Administración de Sistemas Informáticos
Práctica 7ª: Configurar LDAP

Aitor Acedo y Cristina Puértolas

12 de Agosto de 2003

Powered by LaTeX.

Contents

1 Configuración del Servidor LDAP

Lo primero que hemos hecho para utilizar LDAP como sustituto de NIS ha sido instalar en la máquina servidor, en este caso gizmo, los siguientes paquetes, slapd y ldap-utils.

Durante la instalación del paquete slapd nos pide una serie de opciones de configuración que son detalladas a continuación:

(1) Utilización de ficheros ldif para la creación del directorio.
(2) El archivo que contendrá el contenido inicial del directorio será el siguiente /home/aitor/practica7/ldif/entradas.ldif, con el siguiente contenido:

dn: dc=asi,dc=cps,dc=unizar,dc=es
objectClass: dcObject
objectClass: organization
o: asiOrg
dc: asi
description: Organizacion en ASI

dn: cn=Admin,dc=asi,dc=cps,dc=unizar,dc=es
objectClass: organizationalRole
cn: Admin
description: Administrador del Directorio

(3) El nombre del dominio base del directorio será (DN):
dc=asi,dc=cps,dc=unizar,dc=es
(4) La entrada del administrador del directorio será:
cn=Admin,dc=asi,dc=cps,dc=unizar,dc=es
(5) No replicaremos la información contenida en el directorio a otro servidor LDAP, es decir, no tendremos un servidor LDAP esclavo.

Una vez terminada la configuración comprobaremos que el contenido del directorio es el correcto con el siguiente comando:

slapcat | less

Ahora modificaremos algunas entradas dentro del fichero de configuración del servidor /etc/ldap/slapd.conf quedando el contenido del mismo de la siguiente manera:

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/inetorgperson.schema

schemacheck on

pidfile /var/run/slapd.pid

argsfile /var/run/slapd.args

replogfile /var/lib/ldap/replog

loglevel -1

database ldbm

suffix "dc=asi,dc=cps,dc=unizar,dc=es"

directory "/var/lib/ldap"

index objectClass eq

rootdn "cn=Admin,dc=asi,dc=cps,dc=unizar,dc=es"

rootpw secret

lastmod on

access to attribute=userPassword,loginShell,gecos
by dn="cn=Admin,dc=asi,dc=cps,dc=unizar,dc=es" write
by self write
by * read
```

access to *
by dn="cn=Admin,dc=asi,dc=cps,dc=unizar,dc=es" write
by * read

Ahora tendremos que parar el servidor LDAP con:

#/etc/init.d/slapd stop

Y volver a arrancarlo:

#/etc/init.d/slapd start

En este momento tendremos que añadir más entradas dentro del directorio gracias a las herramientas proporcionadas con el paquete ldap-utils.

$ ldapadd -D "cn=Admin,dc=asi,dc=cps,dc=unizar,dc=es" -x -W -f /path/foo.ldif

Los ficheros que añadiremos al directorio serán los siguientes, users2.ldif y peopleGroup.ldif.

Nos perdirá la password que hemos introducido en el fichero de configuración del servidor a continuación de la entrada rootpw.

Nota: El fichero /etc/ldap/ldap.conf en el servidor permanecerá intacto.

2 Configuración del Cliente LDAP

Para comenzar la configuración del cliente LDAP tendremos que tener instaladas algunas librerías, como por ejemplo libnss-ldap, libpam-ldap y algún paquete útil como ldap-utils.

Durante el proceso de instalación nos pedirán algunos parámetros para configuración de las librerías, estas opciones quedarán reflejadas en los ficheros

de configuración:
/etc/libnss − ldap.conf

host 155.210.154.194

base dc=asi,dc=cps,dc=unizar,dc=es

ldap_version 3

nss_base_passwd ou=People,dc=asi,dc=cps,dc=unizar,dc=es?one
nss_base_shadow ou=People,dc=asi,dc=cps,dc=unizar,dc=es?one
nss_base_group ou=Group,dc=asi,dc=cps,dc=unizar,dc=es?one

/etc/pam_ldap.conf

host 155.210.154.194

base dc=asi,dc=cps,dc=unizar,dc=es

ldap_version 3

pam_password crypt

También tendremos que modificar el fichero de configuración /etc/ldap.conf que acabará con el siguiente contenido:

BASE dc=asi,dc=cps,dc=unizar,dc=es

HOST 155.210.154.194
PORT 389

Ahora tendremos que realizar la prueba de si el cliente es capaz leer la información del directorio referente a los usuarios y a los grupos, para ello utilizaremos el comando sudo, como se muestra:

$ sudo -u '#1222' touch foo
Nota: 1222 es el identificador del ususario introducido en el directorio

Para que el comando funcione correctamente deberemos tener el contenido del fichero sudoers como sigue:

root ALL=(ALL) ALL
kaipy ALL=(ALL)NOPASSWD:ALL
aitor ALL=(ALL)NOPASSWD:ALL

Nota: Es muy importante los parentesis ya que indicarán que el se podrá utilizar en cualquier máquina.

Antes de la prueba tendremos que configurar el fichero /ect/nsswitch.conf y cambiaremos la configuración de pam:
/etc/nsswitch.conf

passwd: files ldap
group: files ldap
shadow: files ldap

hosts: files dns
#hosts: files nis
networks: files

protocols: db files
services: db files
ethers: db files
rpc: db files

netgroup: nis

/etc/pam.d/passwd

password sufficient pam_ldap.so
password sufficient pam_unix.so
password required pam_deny.so

/etc/pam.d/sudo

auth required pam_ldap.so

Comprobamos que el fichero 'foo' se ha creado con el propietario adecuado y después para configurar la autentificación con LDAP tendremos que cambiar el contenido del fichero siguiente:

/etc/pam.d/login

```
    auth required /lib/security/pam_env.so
auth sufficient /lib/security/pam_unix.so likeauth nullok
auth sufficient /lib/security/pam_ldap.so use_first_pass
auth required /lib/security/pam_deny.so

account sufficient /lib/security/pam_unix.so
account required /lib/security/pam_ldap.so

session required /lib/security/pam_unix.so
session optional /lib/security/pam_ldap.so
```

Únicamente nos quedará probar a autentificarnos en la máquina cliente LDAP con el usuario introducido en el directorio.