CSC252 – UNIX

SYSTEM ADMINISTRATION TASKS

Lisa Frye, Instructor

Kutztown University

frye@kutztown.edu

ACCOUNT FILES

- /etc/passwd

- /etc/shadow

- NIS

- NIS+

- LDAP

USERADD

- useradd [-u uid [-o]] [-g group]

  [-G group [, group, …]] [-d home]   [-s shell]   [-c comment]
  [-m [-k template]] [-f inactive]   [-e expire] [-p
  passwd] [-r]   login

- Default settings
  - useradd -D [-g group] [-b base]   [-f inactive]   [-e expire]

USERMOD AND USERDEL

- usermod [-u uid [-o]] [-g group]   [-G group [, group, …]] [-d home [-m]] [-s shell] [-c comment]   [-l new_logname] [-f inactive] [-e expire] [-p passwd] [-r] login

- userdel [-r]   login

SYSTEM ACCOUNTS

- root

- daemon

- bin

- sys

- adm

- lp

- nobody

GROUPS

- Primary group

- Secondary groups
  - /etc/group

SYSTEM GROUPS

- root
- daemon
- sys
- tty
- bin
- adm
- lp
- mail
- uucp / nuucp
- nobody
- noaccess

BACKUP STRATEGY

- backup from one machine
- label all tapes
- grandfather / father / son
- secure backup tapes
- keep tapes off-site
- backup appropriately
- always check restore procedure periodically
- develop a tape life cycle

BACKUP SCHEDULE DEPENDS ON

- activity on filesystem

- capacity of dump device

- length of "dump window"

- amount of redundancy

- number of tapes available

- how far back you must be able to recover

DUMP COMMANDS

- cpio
  - packs data on tape more efficiently than tar
  - skips bad spots on restore (tar dies)
  - can span tapes

- dump / ufsdump
  - full vs incremental (0-9)
  - info saved in /etc/dumpdate
  - ufsdump N [u] [s length] [d density]   [f dump_file] files_to_dump

RESTORE

- mt [-f tape_device] command
- Command
  - rew
  - offl
  - status
  - fsf [count]

- restore [i] [x file_to_restore] [f tape_device]

DEVICES

- /dev/[r]dsk/cWtXdYsZ
  - W – controller
  - X – SCSI target ID
  - Y – SCSI LUN (almost always 0)
  - Z – partition / slice

TO ADD A NEW DISK DRIVE

- Physically add drive

- Create entries in /devices and/or /dev

- format

- newfs

- Add entry to /etc/fstab (optional)

DISK SUPERBLOCK

- length of a disk block

- size and location of inode tables

- disk block map and usage information

- size of the cylinder groups

- other important parameters of the filesystem

MOUNTING FILESYSTEMS

- mount [-r] [device] <filesystem>

- mount [-f filesystem_types]

- mountall

Dr. Frye

15

UNMOUNT FILESYSTEMS

- umount <filesystem>

- umountall

Dr. Frye

FILESYSTEM COMMANDS

- Who is using a filesystem?
  - fuser [-u] [-k] <device>

- Checking a filesystem
  - fsck [-p] [-n] [-y] [-F filesystem_type] [raw_device]

FSCK TASKS

- fixes damaged or inconsistent inodes

- unreferenced inodes

- large link counts

- unused data blocks not recorded in block maps

- data blocks listed as free but also used in a file

- incorrect summary info in superblock

QUOTAS

- rq in /etc/vfstab

- quotas file in filesystem

- edquota [-p prototype_user] <user>

- quota

NFS

- runs on top of RPC protocol

- Daemon or service

- /etc/exports

BOOT PROCESS

- Loading and initialization of kernel

- Device detection and configuration

- Creation of system processes

- Operator intervention (manual boot only)

- Execution of startup scripts (by init)

- Multiuser operation (init spawns getty process)

INIT STATES

- Also known as run levels

- 0   system is completely shut down

- 1   single-user mode

- 2   multi-user mode without NFS

- 3   full multi-user mode

- 4   unused

- 5   X11

- 6   reboot

STARTUP SCRIPT TASKS

- setting the name of the computer

- setting the time zone

- checking the disks with fsck

- mounting the system's disks

- removing old files in /tmp

- configuring network interfaces

- starting up daemons and network services

SHUTDOWN STEPS

- logs shutdown

- kills nonessential processes

- executes sync

- waits for filesystem writes to complete

- halts the kernel

SHUTDOWN COMMANDS

- boot [path_to_kernel] [-s] [-r]

- shutdown [-g seconds] [-i state] [-y]

- halt [-n] [-q]

- reboot [-n] [-q]

- init <run_level>

SYNC

- flushes cached superblocks to disk

- flushes modified inodes and cached data blocks

LOGGING POLICIES

- throw away all data immediately

- reset log files at periodic intervals

- rotate log files, keeping data for a fixed time

- compress and archive logs to tape or other media

COMMON LOGS ON LINUX

- /var/log/messages

- /var/log/auth.log

- /var/log/kern.log

- /var/log/cron.log

- /var/log/maillog

- /var/log/httpd

- /var/log/boot.log

- /var/log/mysqld.log

- /var/log/utmp or /var/log/wtmp

- /var/log/yum.log

SYSLOGD

- programs write to the special file /dev/log

- syslogd reads messages from this file

- consults configuration file syslog.conf

- dispatches each message to appropriate destination

SYSLOG.CONF

- \<selector>   \<TAB> \<action>

- \<selector> is:

      \<facility>.\<level>

FACILITY NAMES

- kern   The kernel

- user   User processes (default)

- mail   sendmail and other mail-related software

- daemon   System daemons

- auth   Security and authorization related commands

- lpr   The BSD line printer spooling system

- uucp   Reserved for UUCP (doesn't use it)

FACILITY NAMES (CONT.)

- cron   The cron daemon

- mark   Timestamps generated at regular intervals

- local0-7   Local messages

- syslog   syslogd internal messages

- authpriv   Private authorization messages

- ftp   The ftp daemon, ftpd

- news   news service

- *   All facilities except mark

PRIORITY LEVELS

- emerg   Panic situations (can also use panic)

- alert   Urgent situations

- crit   Critical conditions

- err   Other error conditions (can also use error)

- warn   Warning messages (can also use warning)

- notice   Things that might merit investigation

- info   Information messages

- debug   For debugging only

- none   no priority

- *   all priorities

SYSLOG ACTIONS

- filename   Writes the message to a file on the local machine

- @hostname   Forwards the message to the syslogd on hostname

- @ipaddress   Forwards message to host at IP address ipaddress

- user1,user2,…   Writes the message to users' screens if logged in

- *   Writes the message to all users logged in

DAEMON

- A background process that performs a specific function or system-related task

INETD

- a daemon that manages other daemons

- Consults config file to determine which network ports to listen to

- Uses /etc/services or portmap daemon to map service names to port numbers

INETD.CONF

- 1 service name
- 2 type of socket service uses (stream or dgram)
- 3 communication protocol service uses (tcp or udp)
- 4 wait: service can process multiple requests at one time

 nowait - fork a new copy of daemon for each request

- 5 username under which daemon should run
- 6 fully qualified pathname of the daemon and its command-line arguments

PORTMAP / RPCBIND

- a daemon that manages port assignments for daemons that use RPC

VMSTAT

- Two arguments
  - number of seconds between measuring and reporting values
  - number of times to measure and report values

- Report
  - First line will be average values since last system reboot
  - Other lines represents current values

- man vmstat

NETSTAT

- Network connection information

- Common options
  - netstat –v
  - netstat –nt
  - netstat –nl
  - netstat –I
  - netstat –rn
  - netstat -s

PATCHES

- Updates to system files

- Correct errors or provide security fix

- patch

SOFTWARE

- CD

- Download source code

- Download package

MAINTAIN SOFTWARE PACKAGES

- yum

- apt-get

YUM

yum install <packageName>	Install package and dependency packages
yum update [<packageName>]	Without package name, updates all installed packages
yum check-update	Lists available updates for installed packages
yum clean all	Removes all header files used for resolving dependencies and cached packages
yum list available	Lists all available packages
yum search <word>	Searches for word in package description, summary, packager, and name

- Groups of packages
  - yum grouplist
  - yum groupinfo

- Yumdownloader

- Configuration file: yum.conf

APT-GET

apt-get update	Update local package list
apt-get check	Check status of local dependency tree
apt-get install <package>	
apt-get remove <package>	
apt-get upgrade	Upgrade all packages on the system that don't require any new packages
apt-get dist-upgrade	Upgrade all packages on the system and install any new packages necessary