

ADMINISTRACIÓN DE USUARIOS CON LDAP Y GNU/LINUX

Dr. Luis Gerardo de la Fraga

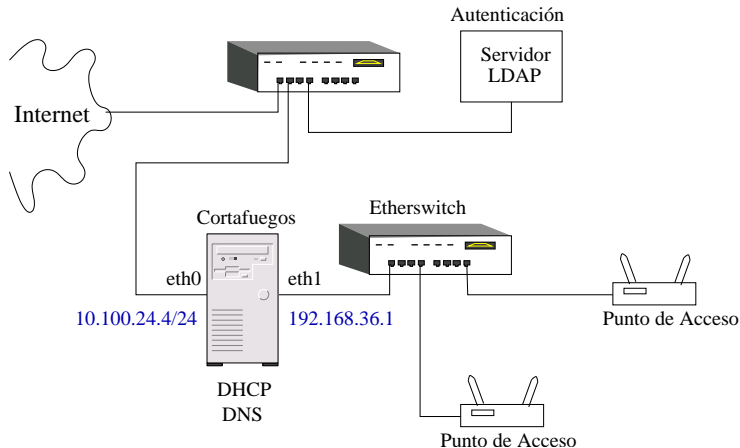
Departamento de Computación
Cinvestav

Correo-e: fraga@cs.cinvestav.mx

23 de noviembre de 2006

En esta charla se presenta la implantación de un servidor con OpenLDAP para autenticar a todos los usuarios de una red.

SERVIDOR NOCAT PARA LA RED INALÁMBRICA



M. Kershaw, Linux-Powered Wireless Hot Spots, *Linux Journal*, 133, Sep 2003.

El Protocolo Ligero de Acceso a Directorio (Lightweight Directory Access Protocol) puede ser visto como un repositorio donde podemos colocar información para después consultarla para su procesamiento. El repositorio se asemeja a una base de datos, pero en LDAP ha sido diseñada y optimizada para realizar operaciones de consulta.

Las principales características de LDAP son:

- ▶ Está basado en el modelo cliente-servidor
- ▶ Organiza la información de modo jerárquico, utilizando directorios.
- ▶ Es capaz de propagar sus directorios a otros servidores LDAP
- ▶ Tiene un API de programación bien definido

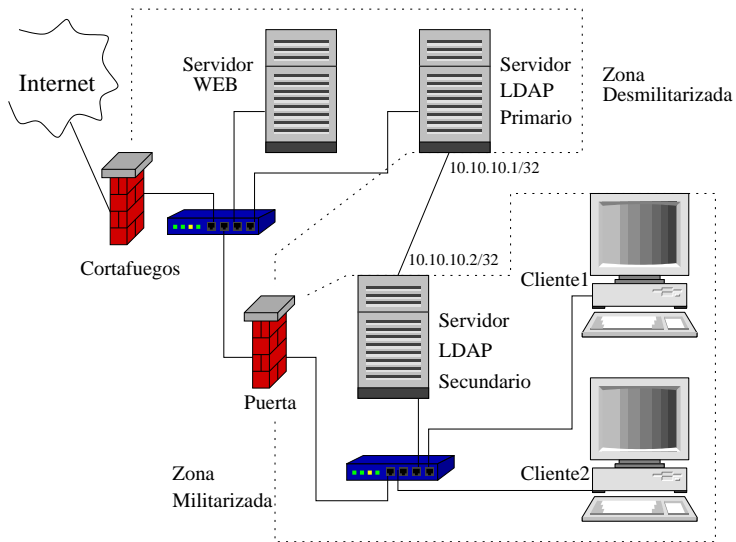
Un directorio LDAP puede contener cualquier tipo de información, desde imágenes, direcciones de correo electrónico, contraseñas y referencias html, hasta certificados digitales, direcciones IP, etc.

La gran diversidad de información que puede ser almacenada en estos directorios los hace aptos para utilizarse en aplicaciones como:

- ▶ Directorios de páginas blancas o amarillas
- ▶ Servidor de direcciones electrónicas
- ▶ Servidores de nombres de dominio (DNS)
- ▶ Repositorio para certificados digitales
- ▶ Repositorios de cuentas de usuario

Se presentará la configuración del servicio de LDAP como un repositorio de la información de cuentas de usuario y una medición de su rendimiento en redes IPv6.

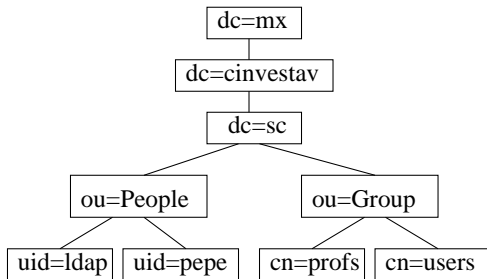
1. *Ventaja*: Facilita la administración de una red al centralizar la información.
2. *Desventaja*: LDAP resulta complicado de configurar ya que es un sistema complejo.



El servicio de autenticación nos permitirá:

- ▶ Administrar mejor la red. Se centraliza el dar de alta, baja o cambiar las cuentas y contraseñas de usuarios.
- ▶ Un usuario podrá cambiar su contraseña desde cualquier máquina cliente.

1. Organización del directorio
2. Configuración del servidor LDAP primario
3. Configuración de los clientes
4. Creación y mantenimiento de la base de datos
5. Autenticación
6. Replicación del servidor LDAP



Nuestro *reino* es “dc=sc,dc=cinvestav,dc=mx”

CONFIGURACIÓN DEL SERVIDOR LDAP PRIMARIO

(1/4)

El software necesario se instaló de los RPMS de RedHat:

- ▶ `openldap`
- ▶ `openldap-clients`
- ▶ `openldap-servers`

El archivo que mantiene la configuración del servidor LDAP es:

```
/etc/openldap/slapd.conf
```

CONFIGURACIÓN DEL SERVIDOR LDAP PRIMARIO

(2/4)

```
idletimeout 60
```

```
TLSCertificateFile /usr/share/ssl/certs/slapd.pem
```

```
TLSCertificateKeyFile /usr/share/ssl/certs/slapd.pem
```

Para encriptar las comunicaciones

CONFIGURACIÓN DEL SERVIDOR LDAP PRIMARIO

(3/4)

```
# Control de acceso a la base de datos
```

```
access to dn=".*,dc=sc,dc=cinvestav,dc=mx" attr=userPassword
by dn="cn=Manager,dc=sc,dc=cinvestav,dc=mx" write
by dn="cn=replicator,dc=sc,dc=cinvestav,dc=mx" write
by dn="cn=proxyuser,dc=sc,dc=cinvestav,dc=mx" auth
by self write
by anonymous auth
by * none
```

```
access to *
by dn="cn=Manager,dc=sc,dc=cinvestav,dc=mx" write
by dn="cn=replicator,dc=sc,dc=cinvestav,dc=mx" write
by * read
```


CONFIGURACIÓN DEL SERVIDOR LDAP PRIMARIO

(4/4)

```
#####  
# Definiciones de la base de datos  
  
database ldbm  
suffix      "dc=sc,dc=cinvestav,dc=mx"  
rootdn      "cn=Manager,dc=sc,dc=cinvestav,dc=mx"  
# rootpw secret  
rootpw      {SSHA}CipB6+P3iqIeV+XVZ2Tn8xbmhUk/M0nc  
  
# The database directory MUST exist prior to running slapd AND  
# should only be accessible by the slapd/tools. Mode 700 recommended.  
directory   /var/lib/ldap  
  
# Indices to maintain  
index       objectClass,uid,uidNumber,gidNumber,memberUid    eq  
index       cn,mail,surname,givenname      eq,subinitial
```

Contraseña generada con el comando `/usr/sbin/slappasswd`.

```
/etc/rc.d/init.d/ldap start|stop|restart
```

El archivo de configuración

`/etc/ldap.conf`

es usado para aplicar los valores por defecto a los parámetros usados por los clientes de ldap.

CONFIGURACIÓN DE UN CLIENTE (2/2)

```
host 10.200.100.1
base dc=sc,dc=cinvestav,dc=mx
uri ldaps://servidor.sc.cinvestav.mx

pam_login_attribute uid

# Specify a minimum or maximum UID number allowed
pam_min_uid 100
pam_max_uid 9000

pam_password md5

nss_base_passwd ou=People,dc=sc,dc=cinvestav,dc=mx?one
nss_base_shadow ou=People,dc=sc,dc=cinvestav,dc=mx?one
nss_base_group ou=Group,dc=sc,dc=cinvestav,dc=mx?one

ssl start_tls
ssl on
```

Para probar el servidor podemos agregar un usuario a la base de datos y realizar la consulta. Para la prueba debemos agregar un usuario que no aparezca en `/etc/passwd` y realizar

```
ldapsearch -x uid=prueba
```

CREACIÓN Y MANTENIMIENTO DE LA BASE DE DATOS (1/7)

Se usaron las *herramientas de migración*, que en realidad son scripts hechos en perl, que vienen en la distribución de OpenLDAP en `/usr/share/openldap/migration`.

Se usaron los scripts

- ▶ `migrate_base.pl`
- ▶ `migrate_group.pl`
- ▶ `migrate_passwd.pl`

CREACIÓN Y MANTENIMIENTO DE LA BASE DE DATOS (2/7)

Usando el script `migrate_base.pl` se generan los primeros registros de la base de datos:

```
./migrate_base.pl > base.ldif
```

y el contenido del archivo `base.ldif` debe de editarse ya que no necesitamos toda la información.

CREACIÓN Y MANTENIMIENTO DE LA BASE DE DATOS (3/7)

Para que el archivo `base.ldif` refleje la información del diseño del directorio, su contenido debe ser:

```
dn: dc=sc,dc=cinvestav,dc=mx
dc: sc
objectClass: top
objectClass: domain
```

```
dn: ou=People,dc=sc,dc=cinvestav,dc=mx
ou: People
objectClass: top
objectClass: organizationalUnit
```

```
dn: ou=Group,dc=sc,dc=cinvestav,dc=mx
ou: Group
objectClass: top
objectClass: organizationalUnit
```


CREACIÓN Y MANTENIMIENTO DE LA BASE DE DATOS (4/7)

El script `migrate_group.pl` cambia la información en `/etc/group` a formato LDIF.

El script `migrate_passwd.pl` cambian la información de los archivos `/etc/passwd` y `/etc/shadow` a formato LDIF.

CREACIÓN Y MANTENIMIENTO DE LA BASE DE DATOS (5/7)

Archivo LDIF para el usuario *prueba*

```
# prueba, People, cs, cinvestav, mx
dn: uid=prueba,ou=People,dc=sc,dc=cinvestav,dc=mx
uid: prueba
cn: Cuenta de prueba
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:: e2NyeXB0fXg=
shadowLastChange: 12661
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 700
gidNumber: 700
homeDirectory: /home/prueba
gecos: Cuenta de prueba
```

CREACIÓN Y MANTENIMIENTO DE LA BASE DE DATOS (6/7)

Ahora podemos agregar los archivos%.ldif creados para llenar la base de datos. Esto se realiza con el comando ldapadd:

```
ldapadd -x -W -D 'cn=Manager,dc=sc,dc=cinvestav,dc=mx' -f base.ldif
ldapadd -x -W -D 'cn=Manager,dc=sc,dc=cinvestav,dc=mx' -f group.ldif
ldapadd -x -W -D 'cn=Manager,dc=sc,dc=cinvestav,dc=mx' -f usuarios.ldif
```

CREACIÓN Y MANTENIMIENTO DE LA BASE DE DATOS (7/7)

Para generar automáticamente una contraseña para el usuario *prueba* realizamos;

```
ldappasswd -x -W -D 'cn=Manager,dc=sc,dc=cinvestav,dc=mx' \  
  'uid=prueba,ou=People,dc=sc,dc=cinvestav,dc=mx'
```

Para borrar el usuario *prueba* realizamos:

```
ldapdelete -x -v -W -D 'cn=Manager,dc=sc,dc=cinvestav,dc=mx' \  
  'uid=prueba,ou=People,dc=sc,dc=cinvestav,dc=mx'
```

AUTENTICACIÓN (1/3)

La información del usuario consiste del mapeo entre los números de identificación de usuario y los nombres de usuario (que se usa, por ejemplo, al realizar el comando `ls -l`) ó la localización de los directorios de casa (usado, por ejemplo, al realizar `cd ~`. La consulta a tal información es manejada por el subsistema del Servicio de Conmutación de Nombres (NSS, Nameservice Switch).

La autenticación, que es el chequeo de las contraseñas, es manejada por el subsistema PAM (plugable authentication module). Estos dos subsistemas se configuran de forma separada, pero los requerimos para trabajar con LDAP.

El NSS se configura en el archivo `/etc/nsswitch.conf`. Deben de modificarse las líneas siguientes:

```
# /etc/nsswitch.conf
# con permisos 644
passwd:  files ldap
shadow:  files ldap
group:   files ldap
```

Prueba: `finger prueba`

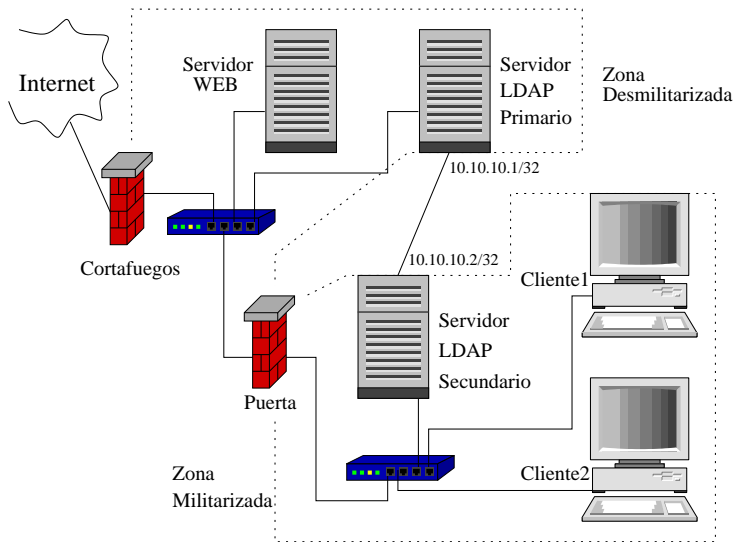
La forma fácil de configurar la autenticación en RedHat es usando el comando

```
authconfig
```

Este comando abre una interfaz gráfica y modifica los archivos

```
/etc/ldap.conf y
```

```
/etc/pam.d/system-auth
```

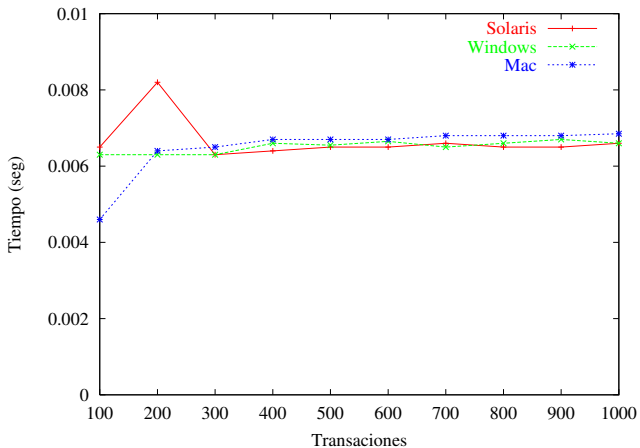


La configuración del servidor secundario LDAP se realiza de la misma forma que la configuración del servidor primario. Además se debe agregar la siguiente información en el archivo `/etc/openldap/slapd.conf` del servidor primario:

```
# Replicas to which we should propagate changes
repllogfile    /var/lib/ldap/repllog

replica host=replicador:389 tls=yes
binddn="cn=replicator,dc=sc,dc=cinvestav,dc=mx"
bindmethod=simple credentials=a890linux
```

RENDIMIENTO DE UN SERVIDOR LDAP



1. Se ha presentado la configuración de un servicio para centralizar la información y autenticación de usuarios usando LDAP.
2. El proceso de configuración resultó una tarea árdua de varias semanas, conllevó la activación y revisión de los archivos de auditoría para la verificación del funcionamiento de cada parte de la configuración.
3. El funcionamiento en IPv6 es eficiente por lo que se podría migrar este servicio a una red IPv6 sin ningún problema.

Probar realizaciones del servidor de autenticación con RADIUS y kerberos.

Esta presentación puede encontrarse en:

<http://delta.cs.cinvestav.mx/~fraga/Charlas/>

Ofrecemos:

1. Maestría en Ciencias en Computación
2. Doctorado en Ciencias en Computación

<http://www.cs.cinvestav.mx>