LDAP Autenticazione

Autenticazione utenti tramite PAM e LDAP

Author: Andrea Manni

Version: 0.3

Appunti sull'installazione e configurazione di un sistema di autenticazione distribuito per sistemi operativi Debian Gnu/Linux (e derivati) basato su LDAP.

Questa guida resta come riferimento per gli operatori del progetto Netgarage a Modena e come reference della sessione di laboratorio tenuta da Andrea Manni in occasione del Linux Day 2009 sempre a Modena.

--

Indice

Generato con: http://docutils.sourceforge.net/rst.html

Concetti generali

Un sistema di autenticazione serve a identificare l'utente (la persona) di un servizio (ad es. l'accesso alla propia casella email, a una cartella condivisa, o allo stesso sistema operativo al momento del *log-in*). La procedura tipica prevede l'accoppiata di due elementi: un *nome-utente* per identificare l'utente (UID) e un *segreto* (in genere una password) conosciuto solo da questo. A seconda dello scenario e delle esigenze la *segretezza* puo' essere garantita da sistemi piu' o meno sofisticati: criptazione, ash, supporti fisici removibili, parametri biometrici).

E' importante distinguere tra un sistema di autenticazione e uno di *autorizzazione*: mentre il primo serve per accertare l'identita' dell'utente il secondo viene utilizzato per negoziare l'accesso a diversi servizi che l'utente potrebbe avere a disposizione.

Configurazione Client

I clients dovranno effettuare la procedura di autenticazione interrogando il server LDAP, che manterra' all'interno della sua directory i dati relativi a username, passwords e eventuali informazioni aggiuntive (ad esempio nome e cognome, email, percorso della home directory dell'utente, shell utilizzata).

Le informazioni ottenute dal Server LDAP verranno utilizzate al posto dei file utilizzati normalmente per le procedure di autenticazione:

- /etc/passwd
- /etc/shadow

In caso di non disponibilita' temporanea del server LDAP e' possibile configurare il client per utilizzare comunque i file locali, in modo da poter accedere al sistema con un utente inserito localmente (valido anche per l'utente *root* locale).

Il server LDAP andra' interrogato per i soli utenti di sistema, generalmente caratterizzati da una *UID* superiore a 1000, altri utenti validi utilizzati per funzioni di servizio (demoni e root) continueranno a essere gestiti tramite i file disponibili in locale. Questo sia per non caricare inutilmente i server, intasare la rete con traffico evitabile, ottimizzare le prestazioni del sistema operativo client (l'autenticazione in locale e' praticamente istantanea).

Pacchetti da installare

Installare i pacchetti:

```
ldap-utils libpam-ldap libnss-ldap nscd
```

Assicurarsi di impostare i valori corretti per `dn` e utente amministratore: quest'ultimo talvolta non e' consistente nei valori preimpostati (compare `admin` o in alternativa `manager`).

Links:

- http://wiki.archlinux.org/index.php/HOWTO-LDAP-authentication
- http://wiki.debian.org/LDAP/PAM
- http://www.linux.com/feature/114074?theme=print
- http://wiki.linuxquestions.org/wiki/Pam_ldap

Configurazione Client Ubuntu 9.10

Per la configurazione delle Ubuntu 9.10 *Karmik* nella modalita' *chiosco per navigazione in internet* usata all'interno dei Netgarage, e' sufficiente modificare solo i files di configurazione del client LDAP (/etc/ldap/ldap.conf) e la sessione standard di autenticazione di PAM: /etc/pam.d/common-session. Vengono qui riportati anche gli altri file di configurazione di una Debian Lenny (5.03) per abilitare tutte le altre funzionalita' delle workstation.

/etc/ldap/ldap.conf

/etc/ldap/ldap.conf LDAP Defaults

```
BASE    dc=garage
URI     ldap://garage

SIZELIMIT       12
TIMELIMIT       15
```

Client esterni alla rete privata

I client che dovranno accedere al server LDAP dall'esterno della rete locale dovranno aggiungere i riferimenti per raggiungere il server e specificare una connessione criptata con disponibilita' ad accettare il certificato del server:

```
BASE    dc=garage
HOST    garage.piffa.net
URI     ldaps://garage
TLS_REQCERT allow

SIZELIMIT       12
TIMELIMIT       15
```

Dato che questi host non sono serviti dal DNS interno sara' poi necessario aggiungere una voce a /etc/resolv.conf:

> 83.216.162.15 garage.piffa.net garage

/etc/nsswitch.conf

/etc/nsswitch.conf

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

hosts:          files dns
networks:       files

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

netgroup:       nis
```

Lenny non gradisce file al posto di compat per passwd, group, shadow. o

/etc/libnss-ldap.conf

/etc/libnss-ldap.conf

riga 60:

```
scope sub
bind_policy soft
```

La bind policy sarebbe alla riga 78

Volendo si potrebbero mettere qua altri parametri:

```
timelimit 5
bind_timelimit 5
nss_reconnect_tries 2
pam_login_attribute uid
pam_member_attribute gid
pam_password md5
pam_password exop
nss_base_passwd         ou=People,dc=garage
nss_base_shadow         ou=People,dc=garage
```

/etc/pam.d/common-auth

/etc/pam.d/common-auth - authentication settings common to all services

```
auth    sufficient      pam_unix.so nullok_secure
auth    requisite       pam_succeed_if.so uid >= 1000 quiet
auth    sufficient      pam_ldap.so use_first_pass
auth    required        pam_deny.so
auth    required        pam_unix.so nullok_secure
```

/etc/pam.d/common-account

/etc/pam.d/common-account - authorization settings common to all services

```
auth    sufficient      pam_unix.so nullok_secure
auth    requisite       pam_succeed_if.so uid >= 1000 quiet
auth    sufficient      pam_ldap.so use_first_pass
auth    required        pam_deny.so
# Next line is Lenny Default
auth    required        pam_unix.so nullok_secure
```

/etc/pam.d/common-password

/etc/pam.d/common-password - password-related modules common to all services

```
password    sufficient    pam_unix.so md5 obscure  nullok try_first_pass
password    sufficient    pam_ldap.so
password    required      pam_deny.so
```

Nota: password required potrebbe contenere un Ming=7 per fissare la lunghezza minima della password a 7 caratteri.

/etc/pam.d/common-session

Per creare automaticamente la *home directory* dell'utente al primo log-in si utilizzi l'ultima voce. Questo deve essere ripetuto anche per GDM / KDM o qualsiasi altro log-in manager l'utente possa utilizzare per effettuare il primo log in.

/etc/pam.d/common-session - session-related modules common to all services

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

/etc/pam.d/sshd

NON *necessario!*

Usando i numeri degli uid non ci dovrebbero essere problemi.

Inserire all'inizio:

```
auth    sufficient      pam_ldap.so
account sufficient      pam_permit.so
```

/etc/pam.d/su

NON *necessario!*

Usando i numeri degli uid non ci dovrebbero essere problemi.

Inserire all'inizio:

```
auth    sufficient      pam_ldap.so
account sufficient      pam_permit.so
```

/etc/pam.d/gdm

Nota: se il primo log-in dell'utente avviene in grafica e tramite GDM sara' necessario che la home dir dell'utente venga creata in quel momento.

/etc/pam.d/gdm Configurazione del log in grafico gdm:

```
auth     sufficient     pam_ldap.so
auth     required       pam_nologin.so
auth     required       pam_env.so
auth     required       pam_unix_auth.so

account  sufficient     pam_ldap.so
account  required       pam_unix_acct.so

password required       pam_ldap.so
# Next row is for auto-create home dir at first log-in
session required        pam_mkhomedir.so skel=/etc/skel/ umask=0022

session  sufficient     pam_ldap.so
session  required       pam_unix_session.so
```

nota : questo andrebbe fatto anche per lo screen saver.

Loggin degli utenti

man slapo-accesslog

Home utenti distribuite

Server

Schema per LDAP

Autofs on LDAP

To store eg. auto.home maps on LDAP you can use the following format (user and home mapping shown):

> dn: uid=auser,ou=People,dc=example,dc=com uid: auser uidNumber: 1044 gidNumber: 501 gecos: A. User,,, homeDirectory: /home/auser loginShell: /bin/bash
>
> dn: cn=auser,ou=auto.home,dc=example,dc=com objectClass: automount cn: auser automountInformation: -rw,soft,intr,quota homeserver:/export/home/&

NFS

Aggiungere ad /etc/exports

```
/home/users/ 192.168.0.0/24(rw,sync,no_subtree_check)
```

Provare prima a creare la home di un utente, se tutto funziona con l'automount allora vedere se GDM e' in grado di creare la home dell'utente al primo log in (grafico).

Client

Installare i pacchetti:

```
autofs autofs-ldap
```

Aggiungere a `/etc/auto.master` la mappatura per le home directory sul server NFS, es:

```
/home/users  ldap:garage:ou=auto.home,dc=garage
```

In questo modo i le informazioni sulle home directory verranno servite da LDAP, quindi sara' necessario creare un voce all'interno di "ou=auto.home" per ogni nuovo utente. Esempio di un file LDIF:

```
# Esportazione LDIF per: cn=pippo,ou=auto.home,dc=garage

dn: cn=pippo,ou=auto.home,dc=garage
objectClass: automount
automountInformation: -rw,hard,intr garage:/home/users/pippo
cn: pippo
description: Pippo Home Dir
```

Controllare i dati per l'IP del server NFS dentro ldap. dovrebbe puntare a garage.

Creazione delle directory per gli utenti al primo log in

Utilizzando NFS come filesytem per le home directory degli utenti si pone il problema della creazione della loro *home directory*. Questa non potra' essere attivata dal client tramite `common-session` o simile, dato che NFS non permette di accedere al file system come **root**, a meno che non si disabiliti il `no_root_squash` nelle opzioni di mount del file system stesso sul client. Cosa preferibilmente da evitare per ovvi motivi di sicurezza ed altro (nel caso non si potesse fare altrimenti almeno si monti il filesytem `nosuid , noexec` sul server).

Le alternative allora diventano:

1. Creare direttamente la directory con i giusti permessi e popolarla da `/etc/skell` al momento di inserire gli utenti nella directory LDAP, e comunque da *lato server*.
2. Utilizzare un filesytem di rete che preveda l'autenticazione del client.

Caveat

Allo stato attuale GDM o quant'altro nono crea la home dir dell'utente se non e' montata la directory genitrice. Si puo' ovviare al problema montando l'intera home esportata dal server, a questo punto il client riesce a creare la directory dell'utente. Oppure si potrebbe creare la home dell'utente con relativi permessi quando viene creato l'utente.

Propenderei per la seconda: l'alternativa e' abbandonare autofs.

Altra cosa interessante:

All User Entry

If you want all users to be able to mount their home directory, but don't want to add an entry for each user, you will take the following:

```
dn: cn=tux,ou=auto.home,dc=example,dc=com
cn: tux
objectClass: automount
automountInformation: -rsize=8192,wsize=8192,intr NfsServer.example.com:/home/tux
```

Altra cosa da vedere: /etc/default/autofs come riportato in /usr/share/doc/autofs-ldap/README.ldap_master

Vedere:
http://forum.debianizzati.org/sicurezza/sso-server-kerberos-lenny-client-ubutu-810-t34710.0.html;wap2=

LDAP

Note su LDAP in generale.

Terminologia base

Breve ripasso dei termini di LDAP.

String	Attribute Type
dn	Distinguished Name
cn	Common Name
o	Organisational Name
ou	Organisational Unit Name
dc	Domain Component
uid	User Identification

Troubleshotting LDAP / NSCD

Per esplorare tutto l'albero:

```
ldapsearch -x -b dc=garage
```

Cercare un singolo utente:

```
ldapsearch -h garage -x uid=<username>
```

Cercare una utente nel sistema utilizzando "getent":

```
getent passwd eaman
```

Su puo' cercare anche dentro **shadow** (dovrebbero essere visibili solo gli utenti di sistema) e **groups**.

Caricare un file LDIF

Avendo un file LDIF es user.ldif:

```
ldapadd -x -D "cn=admin,dc="garage" -W -f user.ldif
```

LDAP su SSL

Creazione del certificato

Per creare un certificato monoblocco:

```
mkdir  /etc/ldap/ssl
cd /etc/ldap/ssl
openssl req -newkey rsa:1024 -x509 -nodes \
                -out slapd.pem -keyout slapd.pem -days 3650
# Make this readable to openldap only ..
chown -v openldap:openldap /etc/ldap/ssl/slapd.pem
chmod -v 400 /etc/ldap/ssl/slapd.pem
```

Il nome propio deve essere `garage`

Abilitare il certificato in slapd

/etc/ldap/slapd.conf

```
TLSCACertificateFile  /etc/ldap/ssl/slapd.pem
TLSCertificateFile    /etc/ldap/ssl/slapd.pem
TLSCertificateKeyFile /etc/ldap/ssl/slapd.pem
```

Far ascoltare il server sulla porta ssl 636: /etc/default/slapd

```
SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi:///"
```

Configurazione client con LDAP su SSL

I client esterni alla rete locali dovranno negoziare un accesso al server LDAP usando come riferimento l'FQDN `garage.piffa.net`, corrisondente *al momento* all'IP `83.216.162.15`.

Nel file `/etc/ldap/ldap.conf` avremo quindi:

```
BASE    dc=garage
HOST    garage.piffa.net
URI     ldaps://garage
TLS_REQCERT allow

SIZELIMIT       12
TIMELIMIT       15
```

Testare

1. far ripartire slapd: `/etc/init.d/slapd restart`
2. vedere se il server e' in ascolto: `netstat -plane |grep ":636"`
3. testare il certificato: `openssl s_client -connect localhost:636 -showcerts`

   modificare `/etc/ldap/ldap.conf`:

   ```
   URI     ldaps://garage
   TLS_REQCERT allow
   ```

4. Fare una query col debug: `ldapsearch -x -d8`
5. far partire il server in debug: `slapd -u openldap -d 256 -f /etc/ldap/slapd.conf`