# Directorios LDAP

Julio Sánchez

jsanchez@OpenLDAP.org

Proyecto OpenLDAP

II Congreso Hispalinux

Madrid, noviembre 1999

# Índice

# Introducción

- X.500 ligero
  - ¿X.500 para pobres?
  - ¿X.500 útil?
- La próxima ola
  - Novell
  - Netscape/Sun
  - IBM
  - Microsoft

# ¿Qué es el directorio?

- La guía de teléfonos
  - Base de datos distribuida
- Almacén de información de recursos de la organización
  - Cada entrada representa un recurso
    - Personas y cuentas
    - Máquinas
    - Departamentos
    - Salas

# ¿Base de Datos?

¿Por qué no utilizar una base de datos de propósito general?

- Excesivas
  - Demasiado pesadas
- Insuficientes
  - Dificultad de normalización (Codd)
  - Falta de normalización (estándares)

# Atributos

- Cada entrada tiene atributos
- Cada atributo es un nombre (tipo) y una lista de valores
- El nombre es una cadena de caracteres o un OID
- Cada tipo de atributo puede ser un subtipo de otro
  - Herencia simple
- Sintaxis, reglas de comparación

# Ejemplos de Atributos

| | |
|---|---|
| CN | Nombre habitual |
| O | Organización |
| OU | Departamento |
| C | País |
| MAIL | Dirección de correo electrónico |
| PHONE | Número de teléfono |
| DC | Componente de dominio |

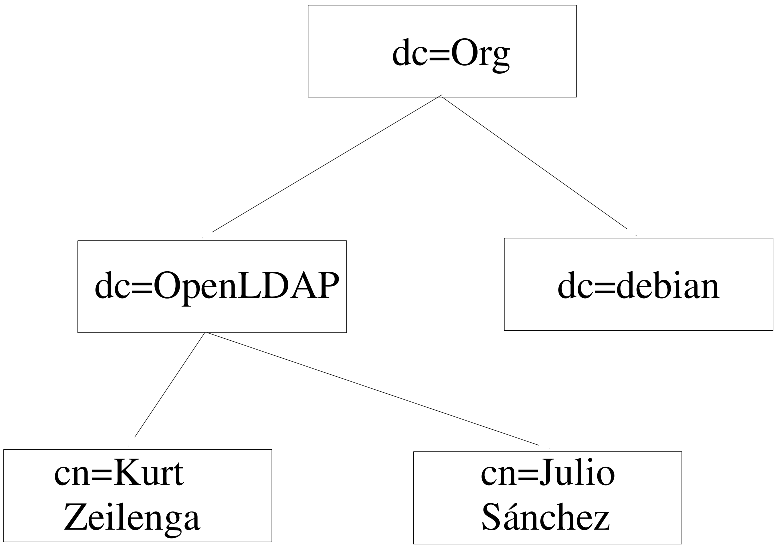
# Jerarquías

- Nombre Distinguido (DN)
  - Cada entrada tiene uno, único y propio
- Secuencia de RDN
  - Cada RDN (Nombre Distinguido Relativo) es un conjunto de Atributos
  - Cada atributo aquí es un nombre y un valor
- Cada parte del RDN debe ser un atributo y valor presente en la entrada
  - Valores distinguidos

# Ejemplos de DN

- cn=Julio Sánchez,dc=OpenLDAP,dc=org
- cn=Julio+mail=jsanchez@OpenLDAP.org, o=sssss,c=es

# Ejemplo de directorio



# Clases

- Cada entrada pertenece a una o más clases
- Atributos requeridos
- Atributos opcionales
- Atributo objectClass
  - Requerido en todas las entradas
  - Indica las clases

# Herencia

- Las clases pueden derivarse de una o más clases
  - Herencia múltiple
- Clase top
  - Superclase última de todas las clases
- Ejemplos:
  - residentialPerson
  - organizationalPerson
  - posixAccount

# Esquema

- Clases conocidas
  - Qué atributos requieren
  - Qué atributos permiten
- Tipos de atributos
  - Sintaxis
  - Reglas de comparación
  - Simples/múltiples
  - Operacionales
- Otras informaciones

# Protocolo LDAP

- Conexión TCP
  - Puerto 389 normalmente
- Asíncrono
  - Múltiples peticiones en curso
  - El servidor contesta cada una cuando puede
- Extensible

# Operaciones del Protocolo

- BIND
  - Autenticación, posiblemente nula
- UNBIND
  - Fin de la conexión

# Operación SEARCH

- Busca en el directorio y devuelve cero o más entradas
- Parámetros
  - Base
  - Ámbito (scope)
  - Filtro
  - Atributos
  - Devolver valores sí/no

# Operación SEARCH

- La Base indica el punto del árbol donde empezar a buscar
- El Ámbito
  - base: se utiliza para leer una entrada concreta
  - onelevel: para buscar entre los descendientes inmediatos de la base, sin incluir ésta
  - subtree: busca en todas las entradas hacia abajo

# Operación SEARCH

- Filtros
  - Filtro universal:

    objectclass=*
  - Simples:

    mail=jsanchez@OpenLDAP.org
  - Compuestos:

    (&(objectclass=person)(cn=julio*))

# Operación COMPARE

- Permite verificar si una entrada cumple una cierta condición

# Operación ADD

- Crea una nueva entrada
- DN
  - El padre debe existir
- Tipos de atributos y sus valores
- La entrada debe resultar conforme al esquema

# Operación DELETE

- Elimina una entrada
- Normalmente, sólo puede eliminarse una entrada terminal

# Operación MODIFY

- Permite añadir, eliminar o modificar los valores de la entrada
- No permite modificar los valores distinguidos
- El resultado debe seguir siendo conforme al esquema

# Operación RENAME

- Permite cambiar el nombre de la entrada
- MODRDN/MODDN
  - MODRDN: V2, no se puede cambiar el padre
  - MODDN: V3, se puede cambiar el padre
- Dificultades
  - ¿Entre servidores?
  - ¿Hijos?
  - ¿Integridad referencial?

# OpenLDAP

- 1998
  - Kurt Zeilenga de Boolean toma el código abandonado de la Universidad de Michigan
    - Forma OpenLDAP
    - Da alojamiento
      - FTP
      - CVS
      - Listas de correo
      - ITS
      - FAQ−O−Matic
    - Líder y principal desarrollador

# OpenLDAP

- 1999
  - Versión 1.2
    - Integrados los parches para Umich
    - autoconf, libtool, etc.
    - Mantenimiento activo
  - Versión 2.0
    - En alpha
    - LDAP V3
    - Esquema
    - TLS, SASL

# Elementos de OpenLDAP

- Bibliotecas
  - libldap, liblber
- Servidores
  - ldapd: pasarela a X.500, obsolescente
  - slapd: servidor autónomo
  - slurpd: mantenimiento de réplicas

# Elementos de OpenLDAP

- Clientes
  - Mantenimiento
    - ldapadd, ldapmodify, ldapdelete, ldapmodrdn
  - Pasarelas
    - mail500, fax500
  - Otros
    - ud

# Utilización en la práctica

- Directorio de correo
  - Encontrar la dirección de correo de alguien
  - Encontrar el certificado digital de alguien
  - Netscape, Outlook
- Libreta de direcciones y teléfonos
- Distribución de correo
  - sendmail, postfix
  - mail500

# Utilización en la práctica

- Sustitución de NIS
- RFC2307
  - esquema para representar los mapas de NIS
- nss_ldap
  - nscd (Name Service Cache Daemon)
- pam_ldap
- ypldapd
  - comercial

# Utilización en la práctica

- Varias interfaces para Perl
- mod_ldap para Apache
- Parches para squid

# Utilización en la práctica

- Integración de todos los recursos de la organización
  - Personal
  - Salas de Reuniones
  - Cuentas de usuario
- Apenas hemos empezado a arañar las posibilidades

# Hace falta más

- El proyecto OpenLDAP necesita ayuda
  - http://www.OpenLDAP.org
  - Hay mucho que hacer
- LDAP necesita ayuda
  - Clientes de correo
  - Herramientas de calendario
  - Etc.

# Reflexión

Si el mundo del software libre no proporciona los elementos necesarios para participar en los directorios corporativos e, incluso, dictar su forma, se verá progresivamente desplazado en esos entornos, independientemente de los progresos que se hagan en otras áreas.

# Conclusión

- El directorio puede representar la próxima barrera de resistencia a Linux
- Afortunadamente, hay mucho avanzado
- Lamentablemente, hay que trabajar más