Introduction to System Administration IAP '95 - Jan 23-25, 1-3pm - NE43-518

Who are we and why are we here?

- Who are we?
  - William Ang - Angstrom Information Systems - ang@ang.com
  - Scott Blomquist - System Administrator - Lab for Computer Science, MIT - sb@theory.lcs.mit.edu
- Why are we here?
  - Educate & Inform people about System Administration
  - Dispel the myths about System Administration
  - Promote Administration as an integral part of deploying Unix machines

What is a System Administrator?

- System Administrator is a person who is responsible for the smooth operation of a set of computer equipment.
- Sometimes also referred to as the System Manager, the Wizard, the God, the Tyrant, the Clueless Guy, the Geek, etc....
- Accomplish the task by
  - designing/implementing policies
  - allocating resources
  - planning and scheduling
  - coercing/threatening users
- Not much different than running a business or running a country, Greenland?.

Who got you in this mess?

- I volunteered!
- I happened to be the only one who has a clue (or computer literate)
- Nobody is doing it.
- Can't afford one.

Who am I?

- I can geek! I can tell you.... what the 3 bit from the left of a tcp upd packet is.
- I can speak! I can get through a sentence without mentioning the words bits, net, or online.
- I can read! Especially, Unix Manpages....
- I can sleuth! Call me the Sherlock Holmes of OS's.
- I can network! If my geekiness fails, I know someone geekier to ask!

What do I think about day to day?

- What should I buy? What is the latest & greatest? I have to know!!!!!
- Will this widget work with that? Compatibility?
- What software can I install? Is is usable? Is it maintained? Is it free?
- What software can I write? How can I automate routine tasks?
- Is my data/System safe? Backups? How safe? From hardware failures? From the wiley hacker?

What do I think about day to day? Cont.

- How can I get the most performance out of my hardware/software. Resource Allocation?
- What are my policies? Written or assumed? Do people know them? Do I know them? Are users being bad? Maybe they don't know it!
- What if something goes wrong? Do I have a plan. Can I recover? What will be the downtime?

Golden Rules

- You always have more work than you can deal with.
- Leverage by Planning, Scheduling, and Organizing
- Let the computer do the work for you.
- Be the Manager, not the Slave.
- logs, logs, logs...
- detail, detail, detail...

Next Up... ...What you need to know!

- Mac or PC or Unix or VMS or ...
- Other things to worry about once you are on the net. (ftp, news, mail, web, etc)

Unix

- Mac and PC - almost impossible to keep the System files lock, might as way forget about managing them.
- Unix as an example for System Administration.
- Please let us know if you want to know about Mac's and PC's

Unix Admin in a Nutshell

- Hostname, IP, Netmask, default router
- Services, Daemon - /etc/services, /etc/inetd.conf, rc files

- **Cron jobs, trimming logs, cleanup tmp files**
- **User relationship, accounts, day-to-day problem resolution**
- **Managing disk space**
- **Disk, partition, printers, modems**
- **Name services (NIS or DNS or Both)**
- **Upgrades, software installations**
- **Hardware Maintenance**

Files and Directories important to Unix Admin - "The root of all evil?"

- **Important directories that you need to keep in top shape**
  - **and write-protect them when you are done with it...**
- **/ root**
  - boot, vmunix, all the root dot-files (.cshrc, .profile, .rhosts, etc)
- **/usr/lib**
- **/usr/spool**
- **/tmp**

Files and Directories important to Unix Admin Cont. - "The root of all evil?"

- **/etc**
  - **hosts**
  - **passwd**
  - **groups**
  - **inetd.conf**
  - **rc.* files**
  - **sendmail.cf (some versions of UNIX has it in /usr/lib)**
  - **printcap**

UNIX (Boot Sequence) - "Boot? Now the shoe is on the other foot!"

- **read boot block**
- **loads /boot**
- **loads /vmunix**
- **start init 0**
- **reads in rc, rc.boot, rc.single, stay single user**
- **fsck (check disks)**
- **multi-user -> rc.local**
- **login prompt**

daemons? “What are those things that are running in the background??!!?”

- init - runs scripts to startup machine (/etc/rc.* or /etc/rc.?/*) and manages ttys (System boot)
- swapper - swaps memory in and out of swap space (boot)
- scheduler/sched - schedules jobs for running (bood)
- update - executes a sync every 30secs in case of crash (boot)
- portmapper - maps TCP ports to RPC program numbers (boot)

daemons? “What are those things that are running in the background??!!?”

- syslogd - manages System messages by forwarding them to files, users or machines (boot)
- rpc.lockd/rpc.statd - handle local and remote file lock requests (boot)
- NIS
  - ypserv - serves NIS information from an NIS server (boot)
  - ypbind - binds client to NIS server (boot)
  - rpc.ypupdated - updates NIS maps on servers (boot)
  - rpc.yppasswdd - handles incomming password change requests (boot)

daemons? “What are those things that are running in the background??!!?”

- NFS
  - nfsd - handles incoming NFS request (boot)
  - biod - handles outgoing NFS requests (boot)
  - rpc.mountd - handles incomming mount requests (boot)
- inetd - listens for Internet connections and starts appropriate server (boot)
- in.routed - manages local network routing table (boot)
- in.named - handles requests for Domain Name Services (DNS) (boot)

daemons? “What are those things that are running in the background??!!?”

- timed - handles synchronizing System clocks (boot)
- cron - runs programs at specified times and dates (boot)
- sendmail - handles sending electronic mail over the internet (boot)
- acct - handle the resource usage accounting system (boot)
- lpd - line printer spooling daemon

daemons? "What are those things that are running in the background??!!?"

- **in.rlogind - handles incomming login/rlogin requests (inetd)**
- **in.telnetd - handles incomming telnet requests (inetd)**
- **getty - manages ttys including calling login (inetd)**
- **in.ftpd - handles incomming ftp requests (inetd)**

daemons? "What are those things that are running in the background??!!?"

- **in.fingerd - handles incomming finger requests (inetd)**
- **Misc. System Specific daemons**
  - **rwhod - network version of who and uptime (boot)**
  - **httpd - handle http requests (boot)**
  - **xdm - manages remote x-terminals using XDMCP**

INETD - "How does the machine answer the finger?" (Need Example)

- **portmapper (Superdaemon)**
- **instead of startup every daemon you ever need, listens for calls, startup deamons such as talkd, telnetd, etc when there is a request.**

CRON - "Who is that guy, Cron, working the late shift?"

- **cron - runs programs at specified times and dates**
- **Binaries/Files**
  - **crontab - allows users to edit the entries in the cron table**
    - syntax: crontab -l - list my crontab file
    - syntax: crontab -e - edit my crontab file using my $EDITOR
    - syntax: crontab <newfile> - replace current cron file with <newfile>
  - **/var/spool/cron/crontabs/<username> - cron file which tells cron what & when to run, submitted by <username>**
    - format - mins hrs day-of-month month weekday <command>

CRON - "Who is that guy, Cron, working the late shift?"

- examples -
  - **15 * * * * /usr/local/etc/myscript.sh 2>&1 > /var/adm/logfile - runs every 15 mins passed the hour**
  - **0 12 * * * /usr/local/etc/security.sh 2>&1 | mail root - runs daily at 12pm**
  - **0 4 * * 0,1,2,3,4,5 /usr/local/etc/daily-backup.sh - runs Sunday-Friday at 4am**
  - **0 17 1 1 * /usr/local/etc/once-only.sh - runs January 1 at 5pm**
- **Tips & Techniques**
  - **Know the time formating well and be sure you are correct about your entry**

- **cron runs <command> within Bourne shell, so syntax for <command> is according to Bourne conventions**
- **Be CAREFUL about spaces and tabs in crontab files**

SYSLOG - "Big brother is watching!"

- **Manages System messages by forwarding them to files, users or machines**
- **Binaries/Files**
  - **syslogd - the daemon**
  - **/etc/syslog.conf**
    - Format
      - **<facility>.<level> <destination>**
        - <facility> - *, kern, mail, lpr, daemon, auth, etc.
        - <level> – emerg, alert, crit, err, warn, notice, info
        - <destination> – device, file, user, remote machine
      - **Examples...**
        - *.err;auth.notice dev/console – sends authorization and all errors to console
        - *.err;daemon,auth.notice /usr/adm/messages – sends all errors, daemon & auth notices to file
        - auth.notice root – sends authorization notices to root

Shells and Scripting Languages - "Sally bash-ed Perl C-shells by the seashore..."

- **Interactive**
  - hostname>
  - hostname>mail mymom@home
  - hostname> logout
- **Batch**
  - hostname> remove.all.my.junk
  - #! /bin/sh
  - rm -rf *
- **Popular shells**
  - sh, csh, ksh, tcsh, bash....
  - Perl

Goodies I can add to or come with my System....

- **Windowing System? Curses, X (public.x.org), NextStep....**
- **Document Editting? vi, ed, Emacs (prep.ai.mit.edu)**
- **Document Formatting? Xroff, TeX/LaTeX (labrea.stanford.edu), PostScript, rtf...**
- **Document Displaying? xdvi(public.x.org), ghostscript/ghostview (prep.ai.mit.edu)**

Goodies I can add to or come with my System....

- **Mail Delivery? sendmail, IDA sendmail (ftp.uu.net), Pop (ftp.uu.net)**

- **Mail Reading? binmail, RMAIL, MH/xmh/exmh, mime (ftp.uu.net), elm**
- **Programming? cc/dbx, gcc/gdb (prep.ai.mit.edu), TCL/Tk (harbor.ecn.purdue.edu), Perl (prep.ai.mit.edu)**

Goodies I can add to or come with my System....

- **Security? COPS, crack, TIGER, Tripwire (cert.org)**
- **Utilities? Don't like the one's you got with your Unix then check out GNU!**
- **Web Browsers/utilities? Mosaic/NetScape/Lynx, xv, mpeg_play, audio_play, ghostview, httpd (ftp.ncsa.uiuc.edu)**
- **Misc Fun Stuff? archie/xarchie, webster/xwebster, ical, ftp, irc**

Workstation-based Tasks & Strategies

User account administration - “Yes! you do need users!”

- **Know your users**
- **User name**
- **UID**
- **Groups to add**
- **Home directory**
- **local or System-wide**
- **Disk Hog? CPU Hog?**

Adding new users - “So you want an account on MY machine? Well...”

- **Login as superuser.**
- **run adduser (or other vendor-supplied add user program) if you have one.**
- **/etc/passwd and /etc/group.**
- **put in username, uid, gid, password, home, shell, etc in /etc/passwd.**
- **edit /etc/group if necessary.**
- **ypmake (if you are running yp)**

Adding new users - “So you want an account on MY machine? Well...”

- **Example entry**
  - **geek:sksa7dJ8djk:1234:2000:Ima Geek:/home/geek:/bin/bash**
- **Tips & Techniques**
  - **make sure the uid is unique and make sure it is not ZERO.**
  - **Change the password for user or ask them to change ASAP.**

- where should I put the home directory (disk allocation policy)
- security, disk space issue, logical, etc.
- periodical check for null password, world-writable home directory, + in .rhosts

Adding New Group

- file sharing among local users
- /etc/group
  - mynewgroup:*:user1, user2, user3
- groups username - find out which group(s) you belong to.
- run ypmake if you are running NIS (YP)

Adding New Groups

- Tips and Techniques
  - you can belong to only limited number of groups.
  - Max of 8 (BSD 4.3), 16 (SunOS 4.1.3), check your OS manual for your systems.
  - group affiliation determined at shell creation time. May need to logout and log back in again.

Disk Management - "The spinning junkyard of users!"

- Physical
  - Drive mechanism (IDE, SMD, SCSI, IPI)
  - Physical location - internal, external, which interface to connect to, disk size, etc
  - Partition info - no of head, cylinder, byte per sector, size of partitions
- Logical partition - / on /dev/sd0a
- Other advance Disk management program
  - Disk suite, Backup copilot (Sun)
  - Storage Works (DEC)

Disk Management - "The spinning junkyard of users!"

- Disk mirroring, RAID disk array
  - performance vs Data integrity
- Tips and Techniques
  - Max of 8 SCSI devices (if you are not using LUN). CPU is always counted as 1 (usually at SCSI ID # 7)
  - SCSI # = Device #? NOT always the same!!!
  - Your OS may not recognize or know how to deal with high capacity disks (> 2G)

Preparing Disk

- Format
- Every workstation is different, check your manual
- Connectors, Cables, Terminators

Preparing Disk

- **Partitioning**
  - **dividing the disk into one or more logical devices**
  - **UNIX convention**
  - **a - 1st partition, b - swap, c - complete disk**
  - **some OS store partition informaton on cylinder 0 block 0 (which is also the 1st partition)**
  - **Make sure you don't swap on the 1st partition!!!**

Preparing Disk

- **Example -**
  - **1G drive - 2000 block of 512 byte @ SCSI Drive #3 (drive 0) on a SUN workstation)**
  - **2 G Drive - 4000 block of 512 Byte @ SCSI Drive #2 (drive 2)**
    - sd0a 0 to 199 (100M)
    - sd0b 200 to 599 (200 M)
    - sd0g 600 to 1999 (700M)
    - sd2c 0 to 3999 (2000M)

Preparing Disk

- **newfs /dev/rsd2c (wrapper to mkfs)**
  - **put unix file structure on partition**
- **... superblocks,.....**
- **make sure you copy down the superblocks, you may need it in the future!!!**
- **mount /dev/sd2c /home or mount /home if /home is defined in /etc/fstab**
- **umount /home**
- **tunefs, du - to be discuss later.**

Setting up Printers - "Enough of this Electronic Stuff, I need a hardcopy!"

- **Binaries/Files/Devices**
  - **lpd - line printer daemon**
  - **lpc - line printer configuration utility**
  - **lpr/lpq/lprm - send to/check-on/remove from line printer queue**
  - **/etc/printcap - configuration file for printers**
  - **/etc/hosts.lpd - hosts allowed to print to locally spooled printers**
  - **/var/spool/<printername> - spool directory for <printername>**
  - **/dev/<something> - serial device for printer**

Backup Strategies - "Help! I just deleted my thesis! Can I get it back?"

- **Types of Backup**
  - **Offline - Need Sys Admin to "restore" backed up files**

- **Near Offline - May need Sys Admin but probably not, kinda like a floppy**
- **Online - Backup is online ready to be retreived by user**

- **Issues**
  - **How much data do you have?**
  - **How often does it change?**
  - **How critical is the data?**
  - **What is the lifetime of the data?**
  - **Does it need to be archived? Forever? How often?**

Backup Strategies - "Help! I just deleted my thesis! Can I get it back?"

- **Hardware/Media....**
  - **1/2in. tape - What are you kidding?**
  - **1/4in. tape - More reasonable - low capacity**
  - **8mm tape - 2Gig and 5Gig compressed format**
  - **4mm tape - 2-16Gig compressed format**
  - **Optical Disks/Removable Hard Disks - great for near offline storage**
- **Tips/Techniques/Things to think about**
  - **Already Compressed data does not compress again when going to tape!!!!!**
  - **Lifetime of media?**
  - **Availability of hardware in the future?**
  - **Standard format?**
  - **Storage of the media?**

Backup Strategies - "Help! I just deleted my thesis! Can I get it back?"

- **Utilities for backup...**
  - **tar -or- cpio - Ok, but Lots-o-script writing**
  - **dump/restore - Best for archive**
    - dump - backs up files or filesystems
      - **options**
        - # - dump levels
        - b - blocking factor (default 64)
        - d - density (default 6250)
        - f - device
        - s - size
        - u - update dump record
    - restore
      - **options**
        - i - interactive - allows unix like picking of file
        - r - restore entire tape
        - f - device

Backup Strategies - "Help! I just deleted my thesis! Can I get it back?"

- **Backup Strategy - A Daily/Weekly/Monthly Strategy using dump that works...**

- **Once a month scehedule a full backup (level 0) of fileSystem. Make the time convenient and logical for users to remember.**
- **Once a week at a time when the System is least used, backup all the files that have been modified since the last full backup. (level 3)**
- **Every day, not including th weekly backup day, at a time when the System is least used backup all the files which have been modified since the last weekly backup**

Backup Strategies - "Help! I just deleted my thesis! Can I get it back?"

Backup Strategies - "Help! I just deleted my thesis! Can I get it back?"

Backup Strategies - "Help! I just deleted my thesis! Can I get it back?"

- **Tips & Techniques**
  - **Make sure you have a tape in the drive!**
  - **Always try to backup / on the fileserver daily!**
  - **Clean tape drive frequently**
  - **1 Tape drive for every 5 Gig of disk. Or if you buy more disk, also buy more tape drives to back it up (Wasting your time changing tapes is very expensive!)**

Setting up Printers - "Enough of this Electronic Stuff, I need a hardcopy!"

- **The PRINTCAP file...**
  - **format : <printer-name>:<capability>=<value>:<capability>=<value>:<more capability/valure pairs>**
    - Printer-based <capabilities> - configuring the software end
      - **br - baud rate**
      - **fc - if device is a tty clear flag bits**
      - **fs - same as fs only set bits**
      - **lp - line printer device**
      - **lf - file where errors are logged**
      - **mx - maximum file size**
      - **rm - remote machine name**
      - **rp - remote printer name**
      - **rw - open printer device read/write instead of read-only**
      - **sd - spooling directory**

Setting up Printers - "Enough of this Electronic Stuff, I need a hardcopy!"

- **sf - suppress form feeds**
- **sb - short banner**
- **tc - use previous printer definition for values**
- **xc - if device is tty then clear local mode**
- **xs - same as xc only set bits**

    - Filter <capabilities> - what filter to use
      - **if - plain text jobs**

- tf - troff formated jobs
- df - TeX jobs
- vf - raster jobs
- of - output banner filter
- gf - graph data filter
- nf - ditroff data filter
- rf - fortran style filter
- vf - raster image filter
- cf - cifplat data filter

Setting up Printers - “Enough of this Electronic Stuff, I need a hardcopy!”

Setting up Printers - “Enough of this Electronic Stuff, I need a hardcopy!”

Setting up Printers - “Enough of this Electronic Stuff, I need a hardcopy!”

- Tips & Techniques
  - Plug printer in! Both power and serial port
  - Make sure printcap file has correct device (ttya,ttyb?)
  - Check and make sure init has not started a getty on your serial port
  - Manage printer queues using lpc

System Monitoring - “Why is this machine sooooo sloooow?”

- standard unix tools
- things to watch for - CPU, System, user, Disk IO, network traffic
- vmstat, iostat, netstat
- smtp-based tools
- run program at background
- gather information at a fixed interval
- save data set on disk or tape for future analysis

System Monitoring - “Why is this machine sooooo sloooow?”

- Daily monitoring
  - Disk space monitoring
    - df
    - du -s *
    - run script at night to compare disk space for each user, notify if any one add more than 2M of files...
  - check for security holes, such as setuid files or null passwords
  - generate a report and keep it somewhere

House Cleaning

- **We don't have infinite amount of disk space!!!**
- **Places to watch out for**
  - **/tmp**
  - **/usr/spool**
  - **/usr/log**
  - **User home directories**
- **daily, weekly, and monthly**
  - **rotation of log files**
- **USER HOME DIRECTORIES**
  - **remove junk files from temporary directory (for files that are older than certain date)**

House Cleaning

- **How to force your roommate to cleanup their room?**
- **send threatening e-mail?**
- **post TOP-TEN Users? Shame-on-you type of tactic**
- **confront users face-to-face?**
- **Best is to have a clear policy on disk usage.**
- **provide users tools to help themselves.**
  - program to look for junk files
  - Don't make it too easy to remove file without confirmation.
- **Make sure users understand it too. What is the consequence? lost files?**
- **strictly enforce it.**

Performance Tuning - "Hot-Rodding your system!"

- **Need System monitoring data first**
- **pstat for swap tables statistics**
- **How is my system doing? where is the bottleneck**

Performance Tuning - "Hot-Rodding your system!"

- **things to tune**
  - **run only daemons (or services) that you need**
  - **Memory**
  - **Disk Caching**
  - **tunefs - disk space vs access time (squeeze out the last 10%)**
  - **Scheduling**
  - **re-arranging IO devices**
  - **Upgrade CPUs**
  - **removing user's accounts**
  - **/nologin as shell for CPU hogs**

Network-based Tasks & Strategies

Network-friendly! "What me worry? I'm connected!"

- **PLUG IN**
- **Where is my network drop?**
- **What connector my workstation has?**
- **Do I have a cable, transceiver, etc?**
- **Most important question -**
- **AM I THE NETWORK MANAGER TOO?**

Network-friendly! "What me worry? I'm connected!"

- **Ethernet (10mb/s)**
  - **10base5 (Thick), 10Base2 (Thin), 10BaseT (Twisted Pair)**
  - **Repeater vs Bridge**
  - **Hub vs Router**
  - **What is my IP number**
    - 18.XX.XX.XX
  - **What is my netmask (subnet)**
    - 0xFFFF0000 (Class B subnet) or 0xFFFFFF00 (Class C subnet)
  - **Broadcast**
    - 18.XX.255.255 or 18.XX.0.0
    - Same Broadcast convention!!!

Network-friendly! "What me worry? I'm connected!"

- **/etc/hosts**
  - **# IP Hostname**
  - **18.26.0.36 Mintaka**
  - **18.26.0.1 Radole**
- **Set IP number in rc file**
  - **ifconfig le0 18.26.0.36 netmask 0xffff0000 broadcast 18.26.255.255**
  - **127.0.0.1 Loopback**
- **Set Default Route**
  - **route -n add default 18.24.0.1 1**
  - **/etc/defaultrouter**

Debugging Network Problems

- **me(System Admin) or him(Network Admin)?**
- **ping [-s] mit.edu (connectivity)**
  - **mit.edu is alive**
  - **64 bytes from MIT.MIT.EDU (18.72.2.1): icmp_seq=0. time=4. ms**
- **Check IP Routing**
  - **netstat -nr**
    - # network, to, status, usage, interface
    - default 18.52.0.1 UG 1234 le0
    - 18.52.0.0 18.52.0.70 U 46 le0

Debugging Network Problems

- **traceroute (router problem?)**
  - **traceroute to mit.edu (18.72.2.1), 30 hops max, 40 byte packets**
  - **1 18.52.0.3 (18.52.0.3) 2 ms 2 ms 2 ms**
  - **2 E40-RTR-FDDI.MIT.EDU (18.168.0.2) 2 ms 2 ms 2 ms**
  - **3 MIT.MIT.EDU (18.72.2.1) 3 ms 3 ms 3 ms**
- **Intelligent Hubs**
- **Network Monitoring software**
  - **traffic**
  - **etherfind**
  - **NetMatrix**

NIS(YP) or DNS - "I'll tell you my name if you tell me yours!"

- **Looking up Host/IP information**
- **NIS (Yellow Pages) - SUN**
  - **broadcast-based**
  - **comprehensive (not just host information, but also users, password, etc)**
- **Setup a NIS server**
  - **set domainname**
  - **ypinit -s on server**
  - **/var/yp**
- **setup a MIS Client**
  - **set domainname**
  - **run ypbind at boot time**
  - **edit files that you want to lookup via NIS**
    - "+"

NIS(YP) or DNS - "I'll tell you my name if you tell me yours!"

- **DNS - Internet**
  - **distributed**
  - **universal**
  - **need to have direct access to internet or DNS services**
  - **cache only**
- **/etc/resolv.conf may be enough**
  - **domain lcs.mit.edu**
  - **nameserver 18.52.0.92**
  - **nameserver 18.26.0.36**
- **/etc/named.boot (named)**
- **primary or secondary**

NFS - "NFS : Not for Sharing!"

- **Binaries/Files**
  - **nfsd, biod, rpc.mountd - daemons, started at boot time**
  - **exportfs & /etc/exports - exporting file systems**

- **mount, umount, /etc/fstab & /etc/mtab - mounting and umounting file systems, systems mounted at startup, and currently mounted systems**
- **showmount - showmounted or exported filesystems**
- **nfsstat - check out stats for nfs**

NFS - "NFS : Not for Sharing!"

- **/etc/exports**
  - **THE file NOT to mess up**
  - **format - directory -option[,option]...**
    - options
      - **ro,rw = <host/netgroup>- read only, read-write for <host/netgroup>**
      - **-access=<host/netgroup> - access restricted to <host/netgroup>**
      - **-root=<host/netgroup> - root access to <machine/netgroup>**

NFS - "NFS : Not for Sharing!"

- **exportfs - actually exports files**
  - **options -**
    - -a - export all filesystems in /etc/exports file
    - -u - unexport filesystem - use -ua to unexport all filesystems
    - -v - verbose
    - no options - print exported filesystems
  - **Run "export -a" after modifing the /etc/exports file**

NFS - "NFS : Not for Sharing!"

- **Example of /etc/exports**

NFS - "NFS : Not for Sharing!"

- **mount/umount - mount and unmount filesystems**
  - **syntax : mount <options> <filesystem> <dir>**
  - **options -**
    - no options : print mounted filesystems
    - -a : mount all in /etc/fstab
    - -t <type> : type of filesystem to mount (nfs, 4.2...)
    - -r : read-only
    - -o <options> : more options (rw|ro,suid,intr,rsize=,wsize=,bg,actimeo=)

NFS - "NFS : Not for Sharing!"

- **Tips & Techniques**
  - **Make sure your exports file is correct!!!!!**
  - **NFS may be slow through gateways change rsize=1024 and wsize=1024 (default=8k)**
  - **Don't put things in your fstab that you don't ABSOLUTELY NEED, use automount instead...**

Automount - "You mean mount-ing isn't automatic?"

- **Binaries/File**
  - **automount - the daemon**

- options -
  - **-f <filename> : primary map is <filename> (usually /etc/auto.master)**
  - **-v : verbose**
- **/etc/auto.master - primary map file - INDIRECT MAP**
  - format -
    - **<mount-point> <map> [-mount-options]**
      - <mount-point> is either a path or /-
      - <map> is another file or -hosts (-hosts allows people to automount filesystems not in the auto.* files)
      - -mount-options are "mount" command options

Automount - "You mean mount-ing isn't automatic?"

- **/etc/auto.* - seconday map files - DIRECT MAPS**
  - format -
    - **key[-mount-options] location**
      - key is a path
      - -mount-options are "mount" command options
      - location is the fileserver:/path that you want to automount

Automount - "You mean mount-ing isn't automatic?"

- **Example - /etc/auto.master**

Automount - "You mean mount-ing isn't automatic?"

- **Example - /etc/auto.ai**

MAIL - "There ain't no disgruntled postal workers here! Hey! Put down that flame!"

- **Mail to where?**
  - **local user -- /vsr/spool/mail, file protection**
  - **Lan-based users -- NFS mounting spool dir?**
  - **Internet, UUCP, etc**
- **smtp protocol**
- **sendmail, mmdf, and others**
- **MX records**
- **/etc/sendmail.cf**

MAIL - "There ain't no disgruntled postal workers here! Hey! Put down that flame!"

MAIL - "There ain't no disgruntled postal workers here! Hey! Put down that flame!"

- **# Forward Everything**
- **#**
- **S0**
- **R@ $#tcp $@$F$:$n handle <> form**

- R$* $#tcp $@$F$:$1 everything
- Mtcp, P=[IPC], F=msDFMueXL, S=11, R=21, A=IPC $h, E=\r\n
- Mlocal, P=/bin/mail, F=rlsDFMmnP, S=10, R=20, A=mail -d $u
- Mprog, P=/bin/sh, F=lsDFMeuP, S=10, R=20, A=sh -c $u

MAIL - "There ain't no disgruntled postal workers here! Hey! Put down that flame!"

- Tips and Techniques
  - keep log in /usr/log/syslog file
  - mail -v
  - telnet machine 25 (talk directly to mailer)
  - Don't trust any e-mail messages, very easy to forge mail
  - privacy enhance mail
  - rewrite "From:" field to your mail hub Name

FTP service - "Oh where, Oh where, have all the files gone?"

- Pick the right ftp daemon
  - vendor/wu-ftp/...
  - look for features, logging, etc.
- configuration
  - /etc/shells -- if you are using non-standard shells
  - /etc/ftpusers (users NOT allowed inbound ftp)
  - add user "ftp" to /etc/passwd for anonymous ftp
  - chroot to ftp directory
  - ~ftp/etc/passwd ~ftp/etc/group ~ftp/usr/lib, etc
- security issues
- policy, copyrighted materials, etc.

NEWS - "No news is good news!"

- Run Server or Client only
- For Client-only, NNTP, NNTPSERVER -- find someone who has a server
- transport protocols
  - nntp
- newsreaders
  - Rn, tin, gnus, gnews

NEWS - "No news is good news!"

- Thinking about running your own server?
  - local storage of articles
  - BIGGGGGG DISKS
  - expiration policies
- innd
  - /news/newsfeeds

- chaos.dac.northeastern.edu\
- :!local,!clari.*,!mit.*,!athena.*\
- :Tf,Wnm:chaos.dac.northeastern.edu

NEWS - "No news is good news!"

- **/news/nnrp.access**
  - *.lcs.mit.edu:Read Post11:38 AM11:38 AM:*
  - ai.mit.edu:Read Post11:38 AM11:38 AM:*
  - gnu.ai.mit.edu:Read Post11:38 AM11:38 AM:*
  - nda.com:Read Post11:38 AM11:38 AM:*,!clari.*
- **ews/expire.ctrl**
  - alt.romance.chat*:A:1:1:1

- **CRONTAB**
  - **3 23 * * * /usr/local/news/bin/asnews /usr/local/news/bin/news.daily expireover**
  - **2,22,42 * * * * /usr/local/news/bin/asnews /news/lib/send-nntp myhostname**

Security -or- "Stick your hands up!"

- **Physical Security**
  - **Can your computer be stolen? Disk removed? Tapes taken?**
  - **Easily Accessable?**
- **Data Security**
  - **Passive Security - Least Intrusive/Least Security**
    - Crack
    - COPS
  - **Active Security - Most Intrusive/Most Secure**
    - Tripwire
    - logging telnet
    - Home Grown....

Security -or- "Stick your hands up!"

- **HOME GROWN Security...**
  - **checksumming**
    - after installing your latest OS generate an MD5 checksum of all your important files
  - **rdist**
    - use rdist to sync files from 1 secure server

Managing Multiple Workstations

- **How to make managing 50 machines as easy as managing one machine?**
- **keep identical /usr**
- **keep identical configuration files**
- **disk partition/allocation techniques**
- **No local files, NFS mount all user files**
- **Scripts to Sync multiple machines (rdist)**
- **NIS (yp)**
- **/etc/hosts.equiv**

Where do we go from here? More Resources!!!!

- Magazines - ;login, sysadmin, Unix Review, Open System Today, Unix World, root, Information Week, etc...
- Books
  - Unix System Administration Handbook - Nemeth, Snyder & Seebass - Prentice Hall
  - Essential System Administration - Frisch - O'Reilly & Associates
  - Programming Perl - Wall & Schwartz - O'Reilly & Associates
- Users Group/Meetings/Conferences
  - BBLisa
  - Usenix
  - LISA

Where do we go from here? More Resources!!!!

- mailing-lists
- News - Pick a group, comp.unix.admin, comp.sys.sun.admin, alt security...
- FTP/Web
- FAQs - Try ftp:January 25, 1995/rtfm.mit.edu/pub/usenet
- AN Pages
- RTFM -or- Your Manuals that came with the System - sometimes these have the most System specific information

Where do we go from here? More Resources!!!!

- Where will our stuff be?
  - ftp:January 25, 1995/theory.lcs.mit.edu/pub/admin-iap-95
  - ttp:January 25, 1995/theory.lcs.mit.edu/~sb/IAP-95.html
- hat will it be?
  - these slides in a outline format
  - scripts -

All Done! Congratulations!