Des stratégies pour sécuriser votre système Linux

Donald Buchan
malak@malak.ca

mai / août 2009

Pourquoi sécuriser son système?

Pourquoi sécuriser sont système Linux

- Malgré que vous utilisez un système moins vulnérable, les “crackers” veulent quand même compromettre votre système;
- Vous ne voulez pas que votre système soit utilisé pour des activitées illicites (pourriel, porno) ou illégales (vol financière ou d'identité);
- La valeure d'un ordinateur linux compromis a une valeur accrue par rapport à un ordinateur Windows;

Pourquoi sécuriser sont système Linux

- Vous avez des fichiers personnels à protéger;
- Il ne touche pas aux autres de connaître que vous êtes amateur de vin, de nature, ou des poupées “Barbie” -- à moins que, bien sûr, vous choisissez de partager cette information!
- ***Simplement, c'est votre ordinateur, à être utilisé pour vos fins, comme vous voyez bon. À ces fins, des mesures de sécurité doivent être mises en place.***

Linux generals command Windows grunts in botnet battlefield

Veteran virus still recruiting for zombie army

Darren Pauli 15/02/2008 15:40:20

Page: 1 2

Linux servers infected with a mutating virus are commanding huge Windows botnets six years after the malware was discovered, according to security researchers.

Have your say! 0

The Linux.RST.B virus infects the working direct[illegible] ELF (executable and linkable format) executable files. It can also create a backdoor by opening a socket and listening for a packet containing the attackers origin and the command to be executed..

SophosLabs United Kingdom research director Billy McCourt said Linux boxes are valuable targets as botnet controllers because they are typically remain online as servers.

"Linux computers are very valuable to hackers. A bot army, similar to real armies, needs a general and infantry [and] Linux boxes are often used as servers, which means they have a high up-time - essential for a central control point," McCourt said.

"A Windows computer, on the other hand, is found at home or as a desktop machine in an office, and these computers are regularly switched off [which] makes them less attractive as controllers, but ideal for infantry, or zombies.

"We run various honeypots [and] as you might also expect, [illegible] honeypots are attacked more frequently than our Linux or[illegible]s, but Linux malware is far more interesting."

> "Linux systems, once compromised, are ideal platforms to unleash all sorts of nastiness."
>
> Peter Linich, network administrator for the University of NSW

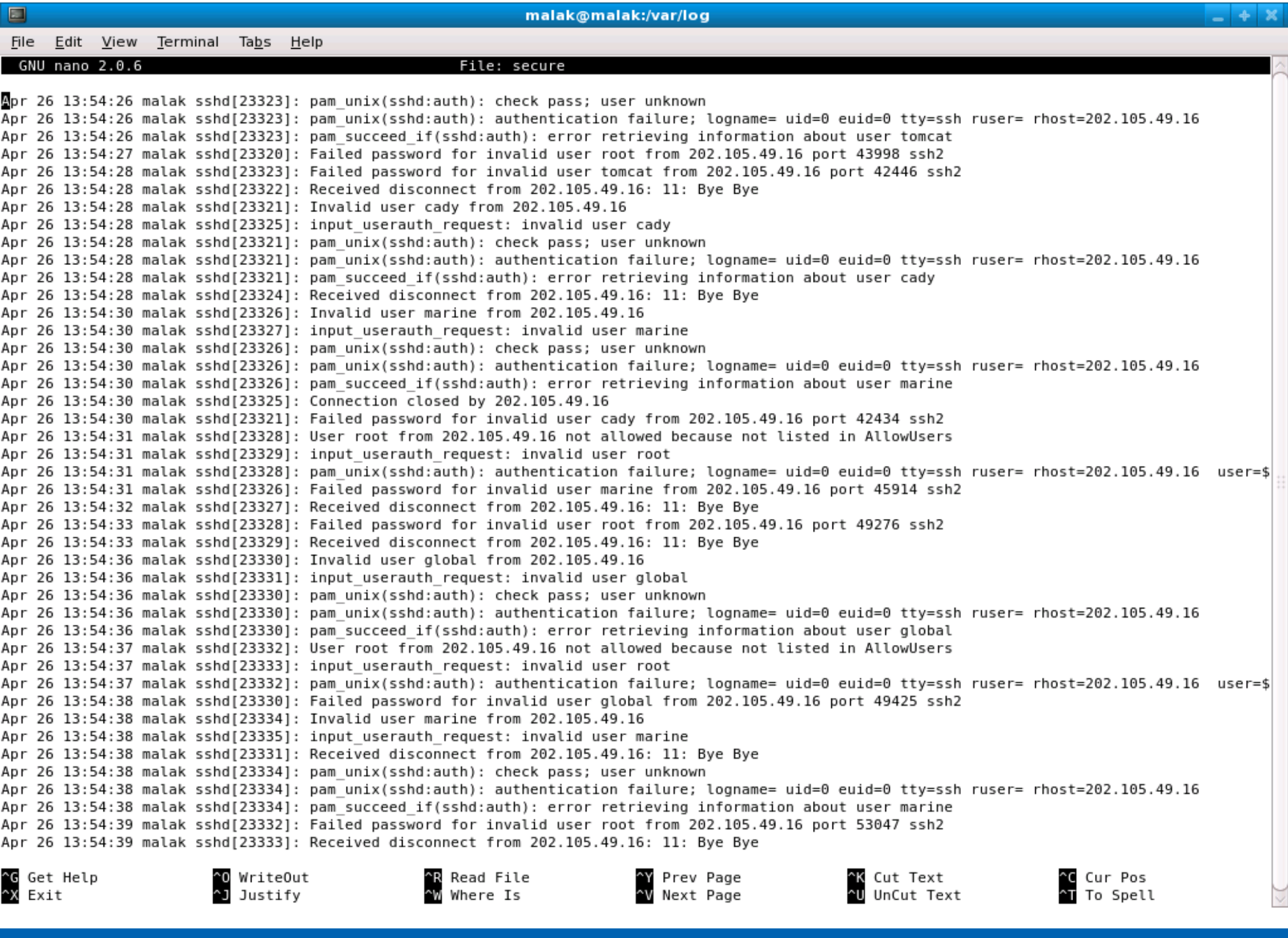
McCourt said the virus, discovered in February 2002, is unique among Linux malware because it can replicate across current distributions.

University of New South Wales senior network administrator for the school of computer science and engineering Peter Linich told Computerworld Linux servers are extremely valuable to hackers since they are typically online more than 10 months are year.

"Just yesterday I was watching our incoming network traffic and noticed an ADSL host in Greece scanning through all our machines and running an SSH (Secure Shell) password-guessing attack on all the SSH servers it found," Linich said, adding such attacks occur multiple times a day.

"Such activity is a real threat in our environment where we have hundreds of Linux systems running 24x7.Linux systems, once compromised, are ideal platforms to unleash all sorts of nastiness.

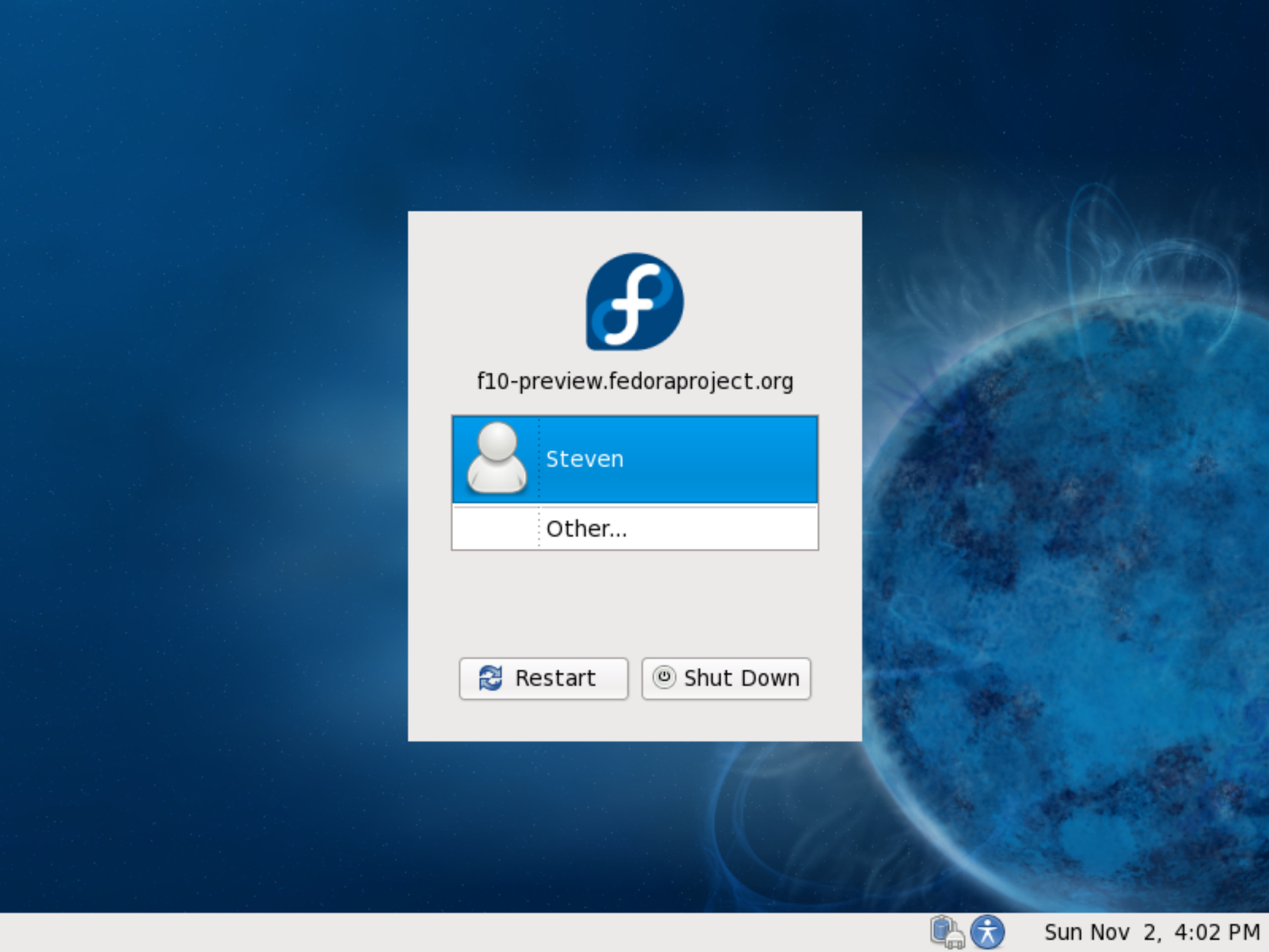
Un système sous attaque


malak@malak:/var/log
File Edit View Terminal Tabs Help
GNU nano 2.0.6 File: secure
Apr 26 13:54:26 malak sshd[23323]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:26 malak sshd[23323]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:26 malak sshd[23323]: pam_succeed_if(sshd:auth): error retrieving information about user tomcat
Apr 26 13:54:27 malak sshd[23320]: Failed password for invalid user root from 202.105.49.16 port 43998 ssh2
Apr 26 13:54:28 malak sshd[23323]: Failed password for invalid user tomcat from 202.105.49.16 port 42446 ssh2
Apr 26 13:54:28 malak sshd[23322]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:28 malak sshd[23321]: Invalid user cady from 202.105.49.16
Apr 26 13:54:28 malak sshd[23325]: input_userauth_request: invalid user cady
Apr 26 13:54:28 malak sshd[23321]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:28 malak sshd[23321]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:28 malak sshd[23321]: pam_succeed_if(sshd:auth): error retrieving information about user cady
Apr 26 13:54:28 malak sshd[23324]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:30 malak sshd[23326]: Invalid user marine from 202.105.49.16
Apr 26 13:54:30 malak sshd[23327]: input_userauth_request: invalid user marine
Apr 26 13:54:30 malak sshd[23326]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:30 malak sshd[23326]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:30 malak sshd[23326]: pam_succeed_if(sshd:auth): error retrieving information about user marine
Apr 26 13:54:30 malak sshd[23325]: Connection closed by 202.105.49.16
Apr 26 13:54:30 malak sshd[23321]: Failed password for invalid user cady from 202.105.49.16 port 42434 ssh2
Apr 26 13:54:31 malak sshd[23328]: User root from 202.105.49.16 not allowed because not listed in AllowUsers
Apr 26 13:54:31 malak sshd[23329]: input_userauth_request: invalid user root
Apr 26 13:54:31 malak sshd[23328]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16 user=$
Apr 26 13:54:31 malak sshd[23326]: Failed password for invalid user marine from 202.105.49.16 port 45914 ssh2
Apr 26 13:54:32 malak sshd[23327]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:33 malak sshd[23328]: Failed password for invalid user root from 202.105.49.16 port 49276 ssh2
Apr 26 13:54:33 malak sshd[23329]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:36 malak sshd[23330]: Invalid user global from 202.105.49.16
Apr 26 13:54:36 malak sshd[23331]: input_userauth_request: invalid user global
Apr 26 13:54:36 malak sshd[23330]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:36 malak sshd[23330]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:36 malak sshd[23330]: pam_succeed_if(sshd:auth): error retrieving information about user global
Apr 26 13:54:37 malak sshd[23332]: User root from 202.105.49.16 not allowed because not listed in AllowUsers
Apr 26 13:54:37 malak sshd[23333]: input_userauth_request: invalid user root
Apr 26 13:54:37 malak sshd[23332]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16 user=$
Apr 26 13:54:38 malak sshd[23330]: Failed password for invalid user global from 202.105.49.16 port 49425 ssh2
Apr 26 13:54:38 malak sshd[23334]: Invalid user marine from 202.105.49.16
Apr 26 13:54:38 malak sshd[23335]: input_userauth_request: invalid user marine
Apr 26 13:54:38 malak sshd[23331]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:38 malak sshd[23334]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:38 malak sshd[23334]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:38 malak sshd[23334]: pam_succeed_if(sshd:auth): error retrieving information about user marine
Apr 26 13:54:39 malak sshd[23332]: Failed password for invalid user root from 202.105.49.16 port 53047 ssh2
Apr 26 13:54:39 malak sshd[23333]: Received disconnect from 202.105.49.16: 11: Bye Bye
^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

Tout le monde doit s'identifier

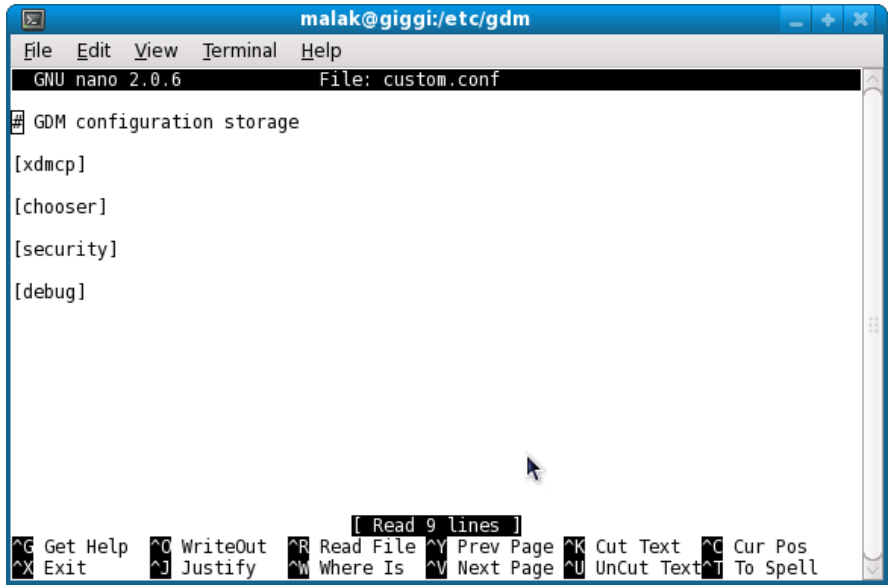
Tout le monde doit s'identifier

- Tout les utilisateurs doivent s'identifier avec leur mot de passe quoique la façon qu'ils veulent se connecter: ssh, ftp, vnc, et même et particulièrement au bureau
- *Si vous faites toujours un “log out” après votre session, votre ordinateur restera allumé et à la fois disponible pour les autres utilisateurs autorisés (le cas échéant), et le VNC sera refusé*
- Il est fortement déconseillé que votre ordinateur ouvre un compte défaut automatiquement

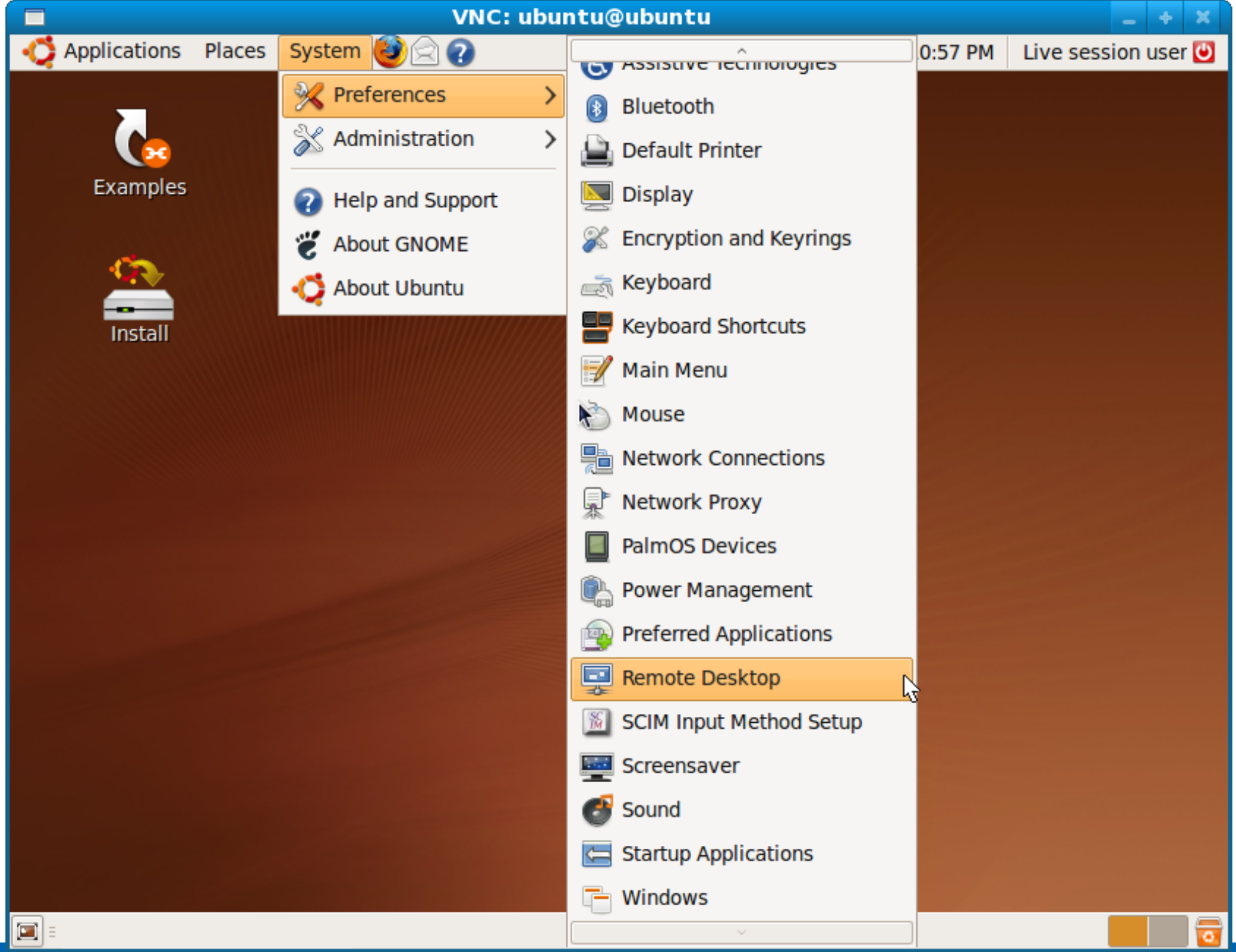

f10-preview.fedoraproject.org
Steven
Other...
Restart
Shut Down
Sun Nov 2, 4:02 PM


ubuntu
Username:
Options
ubuntu // Wed Apr 22, 9:53 AM

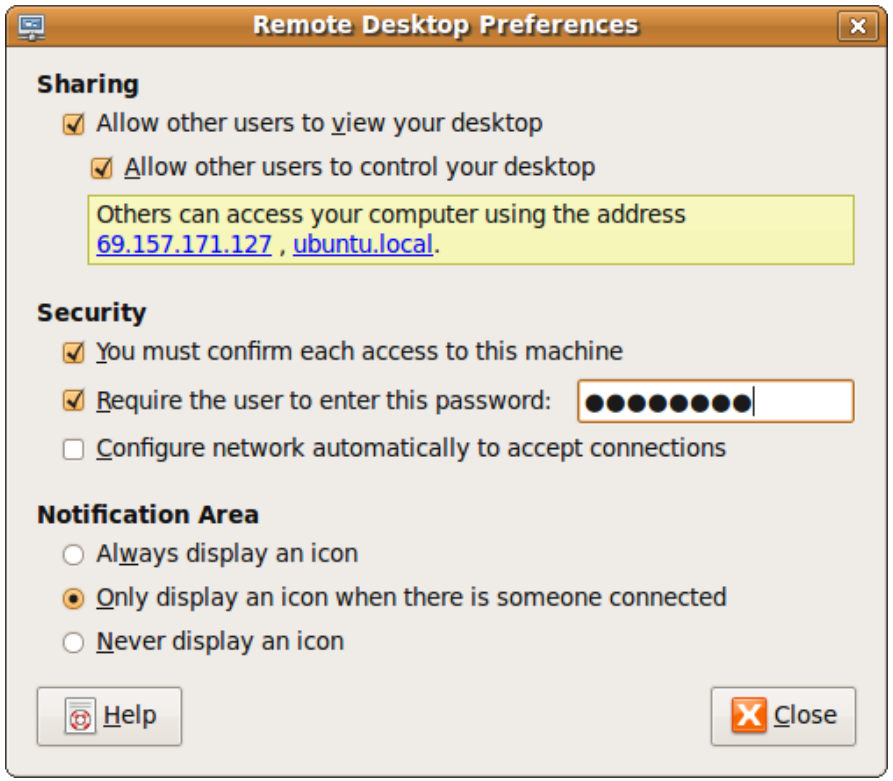
Gestion des mots de passe



- Dans /etc/gdm/custom.conf enlever toute ligne “AutomaticLogin” et “AutomaticLoginEnable”


VNC: ubuntu@ubuntu
Applications
Places
System
0:57 PM
Live session user
Preferences
Administration
Help and Support
About GNOME
About Ubuntu
Examples
Install
Bluetooth
Default Printer
Display
Encryption and Keyrings
Keyboard
Keyboard Shortcuts
Main Menu
Mouse
Network Connections
Network Proxy
PalmOS Devices
Power Management
Preferred Applications
Remote Desktop
SCIM Input Method Setup
Screensaver
Sound
Startup Applications
Windows

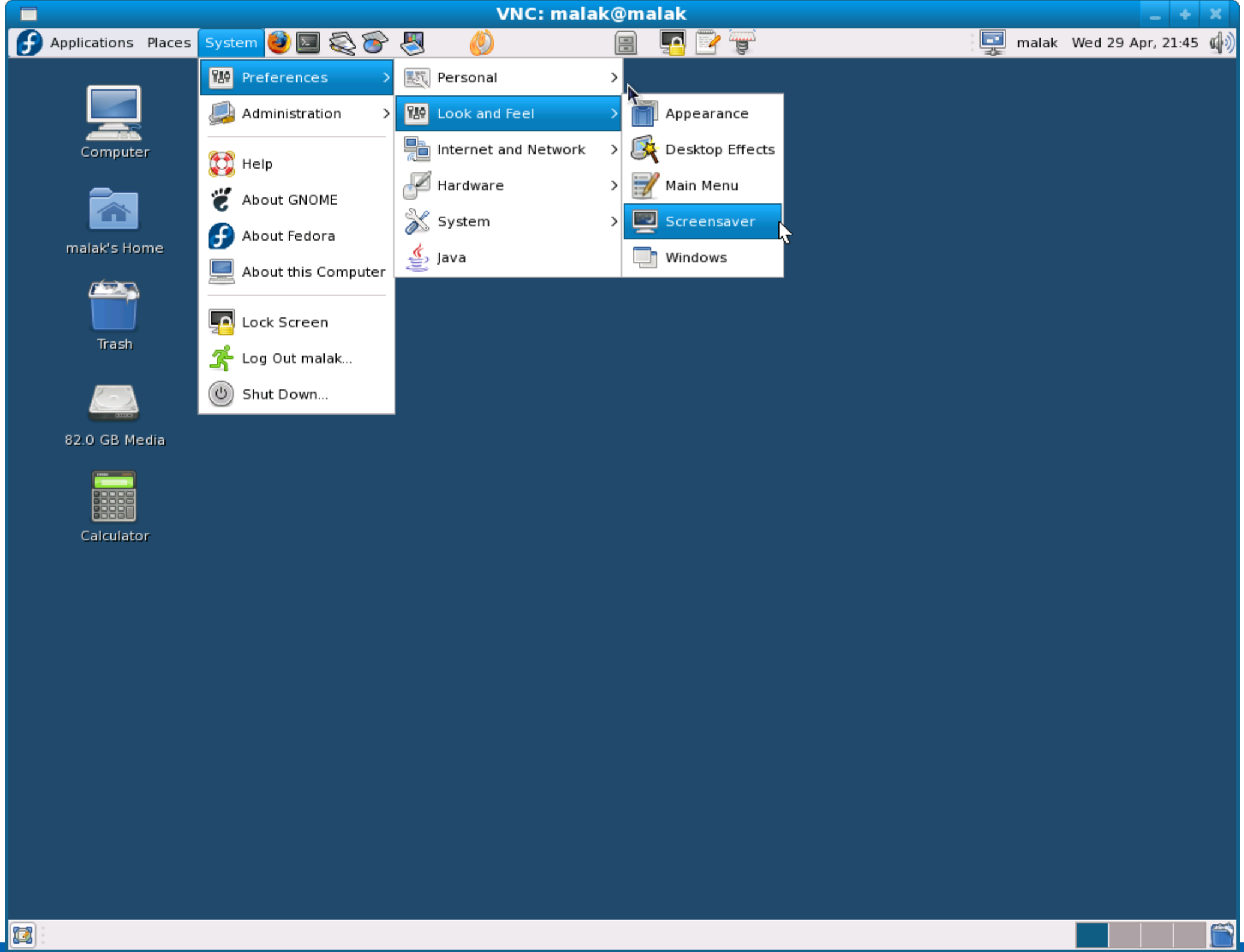
Controllez l'accès à distance à votre bureau



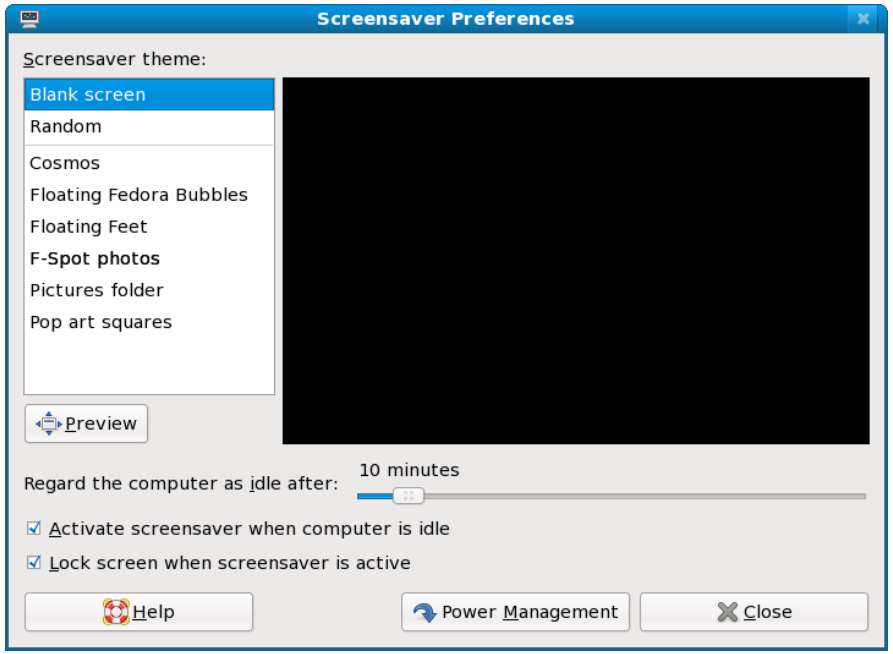
- Vous pouvez décider si votre bureau sera contrôllable à distance à partir de Système | Préférences | Internet et résaux | “Remote Desktop”
- Ubuntu – l'option “Remote Desktop” se trouve directement dans Système | Préférences

Tout le monde doit s'identifier

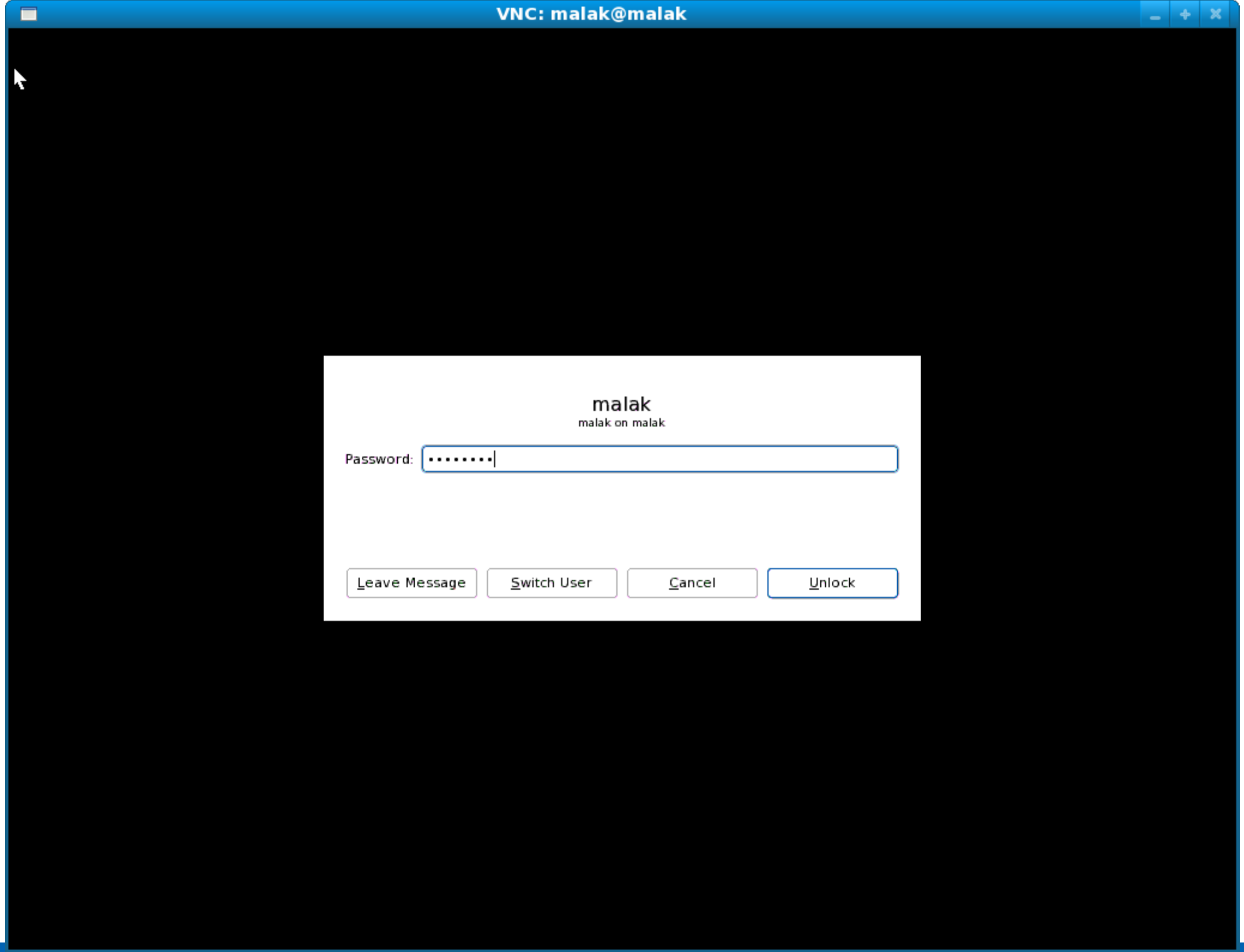
- L'économiseur d'écran devrait exiger un mot de passe afin de libérer l'accès à l'ordinateur
  - système | réglages (preferences en anglais) | “look and feel” | économiseur d'écran
- *Ceci vous donne une certaine protection si vous partez de votre ordinateur pendant quelques minutes (voir la fin de la présentation ...)*


VNC: malak@malak
Applications
Places
System
malak
Wed 29 Apr, 21:45
Preferences
Administration
Help
About GNOME
About Fedora
About this Computer
Lock Screen
Log Out malak...
Shut Down...
Personal
Look and Feel
Internet and Network
Hardware
System
Java
Appearance
Desktop Effects
Main Menu
Screensaver
Windows
Computer
malak's Home
Trash
82.0 GB Media
Calculator

Verrouillage automatique



- Pour verrouiller l'ordi automatiquement par voie de l'économiseur de l'écran dans Gnome c'est dans système | réglages | “look and feel” | économiseur d'écran


VNC: malak@malak
malak
malak on malak
Password:
Leave Message
Switch User
Cancel
Unlock

Gérer les mots de passe

Gérer les mots de passe p.1

- Exiger des mots de passe:
  - d'au moins 8 charactères
    - 1tbm-d+p au lieu de mdp
  - qui ont des caractères majuscules, miniscules et spéciales, et des chiffres, telles
    - °!”#$%?&*()_+=<>/^,
    - 1234567890

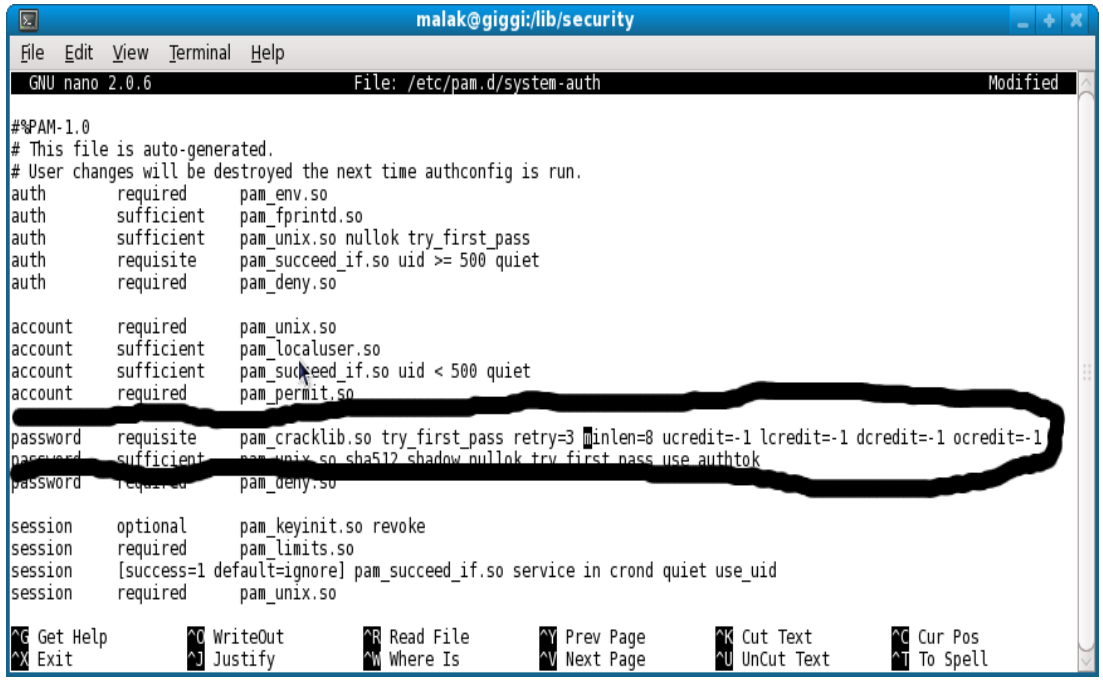
- 1Tbm-D+p au lieu de unmotpas

Gérer les mots de passe p.2

- qui sont faciles à souvenir mais difficiles à deviner, p.ex. les initiales des mots d'une phrase mémorable
  - 1Tbm-D+p --> “un (**1**) **T**rès **b**on **m**ot**-D**e**+p**asse”
- Dans le fichier /etc/login.defs vous pouvez l'expiration des mots de passe

Gérer les mots de passe (p. 4)

(au moins Red Hat / CentOS / Fedora)



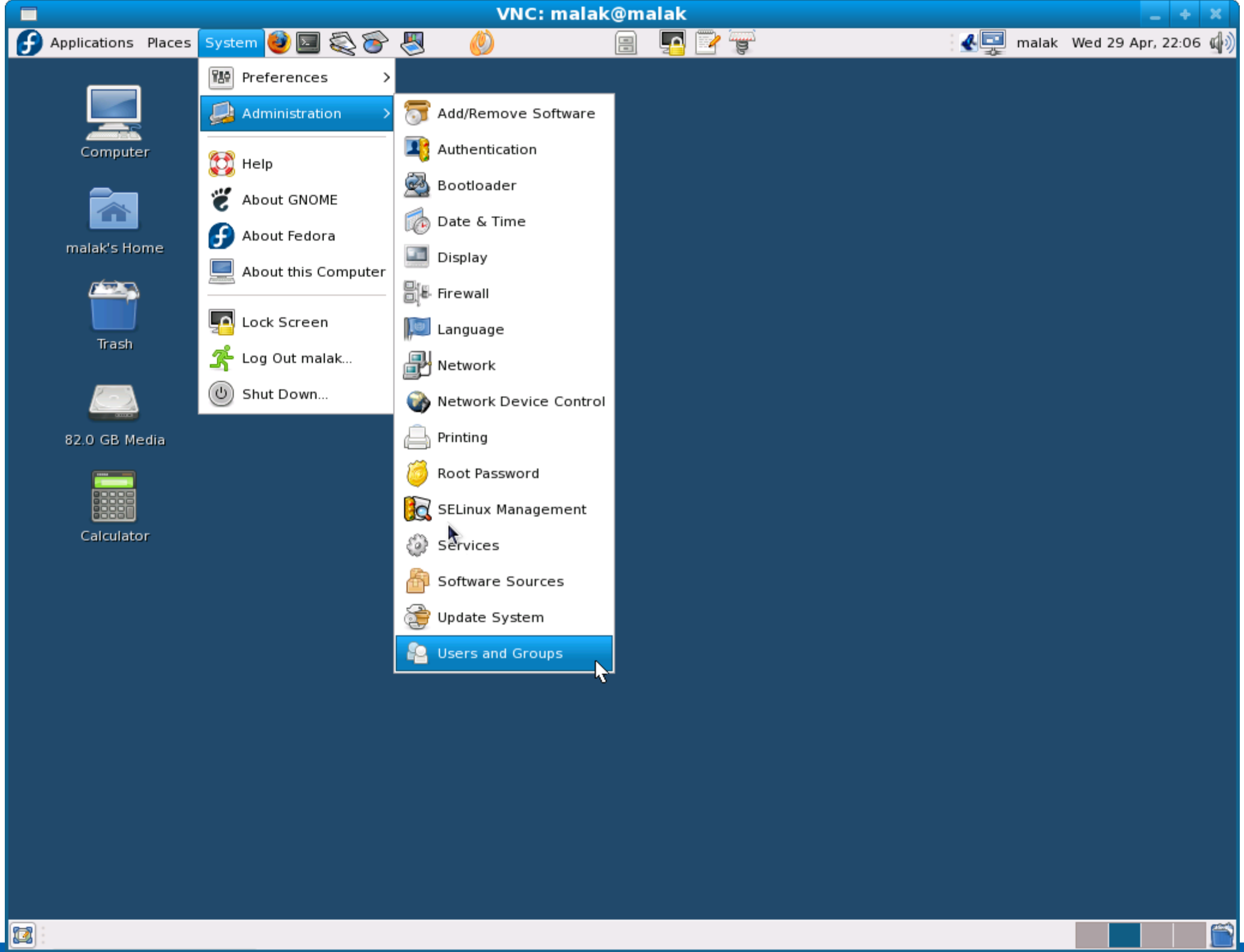
- Dans le fichier /etc/pam.d/system-auth, modifier la ligne:

password requisite /lib/security/$ISA/pam_cracklib.so retry=3

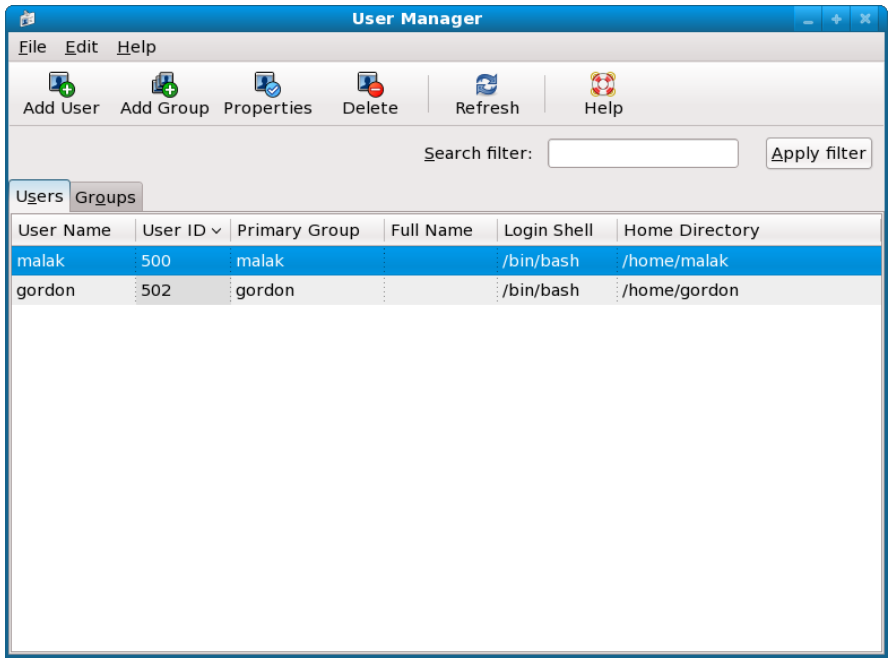
Insérer “minlen=8” (longueur minimale), ucredit=-1 (caractères majuscules),

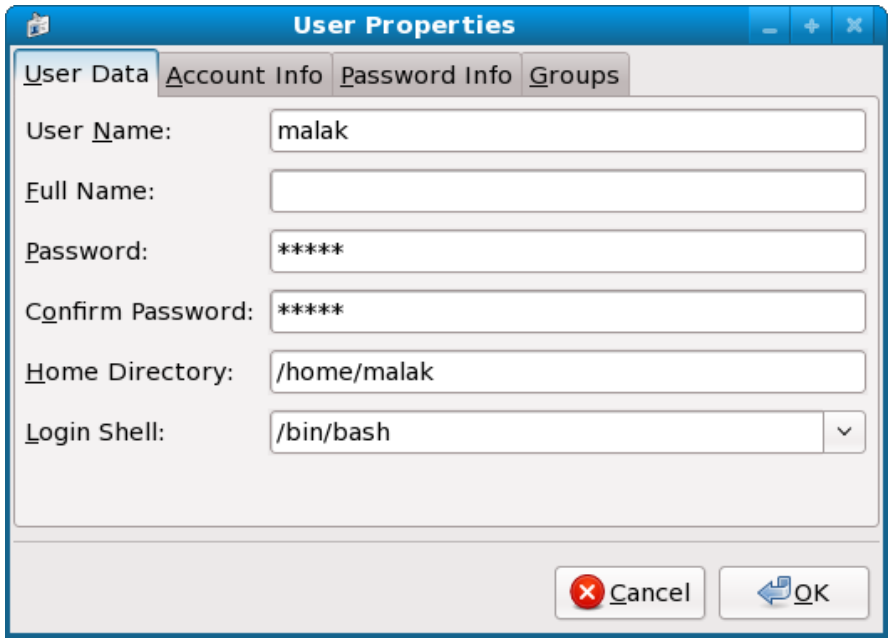
Gérer les mots de passe p.3

- Exiger l'expiration des mots de passe après un certain temps
  - System | Administration | Users and Groups | <fournir le m-d-p de root> | <cliquer sur un nom d'usager> | onglet info m-d-p

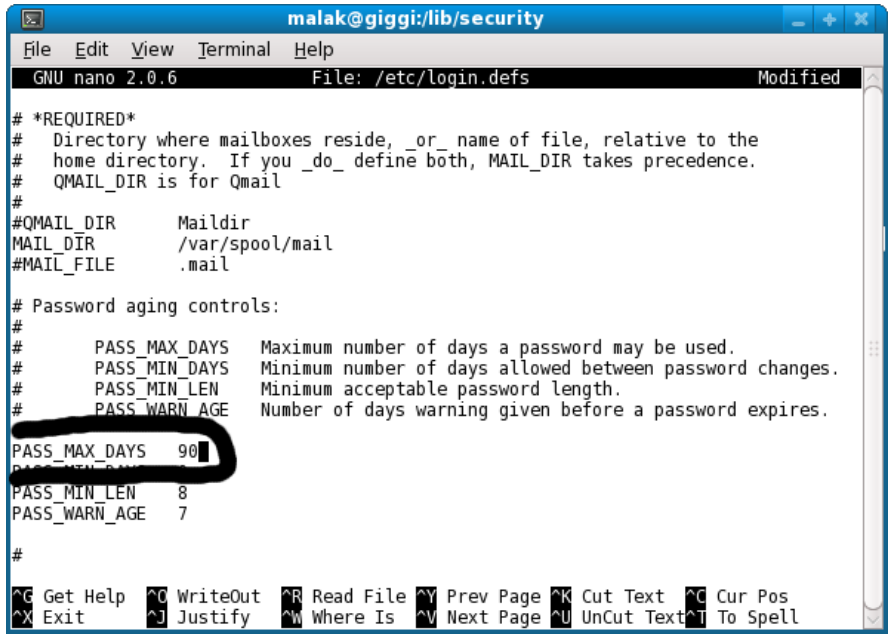

VNC: malak@malak
Applications
Places
System
malak
Wed 29 Apr, 22:06
Preferences
Administration
Help
About GNOME
About Fedora
About this Computer
Lock Screen
Log Out malak...
Shut Down...
Add/Remove Software
Authentication
Bootloader
Date & Time
Display
Firewall
Language
Network
Network Device Control
Printing
Root Password
SELinux Management
Services
Software Sources
Update System
Users and Groups
Computer
malak's Home
Trash
82.0 GB Media
Calculator

Expiration des mots de passe





Expiration des mots de passe (au moins Red Hat / CentOS / Fedora)



- Dans le fichier /etc/login.defs, modifier la ligne “PASS_MAX_DAYS ” à un chiffre comme 90 jours (3 mois)

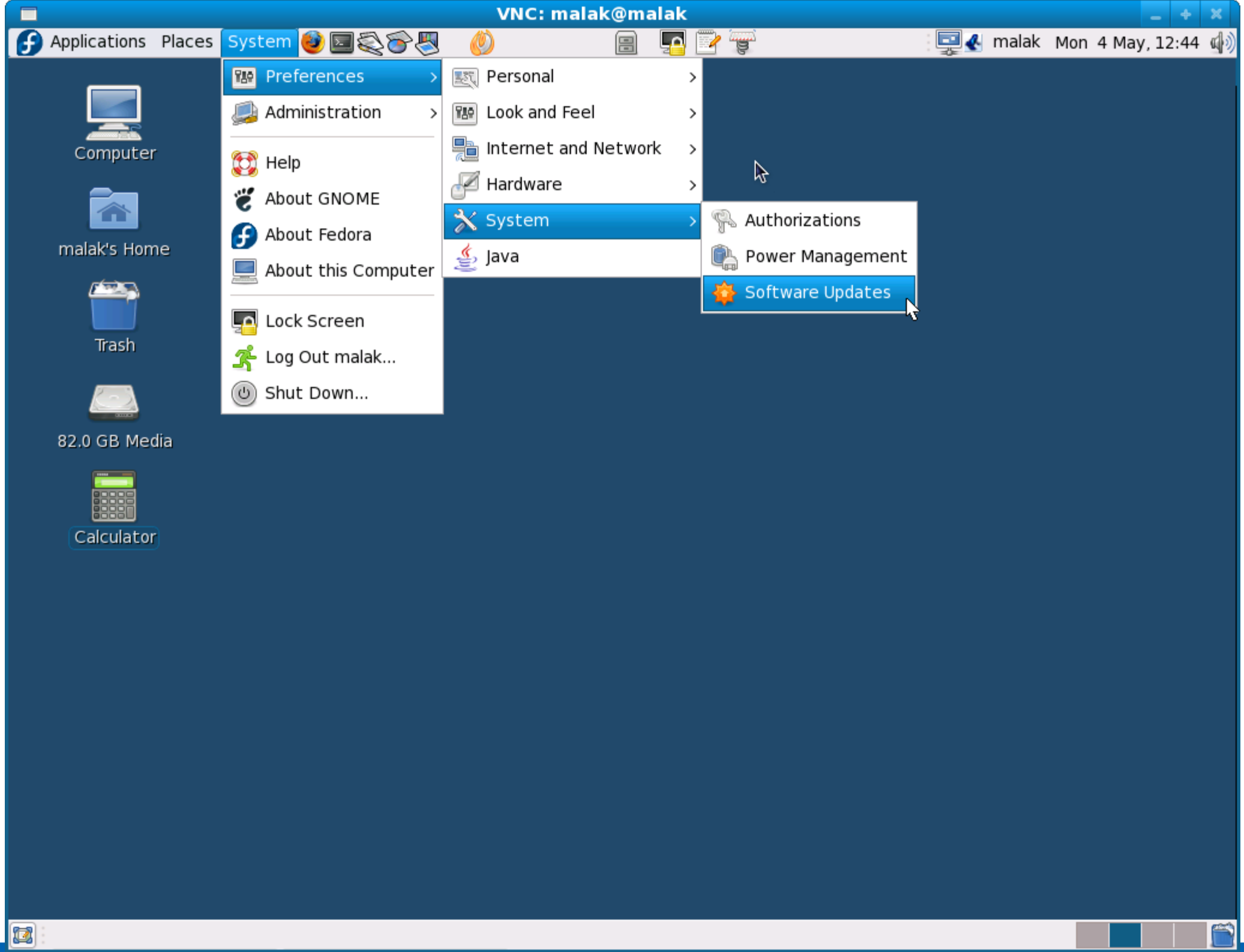
Faire vos mises-à-jour

Faire vos mises-à-jour p.1

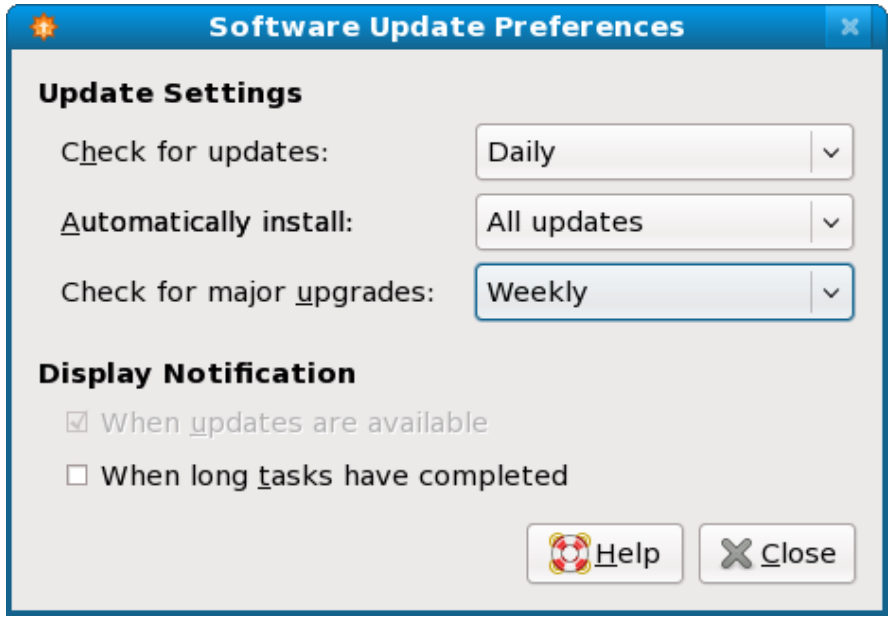
- Les mises-à-jour normalement incluent:
  - Les correctifs de sécurité
  - Les mises-à-jour des logiciels avec des nouveaux fonctions, capacités, améliorations, etc.
  - L'enlèvement ou le remplacement des logiciels désuets et/ou considérés inférieures à des nouveaux logiciels
  - Les installations de nouveaux logiciels susceptibles à être utiles

Faire vos mises-à-jour p.2

- Les mises à jour sont préparées par des équipes de soit des bénévoles, soit des pros, soit les deux, qui se dédient à maintenir votre distribution à jour, et sûr, et s'assurent que ces mises-à-jour sont fonctionnelles, ne “briseront” pas votre système, completes et appropriées.
- Les mises-à-jours normalement devraient se faire automatiquement, à moins que vous préfèrez suivre de près les mises-à-jour


VNC: malak@malak
Applications
Places
System
malak
Mon 4 May, 12:44
Preferences
Administration
Help
About GNOME
About Fedora
About this Computer
Lock Screen
Log Out malak...
Shut Down...
Personal
Look and Feel
Internet and Network
Hardware
System
Java
Authorizations
Power Management
Software Updates
Computer
malak's Home
Trash
82.0 GB Media
Calculator

Faire vos mises-à-jour p.3



- À moins que vous aimez controller les mises-à-jour manuellement, normalement c'est une bonne idée de les faire automatiquement

File Edit View Terminal Tabs Help

```
[malak@malak ~]$ su
Password:
[root@malak malak]# yum update
Loaded plugins: refresh-packagekit
http://livna.cat.pdx.edu/repo/9/i386/repodata/repomd.xml: [Errno 14] HTTP Error 404: Not Found
Trying other mirror.
livna                                                                    | 2.4 kB     00:00
fedora                                                                   | 2.4 kB     00:00
rpmfusion-free-updates                                                   | 2.1 kB     00:00
rpmfusion-nonfree-updates                                                | 2.1 kB     00:00
rpmfusion-free                                                           |  951 B     00:00
adobe-linux-i386                                                         |  951 B     00:00
updates-newkey                                                           | 2.3 kB     00:02
updates-newkey/primary_db                                                | 4.2 MB     04:03
rpmfusion-nonfree                                                        |  951 B     00:00
updates                                                                  | 2.6 kB     00:00
Setting up Update Process
Resolving Dependencies
--> Running transaction check
---> Package firefox.i386 0:3.0.10-1.fc9 set to be updated
---> Package gnome-python2-extras.i386 0:2.19.1-27.fc9 set to be updated
---> Package gnome-python2-gtkhtml2.i386 0:2.19.1-27.fc9 set to be updated
---> Package gnome-python2-libegg.i386 0:2.19.1-27.fc9 set to be updated
---> Package libcurl.i386 0:7.19.4-4.fc9 set to be updated
---> Package libmodplug.i386 1:0.8.7-1.fc9 set to be updated
---> Package totem.i386 0:2.23.2-16.fc9 set to be updated
---> Package totem-gstreamer.i386 0:2.23.2-16.fc9 set to be updated
---> Package totem-mozplugin.i386 0:2.23.2-16.fc9 set to be updated
---> Package totem-nautilus.i386 0:2.23.2-16.fc9 set to be updated
---> Package totem-xine.i386 0:2.23.2-16.fc9 set to be updated
---> Package vlgothic-fonts.noarch 0:20090422-1.fc9 set to be updated
---> Package vlgothic-fonts-common.noarch 0:20090422-1.fc9 set to be updated
---> Package vlgothic-p-fonts.noarch 0:20090422-1.fc9 set to be updated
---> Package xulrunner.i386 0:1.9.0.10-1.fc9 set to be updated
---> Package yelp.i386 0:2.22.1-12.fc9 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                  Arch      Version            Repository         Size
================================================================================
Updating:
 firefox                  i386      3.0.10-1.fc9       updates-newkey     12 M
 gnome-python2-extras     i386      2.19.1-27.fc9      updates-newkey     51 k
 gnome-python2-gtkhtml2   i386      2.19.1-27.fc9      updates-newkey     19 k
 gnome-python2-libegg     i386      2.19.1-27.fc9      updates-newkey     57 k
 libcurl                  i386      7.19.4-4.fc9       updates-newkey    166 k
 libmodplug               i386      1:0.8.7-1.fc9      updates-newkey    171 k
 totem                    i386      2.23.2-16.fc9      updates-newkey    2.4 M
 totem-gstreamer          i386      2.23.2-16.fc9      updates-newkey     69 k
```

File Edit View Terminal Tabs Help

```
---> Package totem-gstreamer.i386 0:2.23.2-16.fc9 set to be updated
---> Package totem-mozplugin.i386 0:2.23.2-16.fc9 set to be updated
---> Package totem-nautilus.i386 0:2.23.2-16.fc9 set to be updated
---> Package totem-xine.i386 0:2.23.2-16.fc9 set to be updated
---> Package vlgothic-fonts.noarch 0:20090422-1.fc9 set to be updated
---> Package vlgothic-fonts-common.noarch 0:20090422-1.fc9 set to be updated
---> Package vlgothic-p-fonts.noarch 0:20090422-1.fc9 set to be updated
---> Package xulrunner.i386 0:1.9.0.10-1.fc9 set to be updated
---> Package yelp.i386 0:2.22.1-12.fc9 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                    Arch      Version            Repository         Size
================================================================================
Updating:
 firefox                    i386      3.0.10-1.fc9       updates-newkey     12 M
 gnome-python2-extras       i386      2.19.1-27.fc9      updates-newkey     51 k
 gnome-python2-gtkhtml2     i386      2.19.1-27.fc9      updates-newkey     19 k
 gnome-python2-libegg       i386      2.19.1-27.fc9      updates-newkey     57 k
 libcurl                    i386      7.19.4-4.fc9       updates-newkey    166 k
 libmodplug                 i386      1:0.8.7-1.fc9      updates-newkey    171 k
 totem                      i386      2.23.2-16.fc9      updates-newkey    2.4 M
 totem-gstreamer            i386      2.23.2-16.fc9      updates-newkey     69 k
 totem-mozplugin            i386      2.23.2-16.fc9      updates-newkey    273 k
 totem-nautilus             i386      2.23.2-16.fc9      updates-newkey     36 k
 totem-xine                 i386      2.23.2-16.fc9      updates-newkey     52 k
 vlgothic-fonts             noarch    20090422-1.fc9     updates-newkey    2.3 M
 vlgothic-fonts-common      noarch    20090422-1.fc9     updates-newkey     15 k
 vlgothic-p-fonts           noarch    20090422-1.fc9     updates-newkey    2.4 M
 xulrunner                  i386      1.9.0.10-1.fc9     updates-newkey    9.0 M
 yelp                       i386      2.22.1-12.fc9      updates-newkey    874 k

Transaction Summary
================================================================================
Install      0 Package(s)
Update      16 Package(s)
Remove       0 Package(s)

Total download size: 30 M
Is this ok [y/N]: y
Downloading Packages:
(1/16): vlgothic-fonts-common-20090422-1.fc9.noarch.rpm                  |  15 kB     00:03
(2/16): gnome-python2-gtkhtml2-2.19.1-27.fc9.i386.rpm                    |  19 kB     00:01
(3/16): totem-nautilus-2.23.2-16.fc9.i386.rpm                            |  36 kB     00:02
(4/16): gnome-python2-extras-2.19.1-27.fc9.i386.rpm                      |  51 kB     00:03
(5/16): totem-xine-2.23.2-16.fc9.i386.rpm                                |  52 kB     00:04
(6/16): gnome-python2-libegg-2.19.1-27.fc9.i386.rpm                      |  57 kB     00:04
(7/16): totem-gstreamer-2.23.2-16.fc9.i386.rpm                           |  69 kB     00:06
(8/16): libcurl-7.19.4-4.fc9.i386.rpm               (1%) 57% [=========================   ]  11 kB/s |  96 kB     00:06 ETA
```

File Edit View Terminal Tabs Help

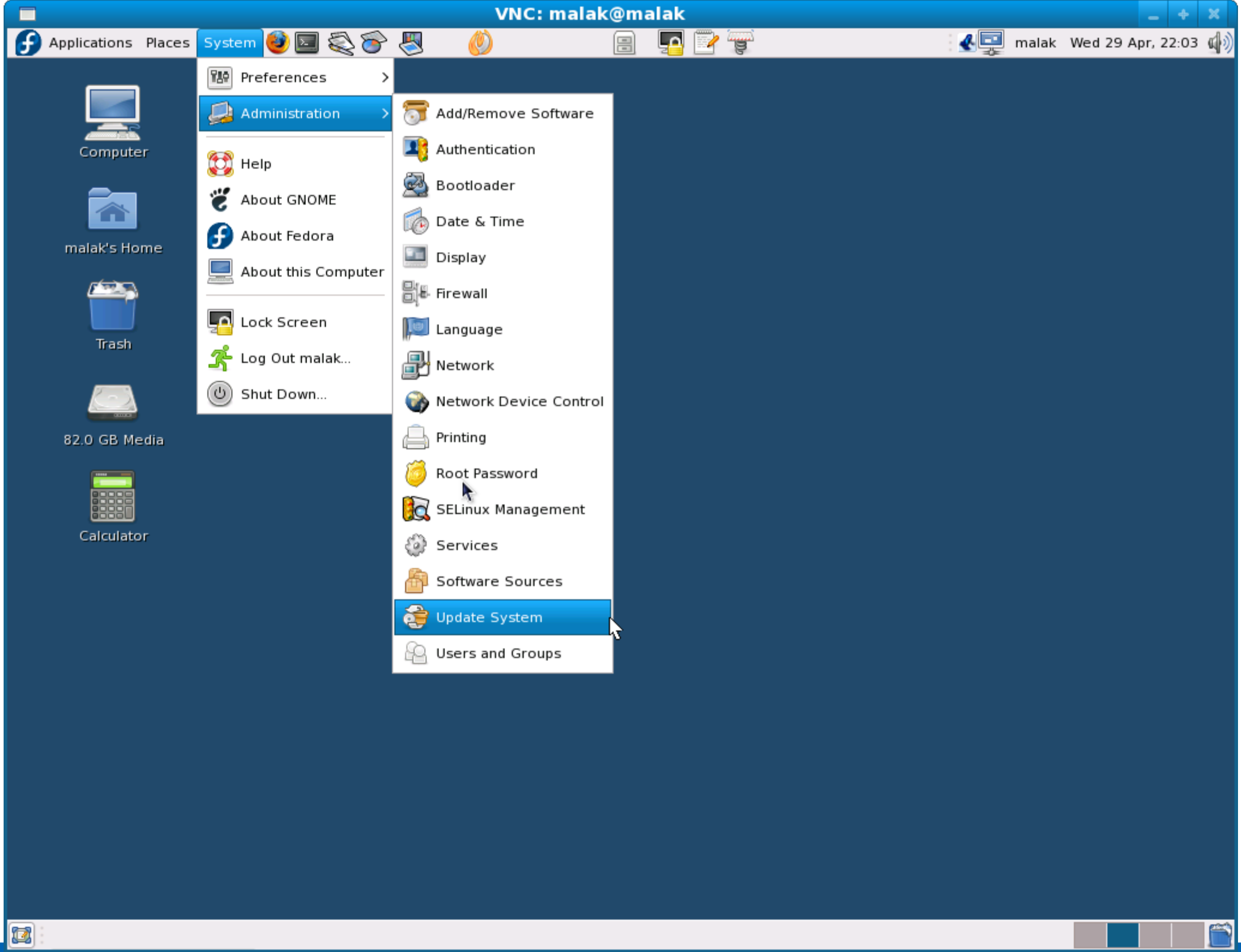
```
gordon@austin:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages have been kept back:
  nvidia-common
The following packages will be upgraded:
  acpid apport apport-gtk apt apt-utils cups cups-bsd cups-client cups-common
  dash dkms doc-base dpkg fakeroot fglrx-amdcccle fglrx-kernel-source
  fglrx-modaliases firefox firefox-3.0 firefox-3.0-branding
  firefox-3.0-gnome-support firefox-gnome-support flashplugin-nonfree foo2zjs
  foomatic-filters ghostscript ghostscript-x gnome-system-tools
  gnome-user-guide gstreamer0.10-alsa gstreamer0.10-gnomevfs
  gstreamer0.10-plugins-base gstreamer0.10-plugins-base-apps
  gstreamer0.10-plugins-good gstreamer0.10-pulseaudio gstreamer0.10-x gvfs
  gvfs-backends gvfs-bin gvfs-fuse libavcodec51 libavformat52 libavutil49
  libcups2 libcupsimage2 libcurl3 libcurl3-gnutls libfreetype6 libglib2.0-0
  libglib2.0-data libgs8 libgstreamer-plugins-base0.10-0 libgvfscommon0
  libicu38 libjasper1 libkrb53 liblcms1 libnm-glib0 libnm-util0 libnss3-1d
  libpam-modules libpam-runtime libpam0g libpango1.0-0 libpango1.0-common
  libpng12-0 libpoppler-glib3 libpoppler3 libpostproc51 libpurple-bin
  libpurple0 libsndfile1 libssl0.9.8 libvolume-id0 libwmf0.2-7
  linux-headers-2.6.27-11 linux-headers-2.6.27-11-generic
  linux-image-2.6.27-11-generic linux-libc-dev network-manager
  network-manager-gnome openssl pidgin pidgin-data poppler-utils python-apport
  python-problem-report sudo tasksel tasksel-data tzdata udev xfonts-scalable
  xorg-driver-fglrx xserver-common xserver-xorg-core xserver-xorg-video-intel
  xulrunner-1.9 xulrunner-1.9-gnome-support
99 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
Need to get 114MB of archives.
After this operation, 73.7kB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://ca.archive.ubuntu.com intrepid-updates/main dash 0.5.4-9ubuntu1.1 [
Get:2 http://ca.archive.ubuntu.com intrepid-updates/main dpkg 1.14.20ubuntu6.2 [
Get:3 http://ca.archive.ubuntu.com intrepid-updates/main ghostscript 8.63.dfsg.1
Get:4 http://ca.archive.ubuntu.com intrepid-updates/main libkrb53 1.6.dfsg.4~bet
Get:5 http://ca.archive.ubuntu.com intrepid-updates/main libcups2 1.3.9-2ubuntu9
Get:6 http://ca.archive.ubuntu.com intrepid-updates/main libpng12-0 1.2.27-1ubun
Get:7 http://ca.archive.ubuntu.com intrepid-updates/main libcupsimage2 1.3.9-2ub
```

File Edit View Terminal Tabs Help

```
Get:97 http://ca.archive.ubuntu.com intrepid-updates/restricted fglrx-amdcccle 2:8.543-0ubuntu4.1 [6749kB]
Get:98 http://ca.archive.ubuntu.com intrepid-updates/main fglrx-modaliases 2:8.543-0ubuntu4.1 [10.9kB]
Get:99 http://ca.archive.ubuntu.com intrepid-updates/main gnome-system-tools 2.22.1-0ubuntu1.1 [2792kB]
Fetched 114MB in 2min47s (685kB/s)
Extracting templates from packages: 100%
Preconfiguring packages ...
(Reading database ... 132418 files and directories currently installed.)
Preparing to replace dash 0.5.4-9ubuntu1 (using .../dash_0.5.4-9ubuntu1.1_i386.deb) ...
Unpacking replacement dash ...
Processing triggers for man-db ...
Setting up dash (0.5.4-9ubuntu1.1) ...

(Reading database ... 132418 files and directories currently installed.)
Preparing to replace dpkg 1.14.20ubuntu6.1 (using .../dpkg_1.14.20ubuntu6.2_i386.deb) ...
Unpacking replacement dpkg ...
Processing triggers for man-db ...
Setting up dpkg (1.14.20ubuntu6.2) ...

(Reading database ... 132418 files and directories currently installed.)
Preparing to replace ghostscript 8.63.dfsg.1-0ubuntu6.2 (using .../ghostscript_8.63.dfsg.1-0ubuntu6.4_i386.deb) ...
Cleaning up font configuration of gs...
Cleaning up category psprint..
Cleaning up category cmap..
Cleaning up category cid..
Cleaning up category truetype..
Cleaning up category gsfontderivative..
Cleaning up category type3..
Cleaning up category type1..
Unpacking replacement ghostscript ...
Preparing to replace libkrb53 1.6.dfsg.4~beta1-3 (using .../libkrb53_1.6.dfsg.4~beta1-3ubuntu0.1_i386.deb) ...
Unpacking replacement libkrb53 ...
Preparing to replace libcups2 1.3.9-2ubuntu6.1 (using .../libcups2_1.3.9-2ubuntu9.1_i386.deb) ...
Unpacking replacement libcups2 ...
Preparing to replace libpng12-0 1.2.27-1 (using .../libpng12-0_1.2.27-1ubuntu0.1_i386.deb) ...
Unpacking replacement libpng12-0 ...
Preparing to replace libcupsimage2 1.3.9-2ubuntu6.1 (using .../libcupsimage2_1.3.9-2ubuntu9.1_i386.deb) ...
Unpacking replacement libcupsimage2 ...
Preparing to replace libgs8 8.63.dfsg.1-0ubuntu6.2 (using .../libgs8_8.63.dfsg.1-0ubuntu6.4_i386.deb) ...
Unpacking replacement libgs8 ...
```

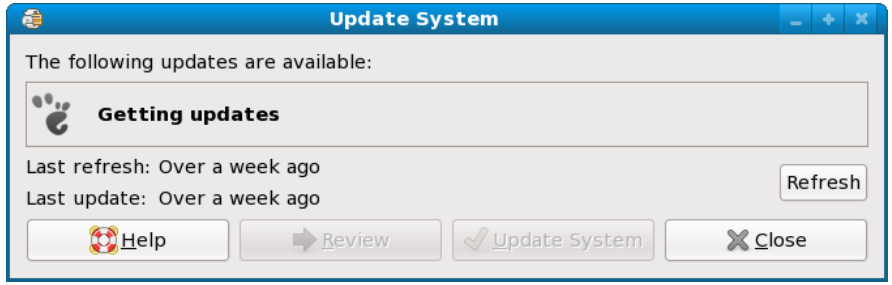
Faire vos mises-à-jour p.2

- Graphique
  - ***Fedora/CentOS/Ubuntu/Debian:*** Système | Administration | Mises-à-jour
  - ***Ubuntu/Debian:*** Système | Administration | Mises-à-jour | Synaptic | (add the appropriate choice here)


VNC: malak@malak
Applications
Places
System
malak
Wed 29 Apr, 22:03
Computer
malak's Home
Trash
82.0 GB Media
Calculator
Preferences
Administration
Help
About GNOME
About Fedora
About this Computer
Lock Screen
Log Out malak...
Shut Down...
Add/Remove Software
Authentication
Bootloader
Date & Time
Display
Firewall
Language
Network
Network Device Control
Printing
Root Password
SELinux Management
Services
Software Sources
Update System
Users and Groups

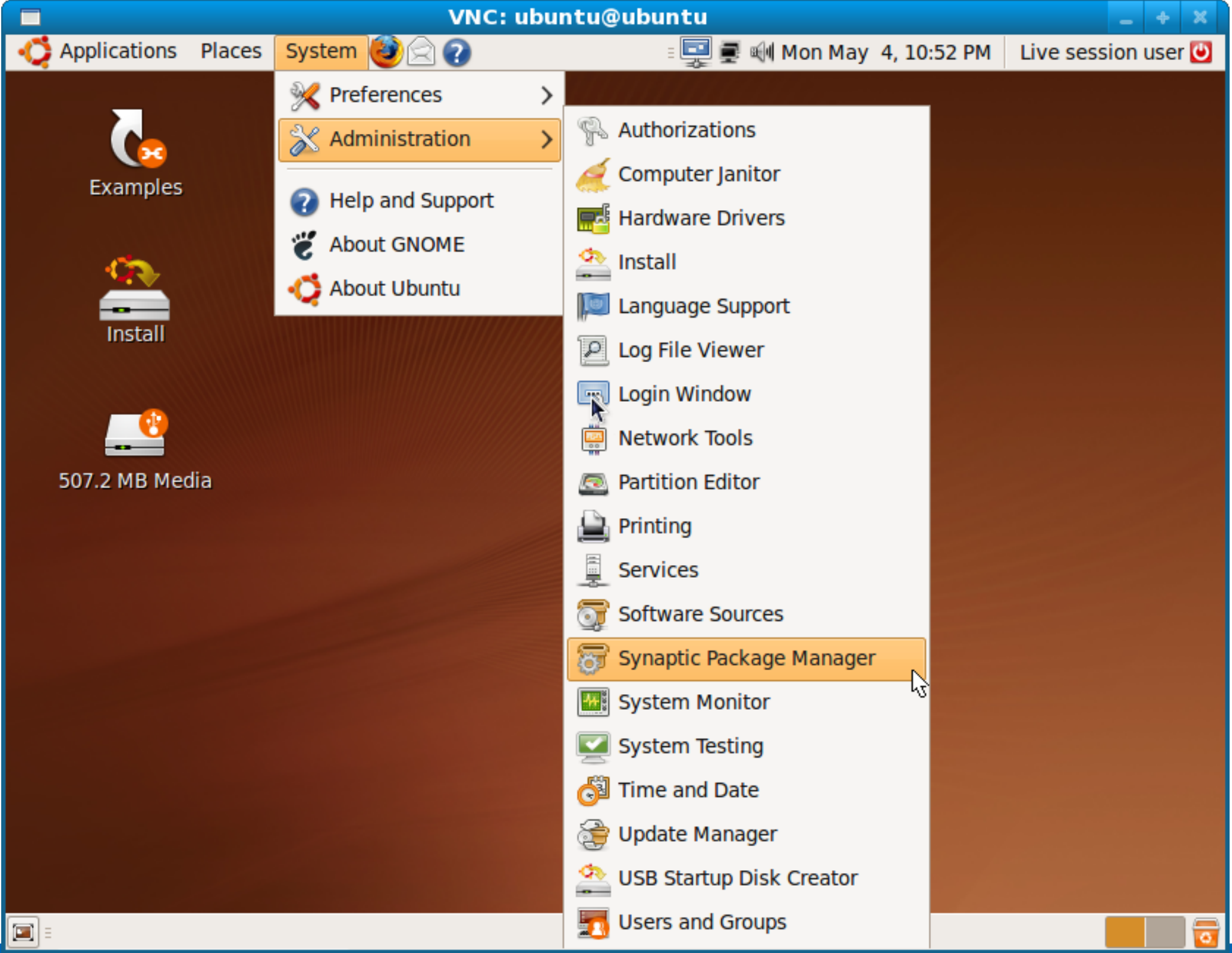
Faire vos mises-à-jour p.3

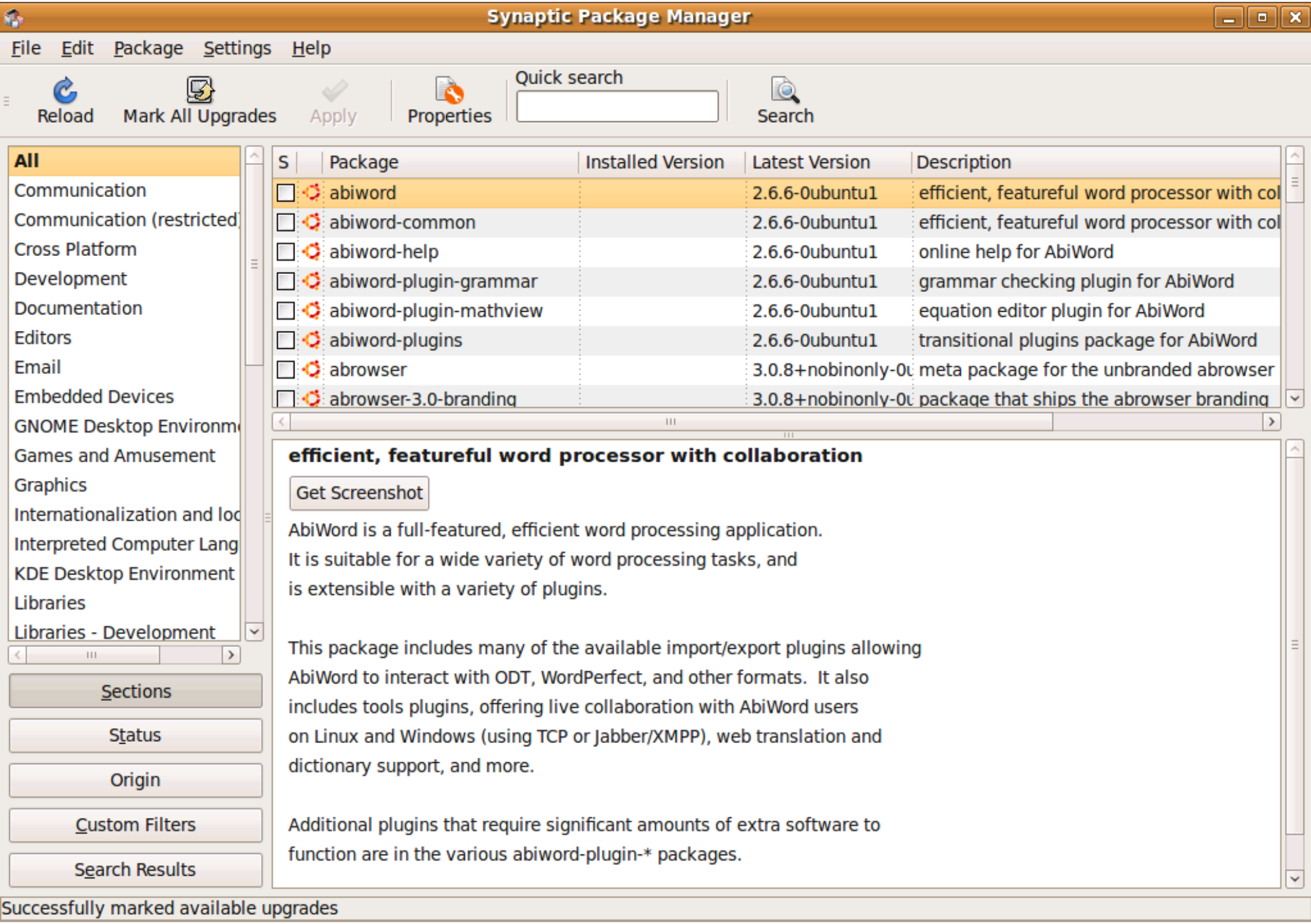
- ***Fedora / CentOS / Ubuntu / Debian:***
  Système | Administration | Mises-à-jour



Faire vos mises-à-jour p.4

- ***Ubuntu/Debian:*** Système | Administration | Mises-à-jour | Synaptic | (Gestionnaire de paquetages) et cliquer sur “Appliquer”


VNC: ubuntu@ubuntu
Applications
Places
System
Mon May 4, 10:52 PM
Live session user
Preferences
Administration
Help and Support
About GNOME
About Ubuntu
Authorizations
Computer Janitor
Hardware Drivers
Install
Language Support
Log File Viewer
Login Window
Network Tools
Partition Editor
Printing
Services
Software Sources
Synaptic Package Manager
System Monitor
System Testing
Time and Date
Update Manager
USB Startup Disk Creator
Users and Groups
Examples
Install
507.2 MB Media


Synaptic Package Manager
File Edit Package Settings Help
Reload
Mark All Upgrades
Apply
Properties
Quick search
Search
All
Communication
Communication (restricted)
Cross Platform
Development
Documentation
Editors
Email
Embedded Devices
GNOME Desktop Environm
Games and Amusement
Graphics
Internationalization and loc
Interpreted Computer Lang
KDE Desktop Environment
Libraries
Libraries - Development
Sections
Status
Origin
Custom Filters
Search Results
S
Package
Installed Version
Latest Version
Description
abiword 2.6.6-0ubuntu1 efficient, featureful word processor with col
abiword-common 2.6.6-0ubuntu1 efficient, featureful word processor with col
abiword-help 2.6.6-0ubuntu1 online help for AbiWord
abiword-plugin-grammar 2.6.6-0ubuntu1 grammar checking plugin for AbiWord
abiword-plugin-mathview 2.6.6-0ubuntu1 equation editor plugin for AbiWord
abiword-plugins 2.6.6-0ubuntu1 transitional plugins package for AbiWord
abrowser 3.0.8+nobinonly-0 meta package for the unbranded abrowser
abrowser-3.0-branding 3.0.8+nobinonly-0 package that ships the abrowser branding
efficient, featureful word processor with collaboration
Get Screenshot
AbiWord is a full-featured, efficient word processing application.
It is suitable for a wide variety of word processing tasks, and
is extensible with a variety of plugins.
This package includes many of the available import/export plugins allowing
AbiWord to interact with ODT, WordPerfect, and other formats. It also
includes tools plugins, offering live collaboration with AbiWord users
on Linux and Windows (using TCP or Jabber/XMPP), web translation and
dictionary support, and more.
Additional plugins that require significant amounts of extra software to
function are in the various abiword-plugin-* packages.
Successfully marked available upgrades

Installer les logiciels à partir des dépots de paquettages

Installer les logiciels à partir des dépots de paquettages

- Dans le Windows, on télécharge un logiciel de n'importe où et on peut l'installer directement; c'est un jeu complet avec tout les composants nécessaires.
- Dans le Windows, apart la partie strictement “Windows”, c'est vous le responsable de suivre touts les logiciels installés, la disponibilité des mises-à-jour et des correctifs, et de les installer -- en présumant que ceux-ci sont même disponibles! (***Admettons que certains logiciels ont un option de mise-à-jour automatique, mais seulement pour eux-mêmes.***)

Installer les logiciels à partir des “repositories”

- *Dans le linux, les logiciels sont plutôt normalement installés à partir d'un* ***gestionnaire de paquettages*** qui:
  - détermine les logiciels de support nécessaires, s'ils existent sur le système déjà ou non, et les cherche au nécessaire;
  - il gère les versions, mises-à-jours et correctifs;
  - il coordonne l'installation des logiciels;
  - etc.

Installer les logiciels à partir des dépots de paquettages

- L'important à saisir c'est qu'avec *TOUT* les logiciels installés à partir de votre gestionnaire de paquettages des dépots de paquettages -- que ça soit “la partie linux”, les logiciels de base tels les fontes, le “desktop”, un logiciel comme OpenOffice.org, ou Firefox -- ***s'il y a un correctif à apporter,*** normalement les grands distributions (Ubuntu, OpenSuse, Fedora, Debian, Mandriva, CentOS, PCLinuxOS, etc.) et les grands distributions desquels y sont dérivés, ***vont sortir ces correctifs, taillés pour leur distribution, dans des brefs délais***.

Installer les logiciels à partir des dépots de paquettages

- ***Et alors, quand vous avez l'option d'installer un logiciel à partir de n'importe où <u>OU</u> à partir d'un dépot de paquettages, il est toujours à privilégier de l'installer à partir du dépot de paquettage.***

Installer les logiciels à partir des dépots de paquettages

- ***Il se peut alors que certains logiciels que vous vouler utiliser ne font pas partie de votre distribution ou un dépot de paquettages taillé pour votre distribution: Le choix alors est de trouver une distribution qui l'a dans ses dépots OU de tolérer ceci, MAIS dans le but de garder au minimum le nombre de logiciels non-supportés.***

ubuntu documentation

Search

Community Documentation

RepositoriesUbuntu

What are Repositories?

Contents

There are literally thousands of Ubuntu programs available to meet the needs of Ubuntu users. **Many of these programs are stored in software** archives commonly referred to as *repositories*. Repositories make it very easy to install new software onto Ubuntu using an Internet connection, while also providing a high level of security, as each program available in the repositories is thoroughly tested and built specifically for each version of Ubuntu.

The Ubuntu software repositories are organized into four separate areas or "components", according to the the level of support offered by Ubuntu and whether or not the program in question complies with Ubuntu's Free Software Philosophy.

The repository components are:

- **Main** - Officially supported software.
- **Restricted** - Supported software that is not available under a completely free license.
- **Universe** - Community maintained software, i.e. not officially supported software.
- **Multiverse** - Software that is not free.

For more information regarding the Ubuntu Repository components, click here.

The Ubuntu *Install* CDs contain software from the "Main" and "Restricted" components of the repositories. Once your system is made aware of the Internet-based locations for these repositories, many more software programs are available for installation. By using the software package management tools already installed on your system, you can search for, install and update any piece of software directly over the Internet, without the need for the CD.

Adding Repositories in Ubuntu

Adding Repositories in Ubuntu

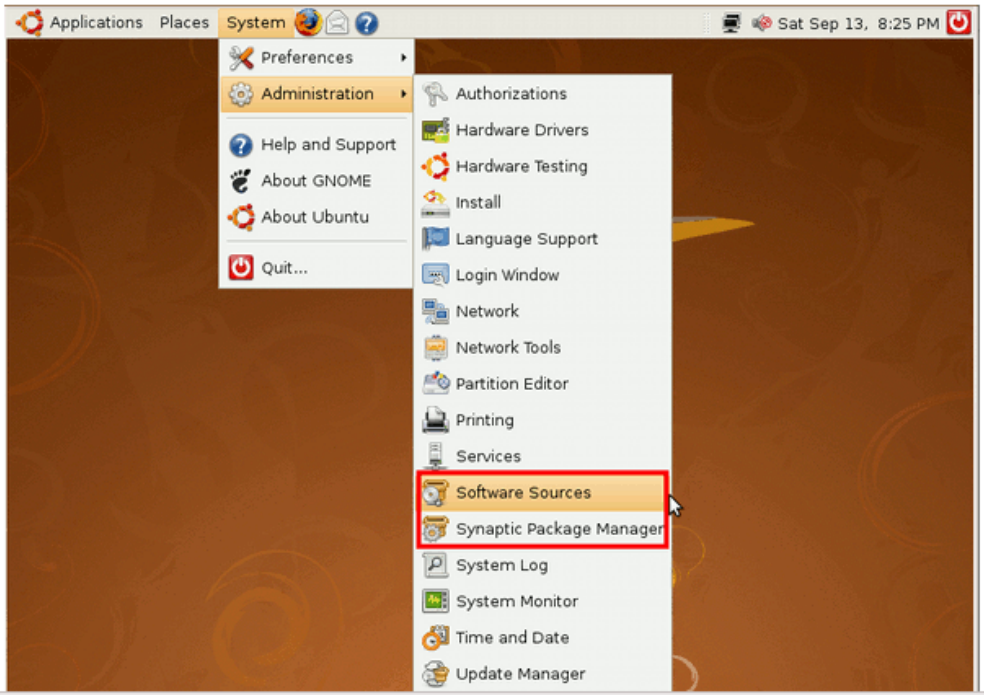
This section describes how to manage software repositories in **Ubuntu 7.04 (Feisty Fawn)** (EOL), **Ubuntu 7.10 (Gutsy Gibbon)** (EOL), **Ubuntu 8.04 (Hardy Heron)**, **Ubuntu 8.10 (Intrepid Ibex)**, and **Ubuntu 9.04 (Jaunty Jackalope)**. For earlier versions of Ubuntu please refer to Repositories/Ubuntu/Dapper. For **Kubuntu** please see Kubuntu repository management.

> The operations described on this page modify the software repositories configuration file located at
>
> ```
> /etc/apt/sources.list
> ```

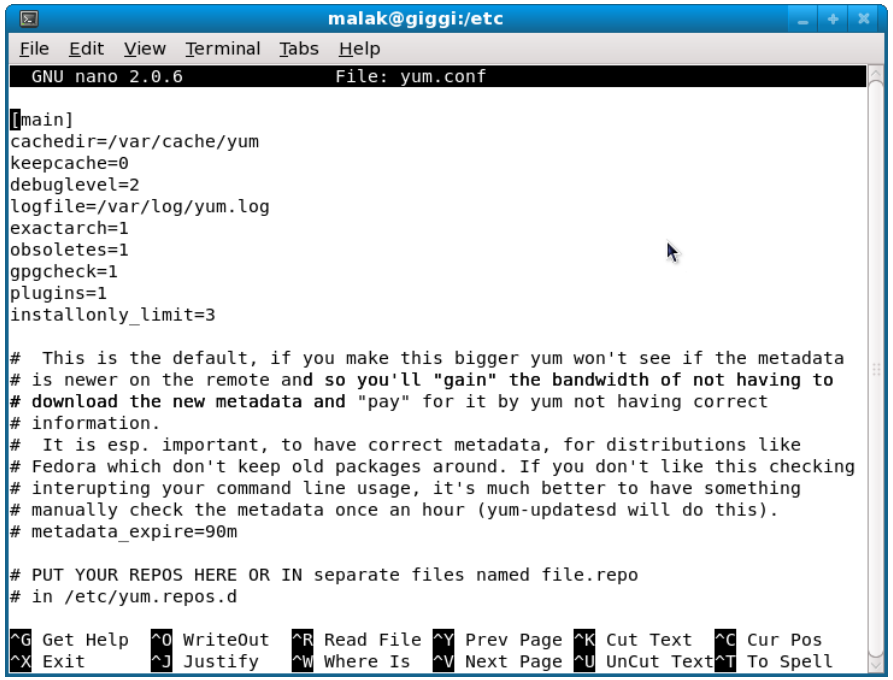
Software sources can also be managed by making direct modifications to this file using the command line. If you prefer to use the command line instead of a graphical user interface, see Managing Repositories from the Command Line instead.

GUI-based repository management is normally accomplished via the "Software Sources" panel. This panel can be accessed via two menus:

- Software Sources: System > Administration > Software Sources.
- *Synaptic*: System > Administration > *Synaptic* >> Settings >> Repositories.
- You will have to enter your password to gain access to the page.

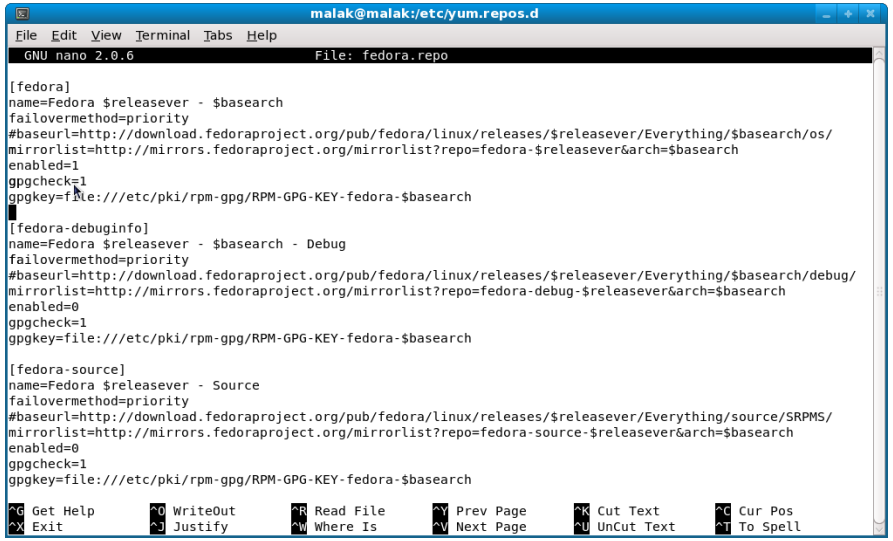


Les fichiers infos pour les “repositories” Red Hat / Fedora / CentOS



- Dans un système Red Hat / Fedora / Centos le fichier à modifier est /etc/yum.conf
- Il se peut que sur la page web du “repository”, il y a un fichier qui s'installe automatiquement qui installe les fichiers nécessaires

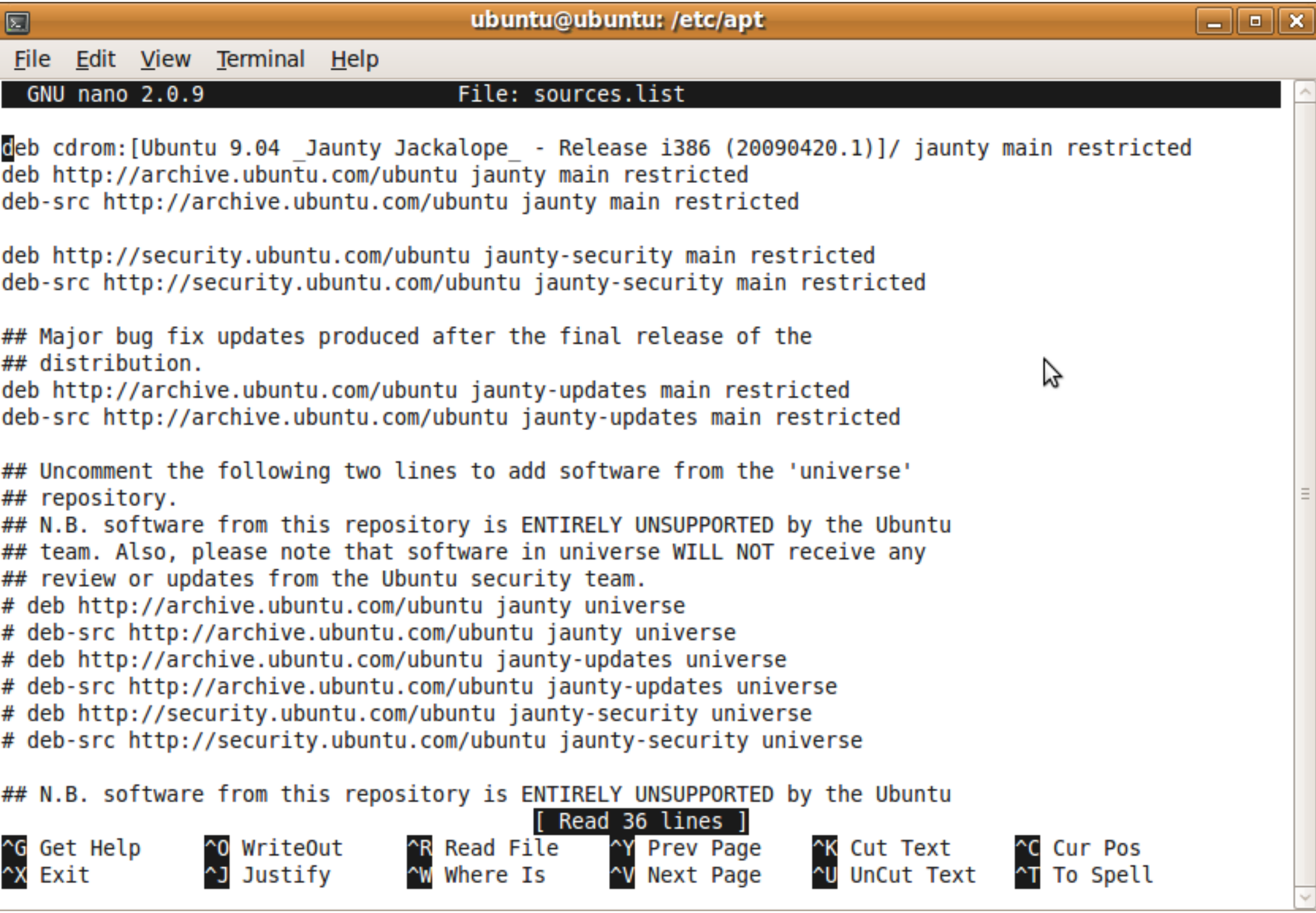
Les fichiers infos pour les “repositories” Red Hat / Fedora / CentOS

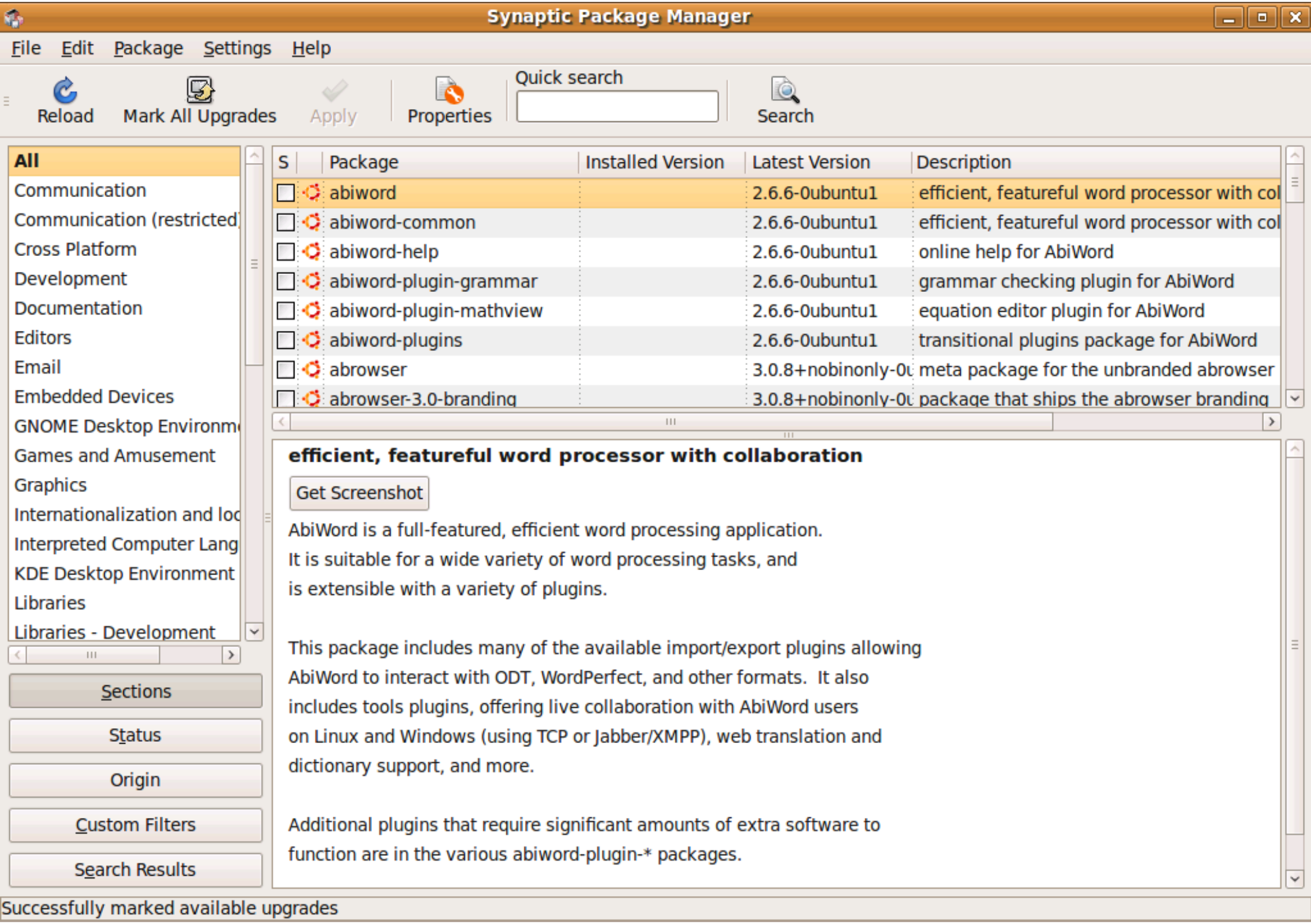


- Vous pourrez aussi avoir des fichiers séparés dans /etc/yum/repo.d qui sont nommés “file.repo” où “file” représente normalement le nom du “repository”
  - ***Normalement sur les pages web des “repositories” le texte à intégrer est disponible pour du copie-collage***

Les fichiers infos pour les “repositories” Ubuntu / Debian

- Dans un système Ubuntu / Debian le fichier à modifier est /etc/apt/sources.list
- Il se peut que sur la page web du “repository”, il y a un fichier qui s'installe automatiquement qui installe les fichiers nécessaires
- ***Normalement sur les pages web des “repositories” le texte à intégrer est disponible pour du copie-collage***
- ***Ubuntu organise ses “repositories” en quatre catégories, soit “main”, “restricted”, “universe” et “multiverse”***


ubuntu@ubuntu: /etc/apt
File Edit View Terminal Help
GNU nano 2.0.9 File: sources.list
deb cdrom:[Ubuntu 9.04 _Jaunty Jackalope_ - Release i386 (20090420.1)]/ jaunty main restricted
deb http://archive.ubuntu.com/ubuntu jaunty main restricted
deb-src http://archive.ubuntu.com/ubuntu jaunty main restricted
deb http://security.ubuntu.com/ubuntu jaunty-security main restricted
deb-src http://security.ubuntu.com/ubuntu jaunty-security main restricted
Major bug fix updates produced after the final release of the
distribution.
deb http://archive.ubuntu.com/ubuntu jaunty-updates main restricted
deb-src http://archive.ubuntu.com/ubuntu jaunty-updates main restricted
Uncomment the following two lines to add software from the 'universe'
repository.
N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
team. Also, please note that software in universe WILL NOT receive any
review or updates from the Ubuntu security team.
deb http://archive.ubuntu.com/ubuntu jaunty universe
deb-src http://archive.ubuntu.com/ubuntu jaunty universe
deb http://archive.ubuntu.com/ubuntu jaunty-updates universe
deb-src http://archive.ubuntu.com/ubuntu jaunty-updates universe
deb http://security.ubuntu.com/ubuntu jaunty-security universe
deb-src http://security.ubuntu.com/ubuntu jaunty-security universe
N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
[Read 36 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

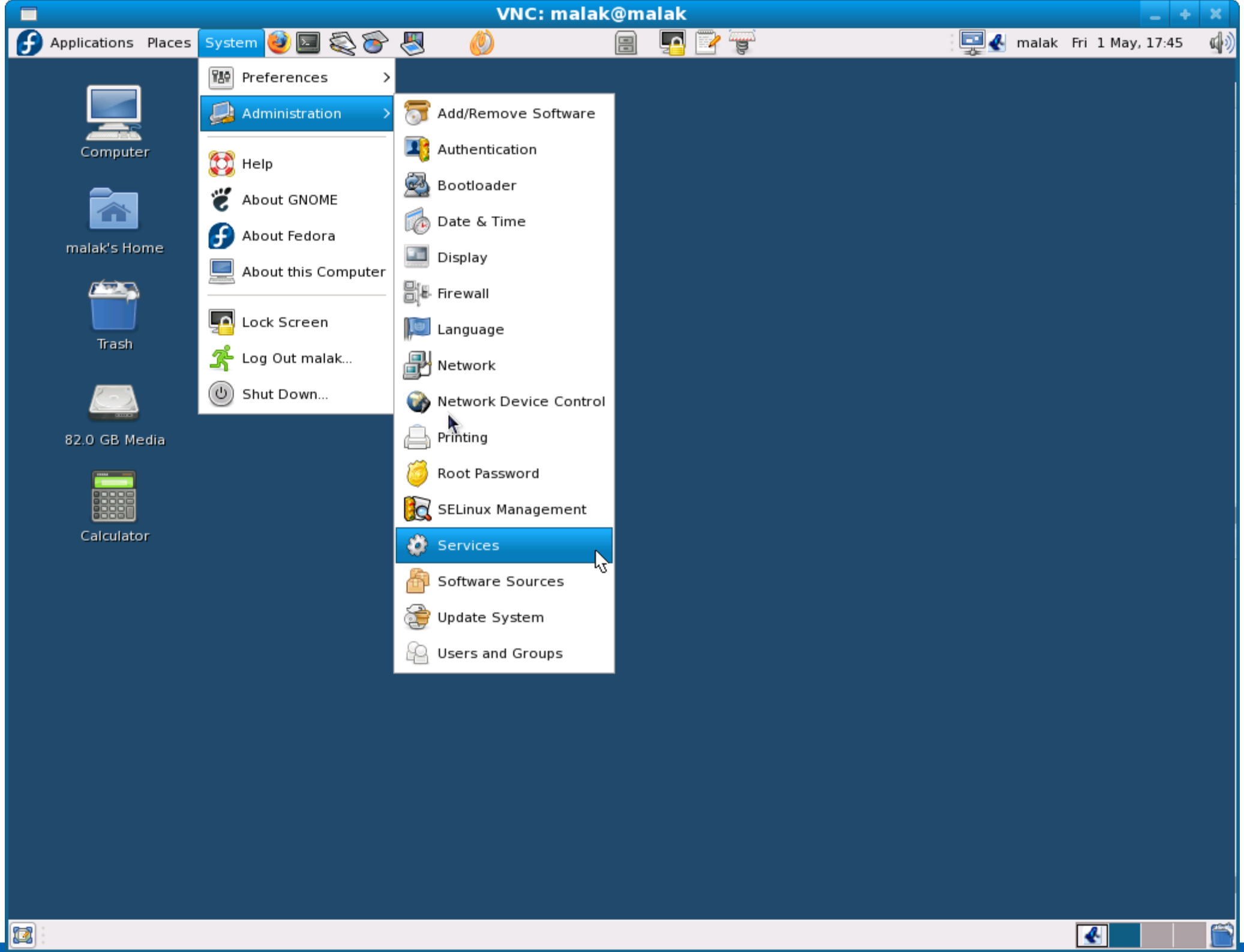

Synaptic Package Manager
File Edit Package Settings Help
Reload
Mark All Upgrades
Apply
Properties
Quick search
Search
All
Communication
Communication (restricted)
Cross Platform
Development
Documentation
Editors
Email
Embedded Devices
GNOME Desktop Environm
Games and Amusement
Graphics
Internationalization and loc
Interpreted Computer Lang
KDE Desktop Environment
Libraries
Libraries - Development
Sections
Status
Origin
Custom Filters
Search Results
S
Package
Installed Version
Latest Version
Description
abiword 2.6.6-0ubuntu1 efficient, featureful word processor with col
abiword-common 2.6.6-0ubuntu1 efficient, featureful word processor with col
abiword-help 2.6.6-0ubuntu1 online help for AbiWord
abiword-plugin-grammar 2.6.6-0ubuntu1 grammar checking plugin for AbiWord
abiword-plugin-mathview 2.6.6-0ubuntu1 equation editor plugin for AbiWord
abiword-plugins 2.6.6-0ubuntu1 transitional plugins package for AbiWord
abrowser 3.0.8+nobinonly-0 meta package for the unbranded abrowser
abrowser-3.0-branding 3.0.8+nobinonly-0 package that ships the abrowser branding
efficient, featureful word processor with collaboration
Get Screenshot
AbiWord is a full-featured, efficient word processing application.
It is suitable for a wide variety of word processing tasks, and
is extensible with a variety of plugins.
This package includes many of the available import/export plugins allowing
AbiWord to interact with ODT, WordPerfect, and other formats. It also
includes tools plugins, offering live collaboration with AbiWord users
on Linux and Windows (using TCP or Jabber/XMPP), web translation and
dictionary support, and more.
Additional plugins that require significant amounts of extra software to
function are in the various abiword-plugin-* packages.
Successfully marked available upgrades

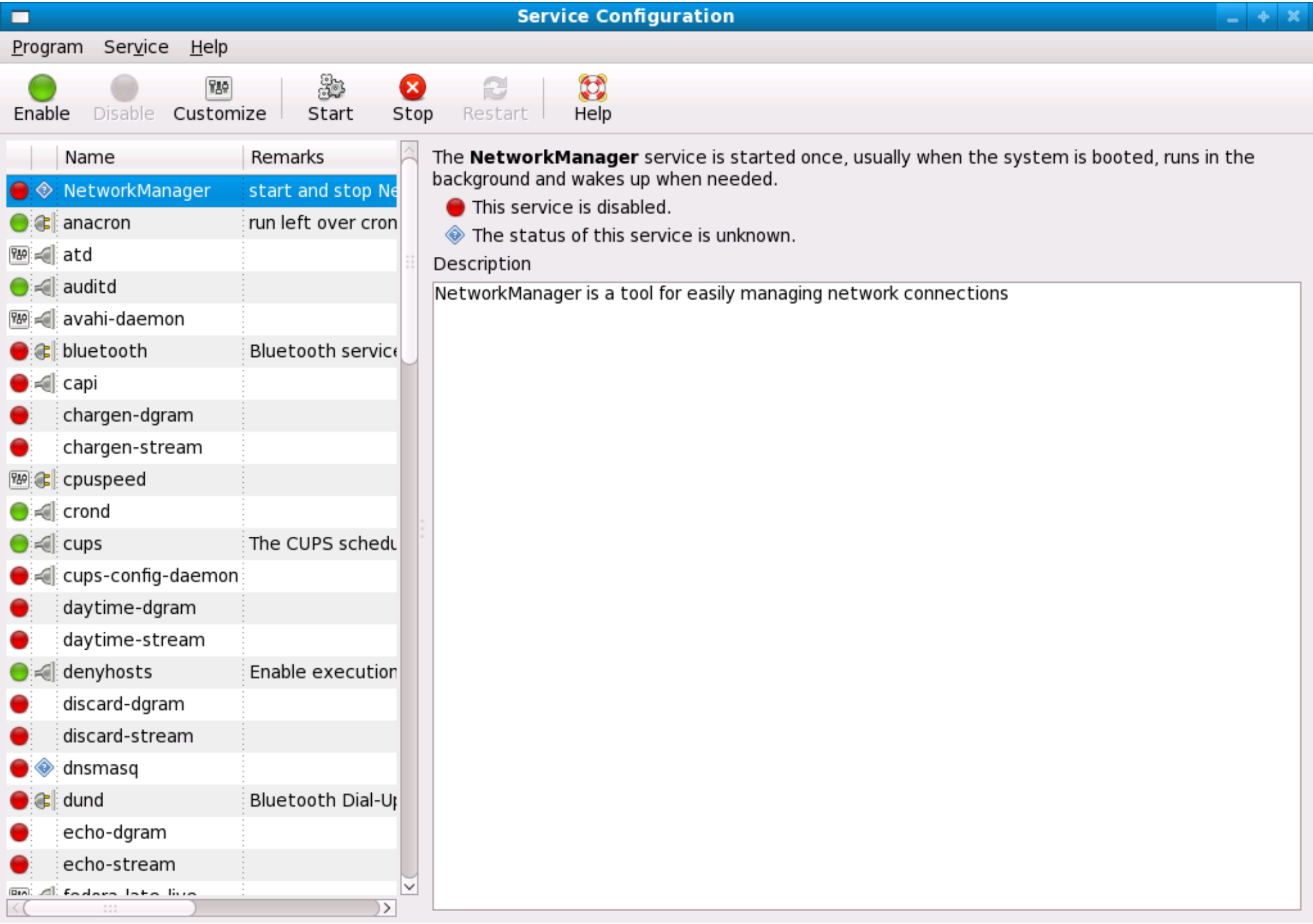
Fermer les services qui ne vous sont pas nécessaires

Fermer les services qui ne vous sont pas nécessaires

- Si vous n'accédez pas votre ordinateur à distance par certains voies, les services non-utilisés devraient çetre fermés afin de limiter ces pistes d'accès par des “crackers”

- ftp
- sshd
- vnc
- httpd
- sendmail
- netconsole

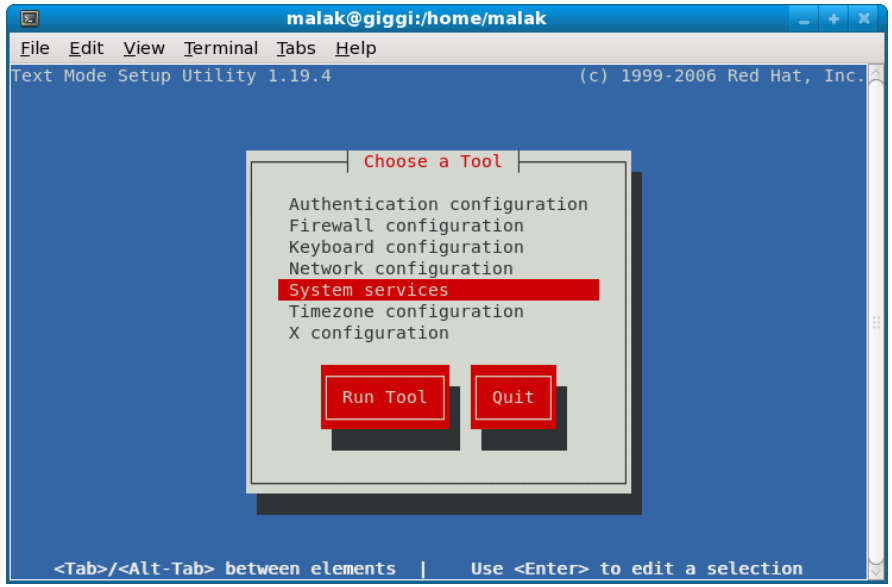

VNC: malak@malak
Applications
Places
System
malak
Fri 1 May, 17:45
Computer
malak's Home
Trash
82.0 GB Media
Calculator
Preferences
Administration
Help
About GNOME
About Fedora
About this Computer
Lock Screen
Log Out malak...
Shut Down...
Add/Remove Software
Authentication
Bootloader
Date & Time
Display
Firewall
Language
Network
Network Device Control
Printing
Root Password
SELinux Management
Services
Software Sources
Update System
Users and Groups


Service Configuration
Program
Service
Help
Enable
Disable
Customize
Start
Stop
Restart
Help
Name
Remarks
NetworkManager
start and stop Ne
anacron
run left over cron
atd
auditd
avahi-daemon
bluetooth
Bluetooth service
capi
chargen-dgram
chargen-stream
cpuspeed
crond
cups
The CUPS schedu
cups-config-daemon
daytime-dgram
daytime-stream
denyhosts
Enable execution
discard-dgram
discard-stream
dnsmasq
dund
Bluetooth Dial-Up
echo-dgram
echo-stream
The NetworkManager service is started once, usually when the system is booted, runs in the background and wakes up when needed.
This service is disabled.
The status of this service is unknown.
Description
NetworkManager is a tool for easily managing network connections

Services sur Ubuntu

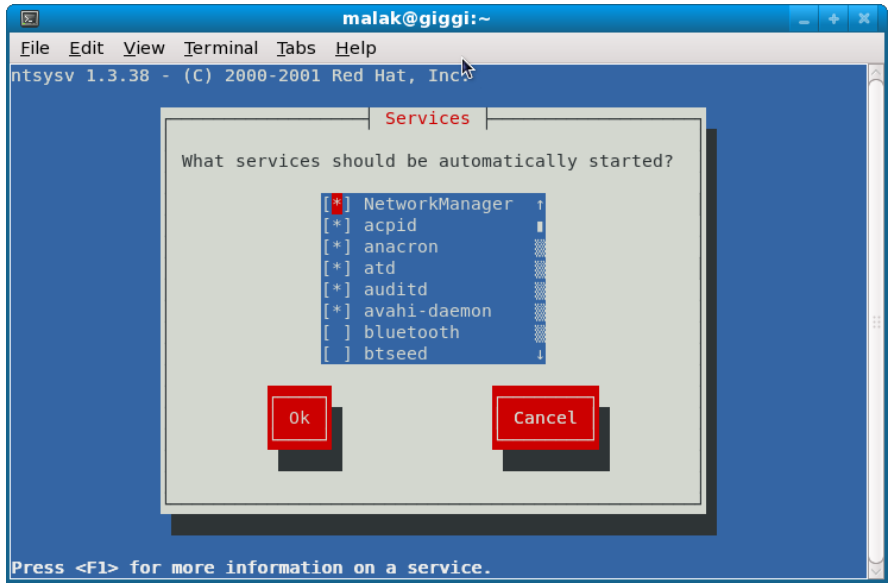
- Présentation des services disponibles sur Ubuntu 9.04 Jaunty Jackalope Live CD

Fermer les services qui ne vous sont pas nécessaires



- Sur un sytème Red Hat / CentOS / Fedora et dérivés, en tant de “root” entrer *setup* et vous aurez ce menu; choisir “System services”

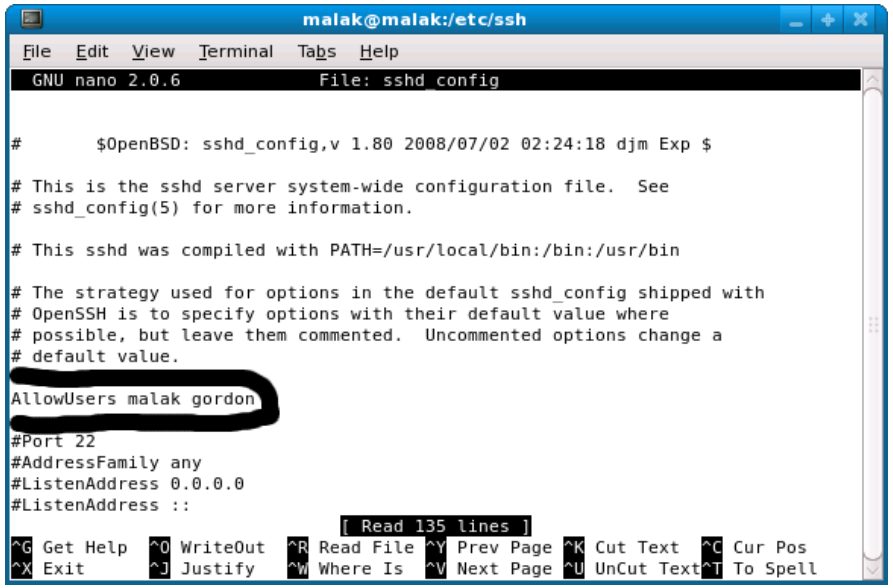
Fermer les services qui ne vous sont pas nécessaires



- Puis, dans la liste de services, surligner les services visés avec les flèches haut et bas, et choisir de l'avoir activé ou désactivé au démarrage du système en cliquant sur <espace> (un étoile indique qu'il sera activé)

Limiter l'accès SSH à certains utilisateurs

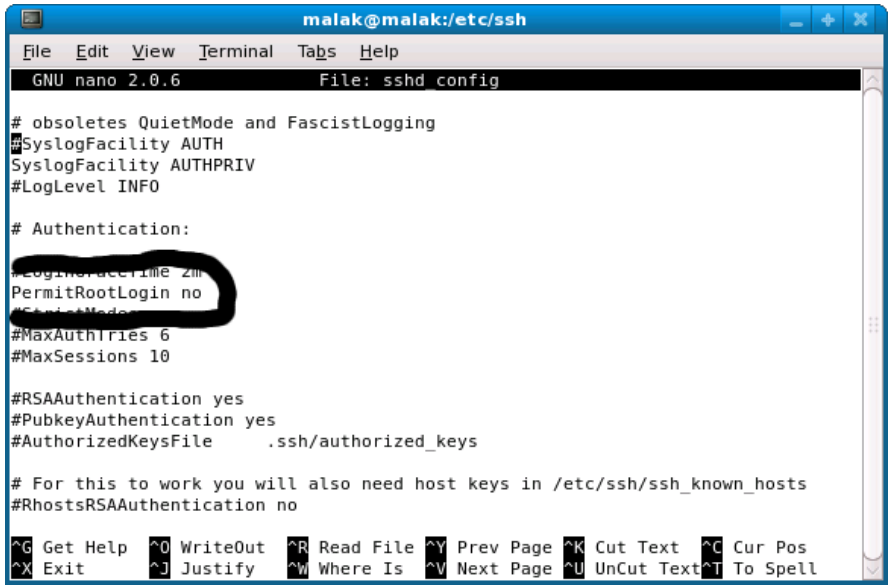
Limiter l'accès SSH à certains utilisateurs



- En tant de “root”, ouvrir le fichier /etc/ssh/sshd_config avec un éditeur de texte et insérer la ligne “AllowUsers” suivi par les noms d'utilisateurs autorisé, séparés par des espaces “ “
- Assurer-vous qu'il n'y a pas de “#” au début de la ligne, sinon la commande serait rendue nulle

Ne pas permettre l'accès SSH direct au compte “root”

Ne pas permettre l'accès SSH direct au compte “root”



- En tant de “root”, ouvrir le fichier /etc/ssh/sshd_config avec un éditeur de texte et éditer la ligne “PermitRootLogin” pour que “no” est indiqué au lieu de “yes”, et supprimer le “#” au début de la ligne, sinon la commande sera rendue nulle


malak@malak:/var/log
File Edit View Terminal Tabs Help
GNU nano 2.0.6 File: secure
Apr 26 13:54:26 malak sshd[23323]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:26 malak sshd[23323]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:26 malak sshd[23323]: pam_succeed_if(sshd:auth): error retrieving information about user tomcat
Apr 26 13:54:27 malak sshd[23320]: Failed password for invalid user root from 202.105.49.16 port 43998 ssh2
Apr 26 13:54:28 malak sshd[23323]: Failed password for invalid user tomcat from 202.105.49.16 port 42446 ssh2
Apr 26 13:54:28 malak sshd[23322]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:28 malak sshd[23321]: Invalid user cady from 202.105.49.16
Apr 26 13:54:28 malak sshd[23325]: input_userauth_request: invalid user cady
Apr 26 13:54:28 malak sshd[23321]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:28 malak sshd[23321]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:28 malak sshd[23321]: pam_succeed_if(sshd:auth): error retrieving information about user cady
Apr 26 13:54:28 malak sshd[23324]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:30 malak sshd[23326]: Invalid user marine from 202.105.49.16
Apr 26 13:54:30 malak sshd[23327]: input_userauth_request: invalid user marine
Apr 26 13:54:30 malak sshd[23326]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:30 malak sshd[23326]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:30 malak sshd[23326]: pam_succeed_if(sshd:auth): error retrieving information about user marine
Apr 26 13:54:30 malak sshd[23325]: Connection closed by 202.105.49.16
Apr 26 13:54:30 malak sshd[23321]:
Apr 26 13:54:31 malak sshd[23328]: User root from 202.105.49.16 not allowed because not listed in AllowUsers
Apr 26 13:54:31 malak sshd[23329]:
Apr 26 13:54:31 malak sshd[23328]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16 user=$
Apr 26 13:54:31 malak sshd[23326]: Failed password for invalid user marine from 202.105.49.16 port 45914 ssh2
Apr 26 13:54:32 malak sshd[23327]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:33 malak sshd[23328]: Failed password for invalid user root from 202.105.49.16 port 49276 ssh2
Apr 26 13:54:33 malak sshd[23329]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:36 malak sshd[23330]: Invalid user global from 202.105.49.16
Apr 26 13:54:36 malak sshd[23331]: input_userauth_request: invalid user global
Apr 26 13:54:36 malak sshd[23330]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:36 malak sshd[23330]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:36 malak sshd[23330]: pam_succeed_if(sshd:auth): error retrieving information about user global
Apr 26 13:54:37 malak sshd[23332]: User root from 202.105.49.16 not allowed because not listed in AllowUsers
Apr 26 13:54:37 malak sshd[23333]: input_userauth_request: invalid user root
Apr 26 13:54:37 malak sshd[23332]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16 user=$
Apr 26 13:54:38 malak sshd[23330]: Failed password for invalid user global from 202.105.49.16 port 49425 ssh2
Apr 26 13:54:38 malak sshd[23334]: Invalid user marine from 202.105.49.16
Apr 26 13:54:38 malak sshd[23335]: input_userauth_request: invalid user marine
Apr 26 13:54:38 malak sshd[23331]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:38 malak sshd[23334]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:38 malak sshd[23334]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:38 malak sshd[23334]: pam_succeed_if(sshd:auth): error retrieving information about user marine
Apr 26 13:54:39 malak sshd[23332]: Failed password for invalid user root from 202.105.49.16 port 53047 ssh2
Apr 26 13:54:39 malak sshd[23333]: Received disconnect from 202.105.49.16: 11: Bye Bye
^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

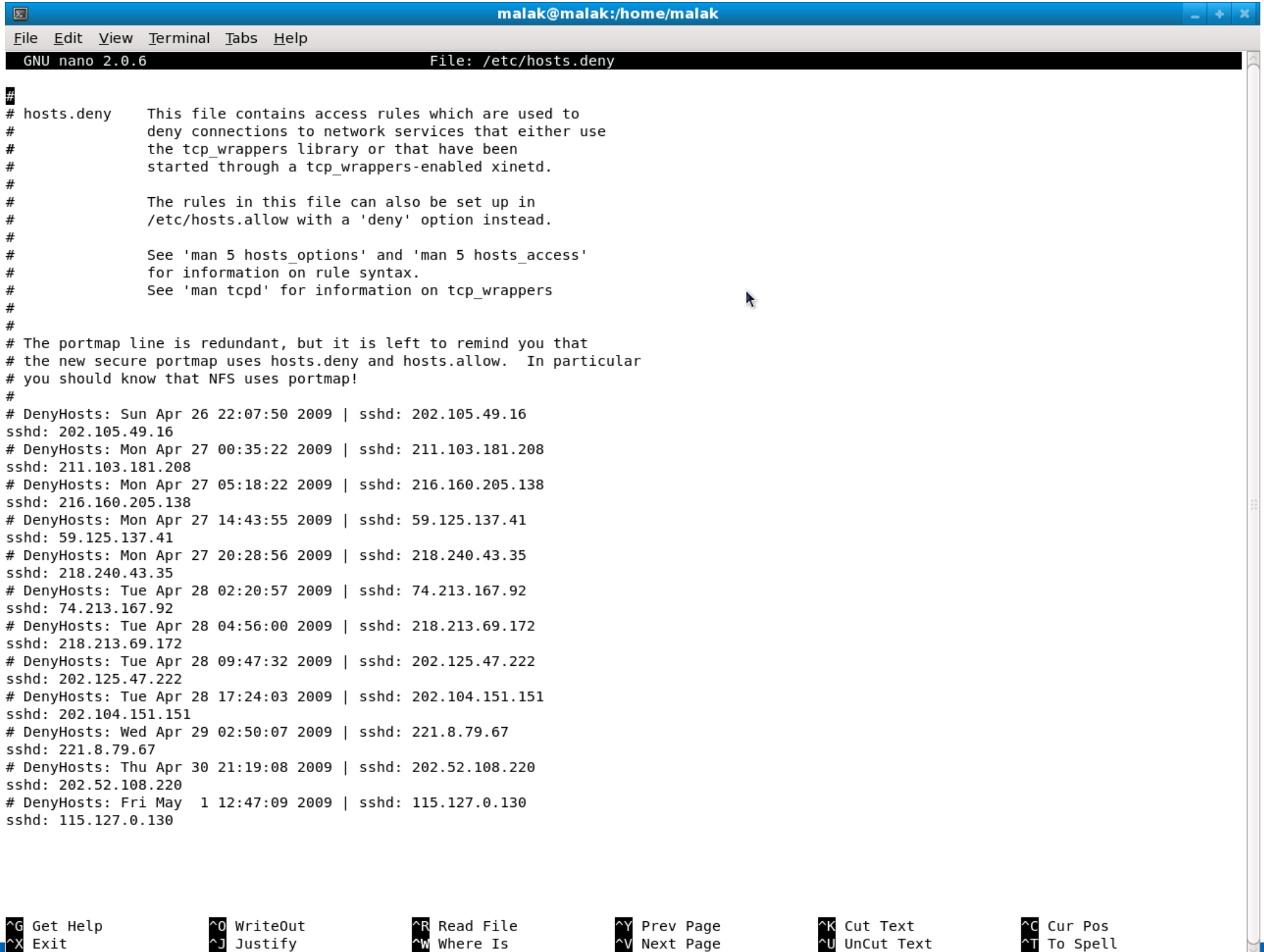
Installer “denyhosts”

Installer “denyhosts”

- denyhosts est un logiciel en scripte Python qui analyse les journeaux de système pour le serveur sshd afin de déterminer les addresses internet (123.456.789.012) desquelles des essais répétés ratés de faire une connexion par ssh proviennent. Il détermine aussi les comptes visés. Il détermine la fréquence d'essais de chaque addresse internet.
- Par la suite d'une campagne répété d'attaque contre votre système d'un addresse internet, il modifie le fichier /etc/hosts.deny avec son addresse internet pour que le système refuse des demandes provenant de cette addresse.

Installer “denyhosts”

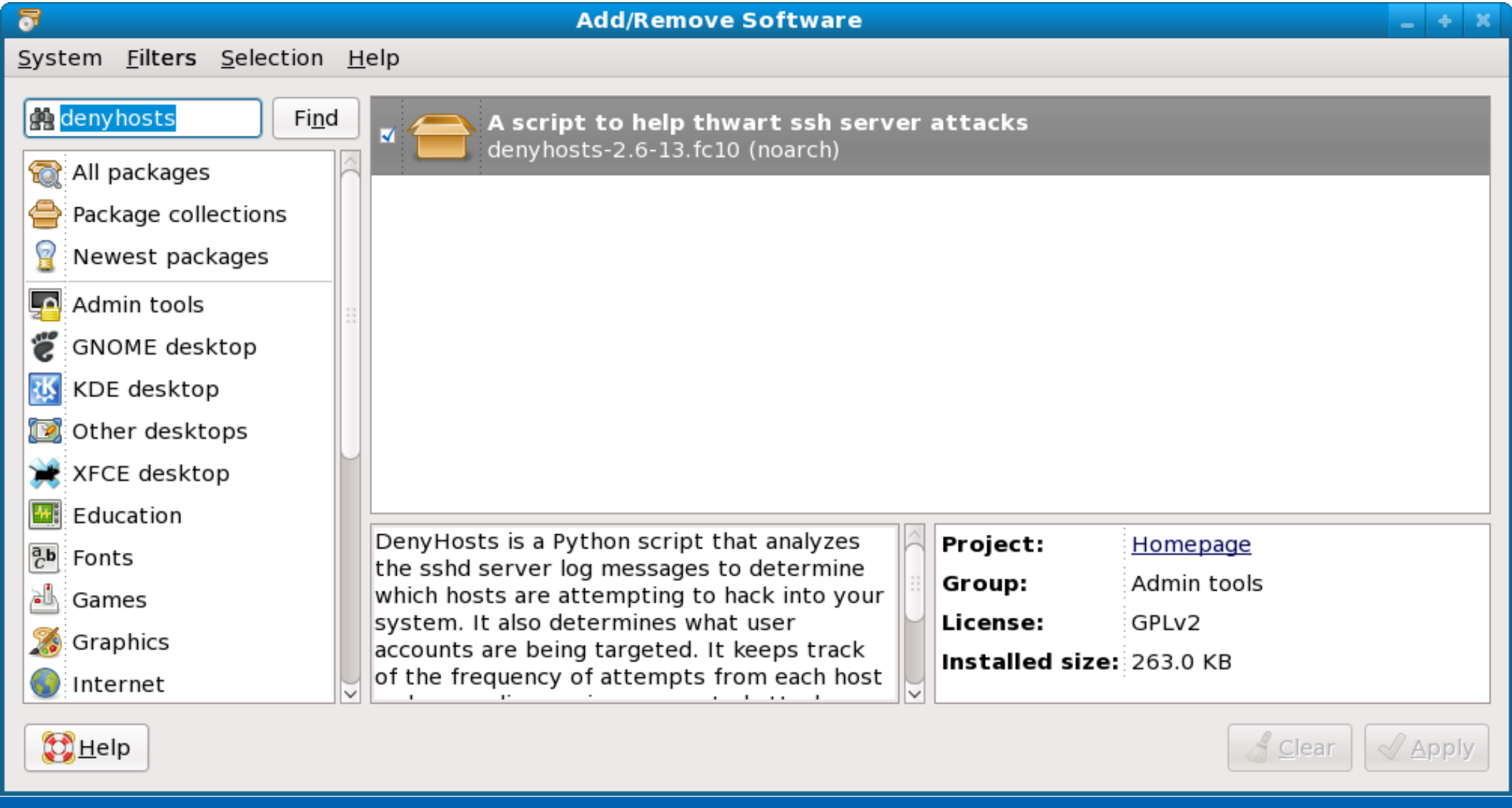
- denyhosts est un logiciel en scripte Python qui analyse les journeaux de système pour le serveur sshd afin de déterminer les addresses internet (123.456.789.012) desquelles des essais répétés ratés de faire une connexion par ssh proviennent. Il détermine aussi les comptes visés. Il détermine la fréquence d'essais de chaque addresse internet.
- Par la suite d'une campagne répété d'attaque contre votre système d'un addresse internet, il modifie le fichier /etc/hosts.deny avec son addresse internet pour que le système refuse des demandes provenant de cette addresse. À noter que DenyHosts modifie le fichier spécifiquement pour le ssh, mais ce fichier peu agir pour tout service ou n'importe quel autre service.


malak@malak:/home/malak
File Edit View Terminal Tabs Help
GNU nano 2.0.6 File: /etc/hosts.deny
#
hosts.deny This file contains access rules which are used to
deny connections to network services that either use
the tcp_wrappers library or that have been
started through a tcp_wrappers-enabled xinetd.
#
The rules in this file can also be set up in
/etc/hosts.allow with a 'deny' option instead.
#
See 'man 5 hosts_options' and 'man 5 hosts_access'
for information on rule syntax.
See 'man tcpd' for information on tcp_wrappers
#
#
The portmap line is redundant, but it is left to remind you that
the new secure portmap uses hosts.deny and hosts.allow. In particular
you should know that NFS uses portmap!
#
DenyHosts: Sun Apr 26 22:07:50 2009 | sshd: 202.105.49.16
sshd: 202.105.49.16
DenyHosts: Mon Apr 27 00:35:22 2009 | sshd: 211.103.181.208
sshd: 211.103.181.208
DenyHosts: Mon Apr 27 05:18:22 2009 | sshd: 216.160.205.138
sshd: 216.160.205.138
DenyHosts: Mon Apr 27 14:43:55 2009 | sshd: 59.125.137.41
sshd: 59.125.137.41
DenyHosts: Mon Apr 27 20:28:56 2009 | sshd: 218.240.43.35
sshd: 218.240.43.35
DenyHosts: Tue Apr 28 02:20:57 2009 | sshd: 74.213.167.92
sshd: 74.213.167.92
DenyHosts: Tue Apr 28 04:56:00 2009 | sshd: 218.213.69.172
sshd: 218.213.69.172
DenyHosts: Tue Apr 28 09:47:32 2009 | sshd: 202.125.47.222
sshd: 202.125.47.222
DenyHosts: Tue Apr 28 17:24:03 2009 | sshd: 202.104.151.151
sshd: 202.104.151.151
DenyHosts: Wed Apr 29 02:50:07 2009 | sshd: 221.8.79.67
sshd: 221.8.79.67
DenyHosts: Thu Apr 30 21:19:08 2009 | sshd: 202.52.108.220
sshd: 202.52.108.220
DenyHosts: Fri May 1 12:47:09 2009 | sshd: 115.127.0.130
sshd: 115.127.0.130
^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

File Edit View Terminal Tabs Help

```
[malak@giggi ~]$ su
Password:
[root@giggi malak]# yum install denyhosts
Loaded plugins: refresh-packagekit
Setting up Install Process
Parsing package install arguments
Resolving Dependencies
--> Running transaction check
---> Package denyhosts.noarch 0:2.6-13.fc10 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                Arch                Version                Repository                Size
================================================================================
Installing:
 denyhosts              noarch              2.6-13.fc10            fedora                    97 k

Transaction Summary
================================================================================
Install      1 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 97 k
Is this ok [y/N]: y
Downloading Packages:
denyhosts-2.6-13.fc10.noarch.rpm                                |  97 kB     00:00
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : denyhosts                                                 1/1

Installed:
  denyhosts.noarch 0:2.6-13.fc10

Complete!
[root@giggi malak]#
```

Installer “denyhosts”



Protéger l'intégriter physique de votre ordinateur

Protéger l'intégriter physique de votre ordinateur

- Que vous êtes débutant ou expert, il y a toujours quelqu'un qui connait plus que vous quant à un sujet donné ... donner leur accès physique à votre clavier, ils pourraient faire toutes sortes de mal, et/ou vol d'informations personnelles, et/ou effacer vos fichiers, et/ou installer des logiciels suspects, etc. ...
- ***Ça vous semble banale comme suggestion?***

Insérez une de ceux-ci dans votre ordinateur...

Ou encore une de ceux-ci:

Hé bein on le discute, pourquoi pas apporter son propre disque dur, soit un HDD USB, soit un HDD traditionnel ...

Protégez votre ordinateur!

- C'est assez facile de fermer et/ou débrancher votre ordinateur et insérer un “Live-CD” ou un “Live-USB”, grandement en vogue de ces jours, ou même une disque dure USB, ou même si on a le temps à passer, une disque dure traditionnelle afin d'avoir accès à vos fichiers personnels ou afin d'installer des logiciels néfastes ...

... et le match est perdu!

Merci!

Questions et discussion

Noter bien:

- Cette présentation a été composé principalement en avril, 2009, et a été complété en août 2009. Elle a été composé sur des systèmes Fedora 9, 10, et 11. Les saisies viennent de Fedora 9, 10 et 11, et Ubuntu 9.04;
- Je ne suis pas un expert en linux; tout mes conseils ici résument un petit peu de ce que j'ai appris
- des 40 ans de sagesse cumulé dans la culture Unix, le gros bon sens, et le résultat d'y avoir parlé au sujet avec un professionnel en informatique, dont c'était moi qui lui fournissait les conseils!

Noter bien:

- Sans que je les ai soumis, plusieurs de mes conseils se sont parus peu après dans la parution juin 2009 de Linux Format!