

# Manual, Packages and Logs

Chonnam National University  
School of Electronics and Computer  
Engineering

Kyungbaek Kim

# Manual pages

- Most Linux commands have an associated manual page
  - Often known as a manpage
- Viewed with the “man” command
  - e.g.) `$man ls`
- Press “q” to quit and return to the shell prompt

# Example of a manual page



A screenshot of a terminal window titled 'kbkim@ubuntu: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Terminal', and 'Help'. The main content area displays the manual page for the 'ls' command, with 'LS(1)' in the top left and right corners. The manual page is divided into sections: 'NAME' (ls - list directory contents), 'SYNOPSIS' (ls [OPTION]... [FILE]...), and 'DESCRIPTION' (List information about the FILES (the current directory by default). Sort entries alphabetically if none of -cftuvSUX nor --sort. Mandatory arguments to long options are mandatory for short options too. -a, --all do not ignore entries starting with . -A, --almost-all do not list implied . and ..). The bottom of the window shows a status bar with 'Manual page ls(1) line 1'.

```
kbkim@ubuntu: ~
File Edit View Terminal Help
LS(1)                                User Commands                                LS(1)

NAME
    ls - list directory contents

SYNOPSIS
    ls [OPTION]... [FILE]...

DESCRIPTION
    List information about the FILES (the current directory by default).
    Sort entries alphabetically if none of -cftuvSUX nor --sort.

    Mandatory arguments to long options are mandatory for short options
    too.

    -a, --all
        do not ignore entries starting with .

    -A, --almost-all
        do not list implied . and ..

Manual page ls(1) line 1
```

# Navigating within manual pages

- “man” uses the “less” viewer
- Use the cursor keys for scrolling
- Other common key strokes:
  - Space → jump down a page
  - b → jump back up a page
  - /word → search for the next occurrence of “word”
  - n → repeat the previous search
  - g → go to the top
  - q → quit
- Help on all keystrokes is available with “h”

# Sections of a Manual page

- Manpages have a traditional format
- Man pages for user commands tend to have some or all of these sections:
  - NAME → name and single-line reason for the command
  - SYNOPSIS → possible arguments
  - DESCRIPTION → fuller explanation of the command
  - OPTIONS
  - FILES → any files the command needs
  - ENVIRONMENT → pertinent environment variables
  - BUGS, AUTHORS, SEE ALSO

# Section of Manual

- Each manpage is in a section of the manual
- User commands are in section 1
- Different sections can contain pages of the same name
  - The “passwd” page in section 1 describes the “/usr/bin/passwd” command
    - passwd(1) : brought by “man 1 passwd”
  - The “passwd” page in section 5 describes THE “/etc/passwd” file
    - passwd(5) : brought by “man 5 passwd”

# Example of section of the manual

```
kbkim@ubuntu: ~  
File Edit View Terminal Help  
PASSWD(1) User Commands PASSWD(1)  
  
NAME  
    passwd - change user password  
  
SYNOPSIS  
    passwd [options] [LOGIN]  
  
DESCRIPTION  
    The passwd command changes passwords for user accounts. A normal  
    user may only change the password for his/her own account, while the  
Manual page passwd(1) line 1
```

```
kbkim@ubuntu: ~  
File Edit View Terminal Help  
PASSWD(5) File Formats and Conversions PASSWD(5)  
  
NAME  
    passwd - the password file  
  
DESCRIPTION  
    /etc/passwd contains one line for each user account, with seven  
    fields delimited by colons (":"). These fields are:  
  
    · login name  
Manual page passwd(5) line 1
```

# Manual Section Numbering

- Most commands are documented in section 1
  - This is the first place man looks
- Other sections may be needed

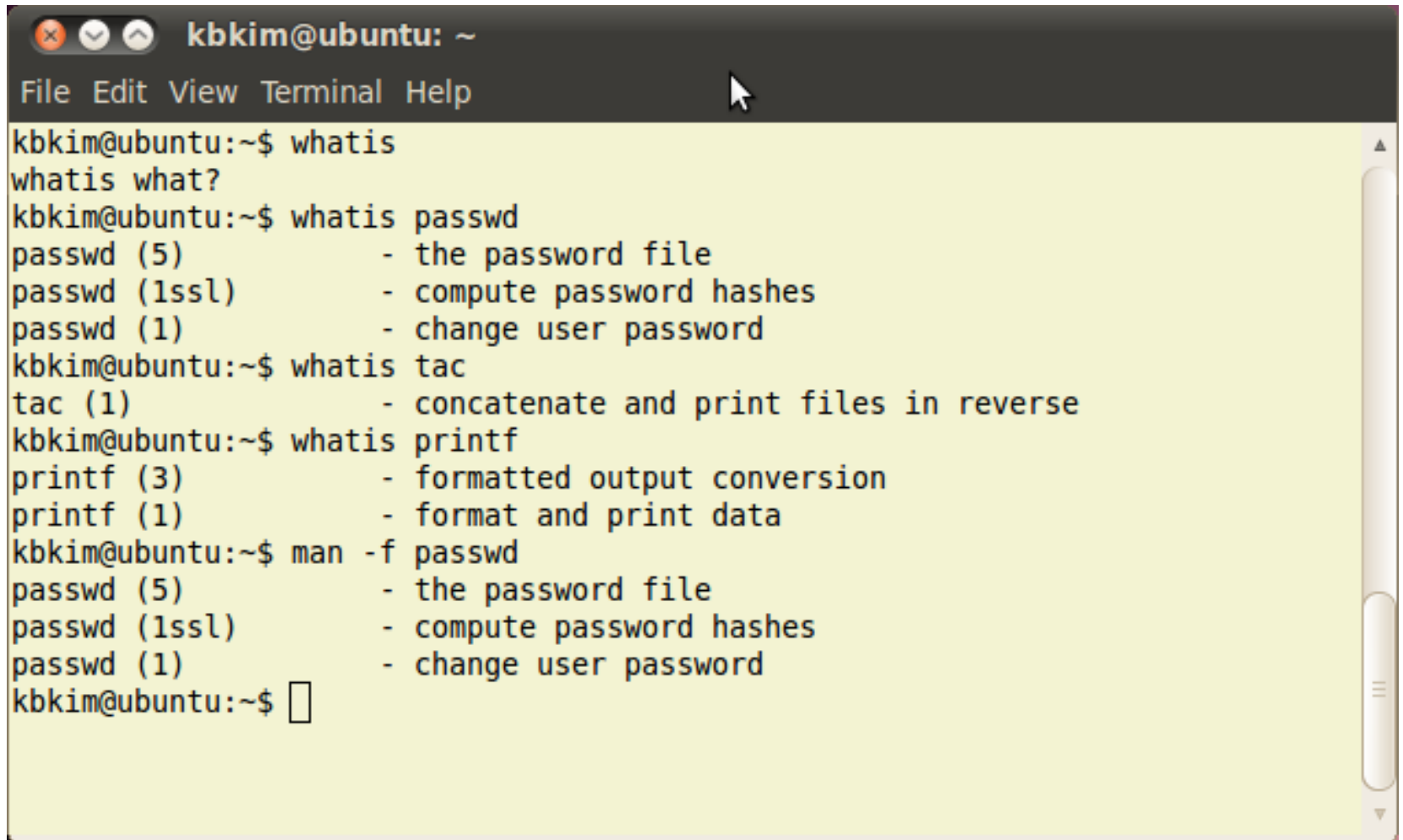
Section	Description
1	General command (or user program)
2	System calls
3	Library functions, covering in particular the C standard Library
4	Special files (usually devices, those found in /dev) and drivers
5	File formats and conventions
6	Games and screensavers
7	Miscellanea
8	System administration commands and deamons



# Determining Available Man pages

- “what is” command
  - Lists manpages with the specified name
- Section number in brackets
- Single-line description from the NAME section
- Useful for quickly discovering what a command does
- “man -f “ is equivalent to “whatis”

# Example of whatis



A terminal window titled 'kbbkim@ubuntu: ~' with a menu bar containing 'File', 'Edit', 'View', 'Terminal', and 'Help'. The terminal shows the following commands and their outputs:

```
kbbkim@ubuntu:~$ whatis
whatis what?
kbbkim@ubuntu:~$ whatis passwd
passwd (5)          - the password file
passwd (1ssl)       - compute password hashes
passwd (1)          - change user password
kbbkim@ubuntu:~$ whatis tac
tac (1)             - concatenate and print files in reverse
kbbkim@ubuntu:~$ whatis printf
printf (3)          - formatted output conversion
printf (1)          - format and print data
kbbkim@ubuntu:~$ man -f passwd
passwd (5)          - the password file
passwd (1ssl)       - compute password hashes
passwd (1)          - change user password
kbbkim@ubuntu:~$
```

# Printing Manual Pages

- “-t” option generate a postscript version of manual pages



The screenshot shows two overlapping windows. The top window is a terminal titled 'kbkim@ubuntu: ~/tmp' with a menu bar 'File Edit View Terminal Help'. It contains the following commands and output:

```
kbkim@ubuntu:~/tmp$ man -t passwd > passwd_man.ps
kbkim@ubuntu:~/tmp$ evince passwd_man.ps
```

The bottom window is a document viewer titled 'passwd\_man.ps' with a menu bar 'File Edit View Go Help'. It displays the first page of the 'passwd' manual page. The page has a header with 'PASSWD(1)' on the left and right, and 'User Commands' in the center. The content includes sections for NAME, SYNOPSIS, and DESCRIPTION.

**NAME**  
passwd – change user password

**SYNOPSIS**  
passwd [options] [LOGIN]

**DESCRIPTION**  
The **passwd** command changes passwords for user accounts. A normal user may only change the password for his/her own account, while the superuser may change the password for any account. **passwd** also changes the account or associated password validity period.

**Password Changes**  
The user is first prompted for his/her old password, if one is present. This password is then encrypted and compared against the stored password. The user has only one chance to enter the correct password. The superuser is permitted to bypass this step so that forgotten passwords may be changed.

After the password has been entered, password aging information is checked to see if the user is permitted

# Searching for Manpages

- “apropos”
  - To search for pages with a NAME section matching a particular keyword
- Can’t restrict the search to a particular section
  - We can use “grep”
- “man -k” is equivalent to “apropos”

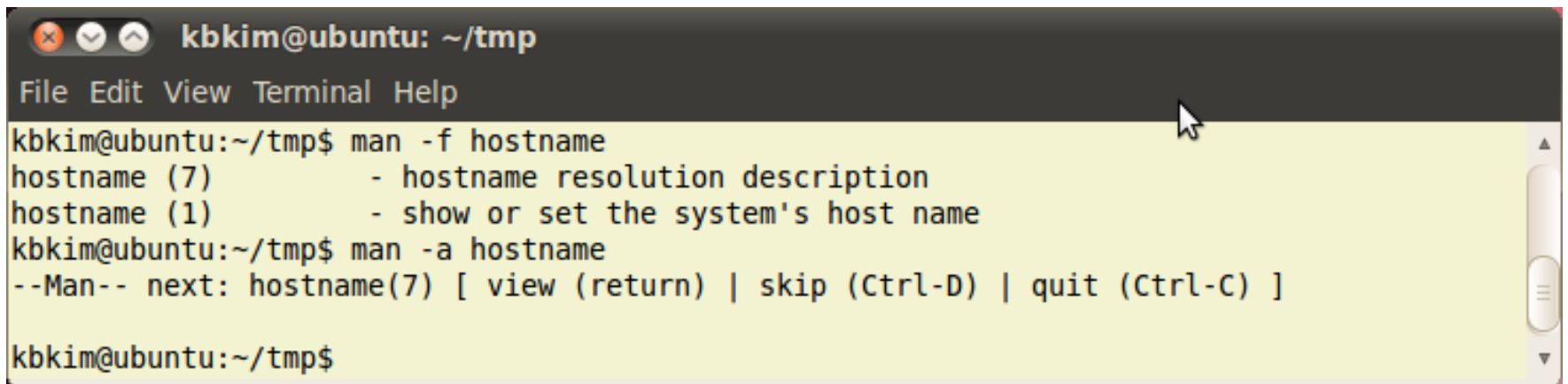
# Example of apropos

```
kbkim@ubuntu: ~/tmp
File Edit View Terminal Help

kbkim@ubuntu:~/tmp$ apropos open | wc
   66    536   3787
kbkim@ubuntu:~/tmp$ man -k open | wc
   66    536   3787
kbkim@ubuntu:~/tmp$ apropos open | grep '(1)'
compiz (1)      - OpenGL window and compositing manager
gnome-open (1)  - Open files and URLs using the GNOME file handlers
gpg (1)        - OpenPGP encryption and signing tool
gpgsplit (1)   - Split an OpenPGP message into packets
gpgv (1)       - Verify OpenPGP signatures
nc_openbsd (1) - arbitrary TCP and UDP connections and listens
oocalc (1)     - OpenOffice.org office suite
oodraw (1)     - OpenOffice.org office suite
ooffice (1)    - OpenOffice.org office suite
oofromtemplate (1) - OpenOffice.org office suite
oointpress (1) - OpenOffice.org office suite
oomath (1)     - OpenOffice.org office suite
ooweb (1)      - OpenOffice.org office suite
oowriter (1)   - OpenOffice.org office suite
open (1)       - start a program on a new virtual terminal (VT).
openoffice (1) - OpenOffice.org office suite
openvt (1)     - start a program on a new virtual terminal (VT).
rlogin (1)     - OpenSSH SSH client (remote login program)
rsh (1)        - OpenSSH SSH client (remote login program)
slogin (1)     - OpenSSH SSH client (remote login program)
ssh (1)        - OpenSSH SSH client (remote login program)
unopkg (1)     - OpenOffice.org Extension Manager
xdg-open (1)   - opens a file or URL in the user's preferred application
kbkim@ubuntu:~/tmp$
```

# Displaying all manpages

- “man -a”
  - Display all pages which have a particular name, regardless of their section
    - Display and wait for quit
    - Then chose to view/skip/quit the next manpage

A terminal window titled 'kbbkim@ubuntu: ~/tmp' with a menu bar (File, Edit, View, Terminal, Help). The terminal shows the execution of 'man -f hostname', listing 'hostname (7) - hostname resolution description' and 'hostname (1) - show or set the system's host name'. Then, 'man -a hostname' is executed, showing '--Man-- next: hostname(7) [ view (return) | skip (Ctrl-D) | quit (Ctrl-C) ]'. The prompt returns to 'kbbkim@ubuntu:~/tmp\$'.

```
kbbkim@ubuntu: ~/tmp
File Edit View Terminal Help
kbbkim@ubuntu:~/tmp$ man -f hostname
hostname (7)          - hostname resolution description
hostname (1)          - show or set the system's host name
kbbkim@ubuntu:~/tmp$ man -a hostname
--Man-- next: hostname(7) [ view (return) | skip (Ctrl-D) | quit (Ctrl-C) ]
kbbkim@ubuntu:~/tmp$
```

# Searching the contents of all Man pages

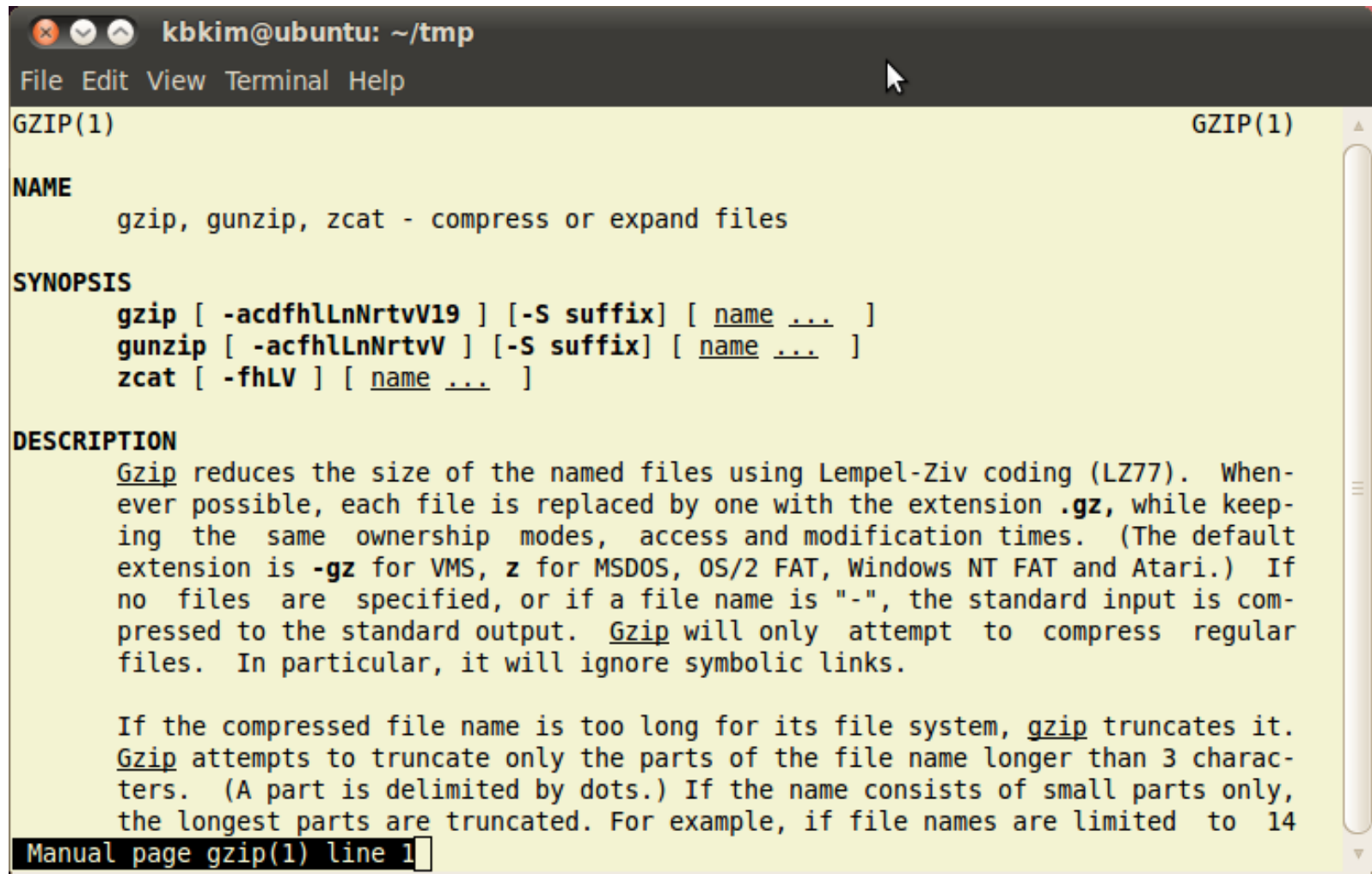
- “man -K”
  - Search through the textual contents of the entire manual
  - Uppercase k !!
- Not particularly useful
  - Many false matches obscuring the desired data
  - Slow to search so much text
  - Tedious to respond to each prompt

# Finding the right manual page

- Sometimes commands' documentation are not quite where expected
- Related commands can be grouped together on one page
  - e.g.) gzip, gunzip and zcat are in one man page
  - Can be misleading if you look up one command and start reading the description of another



# Example of “man gzip”

A terminal window titled 'kdkim@ubuntu: ~/tmp' with a menu bar 'File Edit View Terminal Help'. The terminal displays the output of the 'man gzip' command. The output is formatted with section headers in bold: NAME, SYNOPSIS, and DESCRIPTION. The NAME section lists 'gzip, gunzip, zcat - compress or expand files'. The SYNOPSIS section shows the command syntax for 'gzip', 'gunzip', and 'zcat'. The DESCRIPTION section explains that 'Gzip' uses Lempel-Ziv coding (LZ77) to reduce file size and mentions file name truncation rules. At the bottom, a status bar indicates 'Manual page gzip(1) line 1'.

```
kdkim@ubuntu: ~/tmp
File Edit View Terminal Help

GZIP(1) GZIP(1)

NAME
    gzip, gunzip, zcat - compress or expand files

SYNOPSIS
    gzip [ -acdfhLLnNrtvV19 ] [-S suffix] [ name ... ]
    gunzip [ -acfhlLnNrtvV ] [-S suffix] [ name ... ]
    zcat [ -fhLV ] [ name ... ]

DESCRIPTION
    Gzip reduces the size of the named files using Lempel-Ziv coding (LZ77). When-
    ever possible, each file is replaced by one with the extension .gz, while keep-
    ing the same ownership modes, access and modification times. (The default
    extension is -gz for VMS, z for MSDOS, OS/2 FAT, Windows NT FAT and Atari.) If
    no files are specified, or if a file name is "-", the standard input is com-
    pressed to the standard output. Gzip will only attempt to compress regular
    files. In particular, it will ignore symbolic links.

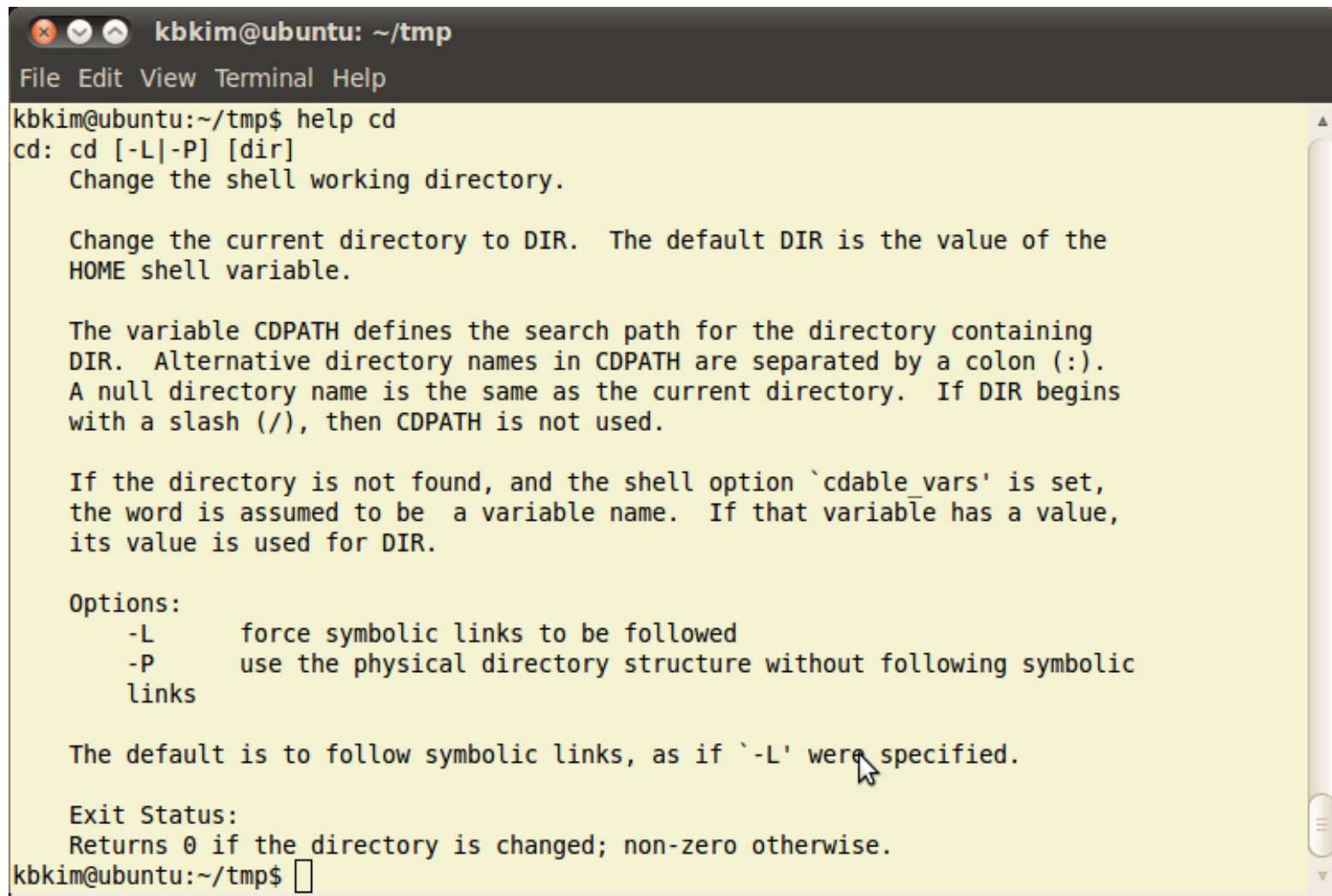
    If the compressed file name is too long for its file system, gzip truncates it.
    Gzip attempts to truncate only the parts of the file name longer than 3 charac-
    ters. (A part is delimited by dots.) If the name consists of small parts only,
    the longest parts are truncated. For example, if file names are limited to 14

Manual page gzip(1) line 1
```

# Help on Shell Builtins

- Shell built-in commands are documented in shell's manpages
  - `cd(1)` refers the reader to `bash(1)`
  - `echo(1)` relates to “`/bin/echo`”, but in most shells “`echo`” is a separate built-in command
- “`help`” command
  - Display brief explanations of builtin functions

# Example of help



```
kbkim@ubuntu: ~/tmp
File Edit View Terminal Help
kbkim@ubuntu:~/tmp$ help cd
cd: cd [-L|-P] [dir]
    Change the shell working directory.

    Change the current directory to DIR.  The default DIR is the value of the
    HOME shell variable.

    The variable CDPATH defines the search path for the directory containing
    DIR.  Alternative directory names in CDPATH are separated by a colon (:).
    A null directory name is the same as the current directory.  If DIR begins
    with a slash (/), then CDPATH is not used.

    If the directory is not found, and the shell option `cdable_vars' is set,
    the word is assumed to be a variable name.  If that variable has a value,
    its value is used for DIR.

    Options:
      -L      force symbolic links to be followed
      -P      use the physical directory structure without following symbolic
              links

    The default is to follow symbolic links, as if `-L' were specified.

    Exit Status:
    Returns 0 if the directory is changed; non-zero otherwise.
kbkim@ubuntu:~/tmp$
```

# Location of manual pages

- Manpages are stored in the filesystem
- “man -aw” to find the locations of a given manpage
  - Show the locations of all manpages with a given name
- Common locations for manpages include “/usr/man” and “/usr/share/man”
  - Locally installed packages often put manpages under “/usr/share/man”

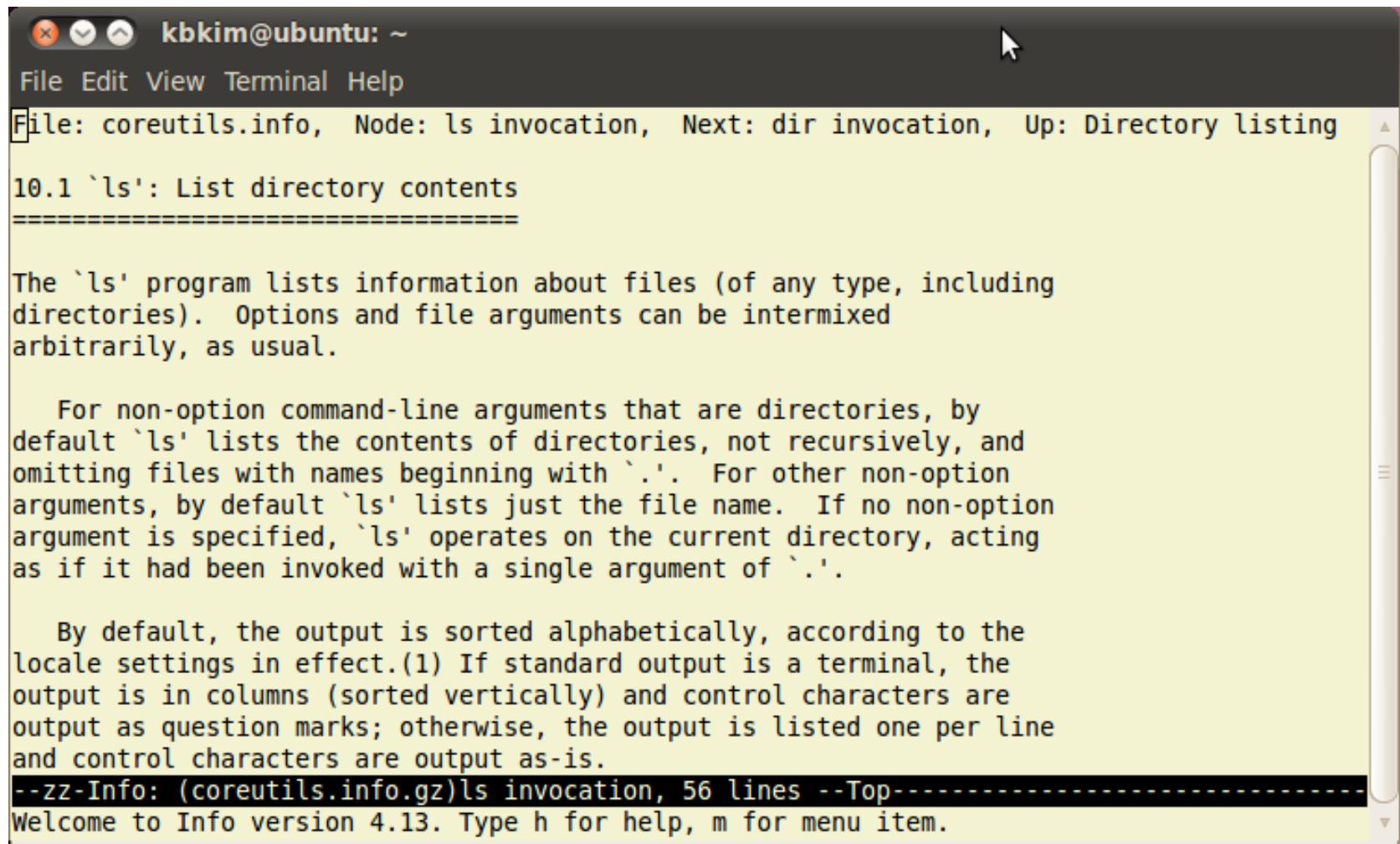
# Example of “man -aw”

```
kbkim@ubuntu: ~  
File Edit View Terminal Help  
kbkim@ubuntu:~$ man -aw passwd  
/usr/share/man/man1/passwd.1.gz  
/usr/share/man/man1/passwd.1ssl.gz  
/usr/share/man/man5/passwd.5.gz  
kbkim@ubuntu:~$ ls /usr/share/man  
cs es fr fr.UTF-8 hu it ko man2 man4 man6 man8 pt_BR sv zh_CN  
de fi fr.ISO8859-1 gl id ja man1 man3 man5 man7 pl ru tr zh_TW  
kbkim@ubuntu:~$ ls -l /usr/share/man/man1 | wc  
1287 10638 82751  
kbkim@ubuntu:~$ man -aw zcat  
/usr/share/man/man1/gzip.1.gz  
kbkim@ubuntu:~$ man -aw gunzip  
/usr/share/man/man1/gzip.1.gz  
kbkim@ubuntu:~$ man -aw gzip  
/usr/share/man/man1/gzip.1.gz  
kbkim@ubuntu:~$ ls -l /usr/share/man/man1/gunzip*  
lrwxrwxrwx 1 root root 9 2012-03-21 07:43 /usr/share/man/man1/gunzip.1.gz -> gzip.1.gz  
kbkim@ubuntu:~$ ls -l /usr/share/man/man1/gzip*  
-rw-r--r-- 1 root root 6250 2010-08-16 23:57 /usr/share/man/man1/gzip.1.gz  
kbkim@ubuntu:~$ ls -l /usr/share/man/man1/zcat*  
lrwxrwxrwx 1 root root 9 2012-03-21 07:43 /usr/share/man/man1/zcat.1.gz -> gzip.1.gz  
kbkim@ubuntu:~$
```

# Info pages

- GNU's documentation system
  - GNU utilities have info pages
  - Often duplicating man pages
  - An info page may be split into nodes
  - Use hyperlinks between nodes
- Scroll with the cursor keys, PgUp and PgDn
- Hyperlinks
  - Tab : find next, Enter : follow hyperlink, I : return to previous location
  - n, p, u : next, previous, up node

# Example of “info ls”

A screenshot of a terminal window titled 'kdkim@ubuntu: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Terminal', and 'Help'. The main content area shows the output of the 'info ls' command. At the top, it says 'File: coreutils.info, Node: ls invocation, Next: dir invocation, Up: Directory listing'. Below this is the section '10.1 `ls`: List directory contents' followed by a separator line '====='. The text describes the 'ls' program, its options, and its default behavior. At the bottom, there is a status bar that reads '--zz-Info: (coreutils.info.gz)ls invocation, 56 lines --Top-----' and a welcome message 'Welcome to Info version 4.13. Type h for help, m for menu item.'

```
kdkim@ubuntu: ~
File Edit View Terminal Help
File: coreutils.info, Node: ls invocation, Next: dir invocation, Up: Directory listing

10.1 `ls`: List directory contents
=====

The `ls` program lists information about files (of any type, including
directories). Options and file arguments can be intermixed
arbitrarily, as usual.

    For non-option command-line arguments that are directories, by
default `ls` lists the contents of directories, not recursively, and
omitting files with names beginning with `.`. For other non-option
arguments, by default `ls` lists just the file name. If no non-option
argument is specified, `ls` operates on the current directory, acting
as if it had been invoked with a single argument of `.`.

    By default, the output is sorted alphabetically, according to the
locale settings in effect.(1) If standard output is a terminal, the
output is in columns (sorted vertically) and control characters are
output as question marks; otherwise, the output is listed one per line
and control characters are output as-is.
--zz-Info: (coreutils.info.gz)ls invocation, 56 lines --Top-----
Welcome to Info version 4.13. Type h for help, m for menu item.
```

# Documents in “/usr/share/doc”

- The main(or only) documentation of a program is not available as man or info pages
- “/usr/share/doc/” contains other format of documentation
  - Usually plain text
  - Sometimes HTML
  - Subdirectory per package, such as “/usr/share/doc/grep/”



# Contents of “/usr/share/doc”

- Documentation in “/usr/share/doc” is often information only relevant to system administration of a package, not users of it
  - Installation instructions, license, change log
- Sometimes more user-friendly documentation than elsewhere
  - HTML help is more common for interactive applications and very rare for traditional unix command
  - Programs ported from other platforms often have documentation in “/usr/share/doc” rather than man pages

# Package Management

- Packages
  - Bundles of software and metadata
    - Software's full name
    - Description of its purpose
    - Version number
    - Vendor
    - Checksum
    - A list of **dependencies** necessary for the software to run properly
- Package Management system
  - A collection of tools to automate the process of
    - Installing software packages
    - Upgrading software packages
    - Configuring software packages
    - Removing software packages

# Different to File archives

- File archiver
  - A computer program that combines a number of files together into one archive file for easier transportation or storage
- Metadata
  - Data (or information) about other data
- Tar (Tarball) and Zip
- Commonly used for source and binary distribution on Unix-like platforms

# Dependency Problems

- Executable programs are derived from source code and libraries
- The make (compiling and linking) process requires the description of all dependencies between those files
- Broken, extraneous, faulty, forgotten, or incompatible dependencies cause programming mistakes or bugs
- Dependency Hell
  - Many dependencies – high coupling
  - Long chains of dependencies
  - Conflicting dependencies
  - Circular dependencies
- Version Numbers
  - Partial solution to dependency problems
  - Naming conventions are inconsistent

# Package Management Systems

- Different Linux distribution may use different package management systems

			Front Ends	
Base	Package	Tool	CLI	GUI
dpkg	.deb	apt	apt-get aptitude dselect jigdo	synaptic
rpm	.rpm	rpm apt-rpm YUM ZYpp	rpm apt-rpm yum yast pcon urpmi jigdo ???	yumex KYum yast gnome- packagekit kpackagekit pup [ pirut ] pyjigdo ???

# dpkg

- A Package manager for Debian-based system
- **dpkg -l**
  - List all packages installed on the system
- **dpkg -L package\_name**
  - List the files installed by a package
- **dpkg -S file\_path**
  - Search a package which contains the given file
- **dpkg -i package\_deb\_name.deb**
  - Install a local package deb file
- **dpkg -r package\_name**
  - Remove a package
  - *Not Recommended !!*

# apt-get

- Ubuntu's Advanced Packaging Tool (APT)
- Command-line tool for server administrators
- **apt-get install package\_name**
  - Install a package
- **apt-get remove package\_name**
  - Remove a package
  - “--purge” option : remove the package configuration files as well
- **apt-get upgrade**
  - Upgrade the installed packages
  - We need updated information : package index
- **apt-get update**
  - Update the APT package index from the repository defined in the “/etc/apt/source.list”
- All the activities are logged in the “/var/log/dpkg.log” file

# Repository

- APT uses APT system repository
- What is a repository?
  - A collection of files, plus an index
  - Centralized repositories by **distribution**
  - Repositories may be structured differently
  - Cryptographically signed with GPG keys to authenticate identity
    - GPG : GNU Privacy Guard
      - Alternative to the PGP (Pretty Good Privacy) suite of cryptographic software



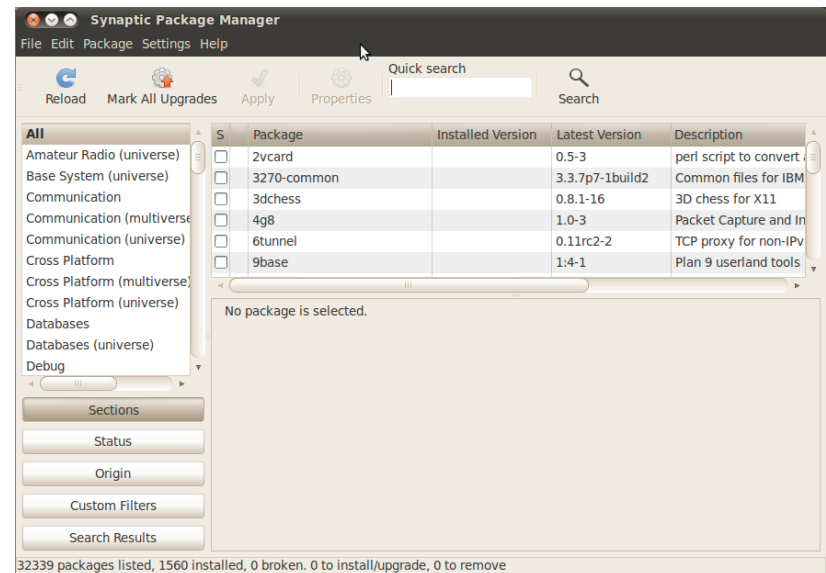
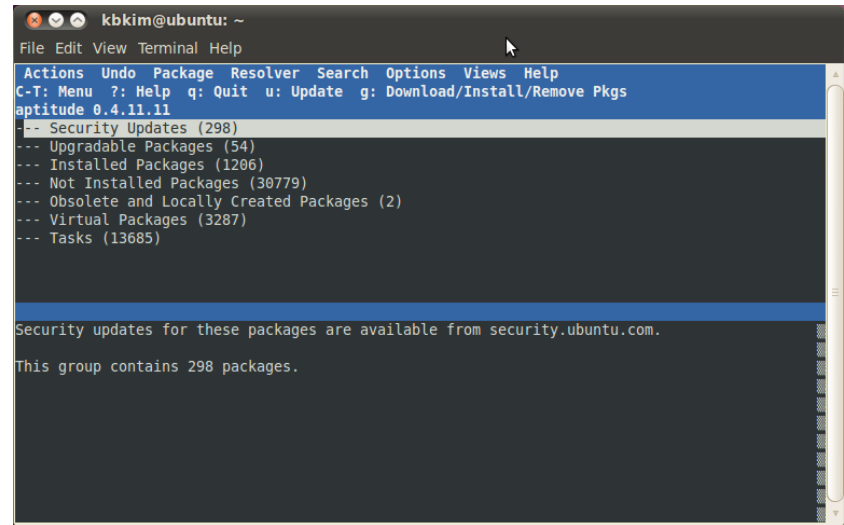
# Ubuntu repository

- “/etc/apt/sources.list”
  - Configuration of Ubuntu’s APT system repositories
- Types
  - **Main** – holds officially supported software
  - **Restricted** – not available under a completely free license
  - **Universe** – is not official, but is maintained by the community
  - **Multiverse** – many “multiverse” wares are not free-like-speech, e.g. DVD player open source software with closed source drivers/libraries

```
kbkim@ubuntu: ~  
File Edit View Terminal Help  
kbkim@ubuntu:~$ cat /etc/apt/sources.list | more  
#deb cdrom:[Ubuntu 10.04.4 LTS _Lucid Lynx_ - Release i386 (20120214.2)]/ lucid  
main restricted  
# See http://help.ubuntu.com/community/UpgradeNotes for how to upgrade to  
# newer versions of the distribution.  
  
deb http://ftp.daum.net/ubuntu/ lucid main restricted  
deb-src http://ftp.daum.net/ubuntu/ lucid main restricted  
  
## Major bug fix updates produced after the final release of the  
## distribution.  
deb http://ftp.daum.net/ubuntu/ lucid-updates main restricted  
deb-src http://ftp.daum.net/ubuntu/ lucid-updates main restricted  
  
## 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://ftp.daum.net/ubuntu/ lucid universe  
deb-src http://ftp.daum.net/ubuntu/ lucid universe  
deb http://ftp.daum.net/ubuntu/ lucid-updates universe  
deb-src http://ftp.daum.net/ubuntu/ lucid-updates universe  
  
## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu  
## team, and may not be under a free licence. Please satisfy yourself as to  
## your rights to use the software. Also, please note that software in  
## multiverse WILL NOT receive any review or updates from the Ubuntu  
## security team.  
deb http://ftp.daum.net/ubuntu/ lucid multiverse  
deb-src http://ftp.daum.net/ubuntu/ lucid multiverse  
deb http://ftp.daum.net/ubuntu/ lucid-updates multiverse  
deb-src http://ftp.daum.net/ubuntu/ lucid-updates multiverse  
  
## Uncomment the following two lines to add software from the 'backports'  
## repository.  
## N.B. software from this repository may not have been tested as  
## extensively as that contained in the main release, although it includes
```

# Other APT systems in Ubuntu

- Aptitude
  - Menu-driven, text-based front-end to the APT system
- Synaptic
  - GUI based APT system



# Logging

- Many events that occur on a Linux system should be logged for administrative purposes
- Linux has a facility called “syslog” that allows any service or part of the system to log such events
  - c.f.) “rsyslog” in ubuntu
- Events can be selected based on severity (level) and/or on the service that encountered the event (facility)
- Messages can go to files, to the system console, or to a centralized syslog server running on another machine

# rsyslog in ubuntu

```
kbkim@ubuntu: ~  
File Edit View Terminal Help  
kbkim@ubuntu:~$ man -k rsyslog  
rsyslog.conf (5)      - rsyslogd(8) configuration file  
rsyslogd (8)         - reliable and extended syslogd  
kbkim@ubuntu:~$ ls /etc/rsyslog*  
/etc/rsyslog.conf  
  
/etc/rsyslog.d:  
20-ufw.conf  50-default.conf  
kbkim@ubuntu:~$ ps -ef | grep rsyslog  
syslog      720      1  0 16:04 ?        00:00:00 rsyslogd -c4  
kbkim      2167    1954  0 16:10 pts/0    00:00:00 grep --color=auto rsyslog  
kbkim@ubuntu:~$
```

# Configuration of rsyslog

- Configuration is in “/etc/rsyslog.conf” and “/etc/rsyslog.d”
  - Form : facility.level destination
- The facility is the creator of the message
  - One of auth, authpriv, cron, daemon, kern, lpr, mail, news, syslog, user, or local0 through local7
- The level is a severity threshold beyond which messages will be logged
  - (lowest to highest)
  - debug, info, notice, warning, err, crit, alert, emerg
- The “destination” indicates where messages selected by the facility and level will be sent
  - Normally the name of a log file or a device

# Details of Facility

- auth → security/authorization messages
- authpriv → security/authorization messages (more sensitive)
- cron → clock daemon
- daemon → system daemon without separate facility
- ftp → ftp daemon
- kern → kernel message
- lpr → line printer subsystem
- mail → mail subsystem
- news → USENET news subsystem
- syslog → message generated internally by rsyslogd

# Details of Level

- emerg → system is unusable
- alert → action must be taken immediately
- crit → critical conditions
- err → error conditions
- warning → warning conditions
- notice → normal, but significant, condition
- info → informational message
- debug → debug-level message



# Example of configuration

```
kbkim@ubuntu: ~  
File Edit View Terminal Help  
# Default rules for rsyslog.  
#  
#           For more information see rsyslog.conf(5) and /etc/rsyslo  
g.conf  
#  
# First some standard log files.  Log by facility.  
#  
auth,authpriv.*          /var/log/auth.log  
*. *;auth,authpriv.none  -/var/log/syslog  
#cron.*                  /var/log/cron.log  
daemon.*                 -/var/log/daemon.log  
kern.*                   -/var/log/kern.log  
lpr.*                    -/var/log/lpr.log  
mail.*                   -/var/log/mail.log  
user.*                   -/var/log/user.log  
#  
# Logging for the mail system.  Split it up so that  
# it is easy to write scripts to parse these files.  
#  
mail.info                -/var/log/mail.info  
mail.warn                -/var/log/mail.warn  
mail.err                 /var/log/mail.err
```

```
kbkim@ubuntu: ~  
File Edit View Terminal Help  
#  
daemon.*;mail.*;\n    news.err;\n    *.=debug;*.=info;\n    [*.=notice;*.=warn    | /dev/xconsole  
68,2-9 Bot
```

# Reconfiguration of rsyslog

- If you change configuration of rsyslog you need to tell rsyslog to re-read the configuration
- Accomplished by sending the rsyslogd process a **SIGHUP (hang up)** signal
  - e.g.) `#kill -HUP /usr/sbin/rsyslogd`
- Alternative way : use init script of rsyslog
  - e.g.) `#service rsyslog start`

# Examining logs

- Sometimes need to manually scan log files for notable activity
- Since logs are plain text, you can use standard text-processing tools like to examine them
- Location of log files
  - /var/log
- Which tools can be used?
  - less, grep, tail, vi...

# Examples

```
kbkim@ubuntu: /var/log
File Edit View Terminal Help

kbkim@ubuntu:~$ cd /var/log
kbkim@ubuntu:/var/log$ ls
apparmor      debug.3.gz      kern.log.3
apt           debug.4.gz      kern.log.4
auth.log      dist-upgrade    lastlog
auth.log.1    dmesg           lpr.log
auth.log.2.gz dmesg.0         lpr.log.1
auth.log.3.gz dmesg.1.gz      mail.err
auth.log.4.gz dmesg.2.gz      mail.info
boot          dmesg.3.gz      mail.log
boot.log      dmesg.4.gz      mail.warn
bootstrap.log dpkg.log         messages
btmp          dpkg.log.1      messages.1
btmp.1.gz     dpkg.log.2.gz   messages.2
ConsoleKit    faillog          messages.3
cups          fontconfig.log  messages.4
daemon.log    fsck            news
daemon.log.1 gdm             pm-powersav
daemon.log.2.gz installer       pm-powersav
daemon.log.3.gz jockey.log      pm-powersav
daemon.log.4.gz jockey.log.1    pycentral.1
debug         kern.log         samba
debug.1       kern.log.1      speech-dis
debug.2.gz    kern.log.2.gz   syslog
kbkim@ubuntu:/var/log$
```

```
kbkim@ubuntu: /var/log
File Edit View Terminal Help

May 20 16:23:46 ubuntu rsyslogd: [origin software="rsyslogd" swVersion="4.2.0"
x-pid="720" x-info="http://www.rsyslog.com"] rsyslogd was HUPed, type 'lightwei
ght'.
May 20 16:28:49 ubuntu kernel: Kernel logging (proc) stopped.
May 20 16:28:49 ubuntu kernel: imklog 4.2.0, log source = /proc/kmsg started.
May 20 16:28:49 ubuntu rsyslogd: [origin software="rsyslogd" swVersion="4.2.0"
x-pid="2597" x-info="http://www.rsyslog.com"] (re)start
May 20 16:28:49 ubuntu rsyslogd: rsyslogd's groupid changed to 103
May 20 16:28:49 ubuntu rsyslogd: rsyslogd's userid changed to 101
May 20 16:28:54 ubuntu kernel: Kernel logging (proc) stopped.
May 20 16:28:54 ubuntu rsyslogd: [origin software="rsyslogd" swVersion="4.2.0"
x-pid="2597" x-info="http://www.rsyslog.com"] exiting on signal 15.
May 20 16:28:54 ubuntu kernel: imklog 4.2.0, log source = /proc/kmsg started.
May 20 16:28:54 ubuntu rsyslogd: [origin software="rsyslogd" swVersion="4.2.0"
x-pid="2607" x-info="http://www.rsyslog.com"] (re)start
May 20 16:28:54 ubuntu rsyslogd: rsyslogd's groupid changed to 103
May 20 16:28:54 ubuntu rsyslogd: rsyslogd's userid changed to 101
May 20 16:29:40 ubuntu kernel: Kernel logging (proc) stopped.
May 20 16:29:40 ubuntu rsyslogd: [origin software="rsyslogd" swVersion="4.2.0"
x-pid="2607" x-info="http://www.rsyslog.com"] exiting on signal 15.
May 20 16:29:40 ubuntu kernel: imklog 4.2.0, log source = /proc/kmsg started.
May 20 16:29:40 ubuntu rsyslogd: [origin software="rsyslogd" swVersion="4.2.0"
x-pid="2646" x-info="http://www.rsyslog.com"] (re)start
May 20 16:29:40 ubuntu rsyslogd: rsyslogd's groupid changed to 103
"messages" [readonly] 24L, 2237C                                     1,1      Top
```

# Log rotation

- rsyslog will normally allow log files to grow without bound
  - Until you run out of disk space
- The solution is to use **log rotation**
  - A scheme whereby existing log files are periodically renamed and ultimately deleted
- “logrotate” command to perform rotation
  - Run daily by “**cron**”
- “logrotate” can be configured with “/etc/logrotate.conf”

# Example of logrotate.conf

```
kbkim@ubuntu: /etc
File Edit View Terminal Help
# see "man logrotate" for details
# rotate log files weekly
weekly
# keep 4 weeks worth of backlogs
rotate 4
# create new (empty) log files after rotating old ones
create
# uncomment this if you want your log files compressed
#compress
# packages drop log rotation information into this directory
include /etc/logrotate.d

/var/log/syslog
{
    rotate 7
    daily
    missingok
    notifempty
    delaycompress
    compress
    postrotate
        reload r
    endscript
}

/var/log/mail.info
/var/log/mail.warn
/var/log/mail.err
/var/log/mail.log
/var/log/daemon.log
/var/log/kern.log
/var/log/auth.log
/var/log/user.log
/var/log/lpr.log
/var/log/cron.log
/var/log/debug
/var/log/messages

/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}

/var/log/btmp {
    "logrotate.conf" [readonly] 32 lines --3%--
}

"/etc/logrotate.d/rsyslog" [readonly] 37L, 515C
1,1 Top
```