Cool Ubuntu Apps

PLUG N 2010-05-11
PLUG W 2010-06-21

JP Vossen, CISSP
www.jpsdomain.org
bashcookbook.org

Cool Ubuntu Apps

- **nullmailer** - simple relay-only mail transport agent
- **fcheck** - IDS filesystem baseline integrity checker
- **logcheck** - mails anomalies in the system logfiles to the administrator
- **monit** - A utility for monitoring and managing daemons or similar programs
- **tmpreaper** - cleans up files in directories based on their age
- **roxterm** - Multi-tabbed GTK/VTE terminal emulator [editable menu key sidebar]
- **thunar** - File Manager for Xfce
- **notecase** - hierarchical note manager (aka outliner)
- **look** -- display lines beginning with a given string
- **lookup** - interactive utility to search text files quickly
- **screen** - terminal multiplexor with VT100/ANSI terminal emulation
- **xsel** - command-line tool to access X clipboard and selection buffers
- **bash-completion** - programmable completion for the bash shell
- System hardware info
  - **hwinfo** - Hardware identification system
  - **lshw** - information about hardware configuration
  - **lshw-gtk** - graphical information about hardware configuration
  - **lspci** - list all PCI devices
- **pessulus** - lockdown editor for GNOME
- **etckeeper** - store /etc in git, mercurial, bzr or darcs
- **localepurge** – automagically delete unneeded locale, etc. files

nullmailer - simple relay-only mail transport agent

- Avoid the complexity of Postfix, or Exim
- Avoid the horror of Sendmail
- Really Freakin' Simple
- Cron and many of the rest of the packages we'll talk about need to be able to send email

nullmailer - simple relay-only mail transport agent

- sudo -s
- echo 'user@example.com' > /etc/nullmailer/adminaddr
- echo '3600' > /etc/nullmailer/pausetime
- echo 'smtp.example.com' > /etc/nullmailer/remotes
- exit

- *pausetime* is optional, default is to try to send messages every 60 seconds. That'll kill you with failure messages on a laptop that's up but not on-line.

fcheck - IDS filesystem baseline integrity checker

- Much less of a PITA than Tripwire, but not as secure
  - (Hint, **after** the intrusion is too late.)
  - Auto-rebuilds DB after change: you miss the email, oh well...
  - See slide notes for a sample
- Perl, claims to run on Windows too (I never tried), code hasn't changed since 2001 or so
- Runs from: */etc/cron.d/fcheck*

fcheck 2 of 3

- Missing exclude needed for /lib/udev/devices/
- https://bugs.launchpad.net/ubuntu/+source/fcheck/+bug/47408
- I recommend:
  CFInclude = /etc/fcheck/fcheck_local.cfg
  - See slide notes for a sample
- Subtle: path needs trailing '/' to recursively check inside the directory!
  - Good: Directory = /var/spool/cron/
  - Bad: Directory = /var/spool/cron

fcheck 3 of 3

- fcheck alternatives:
  - debsums - Verify installed package files against MD5 checksums
  - integrit - A file integrity verification program
  - osiris - network-wide system integrity monitor control interface
  - samhain - Data integrity and host intrusion alert system
  - stealth - A stealthy File Integrity Checker
  - tripwire - file and directory integrity checker

logcheck – system log monitor

- Not quite plug & play or set-it-and-forget-it even though it is built-in to the repos
- You need to be comfortable with grep-style regular expressions
- Runs out-of-the-box but will spam you even with: */etc/logcheck/logcheck.conf* REPORTLEVEL="workstation"
- I recommend an */etc/logcheck/local.ignore*, symlinked into *ignore.d.*/* as appropriate
  - See slide notes for a sample

logcheck 2 of 3

- Read */etc/logcheck/logcheck.conf*
- For testing, create a sample log file and:

  -
    ```
    su -s /bin/bash -c "/usr/sbin/logcheck -tsol {sample}" logcheck
    ```
  - e.g.:
    ```
    su -s /bin/bash -c "/usr/sbin/logcheck -tsol /tmp/mylog" logcheck
    ```
- See slide notes for a sample

logcheck 3 of 3

- Logcheck is a simple yet great idea. You create three pattern (grep regex) lists:
  - Known bad stuff
  - Looks bad but isn't
  - Known good stuff
- Look for “known bad” but then remove “looks bad but isn't” and report
- Remove “known bad” already reported, “looks bad but isn't” and “known good”, then report whatever is leftover

monit – Nagios (really) Lite

- PER HOST (not distributed like Nagios, OpenNMS, Cacti, etc.)
- Email & syslog alerts
- Web server for status screen
- Great docs & examples!
  - I should be using an “include” in */etc/monit/conf.d/* but I started using it before it had that.
  - See slide notes for a sample config

monit 2 of 2

- See slide notes for sample email alerts

tmpreaper - cleans up files in directories based on their age

- Similar to the built-in Red Hat 'tmpwatch'
- **NOT** usually installed by default on Debian or Ubuntu
  - Principle of least-surprise
  - AKA, don't go deleting people's files
- “You can whitelist files and it will not cd into symlinks, or remove symlinks, sockets, fifos, or special files unless specifically told to.”
- After install: vi */etc/tmpreaper.conf*
  - #SHOWWARNING=true

roxterm - Multi-tabbed GTK/VTE terminal emulator

- Looks just like 'gnome-terminal' except you can actually change key-bindings to something useful like ALT+C, ALT+V, CTRL+T
- Added tab “status indicators” as of 1.18.0-1 (see slide notes)!!!

Editable menu keys

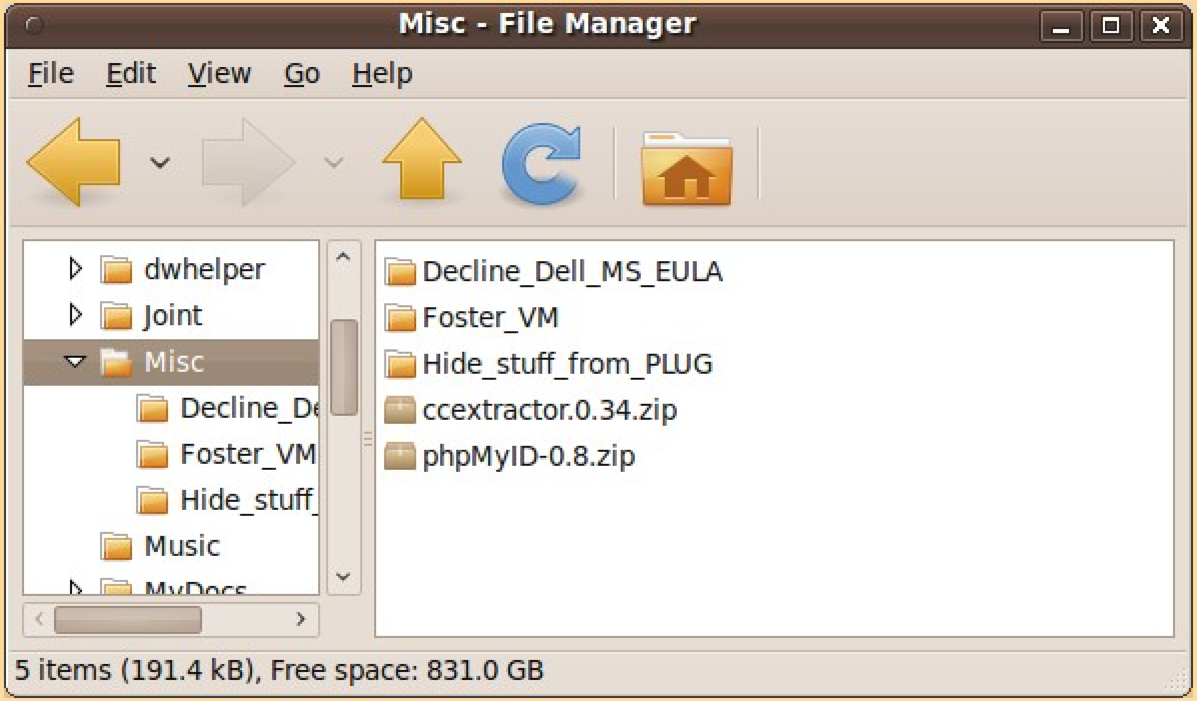
- Pre Ubuntu 10.04
  - 1) System > Preferences > Appearance > Interface: check “editable menu shortcut keys”
  - 2) Run roxterm, hover over Edit > Copy, press ALT+C
  - 3) System > Preferences > Appearance > Interface: Uncheck “editable menu shortcut keys”

Editable menu keys

- Ubuntu 10.04 and future?
  - System > Preferences > Appearance > Interface: check “editable menu shortcut keys” was removed from the GUI (apparently upstream? Really stupid.)
  - Used gconf-editor or:
    - gconftool --set --type bool /desktop/gnome/interface/can_change_accels true
    - gconftool --set --type bool /desktop/gnome/interface/can_change_accels false
  - See slide notes for a trivial script

thunar - File Manager for Xfce

- **MUCH** faster than Nautilus!
- View > Location Selector > Toolbar Style
- View > Side Panel > Tree

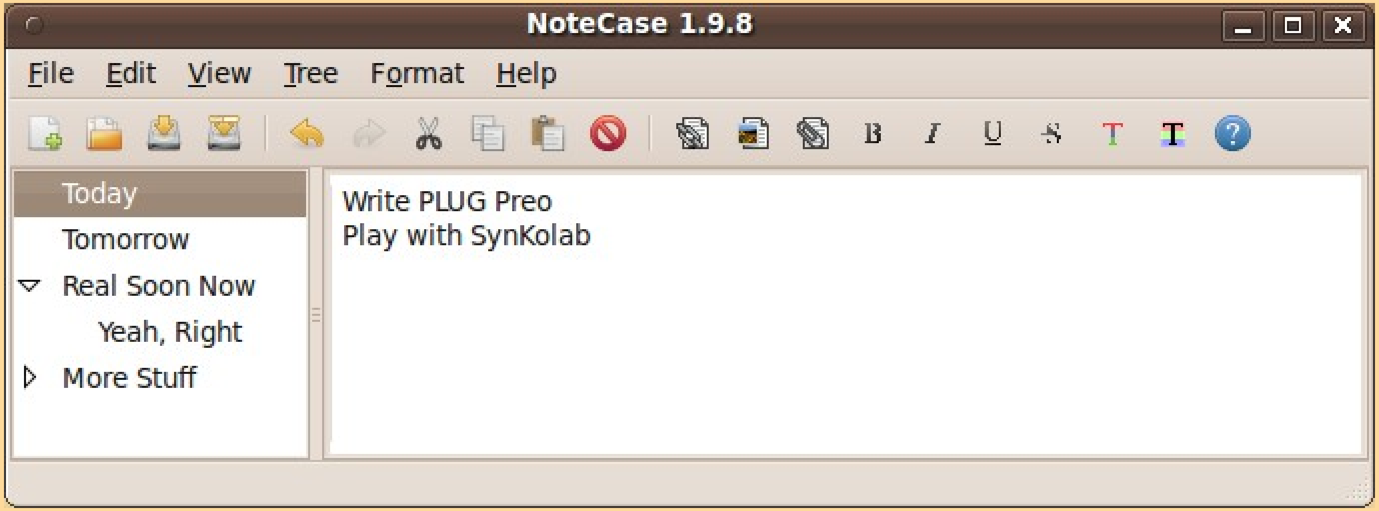


Decline_Dell_MS_EULA
Foster_VM
Hide_stuff_from_PLUG
ccextractor.0.34.zip
phpMyID-0.8.zip

5 items (191.4 kB), Free space: 831.0 GB

notecase - hierarchical note manager

- Not under active development
- Saves in a single, optionally encrypted, XML file
- Auto-save, and can export to HTML



Write PLUG Preo
Play with SynKolab

look -- display lines beginning with a given string

- Huh?
- Simple, it's a command line “how do I spell _____” tool, since it looks in dicts by default, **if any are installed!** (see “wamerican*”)
-
  ```
  $ look neigh
  […]
  neighbor
  neighbor's
  [...]
  ```

lookup - interactive utility to search text files quickly

- I don't really use this, but it sounded neat
- See also: man lookup
- “DESCRIPTION
  “Lookup allows the quick interactive search of text files. It supports ASCII, JIS-ROMAN, and Japanese EUC Packed formated text, and has an integrated romaji-kana converter”
- Indexes the file first
- Not installed by default

xsel - command-line tool to access X clipboard

- See also: xclip - command line interface to X selections
- I find xsel is closer to Just Doing The Right Thing
- Demo
  - echo 'testing xsel from the CLI' | xsel -b
  - xsel | sort | xsel -b
  - alias clip='xsel -b'

screen - terminal multiplexor with VT100/ANSI terminal emulation

- Huh?
  - Unreliable connection, or stop & go home
  - Multi-user training
  - Multiplex terminals
- See also:
  - screenbin - use Amazon EC2 to host a shared screen session
  - screenie - a small and lightweight GNU screen(1) wrapper
  - byobu - a set of useful profiles and a profile-switcher for GNU screen
  - http://sourceforge.net/projects/tmux/

screen 2 of 3

- Steals CTRL+A, fix that in ~/.screenrc:
  - # Change the INSANE C-a default to C-n (use C-n n to send literal ^N)
    escape ^Nn
- sudo mkdir -m 1755 /tmp/screens
- sudo chmod u+s /usr/bin/screen
  - May not need this anymore?

screen 3 of 3

- Multiuser: as the "host"
  - screen -S {name of session, no spaces}, e.g. screen -S training
  - Turn on multi-user mode: CTRL-a:multiuser on
  - CTRL-a:addacl {usernames} of accounts (comma delimited, no spaces!) which may access the display. Note this allows full read/write access! E.g. CTRL-a:addacl alice,bob,carl
  - Use the CTRL-a:chacl {usernames} {permbits} {list} command to refine permissions if needed (rare).
- As the "viewer"
  - Use screen -x {user}/{name} to connect to a shared screen, e.g. screen -x jp/training
  - CTRL-aK to kill the window and end the session.

bash-completion - programmable completion for the bash shell

- “bash completion extends bash's standard completion behavior to achieve complex command lines with just a few keystrokes.”
- Kinda built-in to Ubuntu, but you may have to enable it in */etc/bash.bashrc* or *~/.bashrc*

- sudo apti{tab}
- sudo aptitude in{tab}
- sudo aptitude install roxt{tab}
- sudo aptitude install roxterm

System hardware info

- hwinfo - Hardware identification system
- lshw - information about hardware configuration
- lshw-gtk - graphical information about hardware configuration
- lspci - list all PCI devices

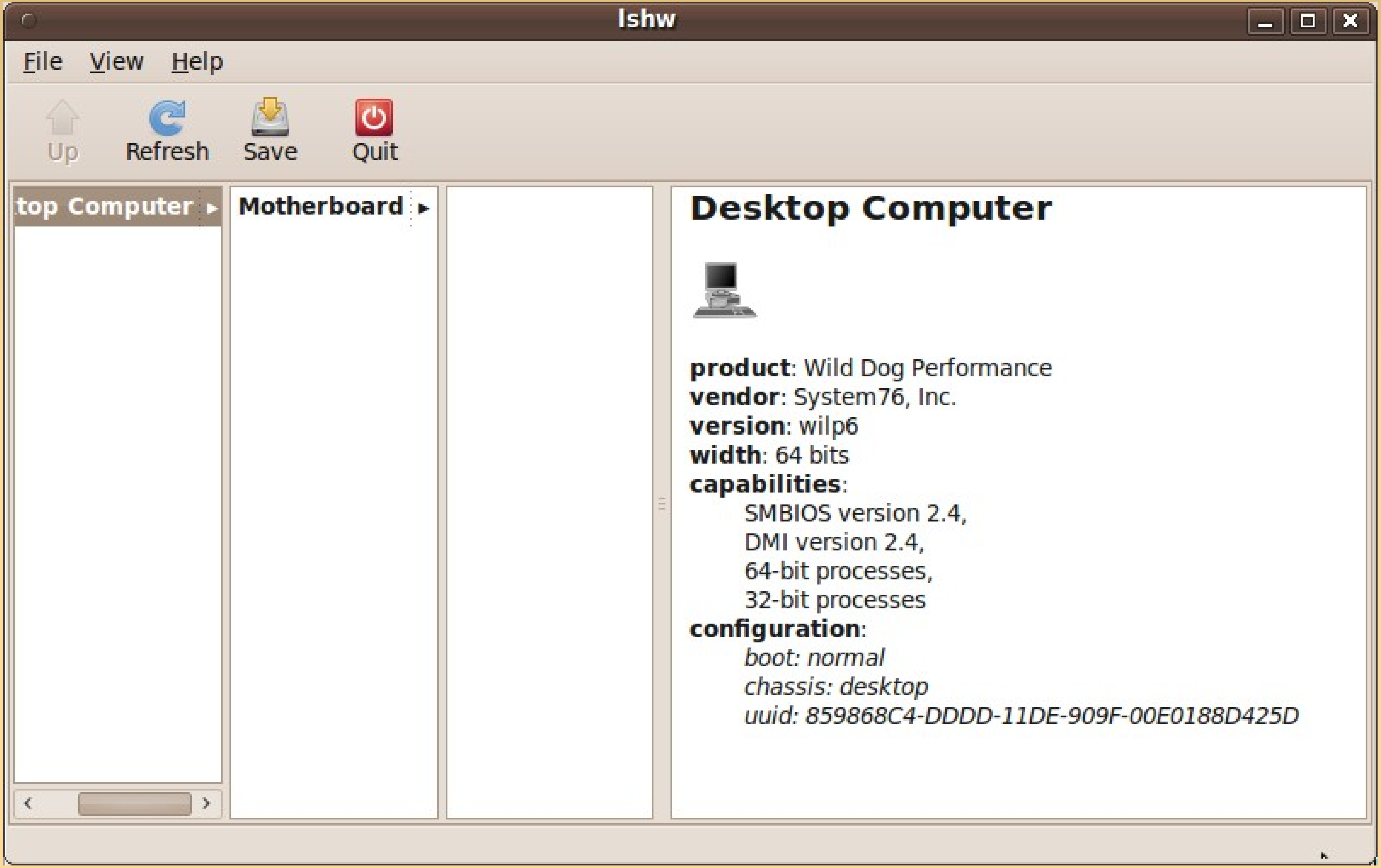
hwinfo

-
  ```
  $ sudo hwinfo --sound | less
  15: PCI 1b.0: 0403 Audio device
    [Created at pci.318]
    UDI:
  /org/freedesktop/Hal/devices/pci_8086_3a3e
    Unique ID: u1Nb.mu__efD1m12
    SysFS ID: /devices/pci0000:00/0000:00:1b.0
    SysFS BusID: 0000:00:1b.0
    Hardware Class: sound
  [...]
  ```

lshw

```
$ sudo lshw | less
ringo
    description: Desktop Computer
    product: Wild Dog Performance
    vendor: System76, Inc.
    version: wilp6
    width: 64 bits
    capabilities: smbios-2.4 dmi-2.4 vsyscall64
[...]
```

lshw-gtk



Desktop Computer

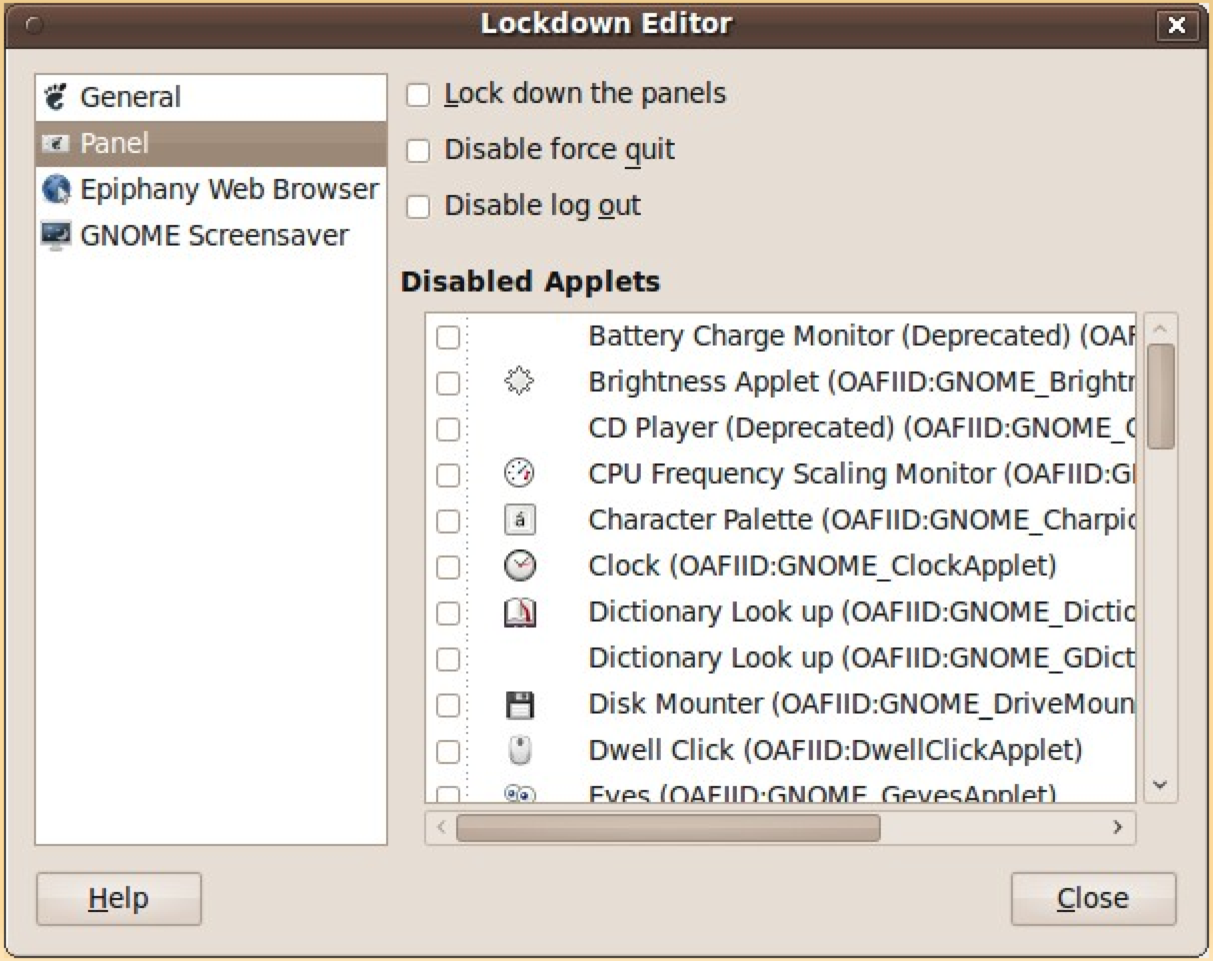
product: Wild Dog Performance
vendor: System76, Inc.
version: wilp6
width: 64 bits
capabilities:
SMBIOS version 2.4,
DMI version 2.4,
64-bit processes,
32-bit processes
configuration:
boot: normal
chassis: desktop
uuid: 859868C4-DDDD-11DE-909F-00E0188D425D

lspci

-
  ```
  $ sudo lspci -v | less
  01:00.0 VGA compatible controller: nVidia Corporation G96 [GeForce 9500 GT] (rev a1)
          Subsystem: eVga.com. Corp. Device c958
          Flags: bus master, fast devsel, latency 0, IRQ 16
          Memory at e2000000 (32-bit, non-prefetchable) [size=16M]
          I/O ports at e000 [size=128]
  [...]
  ```

pessulus - lockdown editor for GNOME

- “pessulus enables the system administrator to set mandatory settings in GConf, which apply to all users, restricting what they can do, which may be of particular usefulness for kiosks (internet cafes, for example).”



□ Lock down the panels

□ Disable force quit

□ Disable log out

Disabled Applets

□ Battery Charge Monitor (Deprecated) (OAF
□ Brightness Applet (OAFIID:GNOME_Brightr
□ CD Player (Deprecated) (OAFIID:GNOME_C
□ CPU Frequency Scaling Monitor (OAFIID:GI
□ Character Palette (OAFIID:GNOME_Charpic
□ Clock (OAFIID:GNOME_ClockApplet)
□ Dictionary Look up (OAFIID:GNOME_Dictic
□ Dictionary Look up (OAFIID:GNOME_GDict
□ Disk Mounter (OAFIID:GNOME_DriveMoun
□ Dwell Click (OAFIID:DwellClickApplet)
□ Eyes (OAFIID:GNOME_GeyesApplet)

etckeeper

- I don't use this one, but if I was starting over I probably would (some URLs in slide notes)
- “Store /etc plus file metadata in git, mercurial, bzr or darcs, with APT hooks to autocommit during updates.”
- The default RCS changes depending on Ubuntu version
  - Hardy == git
  - Jaunty == bzr (Bazaar)
- Also, by default the repository is under /etc/ itself, not great for some kinds of recovery

localepurge

- “...A simple script to recover diskspace wasted for unneeded locale files and localized man pages. It will automagically be invoked upon completion of any apt installation run.”

- Will ask what to keep on install, thereafter it'll nuke anything that you don't want.

Bonus

- **espeak** - A multi-lingual software speech synthesizer
  - Installed by default
  - echo 'Hello world' | espeak
- **openoffice.org-presenter-console** - OpenOffice.org Impress extension for a separate presenter's console
  - In the repos
  - If dual-headed, giving a slide show presents the slides on one display, and notes, timer, sorter, etc. on the other.

Wrap-up and Q&A

- See also:
  - http://blog.thesilentnumber.me/2010/04/ubuntu-1004-post-install-guide-what-to.html http://bit.ly/cKAU58
- Questions?
- I'm on the PLUG list...