

Intro to UNIX Systems Administration

Bill Anderson

Topics

- The UNIX Shell
- User Account Administration
- Special Files
- Networked machines
- Backups
- Package Systems

UNIX Principles

- Everything is a file
- Small, specialized tools which can be combined to perform more complex tasks
- Multitasking/Multithreading
- Memory protection

Devices and Special Files

- /dev
 - Major and minor numbers link file name to kernel driver
- mknod
- Character special
 - Console, ttys, most I/O devices
- Block special
 - Disk drives
- FIFO
 - Named pipe

Superuser (root)

- The "root" user (uid 0) has unrestricted access to the entire system (memory, disk, etc)
- Su (become the superuser (or another user))
- Sudo (su-do – do as superuser)
 - Allows administrator to set up limited access to the superuser account by controlling which programs particular users can execute as the superuser
- SUID (Set User ID) executables
 - Allows the program (at its option) to become the superuser, and to return to normal

NFS/NIS

- NIS (Network Information System)
 - Network–based user and group authentication
- NFS (Network File System)
 - Allows file system to be shared among multiple machines
 - Unencrypted, very weak authentication
 - For use only inside a secure (firewalled) subnet

LILO & grub

- Allows booting of multiple operating systems and multiple kernel versions
 - LILO
 - Controls devices during bootup and passes arguments to kernel (such as "root=" or "single")
 - grub
 - Can understand filesystems
 - Interactive command line

Network Services

- Listing active connections

```
netstat -n
```

- Listing open ports

```
netstat -ntl
```

- Identifying processes listening on a port

```
fuser portname/protocol (i.e. fuser smtp/tcp)
```

```
lsof -i | grep "smtp"
```

Network Troubleshooting

- `ifconfig eth0`
 - Is the card recognized? Do i have an IP address?
 - (if not: is driver module loaded (`lsmod`)? is IP set?)
- `ping -n 192.168.1.2`
 - ping my own ip to rule out various driver and networking problems? use `-n` to avoid DNS lookups, since they will fail if any other piece of the puzzle is broken (if not: check modules, kernel, etc.)
 -

Network Troubleshooting Cont'd

- `ping -n 192.168.1.1`
 - Is my link to the local subnet working? (if not: do i have the right IP, subnet, etc? is the CAT5 bad?)
- `tracert -n 128.146.1.7`
 - Can i get to a known host? (if not: note where tracert stops -- if it goes beyond my gateway/router then there may be a problem at my isp, or a backbone... otherwise start looking at routing table (default route)... `netstat -nr`)
- `tracert www.cis.ohio-state.edu`
 - try it with name to see if DNS is working (if not: check `resolv.conf`; `tracert` to my DNS server)

Init

- `/etc/inittab`
- **Runlevels**
 - 1 – Single user
 - 2 – Multi-user
 - 3 – Networked
 - 5 – X-based logins
- **SysV style**
 - `/etc/rc.d/rc[12345].d/`
 - `/etc/init.d/` – Symlinks from here
- **BSD style**
 - `/etc/rc[12345]`

I/O Redirection and Piping

- Redirecting standard input

```
myprogram < myinputfile
```

- Redirecting standard output

```
ls -l > myoutputfile
```

- Pipes

```
ls -l | less
```

```
ls -a1 | wc -l
```

Partitioning

- Why not just put everything in one partition?
 - Limit impact of device becoming corrupted
 - Limit impact of device becoming full
 - Use different filesystems for different purposes
 - Easier to expand
 -
 -

Disk utilities

- Mounting and unmounting filesystems

```
mount -t ext3 /dev/hdXN /mountpoint
```

```
umount /mountpoint
```

- Disk Usage

```
du -k .
```

```
du -ks * | sort -n
```

```
df -k
```

Partitions

- / (also known as the "root" partition)
 - Enough to boot and do basic maintenance
- /usr
 - End-user software provided by distribution
- /usr/local (or /opt, /opt/local)
 - Locally compiled software (/opt also for 3rd party software)
- /var
 - Data that may increase in size (particularly /var/spool)

Partitions Continued

- /home (or /usr/home, etc)
 - User home directories
- /boot (optional)
 - Sometimes necessary for bootloader (lilo) and kernel to be located on first disk (/dev/hda), possibly within first 1024 cylinders

Package Systems

- .rpm

```
rpm -i packagename.rpm
```

```
rpm -ql packagename
```

```
rpm -qf filename
```

- .deb

```
dpkg -i packagename.deb
```

```
dpkg -L packagename
```

```
dpkg -S filename
```

```
apt-get install packagename
```

```
apt-get update; apt-get upgrade
```

```
apt-get dist-upgrade
```

More packaging

- .tar.gz

GNU Tar:

```
tar -zxvf packagename.tar.gz
```

```
tar -ztf packagename.tar.gz
```

```
tar -zcf packagename.tar.gz [files]
```

non-GNU tar:

```
gzip -cd packagename.tar.gz |tar -xvf -
```

```
gzip -cd packagename.tar.gz |tar -tf -
```

```
tar -cf - [files] |gzip - >pack.tar.gz
```

Other packages

- Solaris .pkg

```
pkgadd -d package.pkg
```

```
pkgrm packagename
```

User accounts

- Adding an account

```
useradd -c "Full Name" -d  
/home/username -m -s "/bin/bash"  
username
```

- Setting a user's password

```
passwd username
```

- Adding a user to a group

```
vi /etc/group
```

Process Control

- `ps`

 - `ps auwwx` (Linux)

 - `ps -ef` (Solaris/BSD)

- `top`

- `kill`

 - `kill -9 [pid]`

 - `kill -9 -1`

- `killall`

 - `killall -9 programname`

/proc

- Filesystem interface to the kernel
 - /proc/cpuinfo
 - /proc/interrupt
 - /proc/pci
 - /proc/sys
 - /proc/sys/net/ipv4

Backups

- Tape
 - dump
- Tar files
- CD-R
 - mkisofs
 - cdrecord
- Amanda