Introducción a LDAP con OpenLDAP

Marco Antonio Villegas Vega
marco.villegas@pucp.edu.pe

basado en la presentación de
Virginia Villanueva Velásquez
para el Linux Week 2007

Lightweight Directory Access Protocol

- Protocolo de tipo cliente-servidor para acceder a un servicio de directorio.
- Basado en el estándar X.500.
- Soporta TCP/IP. Necesario para el acceso a Internet.
- Permite centralizar toda la información en un solo lugar.

Características de LDAP

- Es una clase especial de base de datos.
- Contiene información estructurada en forma de árbol.
- Se realizan lecturas mas que escrituras.
- Proporcionan una respuesta rápida.

¿Para qué usar LDAP?

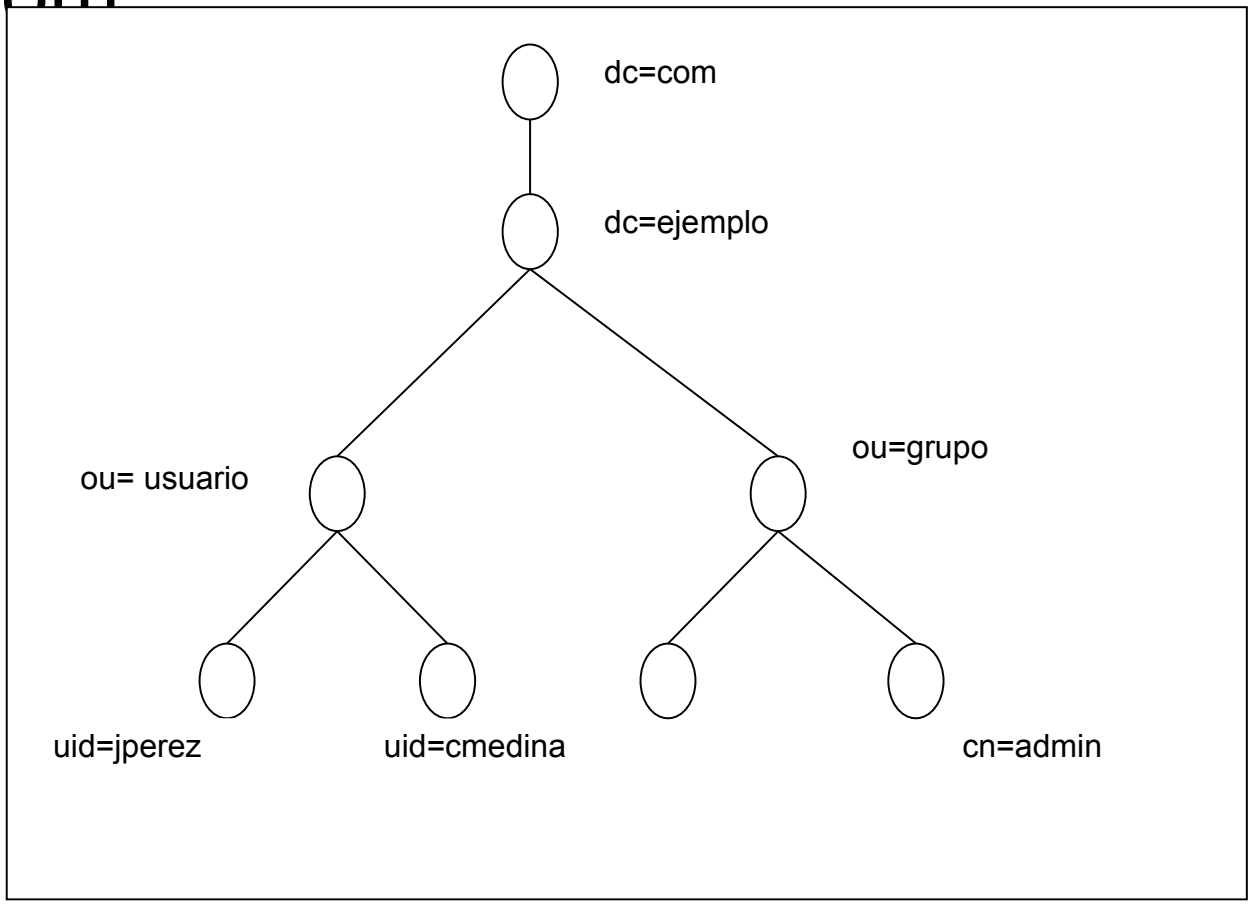
- Directorios de información.
- Sistemas de autenticación/autorización centralizada
- Sistemas de correo electrónico
- Sistemas de alojamiento de páginas web y FTP
- Servidores de certificados públicos y llaves de seguridad
- Autenticación única ó “single sign-on” para la personalización de aplicaciones
- Perfiles de usuarios centralizados.
- Libretas de direcciones compartidas

Definiciones

- Entradas
- DN
- Atributos
- LDIF
- Objetos

Definiciones

- dn: uid=jperez, ou=usuario, dc=ejemplo, dc=com



OpenLDAP

- Implementación libre del protocolo LDAP
- Disponible en la mayoría de las distribuciones de GNU/Linux
- OpenLDAP se compone de varias partes:
  - Cliente (librerías)
  - slapd : El servidor LDAP.
  - slurpd : El servidor de replicación.

OpenLDAP: Instalación

- # apt-get install --no-download slapd
- Inicia la configuración básica:
  - Contraseña maestra: ldapAdmin
  - Configurando slapd (2.3.30-2) ...
    - Creating new user openldap... done.
    - Creating initial slapd configuration... done.
    - Creating initial LDAP directory... done.
  - Starting OpenLDAP: slapd.

OpenLDAP: Configuración

/etc/openldap/slapd.conf

- Sufijo: Base o raiz del directorio

  suffix "dc=ejemplo, dc=com"
- Directorio de la base de datos:

  directory /var/lib/ldap
- Cuenta del administrador:

  rootdn "cn=root, dc=ejemplo, dc=com“

OpenLDAP: Configuración

/etc/openldap/slapd.conf

- Contraseña del administrador

  rootpw <CONTRASEÑA>

- Niveles de acceso

  access to dn=".*,ou=usuario, dc=ejemplo, dc=com"

    attr=userPassword

      by self write

      by dn="cn=root,dc=admon,dc=com" write

      by * auth

OpenLDAP: Uso

- Crear la estructura
  - # slapadd -l inicialweb.ldif

```
dn: dc=ejemplo,dc=com
objectClass: dcObject
objectClass: organization
o: Ejemplo
dc: ejemplo

dn: cn=root,dc=ejemplo,dc=com
objectClass: organizationalRole
cn: root
```

```
dn: ou=grupo,dc=ejemplo,dc=com
ou: grupo
objectClass: organizationalUnit
objectClass: top

dn: ou=usuario,dc=ejemplo,dc=com
ou: usuario
objectClass: organizationalUnit
objectClass: top
```

phpldapadmin

- Una interfase web para navegar por el servidor LDAP.
  - # apt-get install phpldapadmin
- Configuración
  - /usr/share/phpldapadmin/config/config.php

Referencias

- Sobre los Object Class

  http://ldap.akbkhome.com/index.php/objectclass.html
- Configuración Básica de OpenLDAP
  - http://fferrer.dsic.upv.es/cursos/Linux/Avanzado/HTML/ch02s04.html
- OpenLDAP Simples
  - http://www.zytrax.com/books/ldap/ch5/index.html#step1
  - http://www.openldap.org/doc/admin23/quickstart.html

Referencias

- Mini-manuales
  - http://www.ldapman.org/articles/sp_intro.html
- Manuales intermedios
  - http://es.tldp.org/COMO-INSFLUG/COMOs/LDAP-Linux-Como/LDAP-Linux-Como.html
  - http://fferrer.dsic.upv.es/cursos/Linux/Avanzado/HTML/ch02s04.html
  - http://dns.bdat.net/COMOS/LDAP-Como/x214.html (slapd.conf)

Referencias

- Manual oficial
  - http://www.openldap.org/doc/admin23/
- Contenido del archivo replog
  - http://www.openldap.org/lists/openldap-software/200206/msg00323.html
- Error de conección (problema con iptables)
  - ldap_is_socket_ready:error on socket 3: errno: 113 (no route to host)
  - http://www.openldap.org/lists/openldap-software/200404/msg00643.html

Referencias

- TLS
  - http://postfix.state-of-mind.de/patrick.koetter/smtpauth/postfix_tls_support.html
  - http://sapiens.wustl.edu/~sysmain/info/openldap/openldap_configure.html
- Debug
  - http://www.umich.edu/~dirsvcs/ldap/doc/guides/slapd/6.html
- ACL's
  - http://www.zytrax.com/books/ldap/ch5/step4.html#step4-access