



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

HỆ ĐIỀU HÀNH WINDOWS VÀ LINUX/UNIX

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

HỆ ĐIỀU HÀNH WINDOWS VÀ LINUX/UNIX

LINUX/UNIX

KHOA AN TOÀN THÔNG TIN

TS. ĐINH TRƯỜNG DUY

Biên soạn từ giáo trình: Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công nghệ Bưu Chính Viễn Thông, 2016.

Chương 8: Bảo trì, khắc phục lỗi và giám sát hoạt động của Linux/Unix

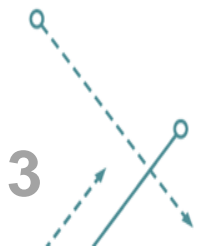
8.1 Cập nhật các bản vá Linux/Unix

8.2 Sao lưu và khôi phục dữ phòng

8.3 Khắc phục các sự cố trong Linux/Unix

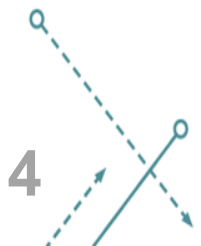
8.4 Giám sát hoạt động và kiểm toán Linux/Unix

8.5 Giới thiệu các công cụ quản trị Linux/Unix từ xa



Cập nhật các bản vá Linux/Unix

- Cập nhật phần mềm?
 - Loại phần mềm: ứng dụng, hệ thống
 - Chu kỳ thay đổi
 - Khả năng tương thích
 - Tính an toàn và bảo mật



Quản lý phần mềm

- Từ khía cạnh kỹ thuật việc quản lý phần mềm được thực hiện
 - Mã nguồn: Cách thức truyền thống. Thực hiện việc biên dịch và cài đặt phần mềm theo các hướng dẫn
 - RPM - Redhat Package Manager : phổ biến cho các phiên bản dựa trên RedHat
 - DPMS – Debian Package Management System: cho các phiên bản dựa trên Debian⁵



Dùng mã nguồn

- Thư viện
 - Xác định vị trí của thư viện
 - Chia sẻ thư viện với các phần mềm khác
- Đoạn mã cấu hình
 - Thiếu đoạn mã configure
 - Thiếu tài liệu (readme/install)
- Mã nguồn bị hỏng/lỗi

Cài đặt courier-imap

Requirements

Now is the good time to read the FAQ, before you start. The FAQ is located in the file `imap/FAQ`

- C++ compiler - A C++ compiler is required. The server is written in C, but there are some C++ code.
- make - The GNU make is recommended. Solaris's make is to be avoided. xBSD already has make (use gmake everywhere this document refers to make).
- GDBM/DB - either the GDBM or the Berkeley DB library is required.
- [The GNU IDN library](http://www.gnu.org/software/libidn/) (<http://www.gnu.org/software/libidn/>).
- [Gamin](http://www.gnome.org/~veillard/gamin/) (<http://www.gnome.org/~veillard/gamin/>) OR [FAM](http://oss.sgi.com/projects/fam/) (<http://oss.sgi.com/projects/fam/>) is installed, it is used for an enhanced IMAP IDLE implementation that provides real-time clients that have the same folder opened.
- The Courier authentication library. Before installing Courier-IMAP, download and install the authentication library.

INSTALLATION

```
$ ./configure [ options, see below ]
$ make
$ make check      # Note - the --enable-workarounds-for-imap-client-bugs
                  # option to configure will result in make check FAILING.

$ su root
# make install    # Or, make install-strip, to strip the executables.
# make install-configure # Install configuration files.
```

Cài đặt DHCP

- Tải về mã nguồn <http://ftp.isc.org/isc/dhcp-4.2.3.tar.gz>
- 1. Giải nén mã nguồn từ thư mục /usr/local/src/
 - tar xvfz dhcp-4.2.3.tar.gz
- 2. Chuyển đến thư mục dhcp được giải nén
- 3. Đặt cấu hình
 - ./configure --prefix=/usr/local/
- 4. Biên dịch và cài đặt
 - make
 - make install
- Phần mềm dịch vụ dhcpd và dhcp client cài vào thư mục /usr/local/sbin/

Quản lý phần mềm DPMS

- Cung cấp công cụ thuận tiện cho việc cài đặt và gỡ bỏ các phần mềm.
- Các gói phần mềm của Debian có đuôi **.deb**
- Phần mềm cốt lõi, **dpkg**, chạy ở chế độ nền làm cơ sở cho các phần mềm tiện ích (dòng lệnh/GUI) khác hoạt động.

DPMS - dpkg

- Liệt kê các gói phần mềm được cài đặt
 - *dpkg -l*
- Liệt kê các file được cài đặt bởi một gói phần mềm
 - *dpkg -L phần_mềm*
- Liệt kê gói phần mềm cài đặt file
 - *dpkg -S /etc/hosts.conf*
- Cài đặt gói phần mềm
 - *sudo dpkg -i phần_mềm.deb*
- Gỡ bỏ gói phần mềm
 - *sudo dpkg -r phần_mềm*

dpkg -l

```
pduy@ux64NoGui: ~
ii  libsnmp-base      5.7.2~dfsg-8 all      SNMP configuration script, MIBs a
ii  libsnmp30:amd64  5.7.2~dfsg-8 amd64    SNMP (Simple Network Management P
ii  libsocket6-per    0.25-1build1 amd64    Perl extensions for IPv6
ii  libsoftware-li    0.103010-3   all      module providing templated softwa
ii  libsonic0:amd64   0.1.18-0ubun amd64    Simple library to speed up or slo
ii  libsoup-gnome2    2.49.92-1    amd64    HTTP library implementation in C
ii  libsoup2.4-1:a    2.49.92-1    amd64    HTTP library implementation in C
ii  libspectre1:am    0.2.7-2ubunt amd64    Library for rendering PostScript
ii  libspeechd2:am    0.8.1-0ubunt amd64    Speech Dispatcher: Shared librari
ii  libspeex1:amd64   1.2~rc1.1-1u amd64    The Speex codec runtime library
ii  libspeexdsp1:a    1.2~rc1.1-1u amd64    The Speex extended runtime librar
ii  libsphinxbase1    0.8-0ubuntu1 amd64    Sphinx base libraries
ii  libspice-serve    0.12.5-1ubun amd64    Implements the server side of the
ii  libsqlite3-0:a    3.8.7.4-1    amd64    SQLite 3 shared library
ii  libss2:amd64      1.42.12-1ubu amd64    command-line interface parsing li
ii  libssh-4:amd64    0.6.3-3ubunt amd64    tiny C SSH library (OpenSSL flavo
ii  libssl1.0.0:am    1.0.1f-1ubun amd64    Secure Sockets Layer toolkit - sh
ii  libstartup-not    0.12-4       amd64    library for program launch feedba
ii  libstdc++-4.9-    4.9.2-10ubun amd64    GNU Standard C++ Library v3 (deve
ii  libstdc++6:amd64  4.9.2-10ubun amd64    GNU Standard C++ Library v3
ii  libsub-exporte    0.986-1      all      sophisticated exporter for custom
ii  libsub-install    0.928-1      all      module for installing subroutines
ii  libsub-name-pe    0.12-1       amd64    module for assigning a new name t
```

- Các thư viện cài cùng với dovecot-imapd

```
pduy@ux64NoGui:~$ dpkg -L dovecot-imapd
/.
/usr
/usr/lib
/usr/lib/dovecot
/usr/lib/dovecot/imap-urlauth-login
/usr/lib/dovecot/imap-login
/usr/lib/dovecot/imap
/usr/lib/dovecot/imap-urlauth-worker
/usr/lib/dovecot/modules
/usr/lib/dovecot/modules/lib11_imap_quota_plugin.so
/usr/lib/dovecot/modules/lib30_imap_zlib_plugin.so
/usr/lib/dovecot/modules/lib95_imap_stats_plugin.so
/usr/lib/dovecot/modules/lib02_imap_acl_plugin.so
/usr/lib/dovecot/imap-urlauth
/usr/share
/usr/share/lintian
/usr/share/lintian/overrides
/usr/share/lintian/overrides/dovecot-imapd
/usr/share/dovecot
/usr/share/dovecot/conf.d
/usr/share/dovecot/conf.d/20-imap.conf
/usr/share/bug
/usr/share/doc
/usr/share/doc/dovecot-imapd
/usr/share/doc/dovecot-imapd/copyright
/usr/share/bug/dovecot-imapd
/usr/share/doc/dovecot-imapd/changelog.Debian.gz
```

APT (Advanced Packaging Tool) (1)

- APT là bộ công cụ tinh vi và hữu ích tương tác trực tiếp với ***dpkg***
- APT không trực tiếp xử lý các gói phần mềm .deb mà quản lý kho phần mềm.
- APT dùng `source.list` để xác định nơi lưu trữ các phần mềm

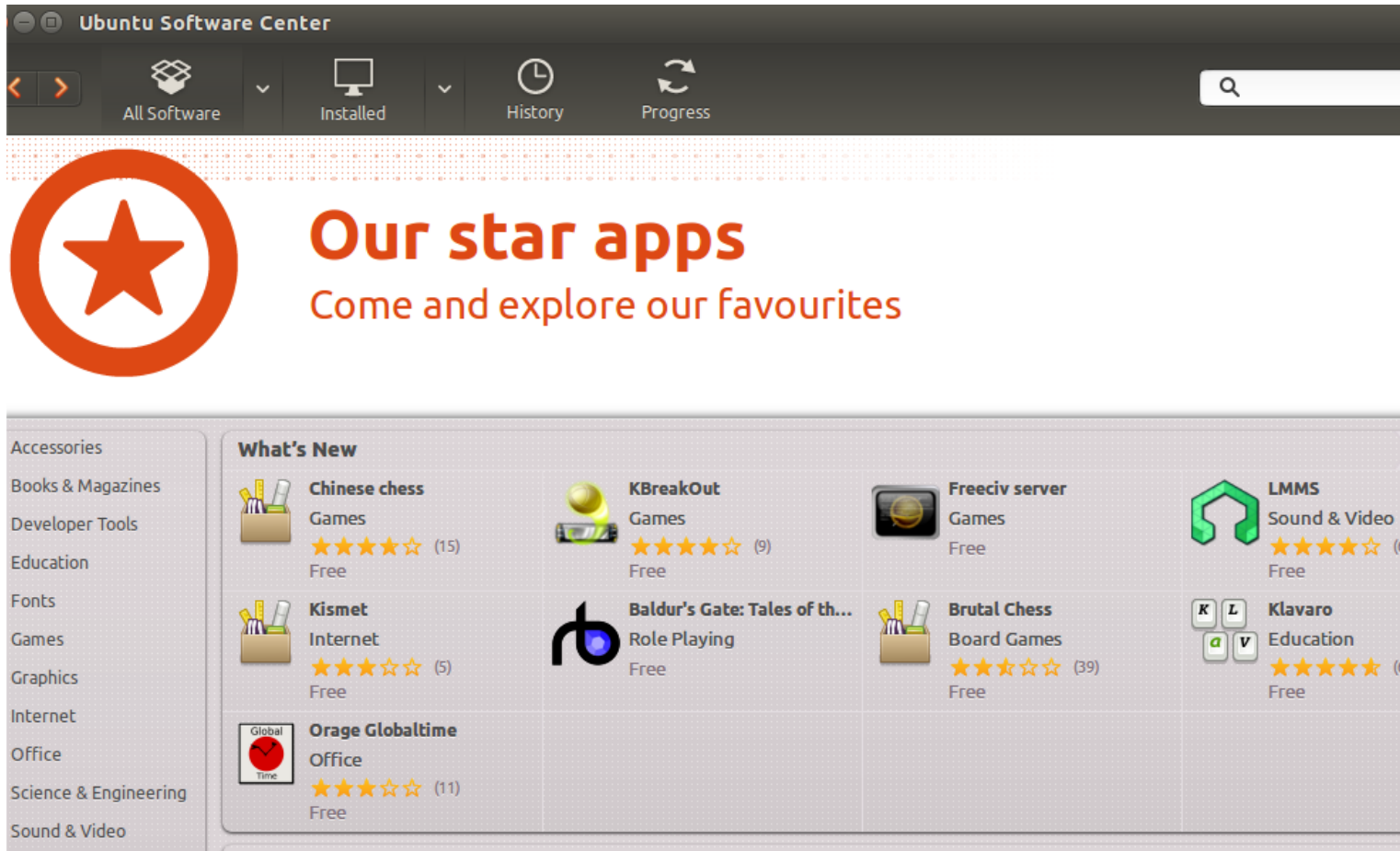
APT (2)

- Cài đặt gói phần mềm
 - *sudo apt-get install phần_mềm*
- Gỡ bỏ phần mềm
 - *sudo apt-get remove phần_mềm*
- Cập nhật thông tin về kho phần mềm
 - *sudo apt-get update*
- Nâng cấp gói phần mềm
 - *sudo apt-get upgrade*

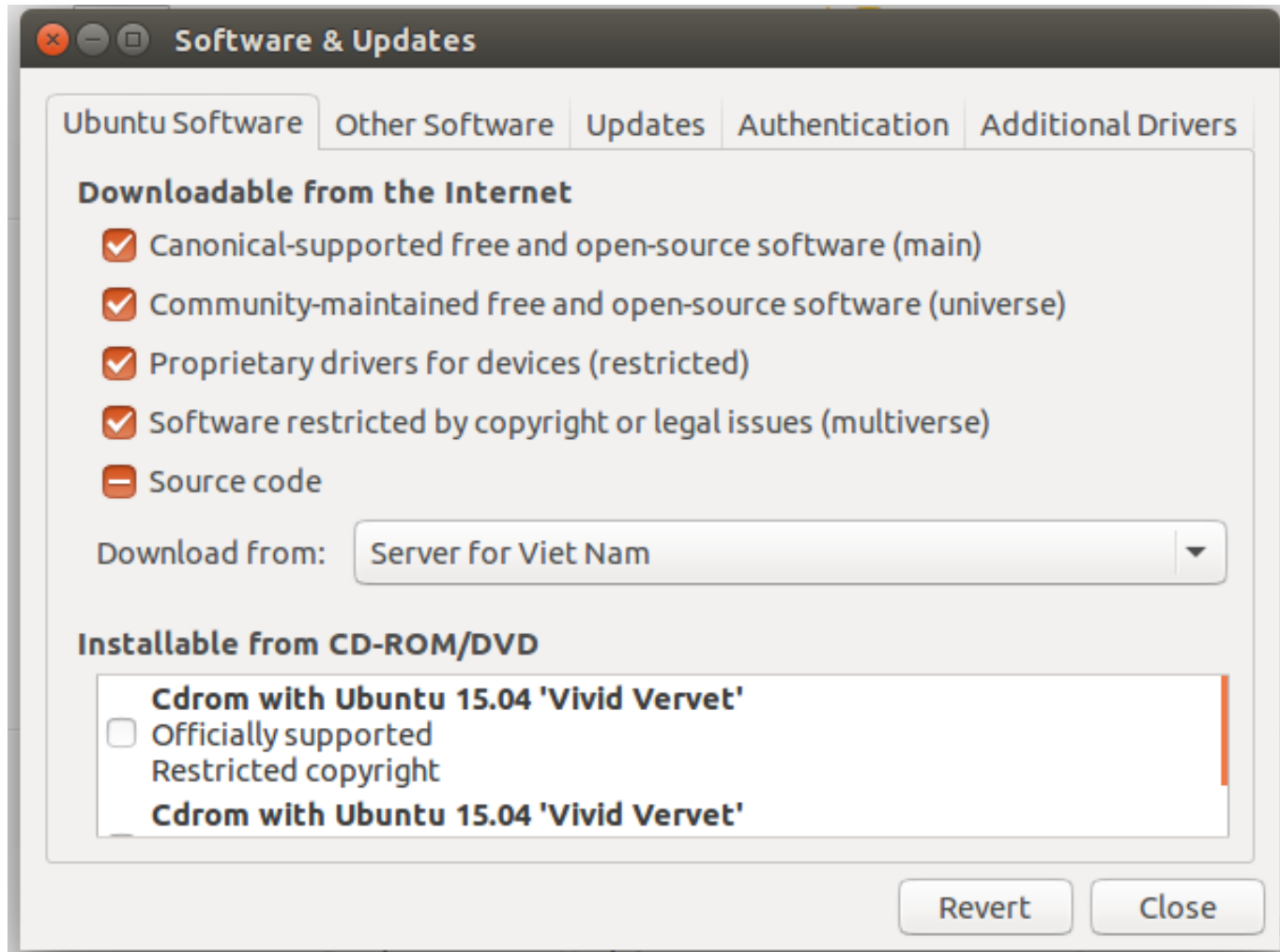
apt-get update

```
bduy@ux64NoGui:~$ sudo apt-get update
Ign http://vn.archive.ubuntu.com vivid InRelease
Ign http://security.ubuntu.com vivid-security InRelease
Ign http://vn.archive.ubuntu.com vivid-updates InRelease
Get:1 http://security.ubuntu.com vivid-security Release.gpg [933 B]
Ign http://vn.archive.ubuntu.com vivid-backports InRelease
Get:2 http://vn.archive.ubuntu.com vivid Release.gpg [933 B]
Get:3 http://security.ubuntu.com vivid-security Release [63.5 kB]
Get:4 http://vn.archive.ubuntu.com vivid-updates Release.gpg [933 B]
Get:5 http://vn.archive.ubuntu.com vivid-backports Release.gpg [933 B]
Hit http://vn.archive.ubuntu.com vivid Release
Get:6 http://vn.archive.ubuntu.com vivid-updates Release [63.5 kB]
Get:7 http://security.ubuntu.com vivid-security/main Sources [44.8 kB]
Get:8 http://security.ubuntu.com vivid-security/restricted Sources [2,792 B]
Get:9 http://security.ubuntu.com vivid-security/universe Sources [18.0 kB]
Hit http://vn.archive.ubuntu.com vivid-backports Release
Get:10 http://security.ubuntu.com vivid-security/multiverse Sources [1,966 B]
Get:11 http://security.ubuntu.com vivid-security/main amd64 Packages [119 kB]
Get:12 http://security.ubuntu.com vivid-security/restricted amd64 Packages [10.
/usr/share/lintian/overrides
```

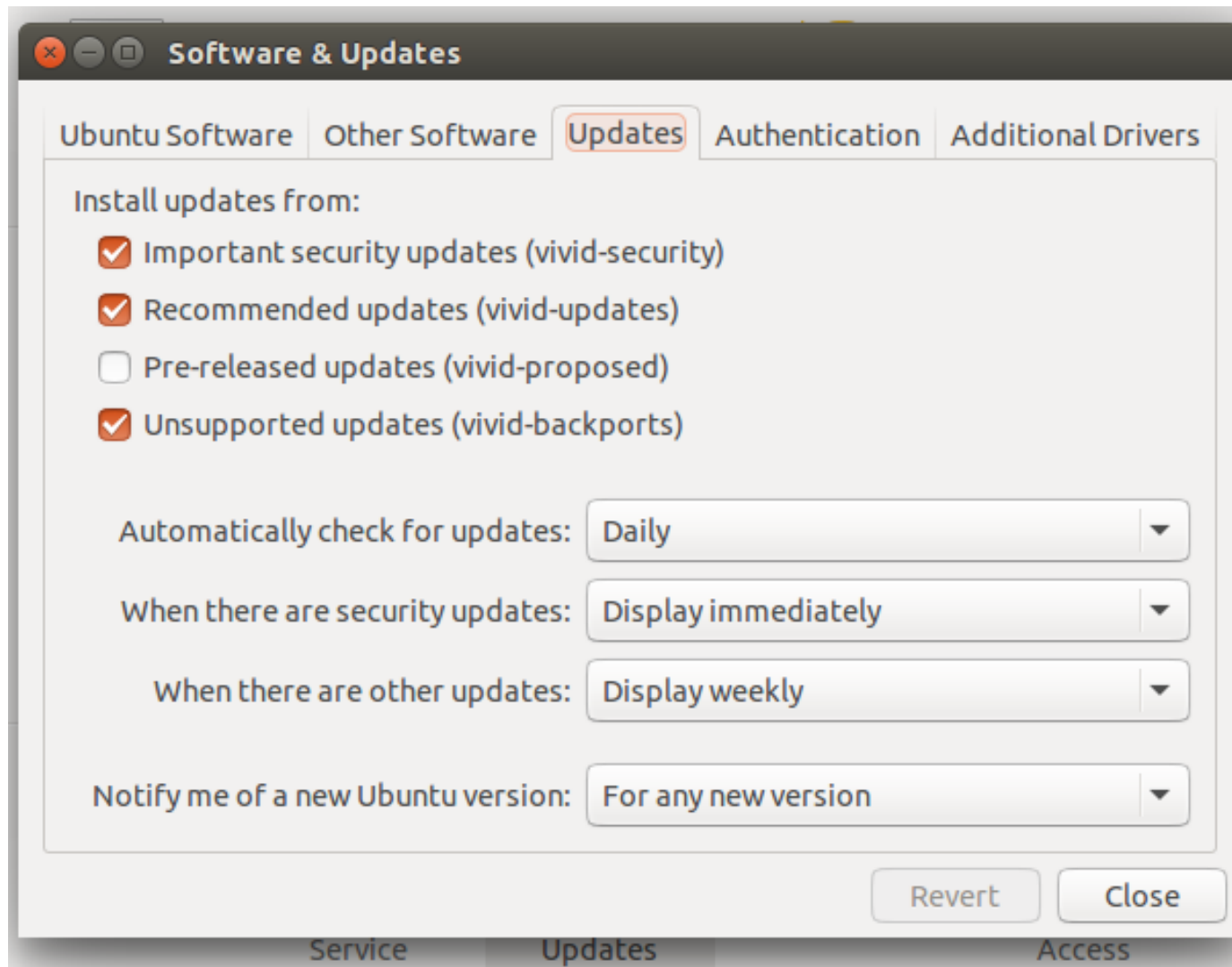
Ubuntu software center



Giao diện cài đặt và cập nhật Ubuntu



Giao diện cài đặt và cập nhật Ubuntu



Chương 8: Bảo trì, khắc phục lỗi và giám sát hoạt động của Linux/Unix

8.1 Cập nhật các bản vá Linux/Unix

8.2 Sao lưu và khôi phục dữ phòng

8.3 Khắc phục các sự cố trong Linux/Unix

8.4 Giám sát hoạt động và kiểm toán Linux/Unix

8.5 Giới thiệu các công cụ quản trị Linux/Unix từ xa

Sao lưu và khôi phục

- Thực hiện sao lưu là công việc tối quan trọng đối với bất kỳ người quản trị cũng như là trách nhiệm của quản trị hệ thống.
- Các vấn đề cần quan tâm
 - Khối lượng dữ liệu
 - Phần cứng và phương tiện sao lưu
 - Năng lực (băng thông) mạng
 - Tốc độ và khả năng khôi phục dữ liệu
 - Vấn đề toàn vẹn dữ liệu
 - Quản lý thiết bị lưu trữ

Các vấn đề (1)

- Khối lượng dữ liệu xác định khó khăn
 - Nhu cầu và tính hình phát triển của cơ quan/tổ chức
 - Tần suất và khối lượng thay đổi dữ liệu
 - Tính chất của dữ liệu: nén, không nén, cá nhân/cơ quan
- Phần cứng sao lưu
 - DVD, bluray: chi phí thấp, tuổi thọ ngắn
 - Ổ đĩa cứng, RAID: tốc độ cao, chi phí vừa phải
 - NAS, SAN: phụ thuộc vào hạ tầng mạng
- Băng thông mạng
 - Tránh sao lưu 2 máy đồng thời trong cùng hub

Các vấn đề (2)

- Tốc độ và khả năng khôi phục
 - Đĩa cứng > DVD, bluray > băng từ
- Xử lý dữ liệu trùng lặp
 - Sao lưu cùng dữ liệu do người dùng cất file ở các vị trí lưu trữ khác nhau: máy chủ, máy cá nhân

Lệnh hỗ trợ sao lưu/khôi phục

- Phần mềm ***dump/restore*** cho phép sao lưu/khôi phục toàn bộ hệ thống file Linux
- ***dump*** thực hiện sao lưu tăng dần và sử dụng tham số *cấp độ sao lưu*
 - *Cấp 0*: sao lưu toàn bộ
 - *Cấp 1*: sao lưu bổ sung so với cấp 0
 - *Cấp 9*: *cấp cao nhất*
- Thông tin về các file sao lưu ghi trong file */etc/dumpdates* cung cấp thông tin về các file sao lưu của hệ thống. Sao lưu toàn bộ phân vùng của ổ đĩa vật lý thứ nhất vào ổ đĩa vật lý thứ hai:
 - *dump -0 -f /dev/sdb1 /dev/sda1*

Lệnh hỗ trợ sao lưu/khôi phục

- *restore* đọc files tạo ra từ phần mềm *dump* và trích ra các file và thư mục
- Các tham số
 - -l: Chế độ tương tác. Phần mềm cung cấp giao diện cho phép người quản trị lựa chọn thư mục và file để khôi phục
 - -r: Khôi phục lại hệ thống file
 - -f tên_file: Đọc từ file sao lưu
 - -v: Hiển thị kết quả khôi phục
- Khôi phục file và thư mục
 - `restore -ivf /dev/sdb1`
- Khôi phục lại hệ thống file
 - `restore -rf /dev/sdb1`

Lệnh hỗ trợ sao lưu/khôi phục

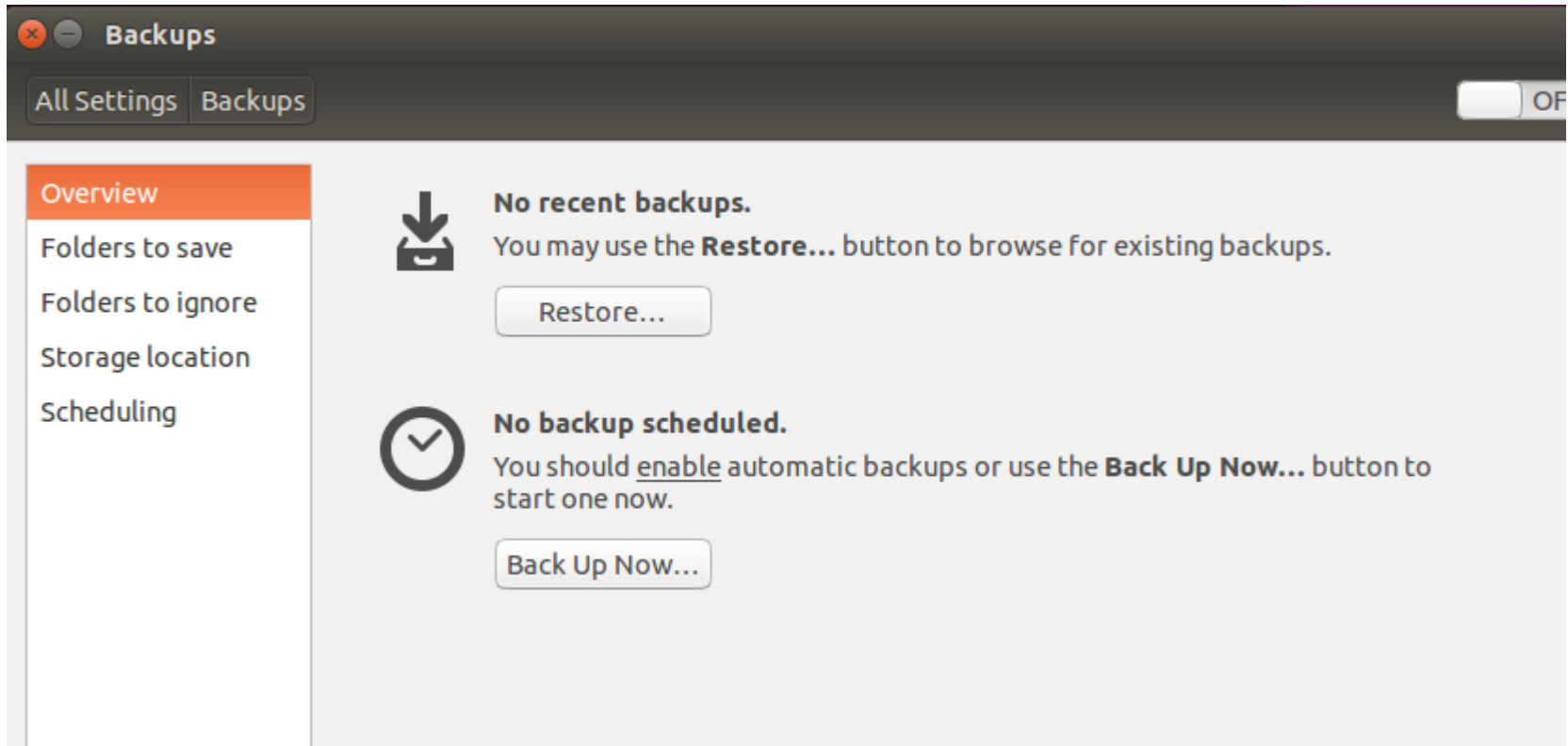
- tar - tape archive: cho phép lưu các file và thư mục vào thành một file duy nhất.
- tar phù hợp sao lưu toàn bộ nội dung thư mục hơn là cả hệ thống file
- Tham số
 - -v: hiện kết quả trong lúc chạy
 - -c: tạo file lưu trữ mới
 - -t: xem nội dung của file lưu trữ
 - -x: trích ra nội dung của file lưu trữ
 - -f: tên file/thiết bị lưu trữ
 - -z: dùng tiện ích nén gzip

Tạo file lưu trữ thư mục người dùng

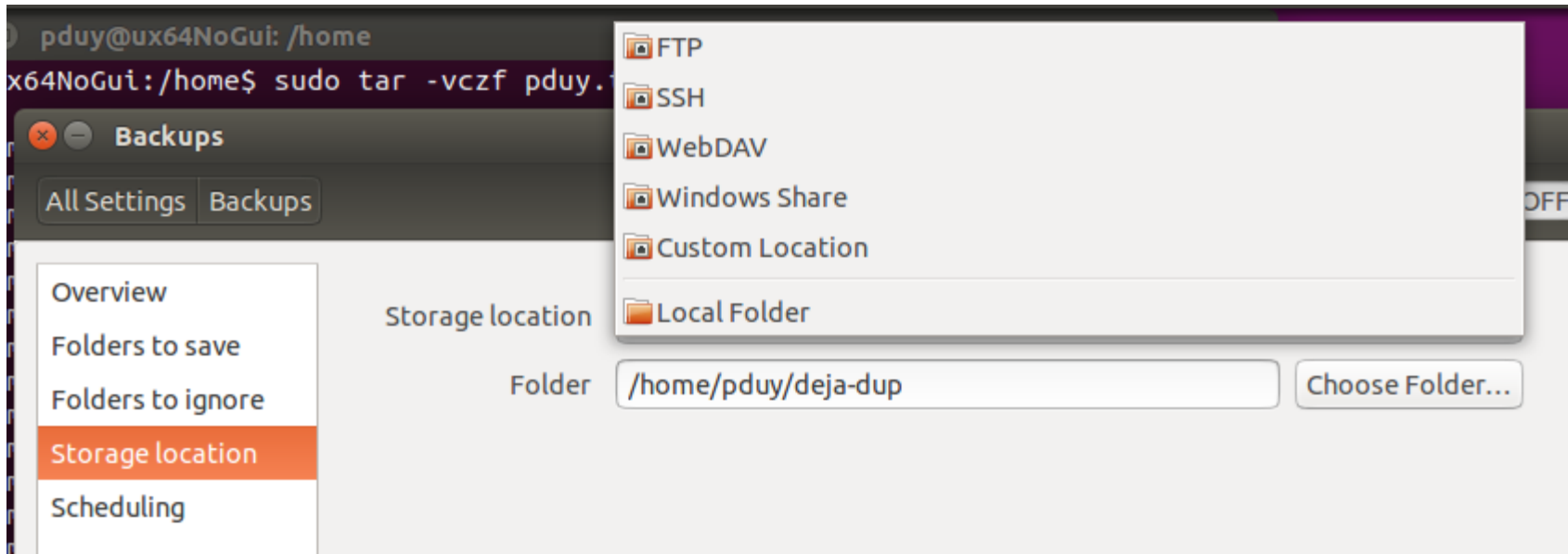
- `tar -vczf pduy.tar pduy`

```
pduy@ux64NoGui:/home$ sudo tar -vczf pduy.tar pduy
pduy/
pduy/.mozilla/
pduy/.mozilla/firefox/
pduy/.mozilla/firefox/Crash Reports/
pduy/.mozilla/firefox/Crash Reports/InstallTime20150826185640
pduy/.mozilla/firefox/Crash Reports/events/
pduy/.mozilla/firefox/profiles.ini
pduy/.mozilla/firefox/dplq1kw2.default/
pduy/.mozilla/firefox/dplq1kw2.default/pluginreg.dat
pduy/.mozilla/firefox/dplq1kw2.default/times.json
pduy/.mozilla/firefox/dplq1kw2.default/permissions.sqlite
pduy/.mozilla/firefox/dplq1kw2.default/secmod.db
pduy/.mozilla/firefox/dplq1kw2.default/cookies.sqlite
pduy/.mozilla/firefox/dplq1kw2.default/healthreport.sqlite-shm
pduy/.mozilla/firefox/dplq1kw2.default/healthreport/
```

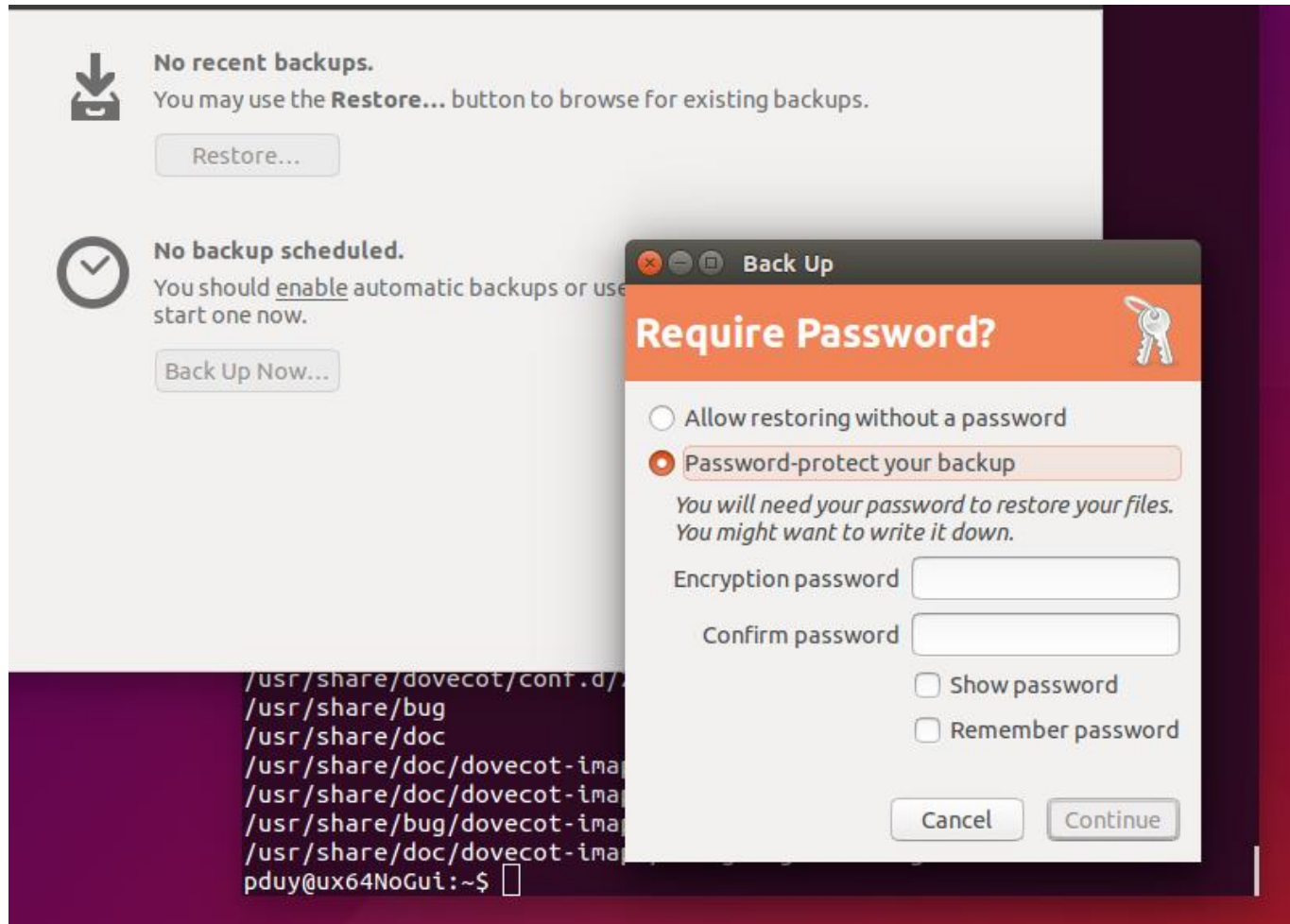
Ubuntu backup/restore



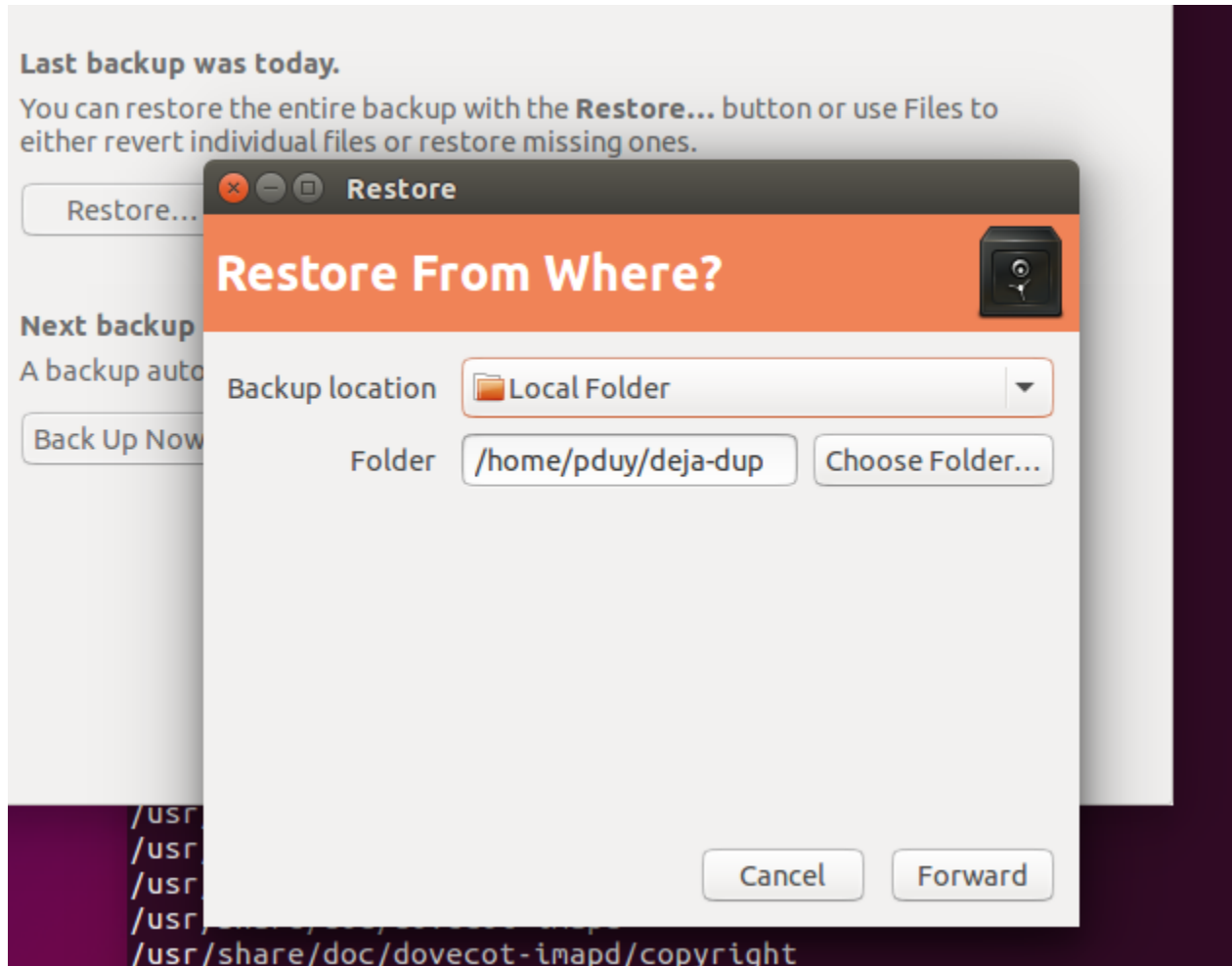
Ubuntu backup/restore



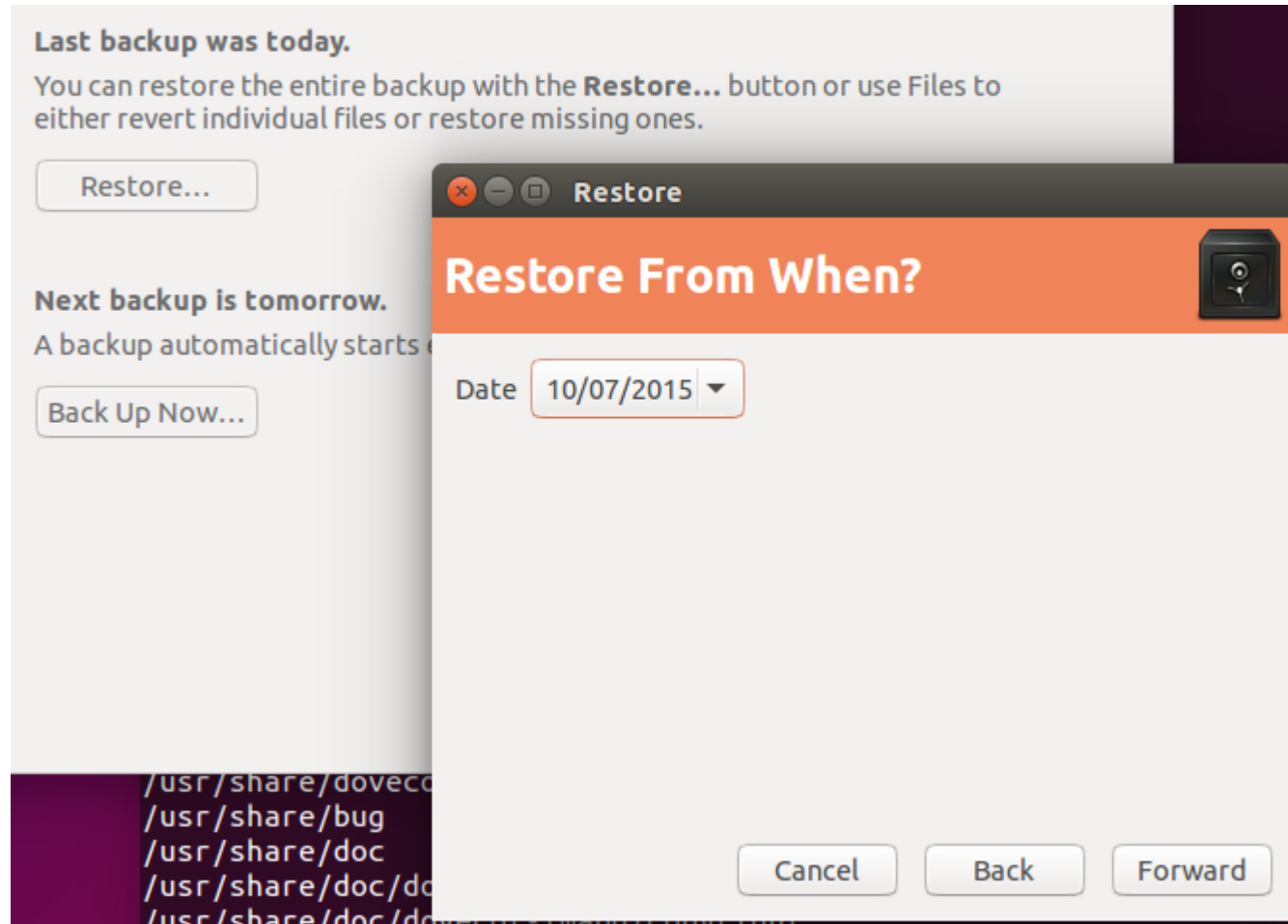
Ubuntu backup/restore



Ubuntu backup/restore

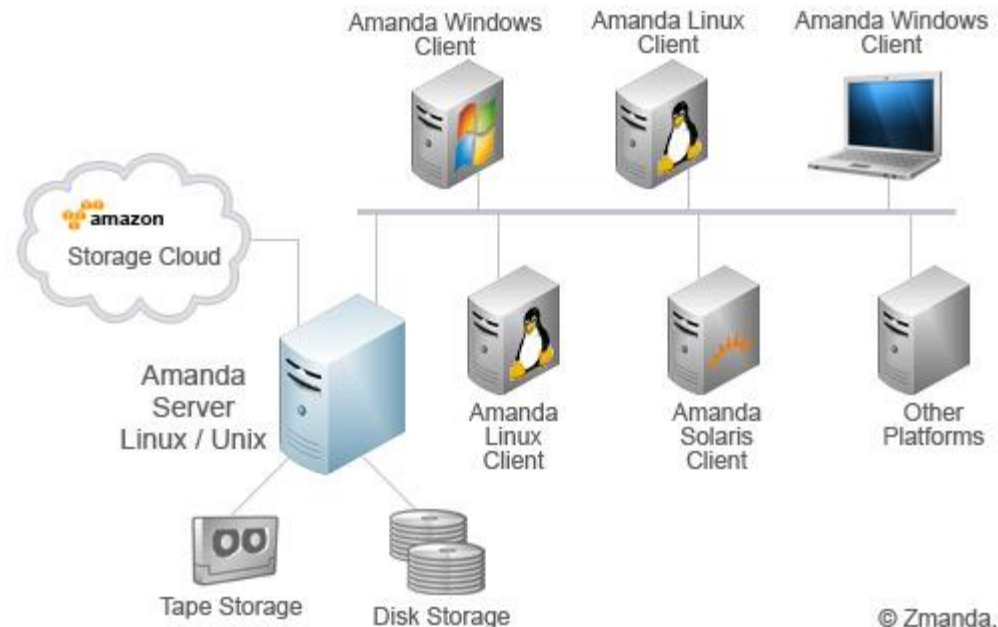


Ubuntu backup/restore



• AMANDA-

Advanced Maryland Automatic Network Disk Archiver: Hệ thống sao lưu cho phép dùng một máy chủ sao lưu để sao lưu nhiều máy qua mạng vào ổ đĩa hay băng từ hay ổ quang.




Các giải pháp sao lưu

- Dirvish: hệ thống sao lưu ra đĩa cứng viết bằng ngôn ngữ Perl sử dụng tiện ích sao lưu của Linux
- Thuận tiện cho việc tự động hóa sao lưu và dễ dàng khôi phục lại
- Thích hợp cho việc sao lưu file và thư mục

BackupPC

- BackupPC hỗ trợ sao lưu cho Linux ra ổ cứng trên máy chủ sử dụng giao diện Web
- BackupPC sao lưu file và thư mục
- BackupPC sử dụng giả pháp nén đĩa để tăng khả năng sao lưu
- Hỗ trợ các giao thức SMB, SSH

BackupPC



Hosts

Server

- [Status](#)
- [Admin Options](#)
- [Host Summary](#)
- [LOG file](#)
- [Old LOGs](#)
- [Email summary](#)
- [Config file](#)
- [Hosts file](#)
- [Current queues](#)
- [Documentation](#)
- [FAQ](#)
- [SourceForge](#)

BackupPC Server Status

General Server Information

- The servers PID is 3706, on host server1.example.com, version 2
- This status was generated at 1/19 15:33.
- The configuration was last loaded at 1/19 15:22.
- PCs will be next queued at 1/19 16:00.
- Other info:
 - 0 pending backup requests from last scheduled wakeup,
 - 0 pending user backup requests,
 - 0 pending command requests,
 - Pool is 0.00GB comprising files and directories (as of 1/19
 - Pool hashing gives repeated files with longest chain ,
 - Nightly cleanup removed 0 files of size 0.00GB (around 1/19
 - Pool file system was recently at % (1/19 15:33), today's ma

Currently Running Jobs

| Host | Type | User | Start Time | Command | PID | Xfer PID |
|------|------|------|------------|---------|-----|----------|
|------|------|------|------------|---------|-----|----------|

Failures that need attention

| Host | Type | User | Last Try | Details | Error Time | Last error (other than no ping) |
|------|------|------|----------|---------|------------|---------------------------------|
|------|------|------|----------|---------|------------|---------------------------------|

Chương 8: Bảo trì, khắc phục lỗi và giám sát hoạt động của Linux/Unix

8.1 Cập nhật các bản vá Linux/Unix

8.2 Sao lưu và khôi phục dữ phòng

8.3 Khắc phục các sự cố trong Linux/Unix

8.4 Giám sát hoạt động và kiểm toán Linux/Unix

8.5 Giới thiệu các công cụ quản trị Linux/Unix từ xa

Khắc phục sự cố trong Unix/Linux

- Ghi nhận tình trạng lỗi: trình soạn thảo văn bản, copy màn hình
 - Ghi lại các thông báo lỗi hay các cảnh báo
 - log file: /var/log
 - File lưu thông tin về phiên làm việc .bash_history
.xsession

```
pduy@ux64NoGui:~$ ls -a
.      Desktop      .local      .sudo_as_admin_successful
..     .dmrc          Maildir     Templates
.bash_history Documents    mbox        Videos
.bash_logout Downloads    .mozilla    .Xauthority
.bashrc   duy.tar      Music       .xsession-errors
.cache    .gconf       Pictures    .xsession-errors.old
.config   .gvfs        .profile    z
.dbus     .ICEauthority Public
deja-dup .lesshst     .ssh
```

Khắc phục sự cố trong Unix/Linux

- Tìm kiếm giải pháp xử lý lỗi thông qua các trạng mạng
 - help.ubuntu.com
 - trang cộng đồng
- Đĩa cài Ubuntu cung cấp công cụ cho phép kiểm tra máy tính
- Sử dụng tính năng “Try Ubuntu without installing” cho phép khởi động Ubuntu

Khôi phục mật khẩu Ubuntu

GNU GRUB version 2.02~beta2-22ubuntu1.1

```
Ubuntu, with Linux 3.19.0-15-generic
Ubuntu, with Linux 3.19.0-15-generic (upstart)
*Ubuntu, with Linux 3.19.0-15-generic (recovery mode)
```

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line. ESC to return previous
menu.

Khôi phục mật khẩu Ubuntu

Recovery Menu (filesystem state: read-only)

| | |
|----------------|------------------------------|
| resume | Resume normal boot |
| clean | Try to make free space |
| dpkg | Repair broken packages |
| failsafeX | Run in failsafe graphic mode |
| fsck | Check all file systems |
| grub | Update grub bootloader |
| network | Enable networking |
| root | Drop to root shell prompt |
| system-summary | System summary |

<Ok>

Khôi phục mật khẩu Ubuntu

| | |
|----------------|----------------------------------|
| resume | Resume normal boot |
| clean | Try to make free space |
| dpkg | Repair broken packages |
| failsafeX | Run in failsafe graphic mode |
| fsck | Check all file systems |
| grub | Update grub bootloader |
| network | Enable networking |
| root | Drop to root shell prompt |
| system-summary | System summary |

<Ok>

```
root@ux64NoGui:~# mount -rw -o remount /
root@ux64NoGui:~# passwd pduy
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@ux64NoGui:~#
```