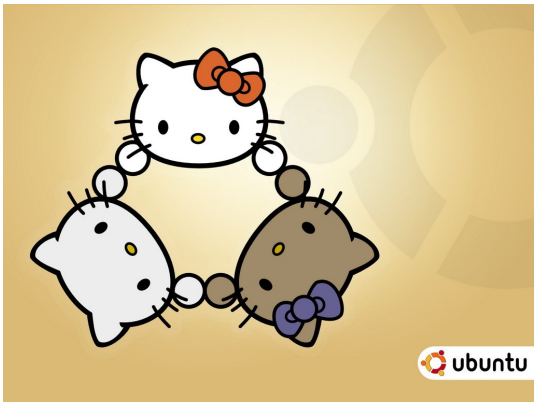
Chapter 10 & 11 System Administration

Thursday, April 2, 2015 11:49 PM

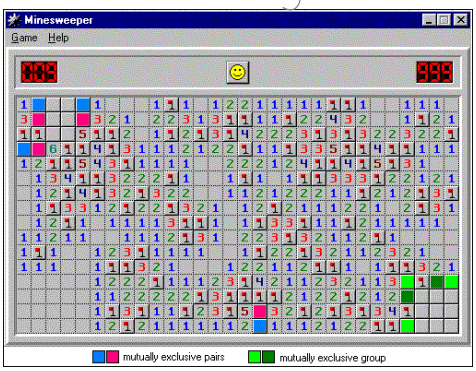


System Administration: Core Concepts

Objectives:

- Explain about privileged user (root)
- Use su and sudo
- Describe about systemd
- Manage which services start on boot
- Start and stop services
- Boot into single user mode for maintainance
- Shutting Down a system
- Secure a system; monitor logs, SELinux, and PAM
- Learn about securing servers

- You are a user but you will be a system administrator too
- Init Systems
  - We are entering a mine field



- the init daemon is the process that "is" the system "and" the service manager

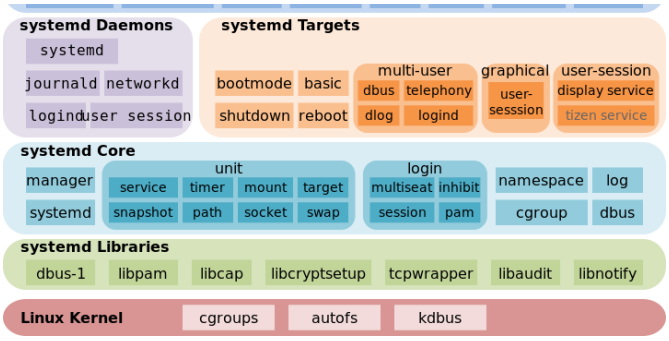
- Once the system has booted and the OS gains control
  - the init daemon starts

- PID 1 ancestor of all processes
- Idea has been around since At&t System V (1983)
- Sometimes abreviated SysVinit
- SysVinit basically reads a bunch of shell scripts to launch networking all of the services and parts of the OS
  - Terminal
  - GUI
  - login
  - etc etc
- Problem, this worked in 1983
  - SysVinit has limitations dealing with modern hardware
    - hotplug
    - USB
    - Network Mounted Filesystems
    - Serial load order - one service at a time (ok on server - not on desk top - why?)

- Some stop gaps / replacements were created
  - upstart → Ubuntu
  - SMF → Sun/Oracle Solaris
  - launchd → Mac OsX
  - systemd → Redhat replaced in Fedora 15

- Until last year most of the non-redhat world used
- SysVinit or upstart
- But! Not so anymore
- Systemd rules the linux world now
- We need to transfer all sysvinit knowledge to systemd
  - → Debian, Redhat, Ubuntu, OpenSuse, RHEL, Centos
  - What is systemd?

systemd Utilities
systemctl journalctl notify analyze cgls cgtop loginctl nspawn



All this is tied to PID 1

- Created by Lennart Poettering

http://www.freedesktop.org/wiki/Software/systemd/

http://0pointer.de/blog/projects/systemd.html ← 21 part story of why

http://en.wikipedia.org/wiki/Systemd

- Basically Poettering (all of 35!) realized for Linux to really advance and unseat Windows and Mac on desktop and to transform into the flexible server core for the clouds, that developers should drop all this UNIX Philosiphy and nestalgia and just make a better product.

- Great idea!
  - But it basically destroys 30+ years of knowledge
  - And

since Lennart ... for RedHat ... pass Linux into RedHat's hands...

- Which is interesting....
  - Can Linux survive outside of a commercial environment?

- Systemd differences
  - Run Levels vs targets
    - SysVinit had run levels
      - a system started at a certain level
        - 3 Command line
        - was
        - 5 was GUI

SysVinit runlevel	systemd runlevel (target unit)	Name/function
0	runlevel0.target, poweroff.target	Shuts down the system
1 or S	runlevel1.target, rescue.target	Brings the system to single-user/ rescue mode
2, 3, 4	runlevel2.target, runlevel3.target, runlevel4.target, multi-user.target	Brings the system to multiuser textual mode
5	runlevel5.target, graphical.target	Brings the system to multiuser graphical mode
6	runlevel6.target, reboot.target	Reboots the system
	emergency.target	Emergency shell

- Systemd introduces "wants" and "availables"
  - systemctl -
    - may be used to introspect and control the state of the systemd system and service manager.

From <http://en.wikipedia.org/wiki/Systemd>

try it -

systemctl show --property "Requires" graphical.target

systemctl show --property "Wants" multi-user.target

What do you see? (hint | fmt 10) see what happens.

One large difference
- Systemd will start services in parallel
- Lets look at a service unit file

cd /lib/systemd/system

ls | less

/ / for httpd (if not there sudo yum install httpd)

look for ... (

do a cat httpd. service

do a do

- what you see?

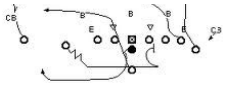
Controlling Services

- systemd has backwards compatible commands with SysVinit, so not all is lost...
- for now....
- sudo service httpd status
- sudo systemctl status httpd.service
- sudo systemctl status network.service
- what do you see?

Configuring Daemons

- In the past you had "service" and "chkconfig"
- Chkconfig told the system to start services at boot
- service told the system to turn on, off, or report status
- (Note Redhat/RHEL services off by default, Ubuntu on)
- sudo systemctl disable httpd.service
(basically takes the link out of the system directory)
sudo systemctl is-enabled httpd.service
- what does it report?
- sudo systemctl stop httpd.service
- Stops the currently running service does opposite
Start from GUI
- Can do this
- system-config-services (may need to install)

ting the system



pe [dmesg] to see all the components loaded

- Rescue Console or single user mode
- This is a root shell that only 1 user can be on
  - There is no password since it is assumed you already have access to the local system to reboot...
  - single user mode can be used to repair a system
  - To replace a forgotten password
- Hold 'space-bar' while booting to get the GRUB menu
- You will see single-user mode.

Admin Tools

- There are various tools to gain various data.
- blkid → reports all block devices on a system
  - → What is a block device "blocks"
    - Sends data multiple kb or mb
  - → What is a character device? character
    - Sends data 1 at a time
  - → What is a serial device?

of course it brings the cereal your mouth...

chsh

- ↳ command lets you permanently modify users default shell

- Clear
  - ↳ this will "clear" the screen of any existing text

- kill

- command is used to send a signal to a process
- this to terminate a
- usually be process
- could to
- could restart
- be used to "re-read" a configuration file.

- ps command is used to find process id (PID)
- so you can kill 3730 for example
- of kill30

There are levels

Level 1 kill -1 called SIGHUP

- Mostly used to make a process re-read a config file
- similar to systemctl ....

Level 2 kill -2 called SIGINT

Hitting Ctrl + C will issue a kill -2 to a running process.

To the process it feels like this

Level 9 kill -9 SIGKILL

Kills a program ungracefully
- like pulling the power plug out of a PC

Use only as a last resort

evel

15 kill -15 SIGTERM

Like a kill 9 but with class...

Gracefully kills a process

- all

te process can by choose to ignore everything but kill -9

ll process name and any associated processes

all will kill

dof

- makes it easier to find a PID (no need to grep)

tat

- gives and

values properties of a file

mask

By default

- when a Unix system creates a file or directory - the permission is the

- But is a filter that is applied in the profile umask to modify what the default permissions should be.

- uname

- Gives information about the system

uname -a

it

GUI controls

Tool	Function
authconfig[-tui]	The authconfig-tui utility displays the pseudographical Authentication Configuration window. The User Information column allows you to configure user accounts to cache information and use LDAP, NIS, IPAv2, or Winbind support. The Authentication column allows you to specify how the system authenticates users, depending on how you configure user accounts. For a purely textual (scriptable) interface use authconfig.
firewall-config	Displays the Firewall Configuration window (page 900).
system-config-bind	Displays the BIND Configuration GUI window (**system-config-bind** package; page 867).

system-config-httpd	Displays the HTTP Server Configuration window (**system-config-httpd** package).
system-config-kickstart	Displays the Kickstart Configurator window, which allows you to create a Kickstart script (**system-config-kickstart** package; page 83).
system-config-nfs	Displays the NFS Server Configuration window (**system-config-nfs** package; page 812).
system-config-printer	Displays the Print Settings window, which allows you to set up printers and edit printer configurations (page 558).
system-config-rootpassword	Displays the Root Password window, which allows you to change the **root** password. Working with **root** privileges, you can also use passwd (page 137) from a command line to change the **root** password (**system-config-rootpassword** package).
system-config-samba	Displays the Samba Server Configuration window, which can help you configure Samba (**system-config-samba** package; page 837).
system-config-selinux	Displays the SELinux Administration window, which controls SELinux (**policycoreutils-gui** package; page 475).
system-config-services	Displays the Service Configuration window, which allows you to specify which daemons (services) run at each runlevel (**system-config-services** package; page 447).
system-config-users	Displays the User Manager window, which allows you to work with users and groups (page 598).
system-switch-mail	Displays the system-switch-mail pseudographical window, which allows you to choose between the **sendmail** (page 739) and Postfix (page 742) MTAs when both packages are installed on the system (**system-switch-mail** package).

Linux

http://twit.tv/show/floss-weekly/156 Podcast with more info

Made by NSA Enhanced Linux Security

Called MAC - Mandatory Access Control

SELinux gives tighter security control over files and process to enforce

- sometimes added on top of things Linux SE is

modes breaks

3 Active/

- -
- Permissible Enforcing / Warning

3 main Policies can be applied

- Targeted - Applies controls to targeted processes
- MLS (Multi level Security protection)

- Minimum Protects Virtual machines as well

https://www.nsa.gov/research/selinux/docs.shtml

http://danwalsh.livejournal.com/

http://stopdisablingselinux.com/

https://www.youtube.com/watch?v=MxjenQ31b70

or Learn how to use SELinux
take ITMS 458

cat /etc/selinux/config

getenforce will tell you status
setenforce

- command allows for changes

~~- system-config-selinux~~

tM

- Pluggable GUI Authentication Module
  - allows authentication methods to be added for this system
  - also allows Linux applications not to have to ~~rebuild "authentication" methods in every application.~~

hapter 10 summary

We use systemctl setup services

- SysVinit was replaced by systemd
- We learned about using kill command for processes
- We learned about system tools and admin GUI tools
- ~~We learned about SELinux and PAM~~

apter

11 Files, Directories, Filesystems

There is an economics pun for anyone who is a Herestory major...

Objectives

- List directories and describe their use
- List four important common system startup files
- Define 7 types of files
- Describe filesystems found in Linux
- View, tune, check ~~mount and unmount filesystems~~ directories

Files

~~important~~ book lists tons of them - I will highlight a couple

/.bash_profile - This

~ Script is run everytime a user logs in
helps customize their environment

~/.bashrc

a non-login shell is launched
Executes everytime

/dev

Contains

files labeled representing "devices" on the system
are

/dev/null /dev/sda sdb sdc and so on
- Drives

- called the bit bucket this
- device "disappears"
- output to
- for instance grep portable * 2> /dev/null
- term
- everywhere
- look any stderr
- will
- This discard
- for the output portable

/dev/random and + /dev/urandom

- systems random number (comes from items like keystrokes and mouse movements)
- urandom is algorithmically generated but potentially not "as random as"

dd - command

dd lets you take a source (if) and write to a destination (of) using say /dev/random or /dev/null above

- dd if=/dev/urandom of=randfile.txt bs=1 count=100
  - 100 bytes of random data
  - it and see!
- Try

/dev/zero
- same as above but instead places numeric zeros

/etc/alternatives
- regardless of OS. find applications
- Java is big winner here, the Java Runtimes and Compile times are stored all over the place
- Your system expected it to hunt for them
  - /etc/alternatives/javac can point it to the executable
  - may be wherever

/etc/default
/etc/group
- holds OS default settings for new accounts
- The existing system groups
- = groupnames of the groups on the

hostname (username) will show what group you are a member of.

/etc/

for hostnamectl

/etc/hosts

a sysconfig/network

/etc/ like small DNS configuration settings

- Network card here

Typically I told you that everything in UNIX is a file

- that's true

half file types

- Actually (text) files
- Ordinary
- Symbolic
- FIFO Files Links special files
- Sockets
- character (named pipes)
- Block and devices Devices
- Raw

systems http://en.wikipedia.org/wiki/Server_Message_Block A way to make a shared filesystem over disperate systems

- cifs
- ext2, ext3, ext4 ← default Linux
- nfs Sun's network filesystem
- vfat microsofts NTFS
- ntfs FAT - created by Microsoft but now a standard every machine can read
- xfs
- ufs → Unron Filesystem, standard accross UNIX/BSD
- → SGI's journaling filesystem. Built to handle large
- btrfs

ZFS is a combined file system and logical volume manager designed by Sun Microsystems. The features of ZFS include protection against data corruption, support for high storage capacities, efficient data compression, integration of the concepts of filesystem and volume management, snapshots and copy-on-write clones, continuous integrity checking and automatic repair, RAID-Z and native NFSv4 ACLs.

from <http://en.wikipedia.org/wiki/ZFS>

Btrfs is intended to address the lack of pooling, snapshots, checksums, and integral multi-device spanning in Linux file systems.[4] Chris Mason, the principal Btrfs author, has stated that its goal was "to let Linux scale for the storage that will be available. Scaling is not just about addressing the storage but also means being able to administer and to manage it with a clean interface that lets people see what's being used and makes it more reliable."[9]

From <http://en.wikipedia.org/wiki/Btrfs>

command

mount is used to add a new filesystem

Why called 'mount' command?

Originally you had to mount a large tape reel

- Mount points
  - create partitions
- You
  - then make filesystems on partitions
  - then mount directories onto filesystems

ytime a system boots techically all drives are "re-mounted"

- /
- /boot
- swap

All of this is located in /etc/fstab

- Let's take a look /etc/fstab
  - You
  - Cat
    - willsee
    - mount or
    - trigger options

- Fsck

Dump (file system check)

↳sck run on mounted

single systems

don't

↳ Run damaged user mode

↳ repairs corrupted files

↳ or (kill -9 anyone?)

an improper shutdown

~~Use only on ext2, 3, & 4~~

↳

Explaining version 7 Centos XFS is default filesystem

7 too)

pport and terabytes designed for large files and filesystems.

- multiple
- Petabytes?
- Exabytes?
- What is next?
-

hint....

system

is the

to

place filesystems on partitions

mkfs.ext command used

---

class Demo

ms hold directories of files. These structures store user data and
ata that are the basis of users' work on the system and the
existence. Linux supports many types of files, including ordinary
ctories, links, and special files. Special files provide access to
system features.

el uses major and minor device numbers to identify classes of
nd specific devices within each class. Character and block devices
t I/O devices such as hard disks and printers. Inodes, which are
by inode numbers, are stored on disk and define a file's existence.

e system comes up, the **/etc/fstab** file controls which filesystems
nted and how they are mounted (readonly, read-write, and so on).
ystem crash, filesystems are automatically verified and repaired if
y by fsck.

ny.safaribooksonline.com/9780133477443/ch11lev1sec5?percentage=0&reader=html>