

# Server OpenLDAP

LDAP, Lightweight Directory Access Protocol (protocollo leggero di accesso alle cartelle, ndt), è una versione semplificata del protocollo X500. Le impostazioni della directory in questa sezione, verranno utilizzate per l'autenticazione. Inoltre, una directory LDAP, può essere usata in molti modi: autenticazione, directory condivisa (per client di posta) o in ogni sorta di applicazione. LDAP è uno standard molto diffuso.

Per descrivere brevemente LDAP, tutte le informazioni vengono archiviate in una struttura ad albero. È necessario determinare la struttura della directory (il DIT, Directory Information Tree). Per iniziare, si consideri un albero base con due nodi sopra la radice:

- Il nodo «People» è dove i propri utenti vengono salvati
- Il nodo «Groups» è dove i propri gruppi vengono salvati

È necessario determinare quale deve essere la radice dell'LDAP. Di base, l'albero viene determinato dal proprio dominio internet. Se il dominio è example.com (quello usato nell'esempio di sopra), la radice è dc=example,dc=com

## Installazione

Prima di tutto, installare il demone ldap (slapd) nel server; installare i pacchetti slapd e ldap-utils.

Inserire il proprio dominio come richiesto e la password scelta per la directory dell'amministratore.

Solo poche modifiche devono essere apportate alla configurazione di base. Prima di tutto, impostare la password di amministrazione nel file di configurazione (invece che nella directory) modificando il file /etc/ldap/slapd.conf.

Non usare una password in chiaro. Per generare una password cifrata usare slappasswd:

```
$ slappasswd
New password:
Re-enter password:
{SSHA}d2BamRTgBuhC6SxC0vFGWol31ki8iq5m
```

L'esempio precedente mostra cosa succede quando viene usata la stringa «secret» come password (per la natura dello schema di cifratura di SSHA, il vostro risultato potrebbe essere differente)

Ora modificare il file /etc/ldap/slapd.conf copiando e incollando la stringa appena generata.

```
# Assicurarsi di modificare o aggiungere queste direttive dopo la prima
direttiva 'database' presente.
```

```
suffix          "dc=example,dc=com"
directory       "/var/lib/ldap"
rootdn          "cn=admin,dc=example,dc=com"
rootpw         {SSHA}d2BamRTgBuhC6SxC0vFGWol31ki8iq5m
```

## Popolare LDAP

La directory è stata creata durante l'installazione, adesso è necessario popolarla. Verrà popolata con una voce "classica" che sarà compatibile con la directory (per esempio per una directory condivisa), con account classici (per un'applicazione web) e con account Unix (posix).

La directory LDAP può essere riempita con un file ldif (ldif indica «ldap directory interchange

format»). Creare il file di esempio «init.ldif» in un percorso qualsiasi del proprio sistema.

```
dn: dc=example,dc=com
objectClass: dcObject
objectClass: organizationalUnit
dc: example
ou: Example Dot Com

dn: ou=people,dc=example,dc=com
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=example,dc=com
objectClass: organizationalUnit
ou: groups

dn: uid=john,ou=people,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: john
sn: Doe
givenName: John
cn: John Doe
displayName: John Doe
uidNumber: 1000
gidNumber: 10000
userPassword: password
gecos: John Doe
loginShell: /bin/bash
homeDirectory: /home/john
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: john.doe@example.com
postalCode: 31000
l: Toulouse
o: Example
mobile: +33 (0)6 xx xx xx xx
homePhone: +33 (0)5 xx xx xx xx
title: System Administrator
postalAddress:
initials: JD

dn: cn=example,ou=groups,dc=example,dc=com
objectClass: posixGroup
cn: example
gidNumber: 10000
```

Nell'esempio precedente sono stati creati la struttura della directory, un utente e un gruppo. In altri esempi si può trovare in ogni sezione il valore «objectClass: top»: è un valore predefinito e non è necessario aggiungerlo esplicitamente.

Ora, aggiungere i propri valori all'LDAP:

- arrestare il demone LDAP: **sudo /etc/init.d/slaped stop**
- cancellare il contenuto aggiunto automaticamente nell'installazione: **sudo rm -rf /var/lib/ldap/\***
- aggiungere il contenuto: **sudo slapadd -l init.ldif**

- avviare il demone LDAP: **sudo /etc/init.d/slaped start**

È possibile controllare che il contenuto sia stato aggiunto correttamente tramite gli strumenti forniti dal pacchetto `ldap-utils`. Per eseguire una ricerca in una cartella LDAP:

```
ldapsearch -xLLL -b "dc=example,dc=com" uid=john sn givenName cn
dn: uid=john,ou=people,dc=example,dc=com
cn: John Doe
sn: Doe
givenName: John
```

Una breve spiegazione di quanto scritto precedentemente:

- `-x` serve perché non viene usato il metodo di autenticazione SASL (in modo predefinito)
- `-LLL` disabilita la stampa a schermo delle informazioni LDIF

## Impostare ACL

L'autenticazione richiede l'accesso ad un campo password che non dovrebbe essere accessibile in modo predefinito. Un altro problema è che durante la modifica della password usando `passwd`, anche `shadowLastChange` deve essere accessibile. Il codice seguente mostra un esempio di impostazione di ACL che permette l'accesso a `shadowLastChange`:

```
access to attr=shadowLastChange
    by dn="cn=manager,dc=example,dc=com" write
    by self write
    by * read
```

## Replicazione di LDAP

Il servizio LDAP spesso diventa un servizio critico in un sistema informativo. Tutto dipende da LDAP, autenticazione, autorizzazione, sistema di mail, ecc. È buona norma impostare un sistema ridondante. È facile da impostare e di seguito ne viene fornita una breve guida.

La replicazione qui descritta si basa su una relazione master-slave (principale-secondario). Prima di implementare la replicazione di LDAP, considerare i seguenti passaggi:

1. Arrestare il demone del server `slaped` principale.
2. Riconfigurare il file `slaped.conf` del server principale per abilitare la replicazione su un nuovo server secondario.
3. Esportare il database del server principale.
4. Configurare il file `slaped.conf` del server di replica.
5. Importare il database del server principale in quello secondario.
6. Ri/Avviare il processo `slaped` del server di replica.
7. Ri/Avviare il processo `slaped` del server principale.

È bene ricordare che le modifiche vanno eseguite sempre sul server principale (master), se eseguite sul server secondario (slave) andranno perse.

### LDAP principale (master)

Nel server principale, è necessario modificare la sezione database del file `/etc/ldap/slaped.conf` per aggiungere le istruzioni di replicazione. Il seguente esempio mostra una replica in `ldap-2.example.com` con l'utente «Manager» e come password «secret». Il file

di log della replicazione è dove le modifiche vengono salvate prima di essere inviate all'LDAP secondario.

```
replica uri=ldap://ldap-2.example.com:389 binddn="cn=Manager,dc=example,dc=com"
bindmethod=simple credentials=secret
```

```
repllogfile      /var/lib/ldap/repllog
```

Esportare il database del server principale usando slapcat, quindi copiare il file «master.ldif» nel secondario usando «scp» o un altro strumento.

```
utente@principale:~$ sudo slapcat -l master.ldif
```

### **LDAP secondario (slave)**

Sul server secondario, è necessario autorizzare il server principale ad aggiornare il database LDAP. Aggiungere le seguenti righe al file `/etc/ldap/slapd.conf` nella sezione database:

```
updatedn      cn=Manager,dc=example,dc=com
updateref     ldap://ldap-1.example.com
```

Importare il file `master.ldif` usando `slapadd`:

```
utenet@secondario:~$ sudo slapadd -c -l master.ldif
```

Riavviare il server principale:

```
utente@principale:~$ sudo /etc/init.d/slapd start
```

Riavviare il server secondario:

```
utente@secondario:~$ sudo /etc/init.d/slapd start
```