Netgarage

Gestione utenti per la rete Netgarage

Author: Andrea Manni
Copyright: GFDL
Version: 1.8

Benvenuto sul server di Netgarage, tramite la gestione utenti gli operatori potranno inserire nuovi utenti o modificare le password di quelli gia' esistenti. Segue la documentazione per Risolvere i problemi nel funzionamento della infrastruttura di autenticazione e Configurare il sistema operativo appena installato per poter abilitare i sistemi operativi Ubuntu freschi di installazione ad accedere al sistema di autenticazione centrale.

Indice

Generato il 2010-11-15, disponibile in PDF per la stampa . La versione originale e' ospitata su http://garage.andreamanni.com

Per gli operatori e chiunque fosse interessato a seguire lo sviluppo del progetto (e inviare suggerimenti e correzioni per questo documento) e' disponibile la mailing list: http://lists.andreamanni.com/cgi-bin/mailman/listinfo/netgarage

1 Risolvere i problemi

Vediamo ora alcuni comandi e procedure che possono essere di aiuto per diagnosticare eventuali problemi dell'infrastruttura di autenticazione. Per cercare di identificare un eventuale problema si tenga conto dei seguenti punti.

1. Il sistema operativo deve funzionare correttamente
2. La rete deve funzionare correttamente
3. Il server LDAP deve essere operativo e raggiungibile
4. Il computer locale deve essere in grado di eseguire richieste (query) sul server LDAP
5. Il sistema di autenticazione del sistema operativo locale deve tener conto delle informazioni reperibili sulla directory LDAP

1.1 Il sistema operativo deve funzionare correttamente

Il sistema operativo deve partire regolarmente e arrivare alla schermata di *log-in* grafico. Talvolta potrebbe darsi che questo richieda piu' tempo del solito, tipicamente per un problema nell'accesso alla rete. In questo caso provare prima di tutto ad accedere con un altro computer, in modo da valutare se il problema sia nella rete.

Se il sistema operativo non dovesse partire si puo' provare a far partire il computer con uno dei CD di installazione / Live. I cd live si possono reperire su: http://mirror.switch.ch/ftp/ubuntu-cdimage/

Nel caso un utente esperto potrebbe far partire il sistema in *single user mode* (una sorta di modalita' di ripristino) aggiungendo la stringa `single` all momento del boot.

1. Alla schermata di boot scegliere la versione da far partire, generalmente la prima
2. Premere il tasto e per modificare la stringa di avvio
3. Selezionare la seconda riga, quella che inizia con `kernel`
4. Premere il tasto e per modificare la stringa di avvio
5. Aggiungere la stringa `Single`
6. Premere invio, se richiesto premere b per fare il *boot* (avvio) del sistema. Il sistema dovrebbe partire a *riga di comando*, senza interfaccia grafica, con la rete disabilitata e senza richiedere le credenziali di *root*.

A questo punto si puo' procedere ad attivare le singole componenti del sistema operativo e cercare di identificare i problemi.

1.1.1 Log in con utente locale.

Il sistema di autenticazione dei computer locali prende i dati da un server LDAP remoto, accessibile tramite rete: quindi senza rete non sara' possibile autenticarsi con le credenziali disponibili sul server. Dovrebbe essere comunque sempre possibile fare il **log-in con un utente le** cui credenziali sono state inserite direttamente nel sistema operativo in fase di installazione: tutti i sistemi dovrebbero avere un utente con *nome-utente* `utente` e password *nota agli operatori* (nope, non verra' riportata in questa guida).

Con questo utente generico dovrebbe essere possibile accedere al sistema anche senza rete / LDAP.

1.2 La rete deve funzionare correttamente

Senza connessione di rete non e' possibile connettersi al server, provare a *navigare in internet* per testare la connessione.

Se ci fossero dei problemi un utente esperto puo' provare a eseguire tramite *terminale* i seguenti comandi per tracciare alcuni problemi comuni.

1. Fare un ping di un indirizzo IP (il server garage non accetta richieste ICMP):

```
ping -c1 198.41.0.4
```

2. Controllare lo stato della scheda di rete:

```
/sbin/ifconfig
```

2.1 Provare a fare un ping del proprio gateway:

```
route -n
ping 192.168.0.254
```

3. Testare la risoluzione dei nomi di dominio:

```
host garage.piffa.net
garage.piffa.net has address 83.216.162.15
```

1.3 Il server LDAP deve essere operativo e raggiungibile

Provare poi a raggiungere l'interfaccia web di gestione degli utenti del server: https://garage.piffa.net/utenti/ (se viene notificato un *problema di sicurezza* non ci si preoccupi, si accetti il certificato). Eseguito il log-in si provi a cercare un utente o a visualizzare la lista degli utenti.

Inoltre il computer locale deve essere in grado di risolvere l'host `garage`:

```
ping garage
PING garage (83.216.162.15) 56(84) bytes of data.
```

Ci si assicuri che i pacchetti vengono indirizzati all'`IP 83.216.162.15` sulle reti esterne, sulla rete del comune puo' essere corretto anche il valore `192.168.15.1`

Se cosi' non fosse si aggiunga la voce `garage` al file `/etc/hosts`

```
sudo echo '83.216.162.15   garage' >> /etc/hosts
```

1.4 Il computer locale deve essere in grado di eseguire richieste (query) sul server LDAP

Cercare un singolo utente all'interno della directory LDAP. Serve per testare che la connessione e il server LDAP funzionino correttamente:

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

Per esplorare tutto l'albero, tenere conto che ci sono centinaia di utenti:

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

Queste query si basano sulla configurazione del client LDAP "/etc/ldap/ldap.conf`` proposta in questa guida, e sono per questo adatte per testarne l'implementazione. Naturalmente e' possibile fare query a server diversi senza che siano *preconfigurati* tutti i parametri. Allo stato attuale non e' pero' possibile evitare di modificare il file `/etc/hosts` per rendere disponibile l'accoppiata `83.216.162.15 garage` .

Query su LDAP in chiaro::

ldapsearch -H ldap://garage -x uid=andrea -b dc=garage

Query su LDAPs criptato:

```
ldapsearch -H ldaps://garage -x uid=andrea -b dc=garage
```

Query da admin:

```
ldapsearch -H ldaps://garage -x uid=andrea -b dc=garage -D cn=admin,dc=garage -W
```

Avvertenza

Per poter usare LDAPS puo' essere necessario accettare i certificati auto firmati: aggiungere `TLS_REQCERT allow` nel file `/etc/ldap/ldap.conf` . Si puo' controllare il certificato SSL (e quindi testare se il server LDAPS accetta richieste con `openssl s_client -connect garage.piffa.net:636 -showcerts` , oppure eseguire una query in modalita' debug: `ldapsearch -x -d8`

1.5 Testare il sistema di autenticazione

Cercare una utente nel sistema operativo utilizzando ''getent''. Serve per testare che il sistema operativo possa effettivamente autenticare gli utenti in base ai dati contenuti nella directory LDAP, posto ovviamente che possa connettersi a questa.

```
getent passwd andrea
```

Se l'utente non viene trovato il sistema di autenticazione PAM non tiene conto di LDAP: si controllino i files `/etc/nsswitch.conf` e `/etc/pam.d/common-sessio` .

Su puo' cercare anche dentro **shadow** (il file delle password locale, dovrebbero essere visibili solo gli utenti di sistema come `utente`) e **groups** (l'elenco dei gruppi di utenti).

1.6 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`, corrispondente *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
```

1.6.1 Testare la connessione SSL

Testare il certificato: `openssl s_client -connect garage.piffa.net:636 -showcerts`

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

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

4. Fare una query col debug: `ldapsearch -x -d8`

2 Configurare il sistema operativo appena installato

> ***Scaricare le ISO del sistema operativo***
>
> Le ISO del sistema operativo Ubuntu possono essere scaricate da http://mirror.switch.ch/ftp/ubuntu-cdimage/

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).

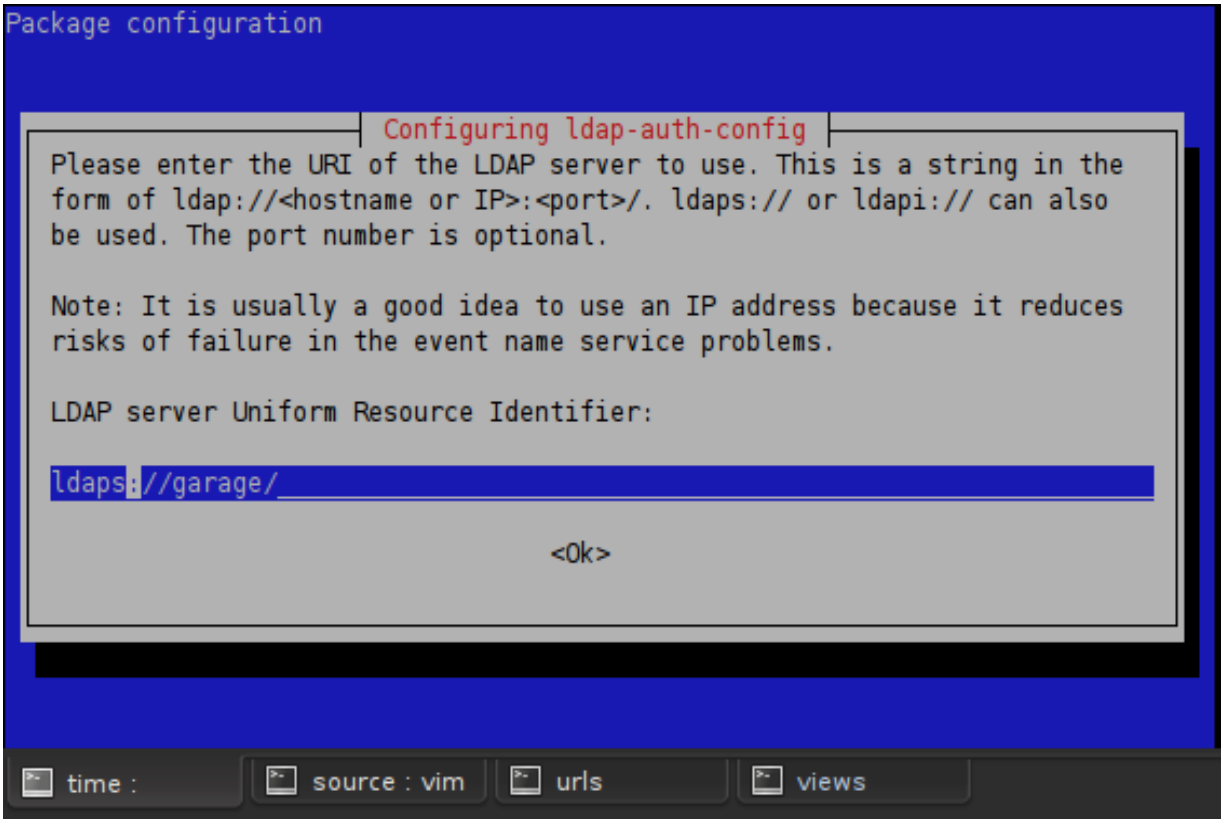
2.1 Pacchetti da installare

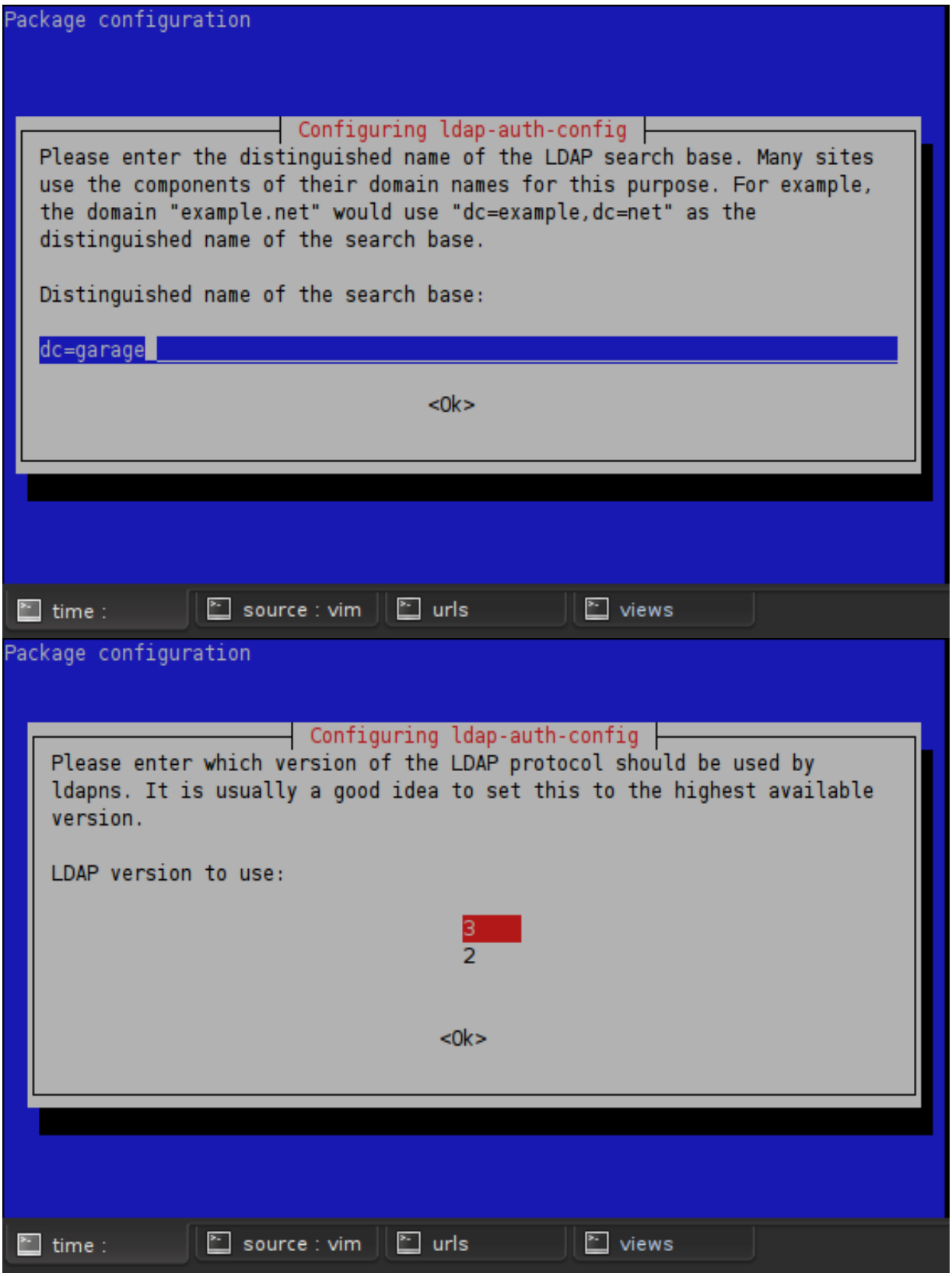
Installare i pacchetti:

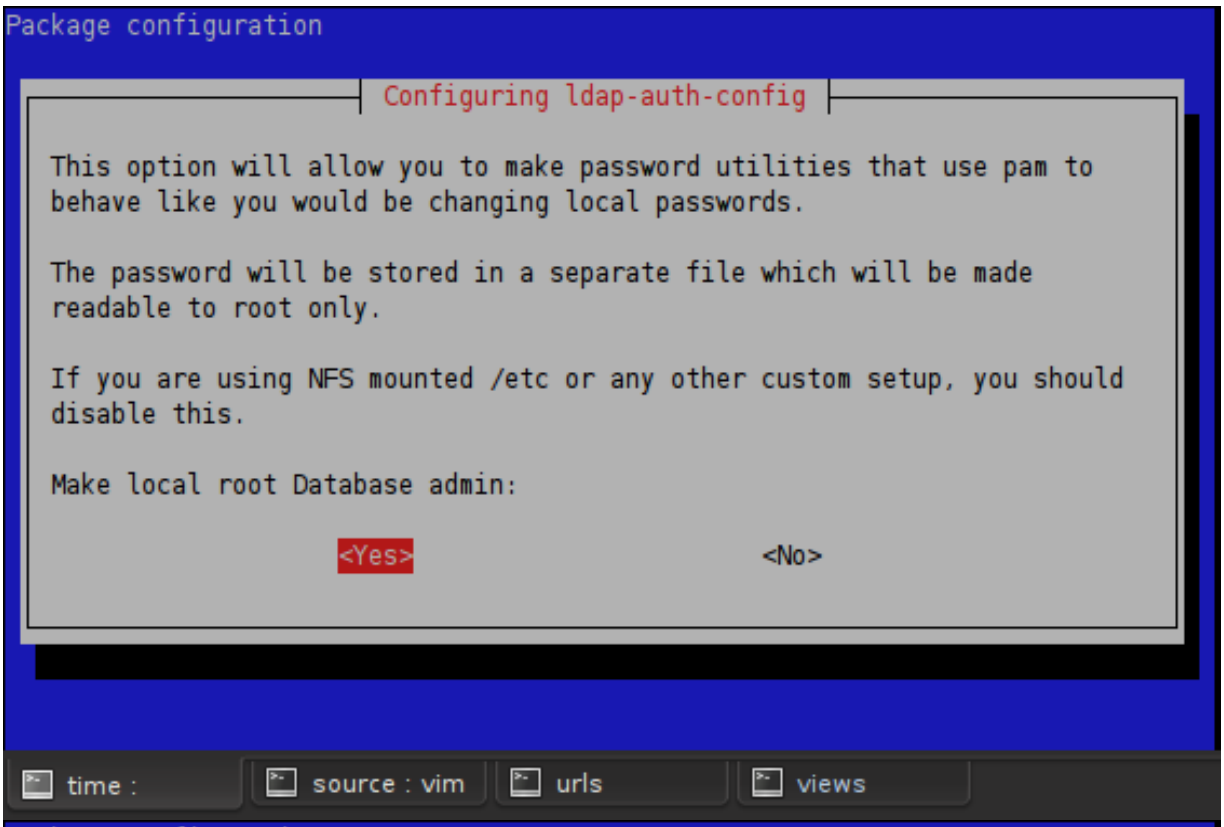
```
ldap-utils libpam-ldap libnss-ldap nscd
```

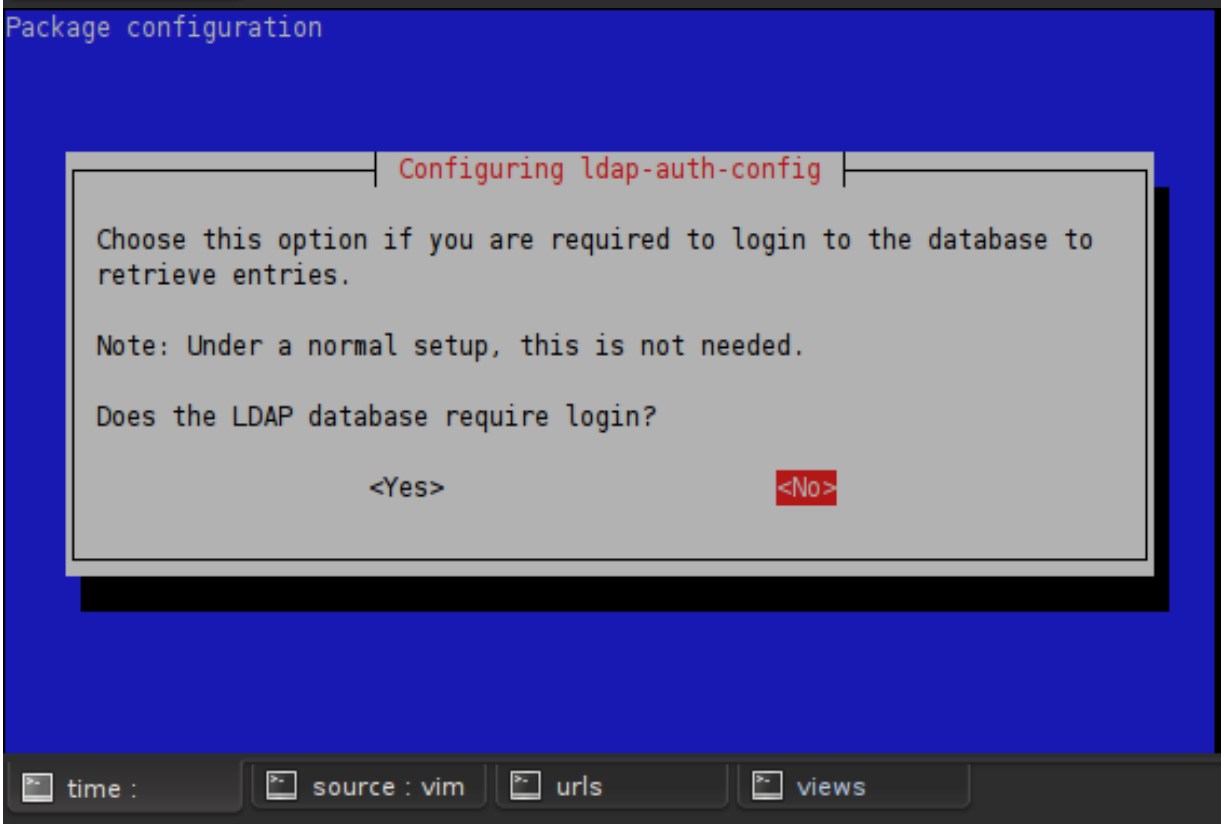
Assicurarsi di impostare i valori corretti per `dn` e utente amministratore: quest'ultimo talvolta non e' consistente nei valori preimpostati (compare `admin` o in alternativa `manager`).

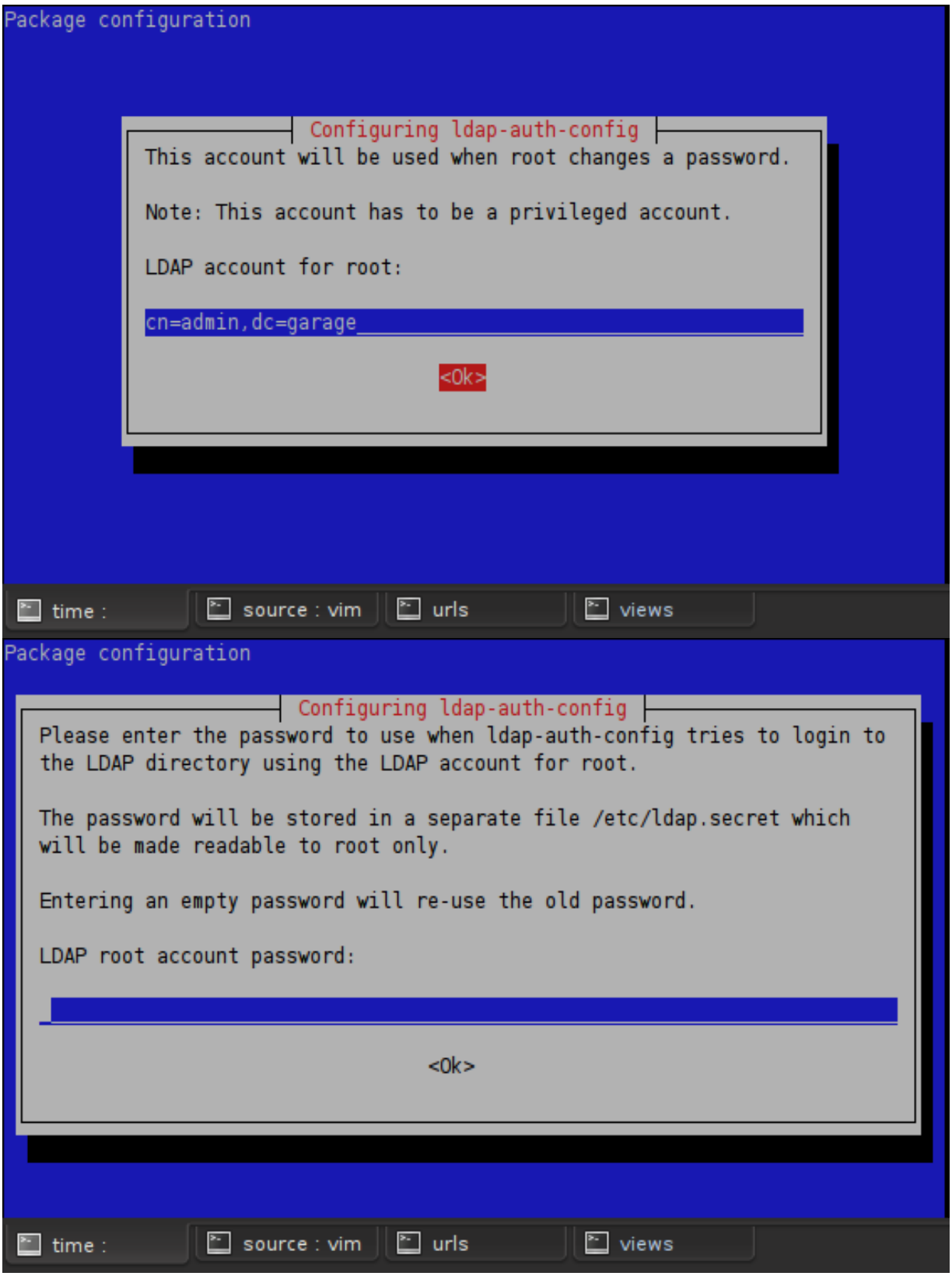
2.1.1 Snapshots configurazione Debconf




Package configuration
Configuring ldap-auth-config
Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.
Distinguished name of the search base:
dc=garage
<Ok>
time :
source : vim
urls
views
Package configuration
Configuring ldap-auth-config
Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to the highest available version.
LDAP version to use:
3
2
<Ok>
time :
source : vim
urls
views


Package configuration
Configuring ldap-auth-config
This option will allow you to make password utilities that use pam to behave like you would be changing local passwords.
The password will be stored in a separate file which will be made readable to root only.
If you are using NFS mounted /etc or any other custom setup, you should disable this.
Make local root Database admin:
<Yes>
<No>
time :
source : vim
urls
views


Package configuration
Configuring ldap-auth-config
Choose this option if you are required to login to the database to retrieve entries.
Note: Under a normal setup, this is not needed.
Does the LDAP database require login?
<Yes>
<No>
time :
source : vim
urls
views



Nota: la password per l'ultima schermata e' conosciuta dagli operatori.

2.2 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.

2.3 /etc/ldap/ldap.conf

/etc/ldap/ldap.conf LDAP Defaults

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

SIZELIMIT       12
TIMELIMIT       15
```

2.3.1 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.

Avremo per `/etc/ldap/ldap.conf`

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

SIZELIMIT       12
TIMELIMIT       15
```

Tener presente che nel file `/etc/ldap.conf` compare:

```
# The distinguished name of the search base.
base dc=garage

# Another way to specify your LDAP server is to provide an
uri ldaps://garage/
```

I client esterni alla rete non si appoggiano al DNS interno, quindi non sono in grado di risolvere correttamente `garage`. Aggiungere al file `/etc/hosts`

```
83.216.162.15   garage
```

2.4 /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

2.5 /etc/pam.d/common-session

Per creare automaticamente la *home directory* dell'utente al primo log-in si utilizzi la penultima voce. Questo dovrebbe essere richiamato automaticamente 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

```
# and here are more per-package modules (the "Additional" block)
session required                        pam_unix.so
session optional                        pam_ldap.so
session required      pam_mkhomedir.so skel=/etc/skel/ umask=0022
session optional                        pam_ck_connector.so nox11
# end of pam-auth-update config
```

3 Riavvio

Per potersi autenticare usando LDAP e' necessario riavviare i seguenti servizi:

```
root@time:~# /etc/init.d/libnss-ldap restart
root@time:~# /etc/init.d/nscd restart
```

In alternativa riavviare l'intero sistema per sicurezza.

4 LDAP

Note su LDAP in generale.

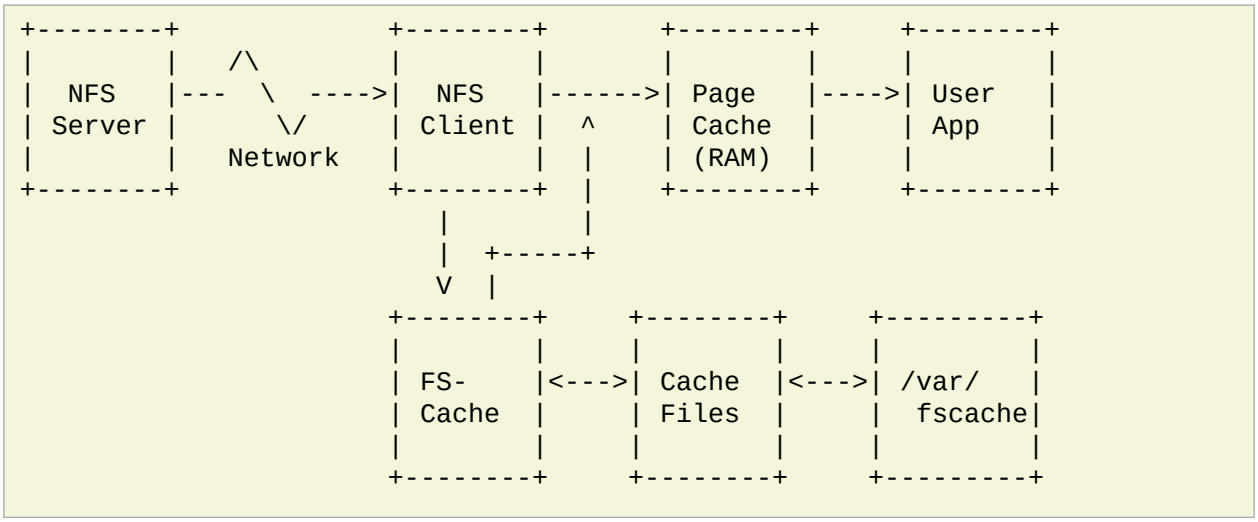
4.1 Terminologia base

Breve riassunto 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

5 Abilitare cachefs per le home condivise

Se si conta di usare NFS per esportare le home degli utenti sui client si dimostra utile usare *fscache* (e *cachefs*) per abbassare le latenze di accesso al file system di rete. In oltre la cache utilizzata e' persistente ai riavvi del sistema, il che insieme al caching dei dati di LDAP contribuisce a ridurre al minimo l'aumento di latenza (e in questo caso il traffico) dovuto alla gestione di utenti e loro file su risorse esterne. La cache non viene usata per i file in scrittura: per questi il client deve interagire direttamente col server NFS.



Pacchetti da installare:

```
cachefilesd
```

Abilitare il demone di cache fs in `/etc/cachefilesd.conf`

```
# You must uncomment the run=yes line below for cachefilesd to start.
# Before doing so, please read /usr/share/doc/cachefilesd/howto.txt.gz as
# extended user attributes need to be enabled on the cache filesystem.
RUN=yes
```

Gli altri parametri sono da regolarsi nel file `/etc/cachefilesd.conf` in base alle caratteristiche della rete locale e delle risorse di storaggio disponibile al client.

5.1 Settare il filesystem per la cache

Assicurarsi che il filesystem su cui risiede la cartella `/var/cache/fscache/` abbia come opzioni di mount `user_xattr` , ad esempio in `/etc/fstab` se non si ha un filesystem dedicato per la cache. Aggiungere l'opzione `fsc` per la cartella NFS (in questo esempio il fs e' su `/dev/sda5`):

```
# /etc/fstab: static file system information.
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
/dev/sda5       /               ext4    errors=remount-ro,user_xattr 0   1
192.168.0.254:/mnt/users /home/users    nfs   rw,auto,vers=3,fsc    0  0
```

5.1.1 Abilitare xattr

Nel caso ci fossero problemi a caricare il file system con `xattr` abilitato si puo' provvedere manualmente ad abilitarlo sul file system:

```
tune2fs -o user_xattr /dev/sda5
# provare a montare il file system:
mount /dev/sda5 /var/fscache/ -o user_xattr
```

Tra le caratteristiche disponibili al fs deve comparire `xattr` ed e' altamente consigliabile per il fs *ext3* `dir_index` (quest'ultimo e' attivato di default sui sistemi recenti):

```
tune2fs -l /dev/sda5 | grep features
```

5.2 Attivare il servizio

Riavviare il demone:

```
/etc/init.d/cachefilesd restart
```

Rimontare il filesystem di rete NFS:

```
mount -o remount,fsc /home/users
```

5.3 Testare

Provare ad accedere ad un file *consistente* su di una cartella condivisa e controllare che la cache venga effettivamente utilizzata:

```
du -sh /var/cache/fscache/
```

I parametri di utilizzo sono consultabile tramite proc: `/proc/sys/fs/nfs/`.

/proc/fs/nfsfs/volumes

NFS disponibili e uso della cache (FSC). Il flag di FSC viene attivato quando si ha *effettivamente utilizzato* la cache.

/proc/sys/fs/nfs/nfs_fscache_to_pages

Numero delle pagine aggiunte da NFS alla cache

-/proc/sys/fs/nfs/nfs_fscache_from_pages

Numero delle pagine recuperate da NFS dalla cache

Tenere conto in fase di benchmark del quantitativo di RAM disponibile al sistema: con centinaia di megabytes di RAM direttamente disponibili per la memoria virtuale / caching in RAM non si notera' immediatamente un miglioramento delle prestazioni.

5.4 NFS server

Non sono necessari interventi sul server che eroga il servizio, dato che tutto il sistema di caching opera a lato client. Per l'export del file system sul server NFS si consideri l'opzione `async`.

- Link: http://lists.us.dell.com/pipermail/linux-poweredge/2007-February/029724.html

5.5 Links

- http://www.linux-mag.com/cache/7378/1.html
- http://www.jukie.net/bart/blog/20090612215638
- Kernel-Doc/Documentation/filesystems/caching/fscache.txt
- Kernel-Doc/Documentation/filesystems/caching/cachefiles.txt

6 Caveat

6.1 Browser web cache

Iceweasel e Firefox sono soliti a gestire la loro cache, che ha la tendenza a raggiungere dimensioni considerevoli, direttamente nella home dell'utente. La cosa ovviamente causa un inutile sovraccarico alla rete e rallenta (invece che migliorare la latenza) il sistema / browser nel caso delle /homes montate su NFS.

E' possibile impostare direttamente alcuni parametri per modificare questo comportamento:

`/etc/iceweasel/pref/iceweasel.js`

```
// Set cache path on /tmp instead of /home/...
pref("browser.cache.disk.parent_directory", "/tmp/");
```

Nel caso di Firefox (Ubuntu) si dovra' intervenire nel file: `/etc/firefox/pref/iceweasel.js`

Per settare la home-page si usi:

```
pref("browser.startup.homepage;http://piffa.net")
```

Per Opera si puo' intervenire sul file: `/etc/operaprefs_fixed.ini`

```
; Settings in this file are not overridable by users
[User Prefs]
// Set cache path on /tmp instead of /home/...
Cache Directory4=/tmp/opera_cache$OPERA_HOME/
```

7 Impostazioni di base del sistema

Per il deployment dei sistemi operativi in ambiente enterprice si rende necessario poter intervenire, per ogni utente esistente o da crearsi, su alcune impostazioni di base come pagine iniziali del browser, configurazioni dei temi del desktop, impostazioni delle applicazioni. questi parametri generalmente possono essere impostati in tre modi:

- File di configurazione *.appnamerc* nella home dell'utente, impostatile in `/etc/skell` quando non vi sia un file con le impostazioni generali di sistema (ad esempio per *wget* il file `/etc/wgetrc` o `/etc/bash.bashrc` per *bash*)
- File di configurazione in `/etc` per le impostazioni di default o mandatarie, ad esempio per Opera `/etc/operaprefs_fixed.ini` e `/etc/operaprefs_default.ini`
- Configurazione del desktop-manager. Ad Esempio per Gnome: `/etc/gconf/gconf.xml.defaults/` e `/etc/gconf/gconf.xml.mandatory/`

Tipicamente abbiamo impostazioni di due tipi:

Default:

impostazione iniziale, superabile da un successivo intervento dell'utente .

Mandataria:

impostazione iniziale non superabile in alcun modo dall'utente: locking.

7.1 Gnome

Per impostare Gnome (in Ubuntu 10.4) si interviene sul *filesytem* in `/etc/gconf` , Gnome usa una sorta di registro di sistema i cui parametri sono contenuti in file (specificando la lor natura: *stringhe, valori booleani, int, liste*) organizzati in un struttura gerarchica mappata sulle directory del filesystem con radice in `/etc/gconf`.

Su puo' intervenire direttamente su detto filesytem (copiando cartelle e files) o con l'utility `gconftool-2`:

```
# Impostare il numero di desktop virtuali
gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.defaults/ --type int --set /apps/metacity/general/num_workspaces 2
```

8 Links:

Links ad altre guide sull'argomento.

- 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