

autenticazione degli utenti centralizzata con LDAP

Stefano Sasso

A.P.S. Faber Libertatis

stefano @ faberlibertatis.org



Cos'è LDAP?

In breve, (molto in breve) LDAP è un database (modello client-server) ottimizzato per operazioni di lettura

Differisce però dai database come struttura dei dati:

Database >> Tabelle

LDAP >> Albero

Un albero?

Un albero? quello con legno, foglie e frutti? ...più o meno...

In informatica, un albero è una struttura dati a nodi, in cui ogni nodo ha un nodo genitore (tranne il nodo root), proprio come i rami degli alberi.

ogni giorno usate abbondantemente una struttura ad albero, e magari non lo sapete...

... il FILESYSTEM

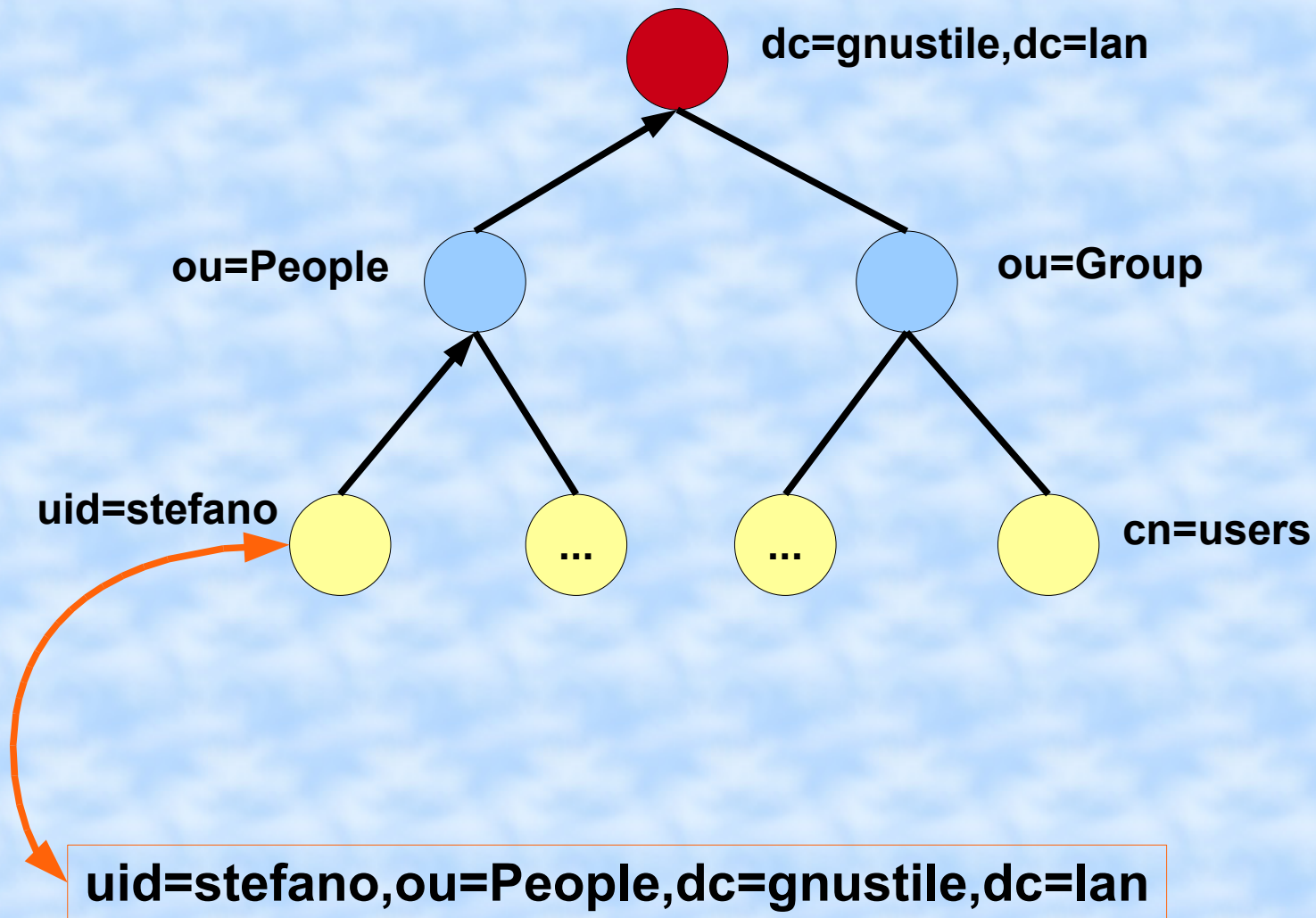
ancora alberi...

ogni nodo del nostro albero LDAP è un oggetto, con determinati attributi

per accedere ai dati contenuti in un nodo si deve specificare il suo percorso completo

es: uid=stefano,ou=People,dc=gnustile,dc=lan

l'esempio di prima... graficamente



Come ogni struttura ad albero, anche la nostra directory LDAP deve avere il suo nodo radice (root), dal quale tutti gli altri oggetti (nodi) discendono

In LDAP ci sono 2 modi di chiamare il nodo root:

- * dc=gnustile,dc=net (più comune)

 - (rappresenta il dominio DNS)

- * o=Faber Libertatis

 - (rappresenta il nome dell'organizzazione)

openLDAP pacchettizzato in debian, ubuntu e redhat utilizza il primo modo

OpenLDAP? che è sta roba?

dimenticavo... :-)

OpenLDAP (www.openldap.org) è la più conosciuta implementazione libera dello standard LDAP. Altre implementazioni libere sono state realizzate da Red Hat e ASF

noi utilizzeremo proprio OpenLDAP

nodi e oggetti

ogni oggetto ha degli attributi; per distinguere i diversi tipi di nodo (utente, gruppo, entry di addressbook, ...) esistono degli attributi speciali chiamati `objectClass` (che definiscono le classi a cui appartiene l'oggetto)

ogni classe permette di inserire diversi attributi nell'oggetto

un nodo può appartenere a più di un `objectClass`

Nel dettaglio, un utente di sistema avrà
come objectClass

account, posixAccount, shadowAccount

mentre un gruppo avrà

posixGroup

sotto la radice possono esserci varie
“sottocartelle” (sempre chiamati nodi) che
hanno come discendenti contenuti specifici.
(es: separazione di utenti e gruppi)

sebbene qualsiasi nodo possa avere dei
discendenti, il tipo di nodo “contenitore”
più usato è l' Organizational Unit
(OU), che ha per objectClass
organizationalUnit


per convenzione, gli utenti di sistema sono figli di ou=People, mentre i gruppi sono figli di ou=Group

i nodi di tipo “gruppo” si identificano con
cn=<nome> (cn=users,ou=Group,dc=gnustile,dc=lan)
mentre i nodi “utente” si
identificano con
uid=<nome> (uid=stefano,ou=People,dc=gnustile,dc=lan)

attributi di un utente

uid: giorgio.rossi
cn: Rossi Giorgio
loginShell: /bin/bash
uidNumber: 1003
gidNumber: 100
homeDirectory: /home/giorgio.rossi
gecos: Rossi Giorgio,,,
shadowMax: 90
shadowWarning: 7
shadowInactive: 14
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {crypt}\$1\$iYwC1zlB\$Mq2pZd8xN5snsmfzhLOUx.
shadowLastChange: 13732

numero di giorni passati dallo
unix time 0 (epoch),
1 gennaio 1970



attributi di un gruppo

cn: cdrom
gidNumber: 24
objectClass: top
objectClass: posixGroup
memberUid: giorgio.rossi
memberUid: stefano.sasso

attenzione: se vogliamo che un utente definito in ldap appartenga ad un gruppo di sistema (in questo caso cdrom), dobbiamo “clonare” il gruppo nell'albero ldap (ovvero il gruppo cdrom deve essere presente sia in ldap che nel file locale /etc/group)

visualizzare, inserire, modificare, cancellare...

per inserire/modificare/cancellare dati da un albero ldap si danno in pasto al server dei file LDIF (Ldap Data Interchange Format), specificando al suo interno le informazioni da aggiungere/modificare/eliminare. ad esempio, per aggiungere un gruppo, basta dare in pasto a "ldapadd" un file contenente

```
dn: cn=users,ou=Group,dc=gnustile,dc=lan
objectClass: posixGroup
objectClass: top
cn: users
gidNumber: 100
```

visualizzare, inserire, modificare, cancellare...

al posto di

* `ldapsearch`

```
ldapsearch -h localhost -x -W -D "cn=admin,dc=fake,dc=net"
```

```
"(uid=stefano.sasso)"
```

* `ldapadd`

```
ldapadd -h localhost -x -W -D "cn=admin,dc=fake,dc=net" -c -f file.ldif
```

* `ldapmodify`

* `ldapdelete`

un utile aiuto ce lo da

[phpLdapAdmin](#)

domande sulla parte teorica?

... passiamo alla pratica!!!

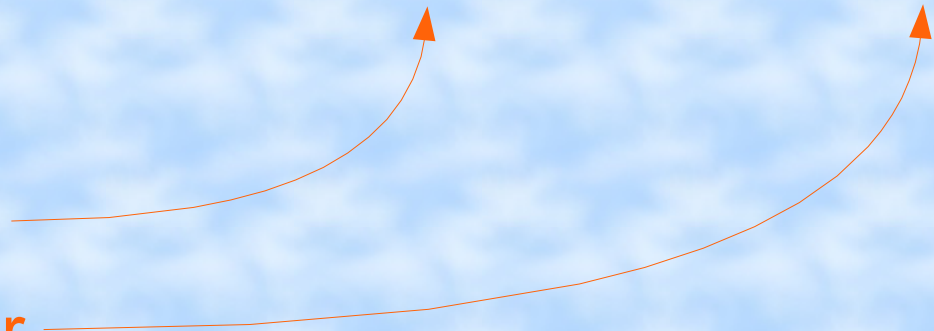


pronti? via!

apt-get install ldap-utils slapd

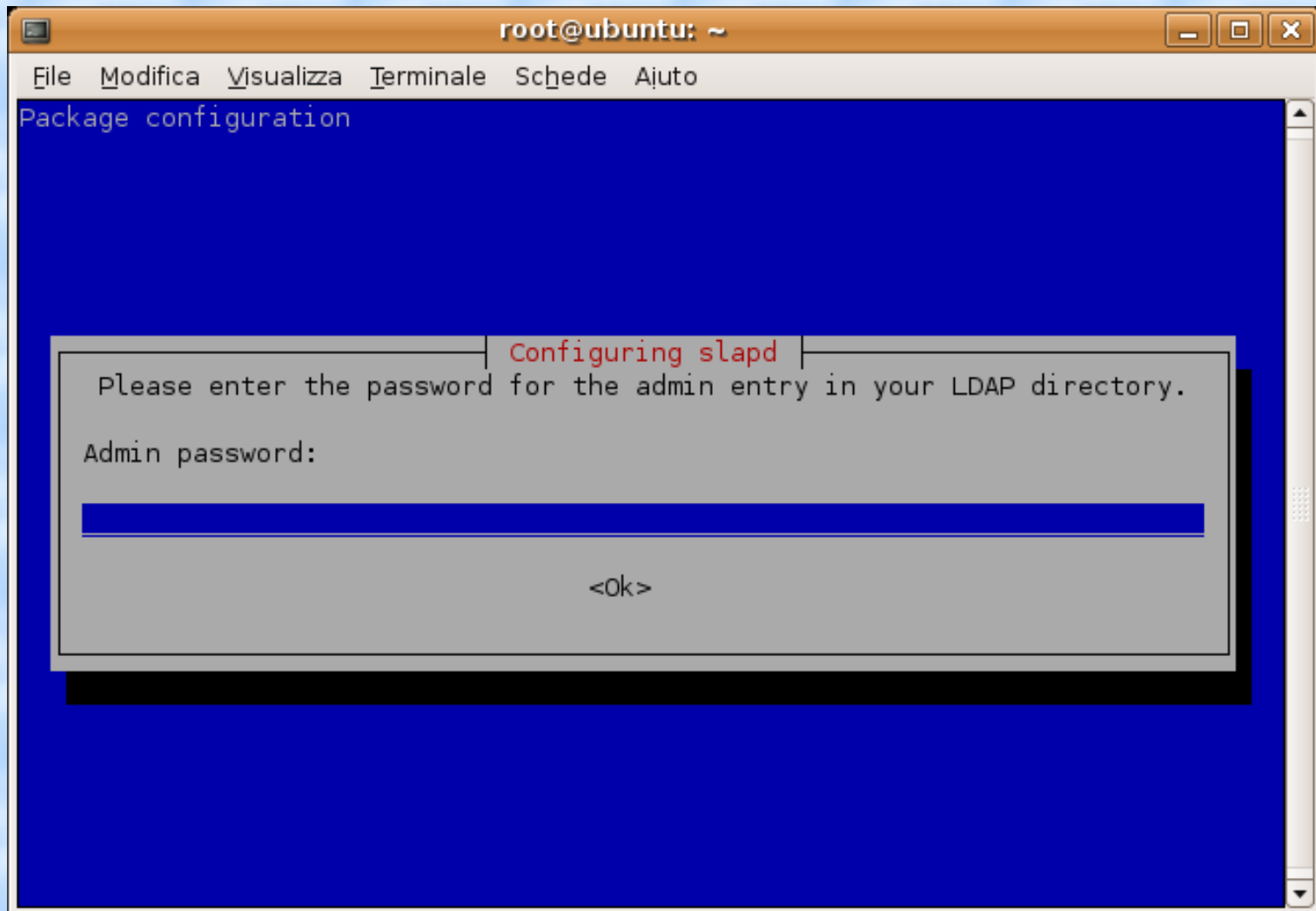
parte client

parte server



debconf e slapd...

debconf nelle nuove versioni debian/ubuntu ha un “basso livello” di domande, e oltre alla password non ci chiederà altro...



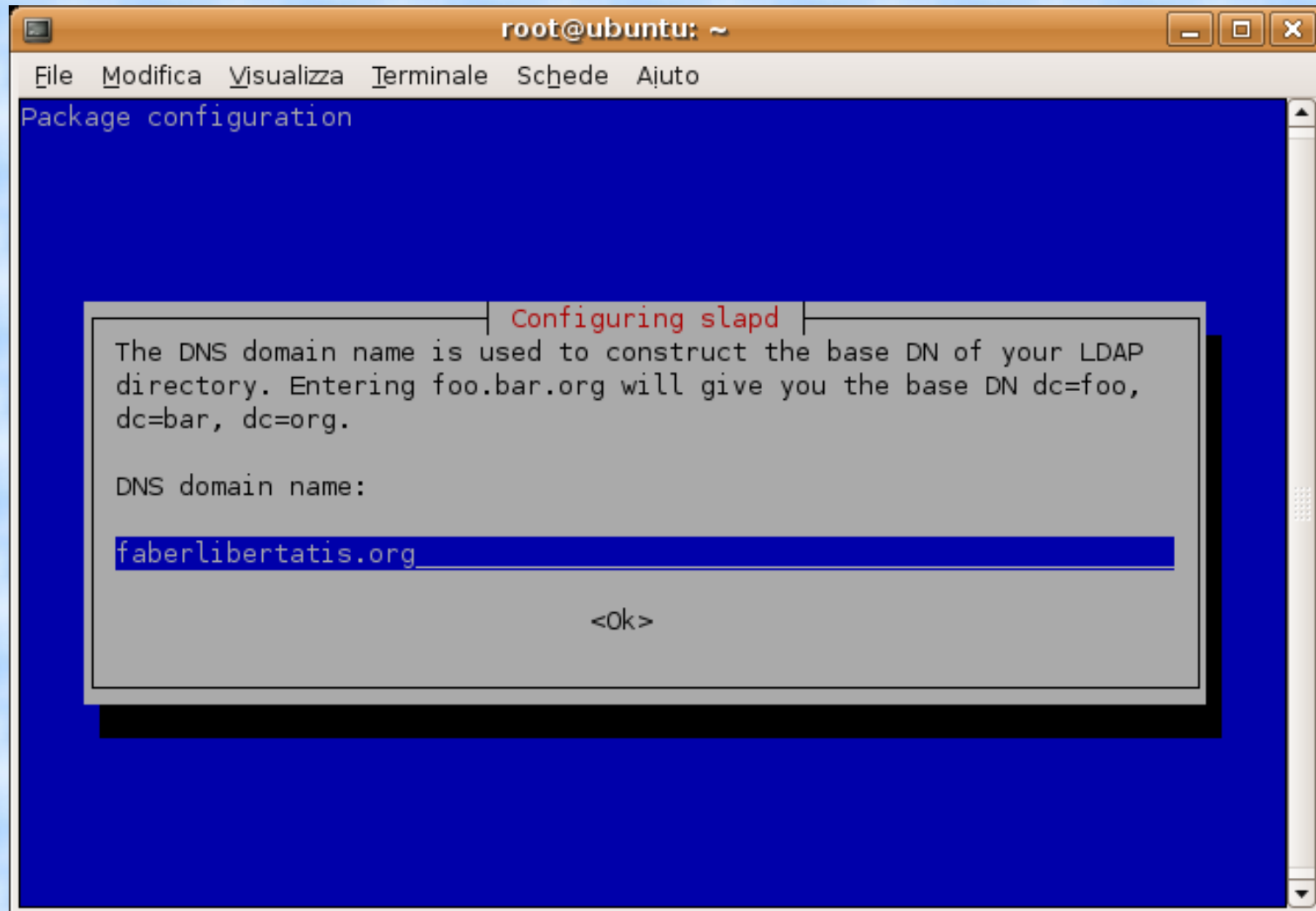
non ci resta che riconfigurararlo...

`dpkg-reconfigure slapd`

Omit server configuration? NO

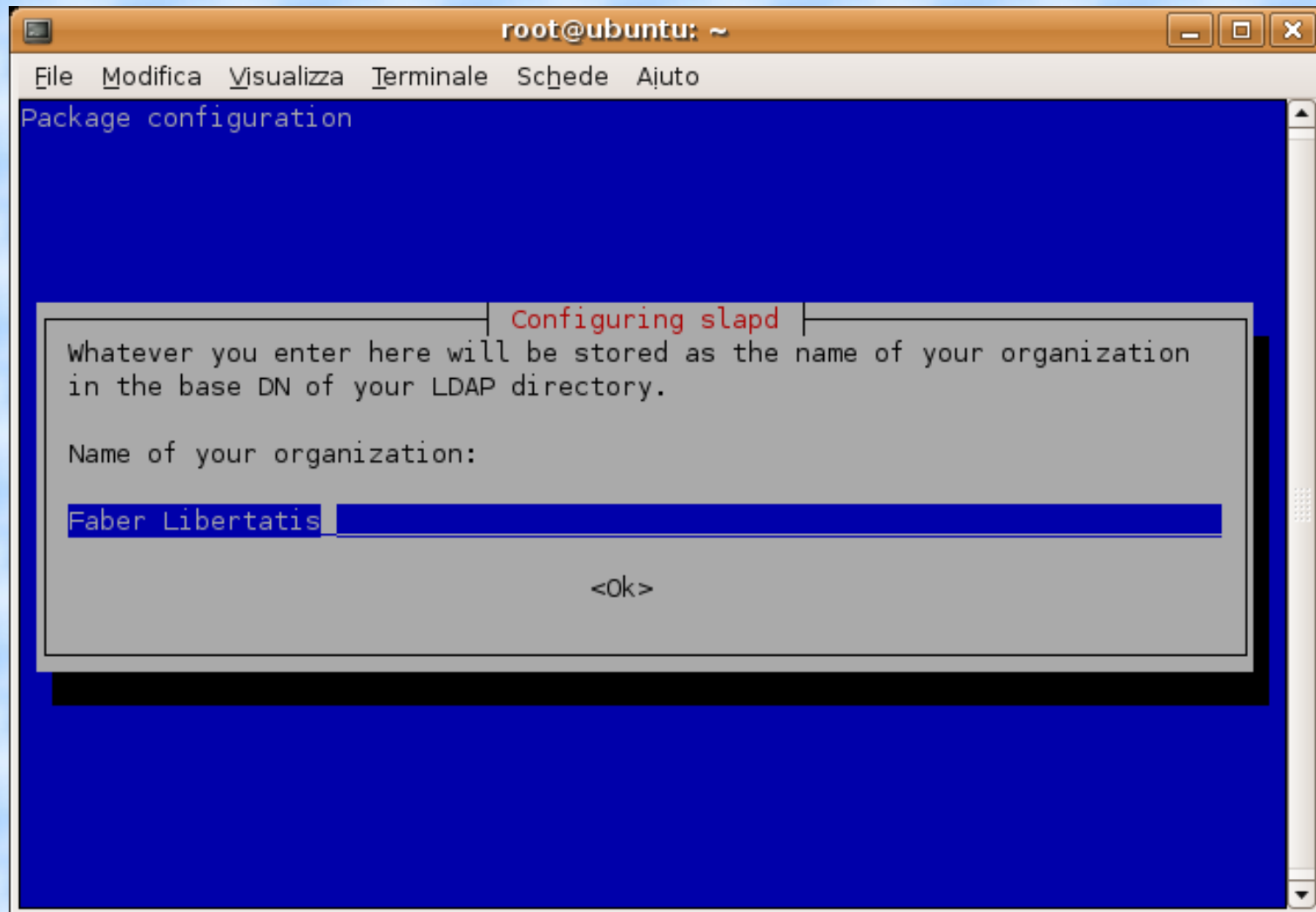
dns domain name...

... per determinare la radice dell'albero



organization...

... attributo "O" aggiuntivo



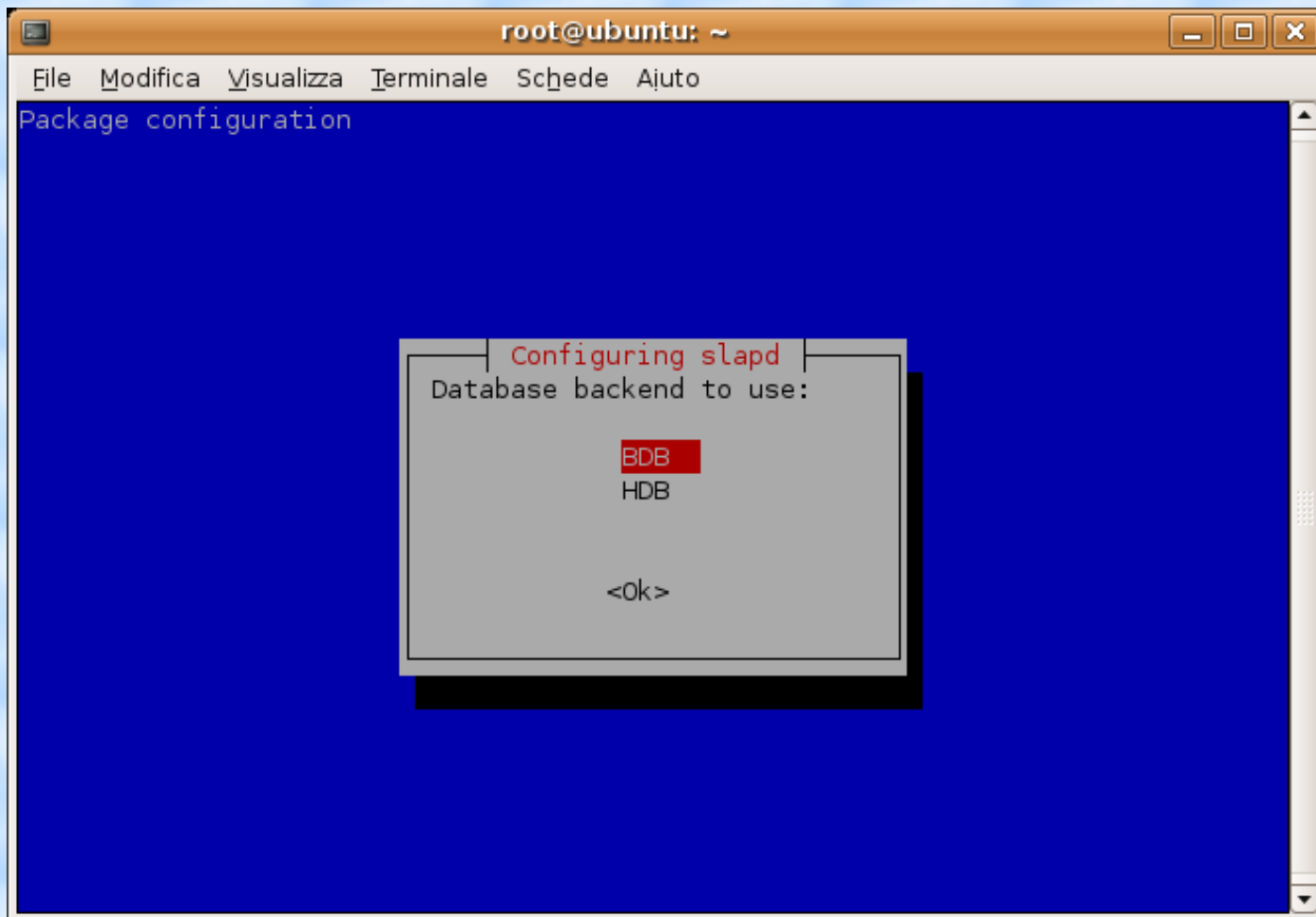
password...

... di nuovo la password

ricordiamoci che questa password è legata
al “nome utente” usato per le query
cn=admin,dc=faberlibertatis,dc=org

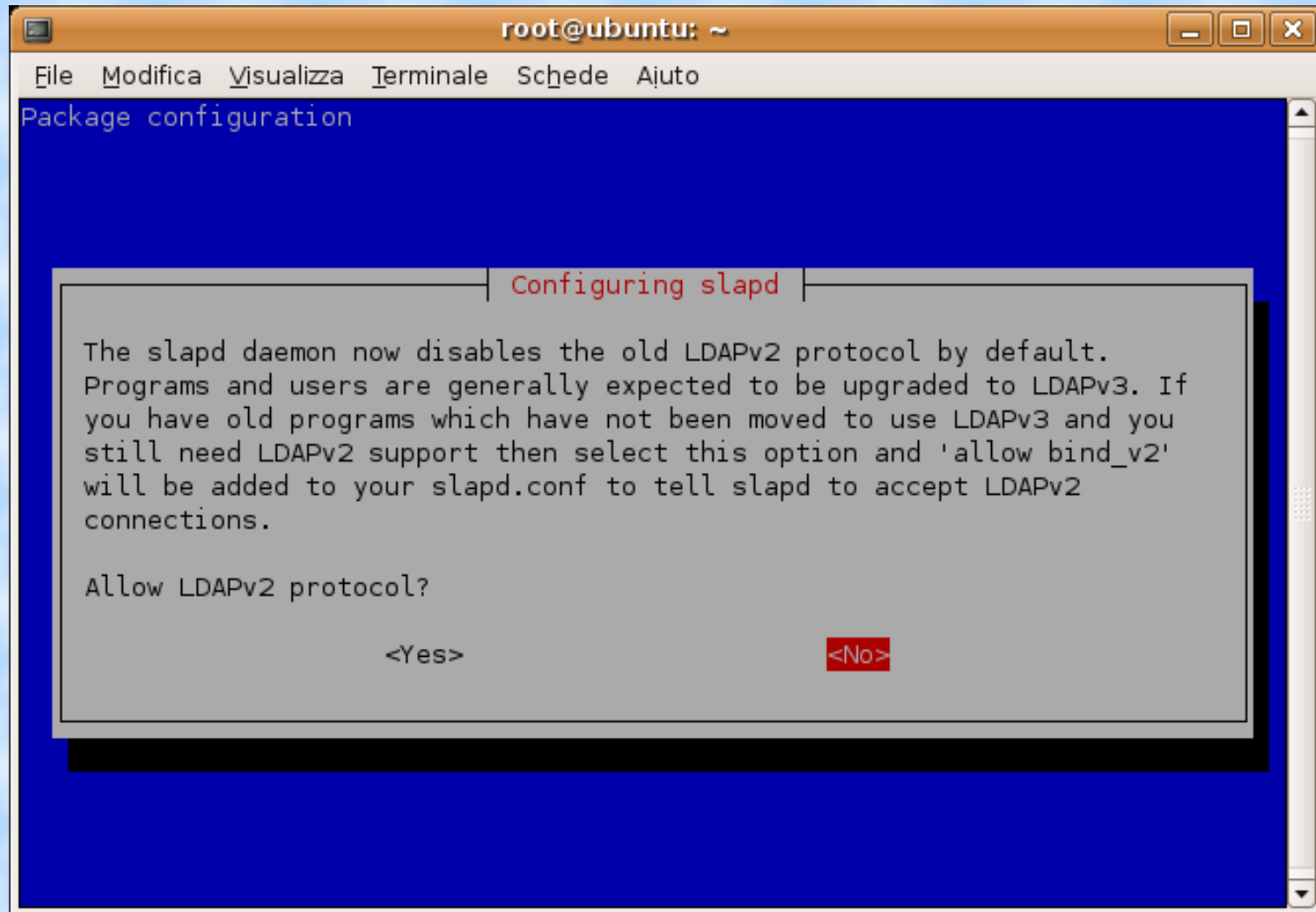
backend...

... in che modo saranno effettivamente salvate le informazioni



versione del protocollo...

... la versione 2 è considerata insicura



```
root@ubuntu: ~
File Modifica Visualizza Terminale Schede Ajuto
Package configuration

Configuring slapd

The slapd daemon now disables the old LDAPv2 protocol by default.
Programs and users are generally expected to be upgraded to LDAPv3. If
you have old programs which have not been moved to use LDAPv3 and you
still need LDAPv2 support then select this option and 'allow bind_v2'
will be added to your slapd.conf to tell slapd to accept LDAPv2
connections.

Allow LDAPv2 protocol?

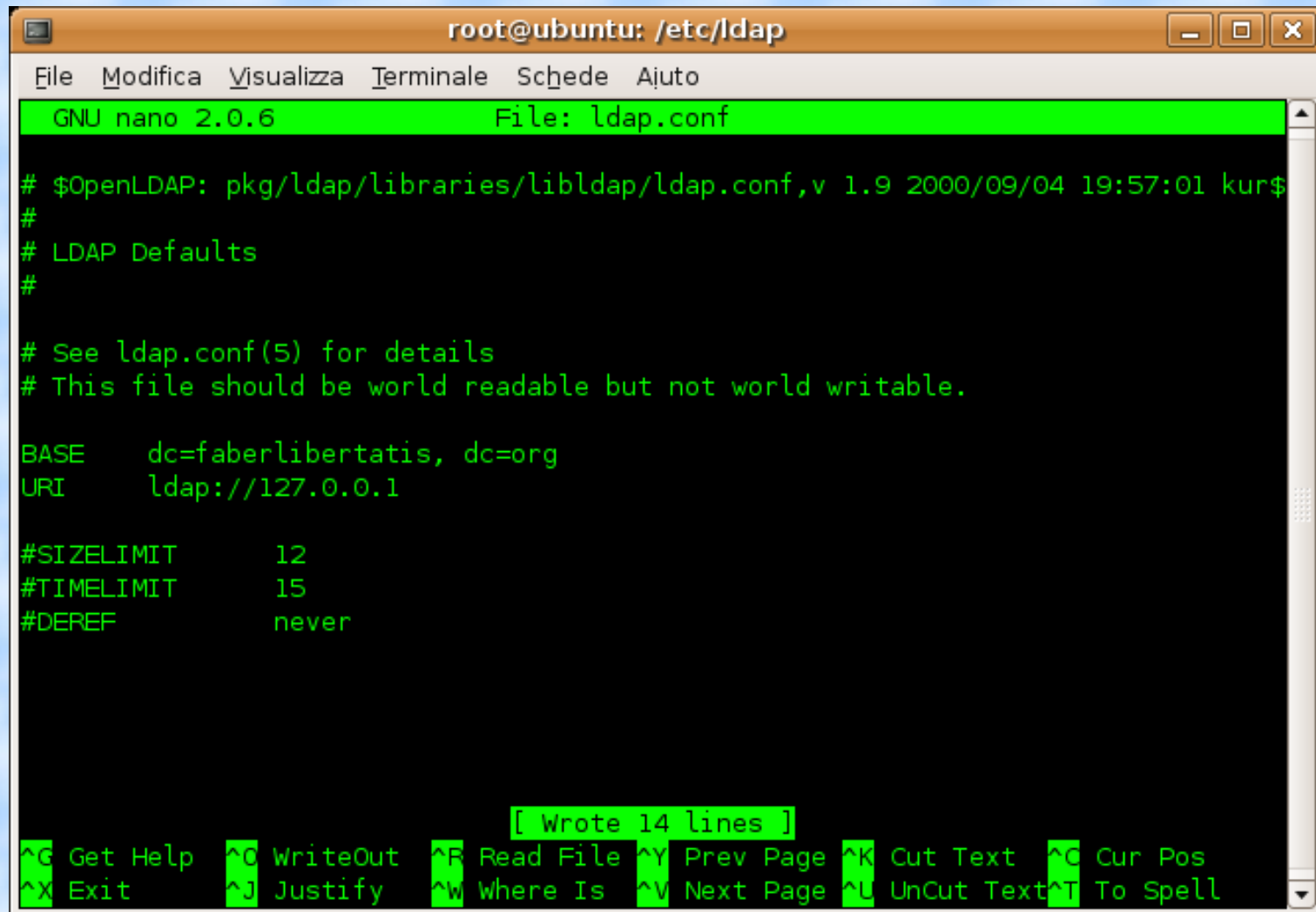
<Yes> <No>
```

ci siamo!

la prima configurazione di slapd
è stata fatta!

configuriamo la parte client

nano /etc/ldap/ldap.conf
(o vi, quello che vi piace di più ;-)



```
root@ubuntu: /etc/ldap
File Modifica Visualizza Terminale Schede Ajuto
GNU nano 2.0.6 File: ldap.conf
# $OpenLDAP: pkg/ldap/libraries/libldap/ldap.conf,v 1.9 2000/09/04 19:57:01 kur$
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE      dc=faberlibertatis, dc=org
URI       ldap://127.0.0.1

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

[ wrote 14 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^L UnCut Text ^T To Spell
```

la prima query ...

verifichiamo la corretta configurazione con una query al server ldap...

```
ldapsearch -x -D "cn=admin,dc=faberlibertatis,dc=org" -W
```

Usa il metodo di autenticazione standard

Effettua il bind con le seguenti credenziali

Prompt per la password

la prima query ...

se vediamo la
root e l'utente
amministratore
significa che
tutto funziona!

root

admin

```
root@ubuntu: /etc/ldap
File Modifica Visualizza Terminale Schede Ajuto
root@ubuntu:/etc/ldap# ldapsearch -x -D "cn=admin,dc=faberlibertatis,dc=org" -w
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# faberlibertatis.org
dn: dc=faberlibertatis,dc=org
objectClass: top
objectClass: dcObject
objectClass: organization
o: Faber Libertatis
dc: faberlibertatis

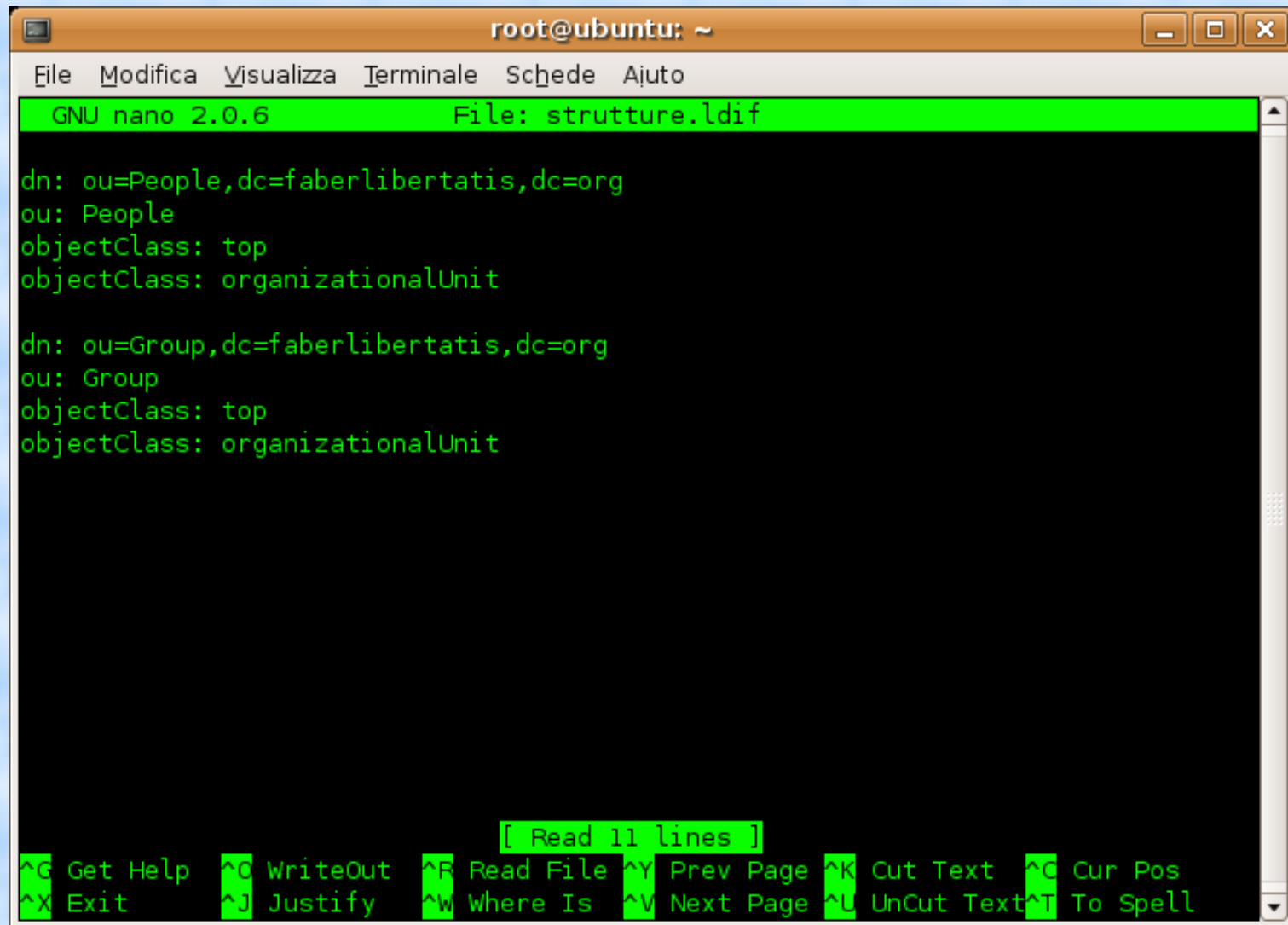
# admin, faberlibertatis.org
dn: cn=admin,dc=faberlibertatis,dc=org
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e2NyeXB0fVE1NEpMNzN2WmdCU2s=

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
root@ubuntu:/etc/ldap#
```

OU per utenti e gruppi

nano /root/strutture.ldif



```
root@ubuntu: ~
File Modifica Visualizza Terminale Schede Ajuto
GNU nano 2.0.6 File: strutture.ldif
dn: ou=People,dc=faberlibertatis,dc=org
ou: People
objectClass: top
objectClass: organizationalUnit

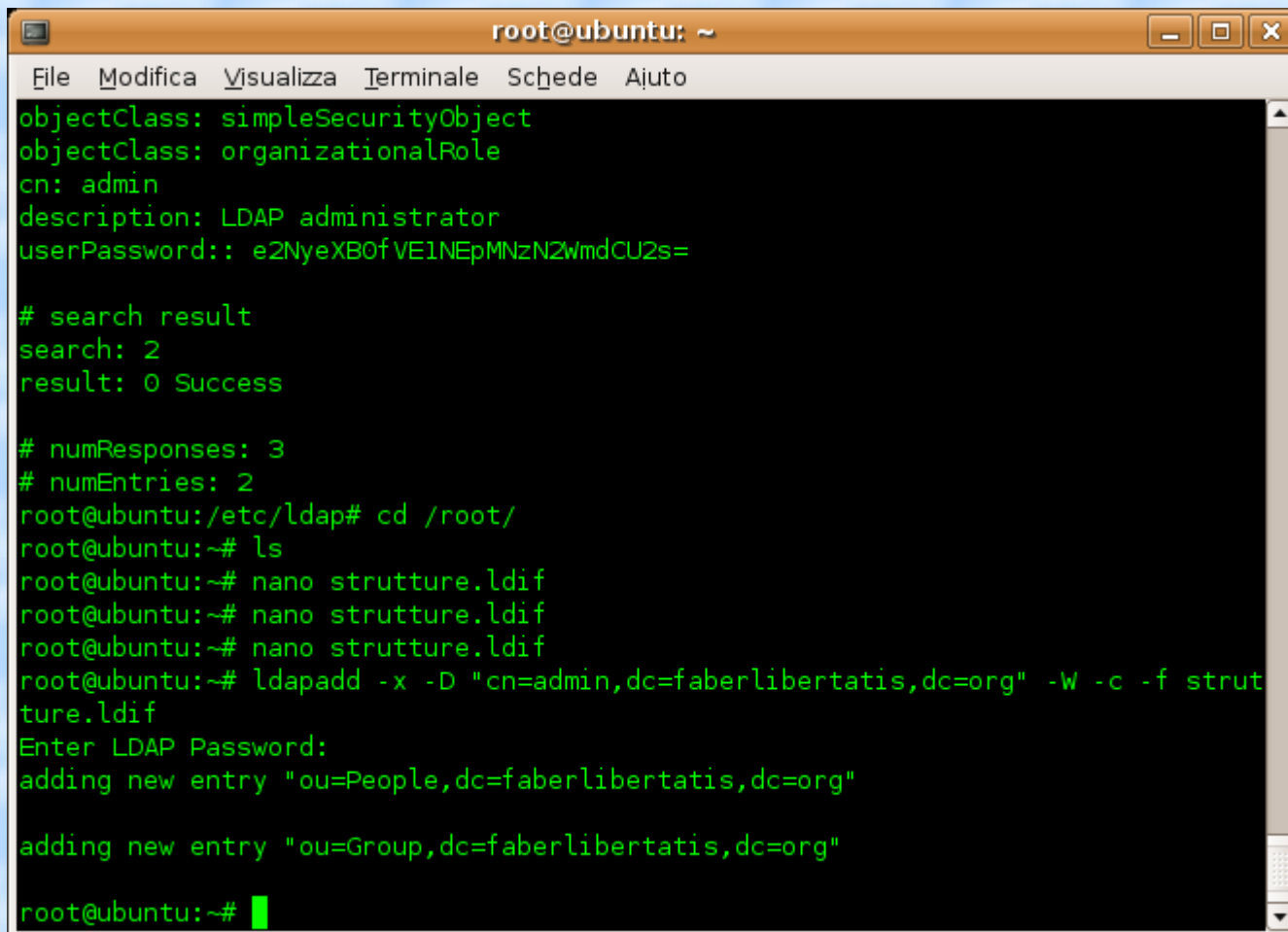
dn: ou=Group,dc=faberlibertatis,dc=org
ou: Group
objectClass: top
objectClass: organizationalUnit

[ Read 11 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page  ^U UnCut Text ^T To Spell
```

ldapadd

aggiungiamo l'ldif appena creato...

```
ldapadd -x -D "cn=admin,dc=faberlibertatis,dc=org" -W -c -f strutture.ldif
```




```
root@ubuntu: ~
File Modifica Visualizza Terminale Schede Ajuto
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e2NyeXB0fVE1NEpMNzN2wmdCU2s=

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
root@ubuntu:/etc/ldap# cd /root/
root@ubuntu:~# ls
root@ubuntu:~# nano strutture.ldif
root@ubuntu:~# nano strutture.ldif
root@ubuntu:~# nano strutture.ldif
root@ubuntu:~# ldapadd -x -D "cn=admin,dc=faberlibertatis,dc=org" -W -c -f strutture.ldif
Enter LDAP Password:
adding new entry "ou=People,dc=faberlibertatis,dc=org"

adding new entry "ou=Group,dc=faberlibertatis,dc=org"

root@ubuntu:~# █
```



-c : continua anche in caso di errori
-f : file da aggiungere

ancora query...

possiamo ora lanciare un'altra query, per verificare l'inserimento

```
ldapsearch -x -D "cn=admin,dc=faberlibertatis,dc=org" -W
```

Installiamo ora cpu,
“change password utility”

nonostante il nome, non si limita al banale
cambio password, ma ci consente di
gestire utenti e gruppi su ldap, in stile
useradd, userdel, usermod, groupadd, ...

```
apt-get install cpu
```

cpu, configurazione

nano /etc/cpu/cpu.conf

```
[GLOBAL]
DEFAULT_METHOD          = ldap
#CRACKLIB_DICTIONARY   = /var/cache/cracklib/cracklib_dict

[LDAP]
LDAP_URI                = ldap://localhost
BIND_DN                 = cn=admin,dc=faberlibertatis,dc=org
BIND_PASS               = admin123
USER_BASE               = ou=People,dc=faberlibertatis,dc=org
GROUP_BASE              = ou=Group,dc=faberlibertatis,dc=org
USER_OBJECT_CLASS       = account,posixAccount,shadowAccount,top
GROUP_OBJECT_CLASS      = posixGroup,top
USER_FILTER              = (objectClass=posixAccount)
GROUP_FILTER             = (objectClass=posixGroup)
USER_CN_STRING           = uid
GROUP_CN_STRING         = cn

SKEL_DIR                = /etc/skel
DEFAULT_SHELL           = /bin/bash
HOME_DIRECTORY         = /home
```

continua...

cpu, configurazione (2)

```
MAX_UIDNUMBER = 10000
MIN_UIDNUMBER = 2000
MAX_GIDNUMBER = 10000
MIN_GIDNUMBER = 2000
ID_MAX_PASSES = 1000
# Whether each user should have its own group created or not
USERGROUPS      = no
# If you change usergroup set this to the default group a user should have
USERS_GID       = 100

# algoritmo di cifratura password
HASH = "md5"

# se vogliamo usare una scadenza password impostiamo
SHADOWMAX      = 90          (es: 90 giorni)

# se vogliamo che degli script vengano eseguiti dopo la creazione o
# rimozione di un user
ADD_SCRIPT = executable oppure DEL_SCRIPT = executable
```

occhio ai permessi, cpu.conf **rw-----!!!** (leggibile solo da root)

inseriamo il gruppo **users** con id **100** nell'albero (come detto prima, si noti che tale gruppo è il “clone” di un gruppo locale definito in /etc/group)

```
cpu groupadd --gid=100 users
```

cpu, test (2)

inseriamo ora un utente di prova...

```
cpu useradd --password=stefano stefano.sasso
```

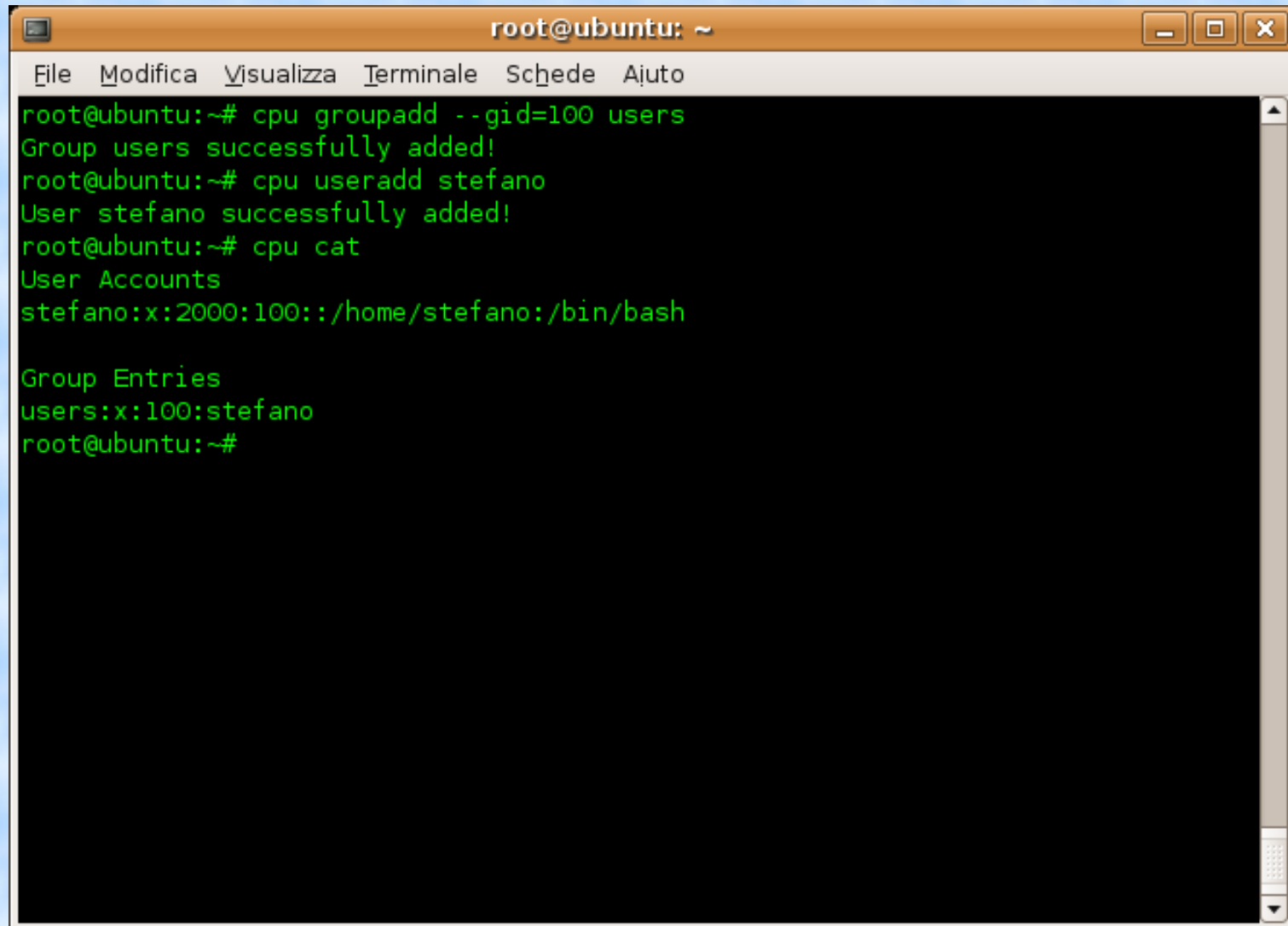
e poi verifichiamo gli inserimenti con

```
cpu cat
```

se vogliamo possiamo anche fare una query diretta a ldap...

cpu, ancora...

ecco il risultato



```
root@ubuntu: ~  
File Modifica Visualizza Terminale Schede Ajuto  
root@ubuntu:~# cpu groupadd --gid=100 users  
Group users successfully added!  
root@ubuntu:~# cpu useradd stefano  
User stefano successfully added!  
root@ubuntu:~# cpu cat  
User Accounts  
stefano:x:2000:100:~/home/stefano:/bin/bash  
  
Group Entries  
users:x:100:stefano  
root@ubuntu:~#
```

Configuriamo ora, sia sul server che sui client, le librerie `nss_ldap` e `pam_ldap`, in modo da poter recuperare i metadati necessari al sistema (`uid`, `gid`, `home directory`, ...), e avere l'autenticazione degli utenti e il cambio password con l'utility `passwd`

```
apt-get install libnss-ldap libpam-ldap
```

Le risposte da dare alle domande (seguendo l'ordine di quelle fatte in Gutsy) sono:

URI della directory LDAP: ldap://ip_del_server/

DN of the search base: dc=faberlibertatis,dc=org

LDAP Version to use: 3

Make local root database admin: Yes

LDAP database require login? No

LDAP account for root: cn=admin,dc=faberlibertatis,dc=org

LDAP root account password: admin123

nss (nsswitch.conf)

il file nsswitch.conf dice a nss dove recuperare le informazioni sugli utenti (metadati). Dobbiamo perciò dirgli di usare LDAP!

editiamo `/etc/nsswitch.conf` e modifichiamo le righe

`passwd: compat`

`group: compat`

`shadow: compat`

in

`passwd: files ldap`

`group: files ldap`

`shadow: files ldap`

Attenzione! è importante l'ordine "files ldap", se noi mettessimo come prima fonte ldap nel server, udev, che parte prima di ldap, non riuscirebbe a partire!

possiamo testare nss lanciando il comando `getent passwd`

pam: pluggable authentication module (1)

Configuriamo ora pam, in modo che un utente possa autenticarsi con la password memorizzata nell'albero ldap.

modifichiamo il file `/etc/pam.d/common-account` e rendiamolo simile al seguente:

```
account sufficient pam_unix.so  
account required pam_ldap.so
```

pam: pluggable authentication module (2)

Continuiamo modificando il file

`/etc/pam.d/common-auth`

rendendolo così:

```
auth [success=1 default=ignore] pam_unix.so nullok_secure
auth required pam_ldap.so use_first_pass
auth required pam_permit.so
```

pam: pluggable authentication module (3)

Facciamo ora in modo che un utente possa cambiare la sua password con l'utility passwd modificiamo il file `/etc/pam.d/common-password` e aggiungiamo, subito prima di

```
password required pam_unix.so n.....
```

la linea

```
password sufficient pam_ldap.so ignore_unknown_user
```

e nel file `/etc/pam_ldap.conf` verificiamo che tutte le righe nella forma

```
pam_password <qualcosa>
```

siano commentate eccetto

```
pam_password exop
```

ldap sicuro: ldaps

Iniziamo generando il certificato SSL

```
# mkdir /etc/ldap/ssl  
# cd /etc/ldap/ssl  
# openssl req -newkey rsa:1024 -x509 -nodes -out \  
server.pem -keyout server.pem -days 3650
```

nel file `/etc/ldap/slapd.conf` inseriamo

```
TLSCipherSuite HIGH:MEDIUM:-SSLv2  
TLSCACertificateFile /etc/ldap/ssl/server.pem  
TLSCertificateFile /etc/ldap/ssl/server.pem  
TLSCertificateKeyFile /etc/ldap/ssl/server.pem
```

Idap sicuro: Idaps

nel file `/etc/default/slapd` decommentiamo la riga

```
SLAPD_SERVICES="ldap://127.0.0.1:389/ Idaps:/// Idapi://"
```

modifichiamo il file `/etc/ldap/ldap.conf` facendolo diventare simile a questo:

```
BASE dc=dominio,dc=com  
URI Idaps://ldap.dominio.com/  
TLS_REQCERT allow
```

parentesi: NFS

NFS, network file system, è il metodo standard di condivisione files dei sistemi unix. Vediamo come installarlo e configurarlo sul nostro server e sui nostri client:

**** server ****

```
apt-get install nfs-common nfs-kernel-server portmap  
nano /etc/exports  
/home (rw,root_squash)
```

**** client ****

```
apt-get install nfs-client portmap  
nano /etc/fstab  
server:/home /home nfs rw,user,async,nodev,nosuid 0 0
```

sguardo "grafico"

apt-get install phpldapadmin

phpLDAPadmin - 0.9.8.4 - Mozilla Firefox

File Modifica Visualizza Vai Segnalibri Strumenti Guida del_icio.us

http://192.168.1.93/phpldapac Vai ternò single sign on

Travian itx Gmail - Posta in arrivo phpLDAPadmin - 0.9.8.4

phpLDAPadmin - 0.9.8.4

- Home
- Purge caches
- Request feature
- Report a bug
- Donate
- Help

My LDAP Server

([schema](#) | [search](#) | [refresh](#) | [info](#) | [import](#) | [exp...](#))

Logged in as: cn=admin

- dc=faberlibertatis,dc=org
 - cn=admin
 - ou=Group (1)
 - ou=People (1)
 - uid=stefano
 - Create new entry here
 - Create new entry here

Server: **My LDAP Server** Distinguished Name: uid=stefano,ou=People,dc=faberlibertatis,dc=org

- Refresh
- Export
- Copy or move this entry
- Show internal attributes
- Delete this entry
- Rename
- Hint: To delete an attribute, empty the text field and click save.
- Compare with another entry
- Add new attribute
- Hint: To view the schema for an attribute, click the attribute name.

cn

stefano
([add value](#))

gidNumber

100

[users](#)

homeDirectory

Completato 192.168.1.93 !!! 1

ultimissime cose, tanto per far capire la versatilità di ldap

ecco che altro è possibile realizzare con ldap:

- * autenticazione radius basata su ldap (hotspot)
- * autenticazione ** basata su ldap
- * replicazione avanzata, clusterizzazione
- * comunicazioni cifrate, ldap over ssl, ldaps
- * interfacciamento con kerberos (single sign-on)
- * integrazione con samba, PDC di rete windows
- * routing posta elettronica
- * addressbook
- * informazioni sudo su ldap
- * chiavi pubbliche ssh su ldap

domande?

grazie per l'attenzione!