LDAP: configuració del servidor i sistema d'autenticació

Amb aquest article pretenem mostrar-vos com instal·lar un servidor LDAP per tal d'autenticar els clients i també com configurar els clients LDAP per a que puguin autenticar-se contra aquest servidor.

Cal recordar que LDAP és un "Directori Lleuger", que tan pot emprar-se per autenticar els clients com per recopilar altres tipus d'informació (des de col·leccions de distribucions de Linux fins a resoldre noms).

Introducció

Farem servir la implementació OpenLDAP, que podem trobar a http://www.openldap.com. De tota manera, aquí ens basarem en els paquets Debian (sid, però és semblant a la resta) per fer-ho.

Podem veure a LDAP com una base de dades optimitzada per realitzar un elevat nombre de lectures i molt poques escriptures o modificacions. A més, està organitzat de manera molt jeràrquica.

Molt sovint (com ara en aquest article) es fa servir LDAP per desar informació dels usuaris. Podem desar allò més típic com ara l'Àlies, l'UID, el GID, la contrasenya, etc... i afegir-hi una fotografia, el telèfon de casa i altres informacions que ens siguin necessàries. Remarcar que en aquest article desarem la informació necessària per a un servidor d'autenticació, no per a un servidor de fitxers. Si ens cal un servidor de fitxers, haurem de fer servir NFS (o Coda, Intermezzo, etc...)

Instal·lació del servidor

Al servidor ens caldrà tenir instal·lats els paquets *libldap2 slapd*. Podem instal·lar a més el paquet *ldap-utils* que ens servirà per realitzar determinades proves.

Un cop instal·lat el servidor OpenLDAP anirem al directori */etc/ldap* i modificarem el fitxer *slapd.conf*. Al fitxer hi modificarem com a mínim el suffix posant, per exemple el nostre domini (no cal que estigui registrat, és per referir-nos a ell des de LDAP). El posarem amb el format `suffix "dc=pinux,dc=info"`.

Hi afegirem també:

```
rootdn "cn=admin,dc=pinux,dc=info"  #per autenticar l'administrador
rootpw secret                       #la contrasenya
```

(la contrasenya la podem xifrar, al final del document veurem com fer-ho)

A la resta del fitxer de configuració només haurem de canviar el cn= i el dc=pinux,dc=info als llocs on sigui necessari.

Un cop enllestit, podem fer `/etc/init.d/slapd restart` per arrencar de nou el servidor LDAP.

Si executem `slapcat` ens hauria de donar informació sobre el nostre LDAP (normalment imprimeix per pantalla tot l'LDAP, de moment només en veurem alguna cosa de l'estructura).

Alta, cerca i eliminació d'usuaris

Ara doncs, el que haurem de fer és donar d'alta alguns usuaris per poder-los autenticar després.

Abans però de donar d'alta els usuaris i els grups, haurem de donar d'alta l'administrador, un usuari per "buscar" la informació sense privilegis i finalment, algun usuari normal que ens permeti verificar que el sistema ens funciona correctament.

Per donar d'alta a usuaris (o dades en general) a l'LDAP s'acostuma a fer mitjançant fitxers .ldif. Un fitxer .ldif conté la informació que afegirem, per afegir-la després al nostre directori.

Abans de començar a donar d'alta els usuaris, crearem l'"estructura" mitjançant aquest fitxer .ldif:

```
dn: ou=Group,dc=pinux,dc=info
objectClass: top
objectClass: organizationalUnit
ou: Group
dn: ou=People,dc=pinux,dc=info
objectClass: top
objectClass: organizationalUnit
ou: People
```

D'aquesta manera tenim dos "Organization Units" que són els grups (Groups) i els usuaris (People).

Cal observar que estem fent servir el *objectClass: organizationalUnit*, d'aquesta manera l'LDAP ja sap quins camps tindran els nostres usuaris/grups Per dir-li a l'LDAP que inserti les dades del fitxer .ldif a la base de dades executarem:

```
ldapadd -x -D 'cn=admin,dc=pinux,dc=info' -w secret -f fitxer.ldif
```

Anotacions:

- Amb -x ens autentiquem de manera simple a LDAP, sense fer servir SASL.
- Al -D li diem el Distinguised Name, el mateix que li vam posar al fitxer de configuració.
- Al -w li passem la contrasenya. Amb -W ens la demanaria de forma interactiva.
- Al -f serveix para passar-li el fitxer de configuració.

A continuació, donarem d'**alta un usuari**. Seguirem el mateix esquema que hem fet servir fins ara, creant un fitxer .ldif i executant la utilitat `ldapadd`. El fitxer .ldif per donar d'alta un usuari pot ser com aquest:

```
#
# New Tester user
#
dn: uid=tester,ou=People,dc=pinux,dc=info
objectClass: top
objectClass: account
objectClass: posixAccount
uid: tester
cn: Test User
userPassword: hola
gecos: Test User
uidNumber: 2000
gidNumber: 2000
homeDirectory: /home/tester
loginShell: /bin/bash
```

I a continuació:

```
ldapadd -x -D 'cn=admin,dc=pinux,dc=info' -w secret -f fitxer.ldif
```

Ara ja podem executar `slapcat` per veure si l'usuari tester està llistat correctament.

Quan fem un `slapcat` ens està fent un llistat en format .ldif (el podríem aprofitar pel que convingués).

Ja que estem donant d'alta usuaris, donem d'alta un grup. Per fer-ho crearem un fitxer .ldif amb aquest contingut:

```
#
# Testing Group
#
dn: cn=testing,ou=Group,dc=pinux,dc=info
objectClass: top
objectClass: posixGroup
cn: testing
gidNumber: 2000
```

Ja tenim un grup amb GID 2000.

També podem aprofitar per **fer cerques**:

```
ldapsearch -x -b 'uid=tester,ou=People,dc=pinux,dc=info'
```

Finalment, si volem **eliminar un usuari** podem fer-ho així:

```
ldapdelete -x -D 'cn=admin,dc=pinux,dc=info' -w secret 'cn=Local Root,ou=People,dc=pinux,dc=info'
```

Configurant un client LDAP

L'objectiu d'aquest apartat és poder fer un `slapcat` des d'una màquina que no sigui el servidor i que funcioni correctament.

Per aconseguir-ho, haurem d'instal·lar com a mínim els paquets *libldap2, ldap-utils*.

Un cop instal·lats els paquets, editarem el fitxer `/etc/ldap/ldap.conf`. Aquest fitxer és el de configuració del client LDAP, cal no confondre'l amb el fitxer `slapd.conf`, que és el de la configuració del servidor.

El fitxer el podem deixar així:

```
host 192.168.1.2
base dc=pinux,dc=info
```

D'aquesta manera li estem dient a on ha de connectar-se i el dc.

Ara, des de la màquina client podem fer servir `slapcat` tal com ho hem fet abans. La configuració per defecte permet la lectura de diversos camps per "tot el món", de manera que encara que no podrem veure la contrasenya, sí que podrem veure informació diversa de l'usuari.

Configurant un client, part nsswitch

Per dur a terme aquesta part, haurem d'instal·lar el paquet `libnss-ldap`.

Quan treballem amb el sistema (`ls -l`, p.e.) normalment podem veure els noms dels usuaris propietaris dels fitxers. Al disc, però, el que s'hi desa és el "número" (UID) d'usuari.

Per tal que els programes puguin saber el nom que correspon a cada UID (i altres coses, com els

grups, els hosts, etc.) fan una crida a funcions de la llibreria GLIBC, i és aquesta la que “esbrina” la relació.

És al fitxer `/etc/nsswitch.conf` on li diem al sistema a on ha d'esbrinar qui és el propietari sabent l'UID. Normalment conté alguna cosa semblant a:

```
passwd:         compat
group:          compat
shadow:         compat
hosts:          files dns
networks:       files
```

El que més ens interessa és la part de passwd, group y shadow. Ho deixarem així:

```
passwd:         compat ldap
group:          compat ldap
shadow:         compat ldap
```

Així doncs, quan un programa li demana a la GLIBC “vull saber el nom de l'usuari 1005”, la GLIBC primer mira a `/etc/passwd` i si no el troba ho consultarà al servidor LDAP.

Per a que l'nsswitch pugui fer les consultes a l'LDAP tindrem al fitxer `/etc/libnss-ldap.conf` alguna cosa com ara:

```
host 192.168.1.2
base dc=pinux,dc=info
```

És a dir, la informació necessària per arribar al nostre servidor LDAP i fer la consulta.
Si fem `man libnss-ldap.conf` podrem veure les opcions que hi podem posar (p. ex. port, ldap_versions, etc.)

Entre altres coses, a vegades ens caldrà que es faci una connexió autenticada contra el servidor. Per fer-ho es farà servir la contrasenya que trobi a `/etc/ldap.secret` (Cal que estigui amb permisos 600, propietari i grup root)

Configurant el client PAM

Per poder configurar el client PAM haurem d'instal·lar el paquet `libpam-ldap`. Hi ha diversos programes que poden fer servir (i que per utilitzen defecte) un mètode d'autenticació "centralitzat" i per mòduls anomenat PAM (Pluggable Authentication Modules). Són unes llibreries suportables pels programes que serveixen d'interfície contra diversos mètodes d'autenticació (p.e. LDAP)

La configuració en Debian és al directori `/etc/pam.d/` on tenim un fitxer de configuració per cadascun dels serveis.

Si la connexió ha de ser amb privilegis, es farà servir la contrasenya que hi hagi a `/etc/ldap.secret`, i que tindrà permisos 600 (com a l'apartat anterior).

Cal disposar de la contrasenya necessària per autenticar-se, amb la configuració per defecte de l'`slapd.conf`, quan l'usuari root vulgui canviar la contrasenya d'un altre usuari. Si no és una connexió autenticada, el servidor LDAP no li deixarà canviar-la. Si no fos així, qualsevol usuari podria canviar la contrasenya d'un altre usuari només formulant la consulta al servidor LDAP.

A continuació, deixarem el fitxer `/etc/pam_ldap.conf` d'una manera semblant a aquesta:

```
host 192.168.1.2
base dc=pinux,dc=info
ldap_version 3
```

```
rootbinddn cn=admin,dc=pinux,dc=info
# don't forget /etc/ldap.secret
```

Ara ja tenim la configuració general del PAM per funcionar amb LDAP.
Passarem a la part específica de cada servei (ssh, su, passwd, etc.).
Estarem tocant els fitxers de configuració del client per tal que s'autentiqui contra el servidor.

ssh

Hem d'anar al fitxer `/etc/pam.d/ssh` i afegir, com a mínim, aquestes línies:

```
auth       sufficient   pam_ldap.so
account    sufficient   pam_ldap.so
session    sufficient   pam_ldap.so
password   sufficient   pam_ldap.so
```

a l'inici del fitxer.

En el cas de l'ssh, segurament haurem de modificar al fitxer `/etc/ssh/sshd_config` el paràmetre `PAMAuthenticationViaKbdInt` a `yes`. Si no ho fem no autenticaria correctament.

su

Serveix per poder executar el `su` amb usuaris que estan donats d'alta a l'LDAP.

El fitxer `/etc/pam.d/su` el deixarem d'una manera semblant a :

```
auth       sufficient pam_rootok.so
auth       sufficient pam_ldap.so
auth       required   pam_unix.so use_first_pass
account    sufficient pam_ldap.so
account    required   pam_unix.so
session    sufficient pam_ldap.so
session    required   pam_unix.so
```

passwd

Aquest és per permetre canviar les contrasenyes dels usuaris. El podem deixar així:

```
password        sufficient      pam_ldap.so
password        required        pam_unix.so nullok obscure min=4 max=8
```

És força útil donar d'alta als usuaris de forma normal i canviar-los la contrasenya amb el mateix passwd com a root (si tenim pocs usuaris de proves, és clar)

login

El deixarem semblant a aquest:

```
auth        required      pam_nologin.so
auth        sufficient    pam_ldap.so
auth        sufficient    pam_unix.so shadow use_first_pass
auth        required      pam_deny.so
```

Hi ha altres maneres, però hem d'anar amb compte amb l'`use_first_pass`: si no el posem, als usuaris que estiguin donats d'alta a l'LDAP se'ls demanaria dues vegades la contrasenya. Una

validaria amb `/etc/passwd`, i al no trobar l'usuari, li demanaria una altra vegada per validar-lo contra LDAP.

Amb els exemples que hem vist fins ara, hauria de ser fàcil fer el mateix amb altres serveis (p. ex. proftpd, xlock, etc.)

També és relativament fàcil modificar els fitxers `common-account common-auth common-password common-session` per no haver de tocar els fitxers de cada servei, a despit de tenir menys "personalització" per cada servei.

Podem millorar

Tenim algunes coses més per fer. Només en comento algunes:

- Per començar, la contrasenya "secret" que la tenim en text pla al fitxer, posar-la xifrada (i una contrasenya de veritat). Per fer-ho executarem `slappasswd` i la que ens doni la posarem al fitxer. Per exemple: `{SSHA}xAR4MvR0AByRx0gYCZGKeWUFAhNGZIud`.
- També hauríem de fer servir certificats perquè ningú pugui suplantar el nostre servidor. I ja que hi som posats, que les dades es transfereixin de forma segura. El mateix OpenLDAP pot fer-ho, com podem llegir en aquest altre article de Bulma. Això ens interessarà sobretot si els clients LDAP i el servidor LDAP no estan a la mateixa xarxa (o que la xarxa no sigui de confiança). Una altra manera de fer-ho seria amb freeswan (una implementació d'IPSEC) o fent túnels segurs amb altres aplicacions.
- Un cas força habitual és voler migrar els usuaris que ja teníem al sistema cap a OpenLDAP. Ho podem aconseguir amb el paquet migrationtools
- Un darrer comentari important és instal·lar el paquet `nscd`. Aquest paquet farà de memòria cau per l'OpenLDAP a la màquina local. Sinó, cada vegada que fem un "ls -l" el sistema preguntarà a l'LDAP “aquest usuari, quin nom té? (carregant així el servidor, la xarxa i, a més, el client respon més lentament)

Enllaços

Alguns enllaços interessants:

- El Web d' OpenLDAP
- Un Web sobre OpenLDAP en Debian
- Per saber com es comença a omplir OpenLDAP
- Els dos genials articles de Bulma sobre LDAP: servidor i client

---

Direcció de Bulma: http://bulma.net/body.phtml?nIdNoticia=1991

Articles relacionats de Bulma 1343 1371
Carles Pina i Estany carles@pinux.info

Traduit al català per Àngel Mompo (*mecatxis*) i *Wildrord* per Catux (http://www.catux.org).