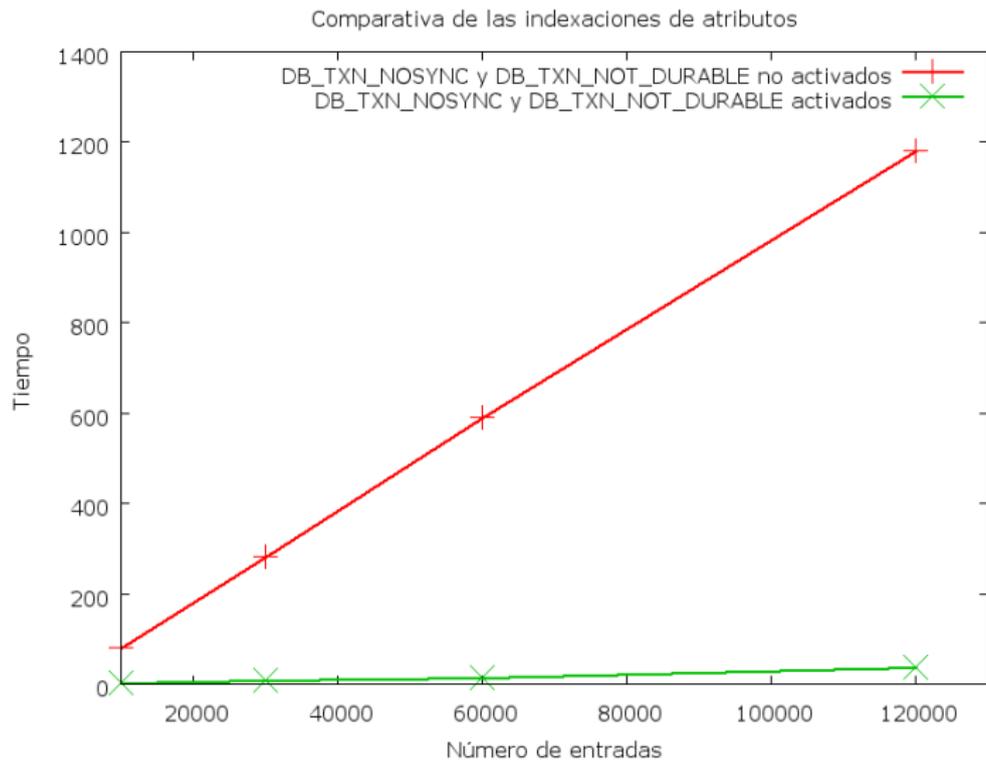
/etc/ldap/slapd.conf en Debian

Parámetros de bases de datos transaccionales (continuación):

- `cachesize`: tamaño de la base de datos en caché de memoria
- **Idealmente** se debe permitir alojar una copia de la BD en memoria principal
- Si no hay tanta memoria \Rightarrow elegir un tamaño en caché de memoria sólo para los índices del árbol B de BDB



Pruebas de rendimiento OpenLDAP-bdb (I)



Otras cuestiones de optimización

Directivas que ralentizan el acceso

- `schema-check`: comprobación de coherencia datos-esquema
- `access`: inclusión de listas de control de accesos (ACL) excesivas

Caché local en los clientes

- NSCD (*Name Service Caching Daemon*): *demonio o servicio de caché de servicio de nombres*
- Crea una caché de llamadas de la biblioteca estándar `libc` (`getpwnam`, `getpwuid...`)

Índice



- 1 Introducción
- 2 Soluciones al problema
- 3 Directorios LDAP
 - El protocolo LDAP
 - Organización de la información
 - Representación de la información
 - Implementaciones LDAP
- 4 Diseño del directorio
- 5 Optimización de OpenLDAP
- 6 Demostración práctica**
- 7 Configuración del servidor y clientes OpenLDAP, PAM-LDAP y NSS-LDAP
- 8 Referencias

Demostración práctica

- 1 Configuración básica de OpenLDAP como servidor
- 2 Configuración de un sistema operativo cliente:
 - Datos LDAP genéricos
 - NSS
 - Módulos PAM
- 3 Configuración de Apache para autenticar contra LDAP
 - Directiva `Directory`
 - Ficheros `.htaccess`
- 4 Acceso a un directorio con PHP
- 5 LDAP Account Manager (LAM) / phpLDAPadmin
- 6 Integración con Mozilla Thunderbird/Evolution

Índice



- 1 Introducción
- 2 Soluciones al problema
- 3 Directorios LDAP
 - El protocolo LDAP
 - Organización de la información
 - Representación de la información
 - Implementaciones LDAP
- 4 Diseño del directorio
- 5 Optimización de OpenLDAP
- 6 Demostración práctica
- 7 Configuración del servidor y clientes
OpenLDAP, PAM-LDAP y
NSS-LDAP**
- 8 Referencias

Instalación y configuración del servidor OpenLDAP

Nota sobre las versiones

Todo lo que sigue a continuación ha sido probado con Ubuntu 10.04.4 LTS (versión del kernel 2.6.32-38-server x86_64 GNU/Linux) y está sacado principalmente de la guía oficial de Ubuntu Server <https://help.ubuntu.com/10.04/serverguide/C/openldap-server.html>. Usaremos el dominio “foo.net” como dominio de ejemplo.

Paquete de herramientas de OpenLDAP

- Demonio: slapd
- Herramientas del servidor (cuando acceden al contenido del directorio lo hacen modificando directamente la base de datos, **en algunos casos slapd debe estar parado**): slapadd, slapcat, slapindex, slappasswd...
- Herramientas clientes (utilizan el protocolo LDAP para comunicarse con el servidor): ldapadd, ldapsearch, ldapmodify...

Instalación y configuración del servidor OpenLDAP

I

1 Instalación y configuración de *slapd*:

```
1 $ sudo apt-get install slapd ldap-utils
```

2 Añadimos los esquemas mínimos necesarios para usar el servidor para autenticación en red:

```
1 $ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/cosine.ldif  
2 $ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ldif  
3 $ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/inetorgperson.ldif
```

3 Cargamos el módulo necesario para usar una base de datos HDB (similar a BDB) y la configuración que vamos a darle:

```
1 $ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f backend-modules.foo.net.ldif  
2 $ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f backend.foo.net.ldif
```

Instalación y configuración del servidor OpenLDAP

II

- 4 Y por último, creamos el archivo `frontend.foo.net.ldif` el cual añade el usuario administrador del directorio para el dominio `foo.net`, los grupos necesarios y un usuario de prueba:

```
1 $ sudo ldapadd -x -D cn=admin,dc=foo,dc=net -W -f frontend.foo.net.ldif
```

- 5 Finalmente debemos cambiar la contraseña de administrador de slapd:

```
1 $ sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f change_adminpass.ldif
```

- 6 Podemos comprobar si el servidor funciona mirando los mensajes de Syslog al arrancar, parar o hacer una búsqueda de prueba:

```
1 $ sudo service slapd restart
2 $ tail /var/log/syslog
3 $ sudo ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b cn=config dn
4 $ ldapsearch -x -b "dc=foo,dc=net" -D "uid=prueba,ou=People,dc=foo,dc=net" "
    uid=*" -w prueba
5 $ tail /var/log/syslog
```

Instalación y configuración de los clientes LDAP I

1 Instalación de los módulos de autenticación para PAM y NSS

```
1 $ sudo apt-get install libpam-ldap
```

- 2 Aunque algunos parámetros de configuración se pueden configurar con el asistente, otros deben tocarse directamente en el fichero `/etc/ldap.conf`. Este fichero contiene la configuración por defecto para los clientes OpenLDAP del sistema operativo. En nuestro caso los datos de configuración del servidor son los siguientes:

```
1 # /etc/ldap.conf
2 base dc=foo,dc=net
3 uri ldap://127.0.0.1/
4 ldap_version 3
5
6 rootbinddn cn=admin,dc=foo,dc=net
7
8 pam_password md5
9
10 nss_base_passwd ou=People,dc=foo,dc=net?one
11 nss_base_group ou=Group,dc=foo,dc=net?one
12
13 ssl no
```

Instalación y configuración de los clientes LDAP II

- 3 Si intentamos entrar con el usuario "prueba" (del directorio) obtendremos el siguiente mensaje de error:

```
1 Could not chdir to home directory /home/prueba: No such file or directory
```

- 4 Por último, debemos configurar PAM para que al iniciar sesión por primera vez se cree el directorio del usuario en la ruta especificada en LDAP. Para ello editamos el archivo `/etc/pam.d/common-auth` y le añadimos:

```
1 session required pam_mkhomedir.so skel=/etc/skel/ umask=0022
```

Algunos ficheros y directorios relevantes I

Durante este proceso, los siguientes ficheros se han ido modificando en las distintas máquinas:

- Servidor:
 - /etc/ldap/slapd.d
 - /etc/ldap/schema
 - /var/lib/ldap/
- Clientes:
 - /etc/ldap.conf
 - /etc/ldap.secret
 - /etc/nsswitch.conf
 - /etc/pam.d: common-auth, common-password, common-account

Índice



- 1 Introducción
- 2 Soluciones al problema
- 3 Directorios LDAP
 - El protocolo LDAP
 - Organización de la información
 - Representación de la información
 - Implementaciones LDAP
- 4 Diseño del directorio
- 5 Optimización de OpenLDAP
- 6 Demostración práctica
- 7 Configuración del servidor y clientes OpenLDAP, PAM-LDAP y NSS-LDAP
- 8 Referencias

Referencias



Understanding and Deploying LDAP Directory Services

Timothy A. Howes Ph.D., Mark C. Smith, Gordon S. Good

AddisonWesley, Segunda edición 2003, ISBN: 0-672-32316-8



RFC 2307: An Approach for Using LDAP as a Network Information Service

L. Howard

<http://www.rfc-archive.org/getrfc.php?rfc=2307>



LDAP System Administration

Gerald Carter

O'Reilly, 2003, ISBN: 1-56592-491-6



Integración de redes con OpenLDAP, Samba, Cups y Pykota

Sergio González González

<http://es.tldp.org/Tutoriales/doc-openldap-samba-cups-python>

Referencias



Web de OpenLDAP

Descargas, guía de administración, preguntas frecuentes. . .

<http://www.openldap.org/>



OpenLDAP performance tips

Kostas Kalevras

[http:](http://kkalev.wordpress.com/2009/01/27/openldap-performance-tips/)

[//kkalev.wordpress.com/2009/01/27/openldap-performance-tips/](http://kkalev.wordpress.com/2009/01/27/openldap-performance-tips/)



MigrationTools

PADL Software Pty Ltd

<http://www.padl.com/OSS/MigrationTools.html>