Instalación de Samba y OpenLDAP en Debian

Sumario

Instalación de OpenLDAP

Vamos a instalar OpenLDAP en Debian:

```
# Para instalar openldap y utilidades
apt-get install slapd ldap-utils

# Durante la instalación definimos una contraseña para el administrador

# Si queremos configurar parámetros adicionales después de la instalación podremos hacerlo con:
dpkg-reconfigure --priority=low slapd

# Pulsaremos en No y a continuación escribiremos el nombre del dominio DNS.
# Seguiremos contestando al resto de preguntas.
# Escogeremos LDAPv2
```

Una herramienta muy interesante para consultar la información de la base de datos DBD (Berkeley DB) se puede hacer con:

```
slapcat
```

Instalación de SAMBA con LDAP

Vamos a instalar Samba y utilidades para LDAP:

```
apt-get install samba smbclient smbldap-tools smbfs

# Una vez todo instalado le vamos a decir que la máquina se autentifique contra el propio LDAP.
# Tendremos que instalar previamente una librería para integrar la información del DNS y del LDAP en el
# propio LDAP.
apt-get install libnss-ldap

# Nombre distintitivo para la base de las búsquedas:
dc=sanclemente, dc=local

# Versión de LDAP a usar:
Versión 3.

# Cuenta LDAP del administrador:
cn=admin, dc=sanclemente, dc=local

# Contraseña del usuario admin:
*******

# Modificaremos el fichero nsswitch.conf a mano:
nano /etc/nsswitch.conf

# Ejecutaremos de nuevo dpkg-reconfigure por si tenemos opciones adicionales de configuración:
dpkg-reconfigure --priority=low libnss-ldap

# Aquí creamos un usuario nuevo (sólo para leer) ya que el administrador ya está creado.
....
# Crearemos el nuevo usuario con privilegios de sólo lectura:
cn=usuario,dc=sanclemente,dc=local
```

Instalación de LIBPAM con LDAP

Con la librería LIBPAM de autentificación de Linux le añadimos la librería de autenticación LDAP:

```
apt-get install libpam-ldap libpam-cracklib libpam-dotfile ldapscripts

# Volvemos a crear los dos usuarios de admin y un usuario adicional con permisos sólo de lectura:
...

# Volvemos de nuevo a ejecutar el reconfigure en búsqueda de opciones adicionales:
dpkg-reconfigure --priority=low libpam-ldap

# Escogeremos el mecanismo de encriptación de contraseñas en el LDAP.
# Escogeremos la opción exop (el LDAP es el que decidirá), es la mejor opción.
```

Configuración adicional de librerías

Revisión de las librerías recién instaladas:

```
nano /etc/libnss-ldap.conf

# Comprobamos la opción de rootbinddm que está correctamente configurada.
rootbinddm cn=admin, dc=sanclemente,dc=local

# Comprobamos otro fichero dónde se almacena la contraseña del usuario admin:
nano /etc/libnss-ldap.secret

# Revisamos estos permisos
chmod 644 /etc/libnss-ldap.conf
chmod 600 /etc/libnss-ldap.secret

# Editamos el fichero pam_ldap.conf y comprobamos el binddn
nano /etc/pam_ldap.conf

binddn cn=conexion,dc=sanclemente,dc=local

bindpw usuario (clave del usuario que puede conectarse al ldap en modo lectura).
```

Creación de un usuario en el LDAP

Se suele crear un archivo con los datos y se importa:

```
nano usuario.ldif

# Introducimos los datos del usuario:
dn: cn=usuario, dc=sanclemente,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: usuario
description: LDAP Usuario
userPassword: xxxx

# Grabamos el archivo y lo importamos en el LDAP con:
ldapadd -x -D "cn=admin,dc=sanclemente,dc=local" -w admin -f usuario.ldif

# -x conexión no segura
# -w contraseña de admin
# -f el fichero a importar
# Si hacemos a continuación slapcat veremos todas las entradas del LDAP
slapcat

# Para modificar la clave de usuario se hace con:
ldappasswd -x -D "cn=admin,dc=sanclemente,dc=local" -w admin -s usuario "cn=usuario,dc=sanclemente,dc=local"

# -w contraseña del usuario con el que te conectas
# -s contraseña del nuevo usuario

# Vamos al directorio de configuración /etc:
```

```
# Creamos un enlace simbólico a pam_ldap.secret
ln -s /etc/pam_ldap.secret /etc/ldap.secret

# Dentro de /etc/ldap:
nano  /etc/ldap/slapd.conf

# Al final del archivo añadimos el algoritmo de criptografía que queremos usar para las claves:
# Le indicamos que escogemos como algoritmo de encriptación:
password-hash {SSHA}

# También se definen los accesos:
en access to...

#Añadimos:
by dn="cn=admin,dc=sanclemente,dc=local"  write
by dn="cn=usuario,dc=sanclemente,dc=local"  read
...


# Con el comando slaptest detectamos errores en los ficheros de configuración
slaptest

# Reiniciamos el servicio:
/etc/init.d/slapd restart

# Haremos un cambio del nsswitch:
# Comprobamos previamente que al poner hostname, el nombre del host aparece en /etc/hosts
# con 127.0.0.1. Si no apareciera lo tenemos que poner.

# Editaremos por último /etc/nsswitch.conf
nano /etc/nsswitch.conf

# Hacemos los siguientes cambios:
passwd:         files ldap
group:            files ldap
shadow:         files ldap
hosts:             files ldap dns

# Para comprobar que funciona todo bien después de ésto:
# Dame entero el passwd (nos da todo lo que contiene el files + el ldap)
getent passwd

# Si ésto funciona entonces va todo bien en principio.
# Saldrán todos los usuarios del tipo POSIX Account.


# Editaremos ahora todos los ficheros del PAM:
nano /etc/pam.d/common-account

# Añadimos la última línea:
account required    pam_unix.so
account sufficient   pam_ldap.so use_firts_pass

# Modificamos también el fichero common-auth:
nano /etc/pam.d/common-auth

# Añadimos la siguiente líneas de reglas para regular la autentificación:
auth sufficient  pam_unix.so
auth sufficient pam_ldap.so use_first_pass
auth required pam_env.so
auth required pam_securetty.so
auth required pam_unix_auth.so
auth required pam_warm.so
auth required pam_deny.so

# Editamos el fichero /etc/pam.d/common-session:
nano /etc/pam.d/common-session

session  required   pam_limits.so
session  required  pam_unix.so
session  optional  pam_ldap.so use_firts_pass
session  required  pam_mkhomedir.so skel=/etc/skel umask=0022
```

```
# Por último editamos /etc/pam.d/common-password:
nano /etc/pam.d/common-password

password  required  pam_cracklib.so 1 retry=3 minlen=8 difok=4
password  sufficient  pam_unix.so  use_authok md5 shadow
password sufficient   pam_ldap.so use_authok use_first_pass
password required   pam_warn.so
password required  pam_deny.so
```

Configuración de SAMBA

Instalamos la configuración de SAMBA que trae muchos ejemplos de configuración:

```
# Instalamos la doc de samba:
apt-get install samba-doc

# Vamos a copiar un ejemplo de un esquema para que funciona samba con ldap:
cd /usr/share/doc/samba-doc/examples/LDAP

# Lo copiamos al directorio de schemas:
cp samba.schema.gz /etc/ldap/schema

# Entramos en el directorio de schemas:
cd /etc/ldap/schema

# Descomprimimos el fichero:
gzip -d samba.schema.gz

# Cambiamos el propietario a openldap:
chown openldap.openldap samba.schema
chmod 644 samba.schema
cd..

# Editamos slapd.conf y añadimos un include:
Include /etc/ldap/schema/samba.schema

#Hacemos un slaptest para ver si va todo ok:
slaptest

# Reiniciamos
/etc/init.d/slapd restart
```

Ahora nos tocaría configura el samba:

```
# En la carpeta /etc/samba editaremos los parámetros:
nano smb.conf

# Con el comando testparm comprobamos errores en los parámetros de samba:
testparm

# Iniciamos el samba:
/etc/init.d/samba restart

# Cambiamos la clave del administrador en samba:
smbpasswd -w admin

# Configuramos las herramientas para interactuar con samba y ldap al mismo tiempo:
nano /etc/ldap/sldap.conf

# Modificamos un par de atributos (sambaldap password y
# en la sección de seguridad access to primera línea agregamos:
access to attrs= .....,sambaLMPassword, sambaNTPassword

# Reiniciamos slapd
/etc/init.d/slapd restart
```

Configuración de smbldap-tools

Mediante esta herramienta podremos crear usuarios y grupos rápidamente.

```
# Vamos al directorio /etc/smbdldap-tools y nos copiamos:
cp /usr/share/doc/smbdldap-tools/examples/smbdldap.conf.gz    /etc/smbldap-tools
cp /usr/share/doc/smbdldap-tools/examples/smbdldap_bind.conf    /etc/smbldap-tools
/etc/smbldap-tools/gzip  -d /etc/smbldap-tools/smbdldap.conf.gz

# Editamos el fichero smbldap_bind.conf:
nano /etc/smbldap-tools/smbldap_bind.conf

# Dejamos sólo un servidor Master, suprimimos el slave:
masterDN="cn=admin,dc=sanclemente,dc=local"
masterPW="admin"

# Editamos el fichero smbldap.conf:
nano /etc/smbldap-tools/smbdldap.conf

# Modificamos los siguiente parámetros:
sambaDomain=sanclemente
slapTLS="0"  // No usamos SSL
suffix="dc=sanclemente, dc=local"
sambaUnixIdPooldn="sambaDomainName=SANCLEMENTE,${suffix}"
userSmbHome="\\%L\%U"
userProfile="\\%L\profiles\%U"
mailDomain="sanclemente.local"


# Editamos el fichero slapd.con para crear unos índices necesarios para acelerar
nano /etc/ldap/slapd.conf

# Agregamos:
index default  sub
index cn   pres, sub,eq
index sn   pres, sub,eq
index mail  eq, subinitial
index uid  pres,sub,eq
index displayName  pres,sub,eq
index uidNumber  eq
index gidNumber eq
index memberUid eq
index sambaSID  eq
index sambaPrimaryGroupSID eq
index sambaDomainName eq

# Ejecutamos el test para ver si está todo ok:
slaptest

# Para poder comenzar a usar las herramientas que nos permiten integrar todo, deberemos ejecutar
# este comando construirá todas las estructuras para que LDAP y SAMBA puedan funcionar juntos:
smbldap-populate

# Ahora podemos hacer:
slapcat

# Paramos openldap:
/etc/init.d/slapd stop

# Regeneramos los índices:
slapindex -vf  /etc/slap/slapd.conf

# Cambiamos el propietario de esos ficheros índices:
/etc/ldap/chown openldap.openldap /var/lib/ldap/*

# Arrancamos de nuevo LDAP:
/etc/init.d/slapd start

# Para añadir un usuario:
# -a para que lo añada también en UNIX
# Añadimos un usuario guest:
smbldap-useradd -a guest

# Añadimos otro usuario prueba:
smbldap-useradd  -a prueba

# Para modificar la clave del usuario prueba:
```

```
smbldap-passwd prueba

# Vamos a ver si autentifica con samba:
# Creamos una carpeta:
mkdir pruebas
mkdir /home/publico

mount -t smb //localhost/publico pruebas/ -o username=prueba

# Directorio de drivers de impresoras:
/var/lib/samba/printers
```

Una vez tenemos todo funcionando...

A los windows se les puede meter PGINA para que autentiquen contra el LDAP.

Fuente original de información extraída del video: http://tv.uvigo.es/video/26832 de la **Charla del profesor Jose Ramón Méndez Reboredo.** Universidad de Vigo.

--Veiga 16:47 30 mar 2012 (CEST)