LDAP Autenticazione

configurazione server per autenticazione utenti tramite PAM e LDAP

Author: Andrea Manni
Copyright: GFDL
Version: 0.2

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 il 2010-11-15 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 Server

La distribuzione di riferimento e' una Debian Gnu/Linux Lenny. Al lato server sara' necessario installare il server Slapd (il software vero e proprio per la gestione di LDAP), le utility per LDAP (`ldap-utils`) per poter caricare i primi dati e fare qualche query di debug.

Nel caso si voglia montare un'interfaccia web per la gestione degli utenti si dovra' mettere a disposizione:

- Un web server, testato con Apache2 o Nginx
- Interprete del linguaggio scelto (es. PHP)
- Il software vero e proprio (es. phpldapadmin)

Pacchetti da installare

Installare i pacchetti:

```
ldap-utils slapd
```

Alla prima installazione Debconf chiederà solamente di assegnare la password dell'amministratore (`admin` e non *manager*!), per poter configurare i restanti parametri si potra' intervenire direttamente sul file di configurazione: `/etc/ldap/slapd.conf` o lanciare un `dpkg-reconfigure`:

```
root@uml-squeeze:~# dpkg-reconfigure -f readline slapd
Stopping OpenLDAP: slapd.
Configuring slapd
-----------------

If you enable this option, no initial configuration or database will be created for you.

Omit OpenLDAP server configuration? n


The DNS domain name is used to construct the base DN of the LDAP directory. For example,
'foo.example.org' will create the directory with 'dc=foo, dc=example, dc=org' as base DN.

DNS domain name: piffa.net


Please enter the name of the organization to use in the base DN of your LDAP directory.

Organization name: piffa.net


Please enter the password for the admin entry in your LDAP directory.

Administrator password:


Please enter the admin password for your LDAP directory again to verify that you have typed
it correctly.

Confirm password:


The HDB backend is recommended. HDB and BDB use similar storage formats, but HDB adds
support for subtree renames. Both support the same configuration options.

In either case, you should review the resulting database configuration for your needs. See
/usr/share/doc/slapd/README.DB_CONFIG.gz for more details.

  1. BDB  2. HDB

Database backend to use: 2



Do you want the database to be removed when slapd is purged? n
```

```

There are still files in /var/lib/ldap which will probably break the configuration process.
If you enable this option, the maintainer scripts will move the old database files out of
the way before creating a new database.
```

```
Move old database? n


The obsolete LDAPv2 protocol is disabled by default in slapd. Programs and users should
upgrade to LDAPv3.  If you have old programs which can't use LDAPv3, you should select this
option and 'allow bind_v2' will be added to your slapd.conf file.

Allow LDAPv2 protocol? n


Moving old database directory to /var/backups:
There are leftover files in /var/lib/ldap. This will probably break
creating the initial directory. If that's the case please move away
stuff in there and retry the configuration.
Creating initial slapd configuration... done.
################## 100.00% eta   none elapsed            none fast!
Closing DB...
done.
Starting OpenLDAP: slapd.
```

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`).

Note:

1. Se si rilancia la configurazione assistita da Debconf si faccia attenzioni ai database di back-up creati in `/var/backups/`, ad esempio: `/var/backups/unknown-2.4.11-1.ldapdb/`. La presenza di questo previene la ri-configurazione del file `/etc/ldap/slapd.conf`: deve essere prima rimosso il file di backup.

/etc/ldap/slapd.conf

File di esempio con TLS abilitato:

```
# This is the main slapd configuration file. See slapd.conf(5) for more
# info on the configuration options.

########################################################################
# Global Directives:

# Features to permit
#allow bind_v2

# SSL crypt
TLSCACertificateFile  /etc/ldap/ssl/slapd.pem
TLSCertificateFile    /etc/ldap/ssl/slapd.pem
TLSCertificateKeyFile /etc/ldap/ssl/slapd.pem


# Schema and objectClass definitions
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile         /var/run/slapd/slapd.pid

# List of arguments that were passed to the server
argsfile        /var/run/slapd/slapd.args

# Read slapd.conf(5) for possible values
loglevel        none
#loglevel        256

# Where the dynamically loaded modules are stored
modulepath      /usr/lib/ldap
moduleload      back_hdb

# The maximum number of entries that is returned for a search operation
sizelimit 500

# The tool-threads parameter sets the actual amount of cpu's that is used
# for indexing.
tool-threads 1

########################################################################
# Specific Backend Directives for hdb:
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
backend         hdb

########################################################################
# Specific Backend Directives for 'other':
# Backend specific directives apply to this backend until another
```

```
# 'backend' directive occurs
#backend                <other>

########################################################################
# Specific Directives for database #1, of type hdb:
# Database specific directives apply to this databasse until another
# 'database' directive occurs
database        hdb

# The base of your directory in database #1
suffix          "dc=auth,dc=piffa,dc=net"

# rootdn directive for specifying a superuser on the database. This is needed
# for syncrepl.
# rootdn          "cn=admin,dc=auth,dc=piffa,dc=net"

# Where the database file are physically stored for database #1
directory       "/var/lib/ldap"

# The dbconfig settings are used to generate a DB_CONFIG file the first
# time slapd starts.  They do NOT override existing an existing DB_CONFIG
# file.  You should therefore change these settings in DB_CONFIG directly
# or remove DB_CONFIG and restart slapd for changes to take effect.

# For the Debian package we use 2MB as default but be sure to update this
# value if you have plenty of RAM
dbconfig set_cachesize 0 2097152 0

# Sven Hartge reported that he had to set this value incredibly high
# to get slapd running at all. See http://bugs.debian.org/303057 for more
# information.

# Number of objects that can be locked at the same time.
dbconfig set_lk_max_objects 1500
# Number of locks (both requested and granted)
dbconfig set_lk_max_locks 1500
# Number of lockers
dbconfig set_lk_max_lockers 1500

# Indexing options for database #1
index           objectClass eq

# Save the time that the entry gets modified, for database #1
lastmod         on
# Checkpoint the BerkeleyDB database periodically in case of system
# failure and to speed slapd shutdown.
checkpoint      512 30

# Where to store the replica logs for database #1
# replogfile    /var/lib/ldap/replog

# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
# These access lines apply to database #1 only
```

```
access to attrs=userPassword,shadowLastChange
        by dn="cn=admin,dc=auth,dc=piffa,dc=net" write
        by anonymous auth
        by self write
        by * none

# Ensure read access to the base for things like
# supportedSASLMechanisms.  Without this you may
# have problems with SASL not knowing what
# mechanisms are available and the like.
# Note that this is covered by the 'access to *'
# ACL below too but if you change that as people
# are wont to do you'll still need this if you
# want SASL (and possible other things) to work
# happily.
access to dn.base="" by * read

# The admin dn has full write access, everyone else
# can read everything.
access to *
        by dn="cn=admin,dc=auth,dc=piffa,dc=net" write
        by * read

# For Netscape Roaming support, each user gets a roaming
# profile for which they have write access to
#access to dn=".*,ou=Roaming,o=morsnet"
#        by dn="cn=admin,dc=auth,dc=piffa,dc=net" write
#        by dnattr=owner write

#######################################################################
# Specific Directives for database #2, of type 'other' (can be hdb too):
# Database specific directives apply to this databasse until another
# 'database' directive occurs
#database        <other>

# The base of your directory for database #2
#suffix         "dc=debian,dc=org"
```

/etc/ldap/ldap.conf

Questo file contiene le informazioni per il client, i parametri qui riporati verranno usati per interrogare il database. Quanto segue e' un esempio per cuna connessione in chiaro:

```
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE   dc=example,dc=com
#URI    ldap://ldap.example.com ldap://ldap-master.example.com:666

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never
BASE    dc=auth,dc=piffa,dc=net
URI     ldap://auth.piffa.net/

SIZELIMIT       12
TIMELIMIT       15
DEREF           never
```

Per una connessione criptata tramite ldaps si usi:

```
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE   dc=example,dc=com
#URI    ldap://ldap.example.com ldap://ldap-master.example.com:666
BASE    dc=auth,dc=piffa,dc=net
# HOST non dovrebbe essere necessario se si dispone di un nome di dominio
HOST    auth.piffa.net
URI     ldaps://auth.piffa.net
TLS_REQCERT allow

SIZELIMIT      12
TIMELIMIT      15
DEREF          never
```

Generare il certificato SSL

Per generare un certificato:

```
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 proprio deve essere equivalente alla directory ldap, es. `garage`

/etc/default/slapd

Parametri di avvio del server slapd: per attivare TLS (criptazione) si dovra' modificare questo file:

```
# Default location of the slapd.conf file. If empty, use the compiled-in
# default (/etc/ldap/slapd.conf). If using the cn=config backend to store
# configuration in LDIF, set this variable to the directory containing the
# cn=config data.
SLAPD_CONF=

# System account to run the slapd server under. If empty the server
# will run as root.
SLAPD_USER="openldap"

# System group to run the slapd server under. If empty the server will
# run in the primary group of its user.
SLAPD_GROUP="openldap"

# Path to the pid file of the slapd server. If not set the init.d script
# will try to figure it out from $SLAPD_CONF (/etc/ldap/slapd.conf by
# default)
SLAPD_PIDFILE=

# slapd normally serves ldap only on all TCP-ports 389. slapd can also
# service requests on TCP-port 636 (ldaps) and requests via unix
# sockets.
# Example usage:
# SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi:///"
SLAPD_SERVICES="ldap:// ldaps:// ldapi://"

# If SLAPD_NO_START is set, the init script will not start or restart
# slapd (but stop will still work).  Uncomment this if you are
# starting slapd via some other means or if you don't want slapd normally
# started at boot.
#SLAPD_NO_START=1

# If SLAPD_SENTINEL_FILE is set to path to a file and that file exists,
# the init script will not start or restart slapd (but stop will still
# work).  Use this for temporarily disabling startup of slapd (when doing
# maintenance, for example, or through a configuration management system)
# when you don't want to edit a configuration file.
SLAPD_SENTINEL_FILE=/etc/ldap/noslapd

# For Kerberos authentication (via SASL), slapd by default uses the system
# keytab file (/etc/krb5.keytab).  To use a different keytab file,
# uncomment this line and change the path.
#export KRB5_KTNAME=/etc/krb5.keytab

# Additional options to pass to slapd
SLAPD_OPTIONS=""
```

La parte importante per TLS e': `SLAPD_SERVICES="ldap:// ldaps:// ldapi://"`. Si faccia a:

- Gli slash
- E' possibile evitare di precisare un IP o nome di dominio, e specificare solo il tipo di URI (`ldap`, `ldaps` , `ldapi`).

Popolare la directory

All'interno della directory LDAP venogo percaricati gli scemi precisati nel file `slapd.conf`:

```
# Schema and objectClass definitions
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
```

Altri file sono disponibili in: `/etc/ldap/schema/`

Ovviamente allo stato iniziale la directory dovrebbe essere praticamente vuota, a parte la organization unit (*ou*) creata in fase di installazione e l'amministratore. Per una prima query si lanci un `ldapsearch -x`:

```
root@uml-squeeze:/etc/ldap# ldapsearch -x
# extended LDIF
#
# LDAPv3
# base <dc=piffa,dc=net> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# piffa.net
dn: dc=piffa,dc=net
objectClass: top
objectClass: dcObject
objectClass: organization
o: piffa.net
dc: piffa

# admin, piffa.net
dn: cn=admin,dc=piffa,dc=net
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

In caso ci fossero problemi provare con una query in modalita' debug:

```
ldapsearch -x -d8
```

Eventualmente far partire il servizio `slapd` in modalita' di *debug* (o piu' precisamente con un livello di notifica eventi superiore al default):

```
slapd -u openldap -d 256 -f /etc/ldap/slapd.conf
```

Livelli di notifica di slapd

E' possibile impostare il server Slapd piu' *verboso* per gli eventi tracciati nel log, il parametro da modificare e' `loglevel`:

```
# Read slapd.conf(5) for possible values
loglevel        none
```

Possibili parametri sono (da http://www.zytrax.com/books/ldap/ch6/#loglevel):

```
number  hex-value log-name  Logging description
-1      0xFFFF              enable all logging
0       0x0000    -         logging inhibited - no logging occurs including critical errors. Not recommended.
1       0x1       acl       trace function calls
2       0x2       packets   debug packet handling
4       0x4       args      heavy trace debugging
8       0x8       conns     connection management
16      0x10      BER       print out packets sent and received
32      0x20      filter    search filter processing
64      0x40      config    configuration file processing
128     0x80      ACL       access control list processing
256     0x100     stats     stats log connections/operations/results
512     0x200     stats2    stats log entries sent
1024    0x400     shell     print communication with shell backends
2048    0x800     parse     print entry parsing debugging
4096    0x1000    cache     caching (unused)g
8192    0x2000    index     indexing (unused)
16384   0x4000    sync      print syncrepl (replica) logging
32768   0x8000    none      A misnomer - it will log message that are not categorized including curial messages
```

Caricare un file

Per caricare manualmente dei dati dentro alla directory si usi:

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

Alcuni file di esempio:

base.ldif:

```
dn: ou=Utenti,dc=piffa,dc=net
ou: Utenti
objectClass: top
objectClass: organizationalUnit

dn: ou=Group,dc=piffa,dc=net
ou: Group
objectClass: top
objectClass: organizationalUnit
```

groups.ldif:

```
dn: cn=ldapusers,ou=Group,dc=piffa,dc=net
objectClass: posixGroup
objectClass: top
cn: ldapusers
userPassword: {crypt}x
gidNumber: 9000
```

Si noti che il `gidNumber` viene inserito manualmente.

user.ldif:

```
dn: cn=User_name,ou=Utenti,dc=piffa,dc=net
cn: Utente Generico
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
sn: User_name
uid: user_id
uidNumber: 1025
gidNumber: 9000
homeDirectory: /home/users/
```

Si noti che i `gidNumber` e lo `uidNumber` vengono inseriti manualmente.

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

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 filesytem 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
```

Testare

1. far ripartire slapd: `/etc/init.d/slapd restart`
2. vedere se il server e' in ascolto per connessioni in chiaro: `netstat -plane |grep ":389"`
3. vedere se il server e' in ascolto per connessioni su SSL `netstat -plane |grep ":636"`
4. testare il certificato: `openssl s_client -connect localhost:636 -showcerts`

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

   ```
   URI     ldaps://piffa.net
   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`