SysAdmin Commands

Debugging

```
  truss executable
/* Trace doing of given command ( useful debugging ) */

  truss -f -p <pid of a shell>
/* Using multiple windows, this can be used to trace setuid/setgid programs */
```

Arp, ethernet trouble shooting

```
  arp -a .
/* Shows the ethernet address arp table */

  arp -d myhost
/* Delete a stale ethernet entry for host myhost */
```

Disk Commands

```
  du -k .
/* Reports disk space used in Kilobytes */

  du -sk .
/* Reports only total disk space used in Kilobytes */

  du -sk *|sort -k1,1n
/* Reports total disk space used in Kilobytes in present directory */

  du -ad /var | sort -nr
/* Tells you how big the /var files are in reverse order */

  fdformat -d -U
/* Format diskette */

  /usr/bin/iostat -E
/* Command to display drives statistics */

  /bin/mount -F hsfs -o ro /dev/sr0 /cdrom
/* Mount an ISO 9660 CDROM */

  newfs -Nv /dev/rdsk/c0t0d0s1
/* To view the superfblocks available */

  prtvtoc /dev/rdsk/c0t0d0s2
/* Disk geometry and partitioning info */

  quot -af
/* How much space is used by users in kilobytes */
```

Driver Parameters

```
  ndd /dev/ip \?
/* Shows IP variables in the kernel */

  ndd /dev/ip ip_forwarding
/* Tells you if forwarding is on (=1) */

  ndd -set /dev/ip ip_forwarding 1
/* Enables IP forwarding between interfaces */
```

File Manipulation

```
  dos2unix | -ascii <filename>
/* Converts DOS file formats to Unix */

  split
/* Split files into pieces */
```

```
  [vi] : %s/existing/new/g
/* Search and Replace text in vi */

  [vi] :set nu
/* Set line numbers in vi */

  [vi] :set ts=[num]
/* Set tab stops in vi */

File System

  cat /dev/null > filename
/* Zero's out the file without breaking pipe */

  dd if=/dev/rdsk/... of=/dev/rdsk/... bs=4096
/* Make a mirror image of your boot disk */

  df -k | grep dg| awk '{print $6}' |xargs -n 1 umount
/* Unmount all file systems in disk group dg */

  fsck -F ufs /dev/rdsk/c0t0d0s0
/* Check a UFS filesystem on c0t0d0s0 */

  fsck -F ufs -y /dev/rdsk/c0t0d0s0
/* Check answering yes to all questions */

  fsck -F ufs -o b=97472 /dev/rdsk/c0t0d0s0
/* Check using an alternate super block */

  gzip -dc file1.tar.gz | tar xf -
/* Unpack .tar.gz files in place */

  gzip -d -c tarball.tgz | (cd /[dir];tar xf - ) &
/* Unpacking tarballs to diff location */

  ln [-fhns] <source file> <destination file>
/* Creating hard links and soft links */

  ls -la | awk '{ print $5,"    ",$9 }' | sort -rn
/* File sizes of current directory */

  mount -f pcfs /dev/dsk/c0d0p1 /export/dos
/* Mount DOS fdisk partition from Solaris */

  mount -F ufs -o rw,remount /
/* Used to remount root to make it writeable */

  mount -o remount,logging /spare
/* Re-mount the ro file system rw and turn on ufs logging */

  pax -rw . /newdir
/* Efficient alternative for copying directories */

  prtvtoc /dev/rdsk/c0t0d0s2 | fmthard -s - /dev/rdsk/c0t1d0s2
/* Cloning Partitiontables */

  tar cvf filename.tar
/* Create a tape (tar) archive */

  tar xvf filename.tar
/* Extract a tape (tar) archive */

  tar cf - . | (cd /newdir ; tar xf -)
/* Recursively copy files and their permissions */

  /sbin/uadmin x x
/* Syncs File Systems and Reboots systems fast */
```

```
  zcat [cpio file] | cpio -itmv
/* Show the contents of a compressed cpio */

  zcat <patch_file.tar.Z | tar xvf -
/* Extract the patch_file that is a compressed tar file */

File Transfer

  get filename.suffix |"tar xf -"
/* Undocumented Feature of FTP */

  put "| tar cf - ." filename.tar
/* Undocumented Feature of FTP */

  find . -depth | cpio -pdmv /path/tobe/copied/to
/* Fast alternative to cp -pr */

  sendport
/* Transferring large numbers of files within the same ftp control session */

General

  /usr/bin/catman -w
/* Create windex databases for man page directories */

  FQ_FILENAME=<fully_qualified_file_name>; echo ${FQ_FILENAME%/*}
/* Extract directory from fully-qualified file name. */

  mailx -H -u <username>
/* List out mail headers for specified user */

  set filec
/* Set file-completion for csh */

  uuencode [filename] [filename] | mailx -s "Subject" [user to mail]
/* Send files as attachments */

Hardware

  cfgadm
/* Verify reconfigurable hardware resources */

  m64config -prconf
/* Print M64 hardware configuration */

  m64config -depth 8|24
/* Sets the screen depth of your M64 graphics accelerator */

  m64config -res 'video_mode'
/* Change the resolution of your M64 graphics accelerator */

Kernel

  /usr/sbin/modinfo
/* Display kernel module information */

  /usr/sbin/modload <module>
/* Load a kernel module */

  /usr/sbin/modunload -i <module id>
/* Unload a kernel module */

  nm -x /dev/ksyms | grep OBJ | more
/* Tuneable kernel parameters */

  /usr/sbin/sysdef
/* Show system kernal tunable details */
```

```
Memory

  prtconf | grep Mem
/* Display Memory Size */

Network Information

  ndd /dev/arp arp_cache_report
/* Prints ARP table in cache with IP and MAC address */

  netstat -a | grep EST | wc -l
/* Displays number active established connections to the localhost */

  netstat -k hme0
/* Undocumented netstat command */

  netstat -i
/* Show the TCP/IP network interfaces */

  netstat -np
/* Similar to arp -a without name resolution */

  netstat -r
/* Show network route table */

  netstat -rn
/* Displays routing information but bypasses hostname lookup. */

  netstat -a | more
/* Show the state of all sockets */

  traceroute <ipaddress>
/* Follow the route to the ipaddress */

Network/Tuning

  ifconfig eth0 mtu 1500
/* Change MTU of interface */

  ifconfig eth0 10.1.1.1 netmask 255.255.255.255
/* Add an Interface */

  /sbin/ifconfig hme0:1 inet 10.210.xx.xxx netmask 255.255.0.0 broadcast
10.210.xxx.xxx
/* Virtual Interfaces */

  /sbin/ifconfig hme0:1 up
/* Bring virtual interface up */

  /usr/sbin/ndd -set /dev/hme adv_100fdx_cap 1
/* Nailling to 100Mbps */

  ndd -set /dev/ip ip_addrs_per_if 1-8192
/* To set more than 256 virtual ip addresses. */

  ndd -set /dev/tcp tcp_xmit_hiwat 65535
/* Increase TCP-transmitbuffers */

  ndd -set /dev/tcp tcp_recv_hiwat 65535
/* Increase TCP-receivebuffers */

Processes

  fuser -uc /var
/* Processes that are running from /var */

  kill -HUP `ps -ef | grep [p]roccess | awk '{print $2}'`
```

```
/* HUP any related process in one step */

  lsof -i TCP:25
/* Mapping port with process */

  pfiles <pid>
/* Shows processes' current open files */

  pkill -n <name>
/* Kill a process by name */

  kill `ps -ef | grep program_name | grep -v grep | cut -f8 -d ' '`
/* pkill for solaris 2.6 */

  prstat -a
/* An alternative for top command */

  /usr/ucb/ps -aux | more
/* Displays CPU % usage for each process in ascending order */

  /usr/ucb/ps -auxww | grep <process name>
/* Gives the full listing of the process (long listing) */

  ps -ef | grep -i <string> | awk '{ print $2 }'
/* Creates list of running PID by */

  ps -ef | grep -v "0:00" | more
/* Gives you a list of any process with CPU time more than 0:00 */

  ps -ef | more
/* Show all processes running */

  ps -eo pid,args
/* List processes in simplified format */

  ps -fu oracle|grep pmon
/* See which instances of Oracle are running */

  /usr/proc/bin/ptree <pid>
/* Print the parent/child process 'tree' of a process */

  /usr/proc/bin/pwdx <pid>
/* Print the working directory of a process */

  top -b 1
/* Returns the process utilizing the most cpu and quits */

Resource Management

  /usr/bin/ldd [filename]
/* List the dynamic dependencies of executable files */

  /usr/proc/bin/pmap pid
/* Report address space map a process occupies */

Route Configuration

  route add net 128.50.0.0 128.50.1.6 1
/* Adds route to 128.50 network via 128.50.1.6 */

  route change 128.50.0.0 128.50.1.5
/* Changes the destination address for a route */

  route delete net 128.50.0.0 128.50.1.6
/* Deletes route to 128.50 network */

  route get [hostname]
/* Which interface will be used to contact hostname */
```

```
  route monitor
/* Monitors traffic to the routes */

  route flush
/* Removes all entries in the route table */

Searching Items

  egrep "patterna|patternb" <filename>
/* Search for multiple patterns within the same file */

  find . -exec egrep -li "str" {} \;
/* Find a string in files starting cwd */

  find / -fstype nfs -prune -o fstype autofs -prune -o -name filename -print
/* Find without traversing NFS mounted file systems */

  find . -mtime -1 -type f
/* Find recently modified files */

  find / -mtime <# of days>
/* Find files modified during the past # of days */

  find . ! -mtime -<days> | /usr/bin/xargs rm -rf
/* Finds and removes files older than <days> specified */

  find . -type f -exec grep "<sub-string>" {} \; -print
/* Find files (and content) containing <sub-string> within directory tree */

  find . -type f -exec grep -l "<sub-string>" {} \;
/* Find filenames containing <sub-string> within directory tree */

  find . -type f -print | xargs grep -i [PATTERN]
/* Recursive grep on files */

  find / -user <username>
/* Find all files owned by <username> */

  find / | grep [file mask]
/* Fast way to search for files */

  find <start_path> -name "<file_name>" -exec rm -rf {} \;
/* Recursively finds files by name and automatically removes them */

  find /proc/*/fd -links 0 -type f -size +2000 -ls
/* Find large files held open by a process */

  ls -lR | grep <sub_string>
/* Fast alternative to find */

Security

  echo 'Please go away' > /etc/nologin
/* Stops users logging in */

  find / -perm -0777 -type d -ls
/* Find all your writable directories */

  find / -type f -perm -2000 -print
/* Find all SGID files */

  find / -type f -perm -4000 -print
/* find all SUID files */

Set Terminal Options

  stty erase ^H
```

```
/* Sets the Backspace Key to erase */

  stty erase ^?
/* Sets the Delete Key to erase */

  stty sane
/* Rreset terminal after viewing a binary file. */

  tput rmacs
/* Reset to standard char set */

Snoop Your Network

  snoop -d pcelx0
/* Watch all network packets on device pcelx0 */

  snoop -o /tmp/mylog pcelx0
/* Saves packets from device pcelx0 to a file */

  snoop -i /tmp/mylog host1 host2
/* View packets from logfile between host1 & host2 */

  snoop -i /tmp/mylog -v -p101
/* Show all info on packet number 101 from a logfile */

  snoop -i /tmp/mylog -o /tmp/newlog host1
/* Write a new logfile with all host1 packets */

  snoop -s 120
/* Return the first 120 bytes in the packet header */

  snoop -v arp
/* Capture arp broadcasts on your network */

Swap File

  mkfile -v 10m /export/disk1/myswap
/* Makes a 10 Megabyte swapfile in /export/disk */

  mkfile -nv 10m /export/disk1/myswap
/* Makes an empty 10 Megabyte swapfile */

Swap Space

  swap -s
/* List the amount of swap space available, also see mkfile */

  swap -a /export/disk1/swapfile
/* Add a swapfile */

  swap -d /dev/dsk/c0t0d0s4
/* Deletes a swap device */

  swap -l
/* List the current swap devices */

System Configuration

  drvconfig ; disks
/* Adding hot-plug disks to system */

  /usr/sbin/eeprom auto-boot? false
/* Changes eeprom autoboot? setting without going to Ok prompt */

  /usr/sbin/eeprom diag-switch? true
/* Set the system to perform diagnostics on the next reboot. */

  /usr/sbin/eeprom local-mac-address?=true
```

```
/* Multiple Port Network Card Setting */

  /usr/sbin/grpck
/* Check /etc/group file syntax */

  /usr/sbin/pwck
/* Check /etc/passwd file syntax */

  /usr/sbin/sys-unconfig
/* Clear host specific network configuration information */

System Information and Monitoring

  coreadm -e log
/* Report global core */

  /bin/echo "0t${stamp}>Y\n<Y=Y" | adb
/* Convert UNIX timestamp to something human-readable */

  /usr/sbin/eeprom
/* Show eeprom parameters */

  grep "\-root" /var/adm/sulog | grep -v \+ | tail -25
/* List most recent attempts to switch to superuser account. */

  isainfo -bv
/* Quickly checkout if machine is in 32 or 64 bit mode */

  last
/* Tells who was or still is on the system */

  logger -i
/* Log the process ID */

  psradm -f [processor id]
/* Take processor offline */

  /usr/sbin/prtconf -vp
/* Show system configuration details */

  /usr/platform/`/bin/uname -i`/sbin/prtdiag -v
/* System Diagnostics */

  prtconf -pv | grep banner-name |awk -F\' ' { print $2 } ' | head -1
/* Show actual model name of machine */

  psrinfo | wc -l
/* Display number of processors */

  sar -A <time in sec>
/* Provides cumulative system report. */

  sar -a <time in sec>
/* Report use of file access system routines. */

  sar -u
/* Report CPU Utilization */

  telnet <remote machine> 13 | grep ':'
/* Get the time on remote Unix machine */

  uname -a
/* Displays system information */

  vmstat 10
/* Displays summary of what the system is doing every 10 seconds */

  who -b
```

```
/* Displays the date of the last system reboot. */

  ypcat hosts | sort -n -t. +0 -1 +1 -2 +2 -3 +3 -4
/* Take the input of "ypcat hosts" or "cat /etc/inet/hosts" and sort by IP. */
```