# 

**Searching**

**history** = print past commands to stdout, grep and use **![line\_number]** to repeat command without retyping; [or] use CTRL-r to search history

**find -03 -L . -type f -name \*.jpg** = look for files (**-type f**) with .jpg extension in or below the current directory (**.**) while following symbolic links (**-L**), also optimize file search order based on likelihood of finding a match (**-03**) (**-d** for recursive)

**find ~ -user alice -mtime 7 -iname “.log” -delete** = locate and delete (**-delete**) log files (**-name**) in or beneath the /home (**~**) directory modified in the last 7 days (**-mtime**) by user alice (**-user**), also ignore case (**-i**)

**find -regex** (instead of **find -name**) = use regex for parameter syntax instead of name globbing

**locate -ice \*.txt** = search for all .txt files, ignore case (**-i**), show number of matches (**-c** for “count”), and verify file’s existence before producing result since database may be old (**-e**) (**-r** for regex)

|  |
| --- |
| *Note: locate is much faster than find, but locate searches a tabulated database instead of actively scrubbing your disk for a match. This means the data locate uses may be a few hours old.* |

**grep -nir ‘ex\*le’ ./f\*.txt** = search for string (**‘’**, use regex) in all .txt files starting with f in or beneath (**-r**) the current directory (**./**) while ignoring case (**-i**) and displaying line number (**-n**)

**grep -l ‘^alice’ /etc/\*** = show only the filenames containing matched results (**-l**) instead of the results themselves

**grep -wv ‘[a-d]’ /\*.txt** = grep for words (**-w**) that DON’T contain the given search terms (**-v**)

**man -k string** = search man pages for given string

**grep** regex (**-E** option)

**^** = match string at start

**$** = match string at end

**|** = logical OR (**grep -E ‘i|a’ file**)

**\*** = zero or more of previous (**grep -E ‘a\*’ file**)

**+** = one or more of previous

**Logical Volumes**

**pvcreate /dev/sdb** = create a physical volume (PV) from sdb

**pvremove /dev/sdb1 /dev/sdc1** = remove physical volumes on partitions sdb1 and sdc1

**pvmove /dev/sdb1 /dev/sdb2** = copy all data from sdb1 to sdb2

**pvdisplay** or **pvscan** = show physical volumes

**vgcreate VG1 /dev/sdb /dev/sdc** = create a volume group containing PVs sdb and sdc called VG1

**vgdisplay** or **vgscan** = show volume groups

**vgextend vgroup /dev/sdb1** = add PV sdb1 to “vgroup” volume group

**lvcreate -L 5G LV1 -n LV2** = create 5 GB logical volumes called LV1 and LV2

**lvdisplay** or **lvscan** = show logical volumes

**lvextend -L 1.5G /dev/mapper/LV1** = extend logical volume LV1 to 1.5 GB

**lvreduce -l -200 /dev/mapper/LV1** = reduce logical volume LV1 by 200 extents

**Filesystems**

**mkfs.ext4 /dev/mapper/LV1** = create ext4 filesystem on LV1 logical volume

**mkfs -t ext4 /dev/mapper/LV1** = create ext4 filesystem that fits size of logical volume LV1

**e2fsck -f /dev/mapper/LV1** = expand filesystem to fit size of LV1

**resize2fs /dev/mapper/LV1** = shrink/grow filesystem of LV1 down to the size of currently used space

**e4degrag /** = defragment all partitions

**fsck /dev/sda2** = check sda2 partition for errors

*note: XFS filesystems* ***cannot*** *be shrunk; use ext4 instead*

**Disks**

**lsblk** = show disk tree layout, including logical volumes

**fdisk -l** = show drives and their partition tables

**fdisk /dev/sdb** = edit the partition table of sdb

**df -Th** = show mounted drives, % full, and mount location in human-readable form (**-h**), use -T to show filesystem type

**mount** = show mounted volumes and their mount locations (the command reads the /etc/fstab file)

|  |
| --- |
| File links  **ln /home/file.txt /var/hardlink.txt** = create hard link to file (**ln -s** for soft/symbolic link), |
| *hard links* create an additional pointer to a file’s inode and remain even if the original file from which the link was created is deleted |
| *symbolic links* can be made for directories and work across partitions (unlike hard links), but break if the original file is deleted (similar to Windows shortcuts) |

**Linux Command Cheat Sheet** v2.2, updated 2019-04-24 variables are in brackets, descriptive text and options are in parenthesis

**Processes & Devices**

**ps -efH | less** = view current running process in tree structure (**H** for hierarchy), everything (**-e**), full-format (**-f**)

|  |  |
| --- | --- |
| process codes | |
| **D**=uninterruptible sleep (waiting for Disk/IO) | **R**=running or in run queue |
| **S**=interruptible sleep (waiting for event) | **T**=stopped by job control signal |

**top -u alice** = show user alice’s currently running processes, use O to sort by colunm

**kill -s 9 7423** = end process with PID 7423

**date** = view current time

**shutdown -r now** = immediately reboot system

|  |  |  |  |
| --- | --- | --- | --- |
| init runlevels - change with **init [#]** | | | |
| **0** | shutdown | **3** | normal |
| **1** | single-user mode | **5** | runlevel 3 w/ X11 |
| **2** | multi-user mode | **6** | reboot |
| change default in **/etc/init/rc-sysinit.conf** | | | |

**du -sh /home/alice** = display directory size, summarize (**-s**) in human-readable format (**-h**)

**du -d1 -h /** = list directory sizes in current path

|  |
| --- |
| **lsof** = list files currently open (useful when unmounting a disk)  **lsof -u root** = list files open by root |
| **lsmod** = show status of kernel modules |
| **lspci** = list pci devices |

**exec bash** = restart bash shell

CTRL-J **reset** CTRL-J = force shell prompt to appear

|  |
| --- |
| **crontab** syntax |
| minofhour|hourofday|dayofmonth|month#|dayofweek |

**Packages & Archives**

**rpm -ivh file.txt** = install .rpm (**-i**), verbose (**-v**), use hash marks to display progress (**-h**)

**tar -czvf ./file.tar.gz ./source** = create tar archive (**-c**), create file (**-f**), verbose (**-v**), use gzip (**-z**)

**C**reate **Z**e **V**’king **F**ile

**X**tract **Z**e **V**’king **F**iles

p

**Users & Groups**

**groups alice** = show what groups user alice is in

**id -G wheel** = show gid of wheel group

**usermod -a -G wheel,group1 alice** = add alice to wheel and group1 groups

**w** = print recently logged-on user data

|  |
| --- |
| **/etc/passwd** = location of user information |
| /etc/passwd user syntax |
| **uname:x:uid:gid:comments:homedir:shell** |
| **/etc/group** = location of group information |
| /etc/group file syntax |
| **groupname:x:groupid:userlist(user1,user2)** |

**Networking**

**ip a** = show all network connections, usually to check the system’s IP address

**ifconfig ens32 [ip] netmask [netmask] up** = change ip

**/etc/sysconfig/network** = see default gateway

**routel** = view routing table

**netstat -plant** = show open ports on local host

**nmap -sTU -p 1-100 [ip/fqdn]** = scan for open tcp/udp ports 1-100 on remote host

**dig domain.com** = perform DNS lookup on domain

**traceroute domain.com** = print the route packets take to a given destination

**iptables -L** = show firewall ruleset

**nmtui** & **nmcli** = NetworkManager text utility

**screen**

|  |
| --- |
| **screen** command keybindings |
| *all screen keybindings are preceded with CTRL-A* |
| **c** = create new window and switch to it |
| **SPACE** or **n** = switch to next window |
| **BACKSPACE** or **p** = switch to previous window |
| **|** = split window vertically (pipe) |
| **S** = split window horizontally (capital **S**)  **x** = un-split window |
| **k** = kill current window |
| **\** = kill all windows |
| **d** = detach from session |
| **r** = toggle line-wrap |

**Text & Logs**

|  |  |
| --- | --- |
| **less** keybindings | |
| **SPACE** = next page | **b** = previous page |
| **>** = last line | **<** = first line |
| **/** = forward search | **?** = backwards search |
| **n** = next search match | **N** = previous search match |
| **q** = quit |  |

**tail -f file.txt** = view text file in as it updates in realtime (**-f** for follow)

**ls -ltrh** = list files sorted by last modified time, include filesize (**-h**)

**journalctl -xe** = show system log files with explanatory (**-x**) text included (systemd-based distros only)

|  |
| --- |
| log locations |
| **/var/log/messages** = generic system activity logs |
| **/var/log/secure** = authentication logs |
| **/var/log/kernel** = logs from the kernel |
| **/var/log/cron** = record of cron jobs |
| **/var/log/maillog** = log of all mail messages |
| **/var/log/faillog** = failed logon attempts |
| **/var/log/boot.log** = dump location of init.d |
| **/var/log/dmesg** = kernel ring buffer logs for hardware drivers |
| **/var/log/httpd** = apache server logs |

**Shell Functions**

**[command] &** = run command in background

**[command1] ; [command2]** = run command2 immediately after command1 (ex: **cd /home ; ls**)

**sudo !!** = execute last command (!!) with sudo privileges

**1>** or **>** = stdout, **2>** = stderr, **2>&1** or **&>** = stdout and stderr

**cat /file.log 2>&1 | grep -i error** = pass both stdout and stderr to grep through pipe, by default pipe only passes stdout

**stat /home/file.txt** = show last modified date, creation date, and other metadata about given file

**tr ‘a-z’ ‘A-Z’** = “translate,” find first parameter (**‘a-z’**) and replace matches with second parameter (**‘A-Z’**)

runlevels

**Permissions**

**chown -R alice:admins /home/Documents** = change ownership of Documents directory recursively (-R) to alice and the admins group

|  |
| --- |
| **chmod** octal permissions (special|user|group|all) |
| **4**=read(r), **2**=write(w), **1**=execute(x), **0**=none(-) |
| 4=setuid(s), 2=setgid(s), 1=sticky bit(t), 0=none(-) |
| (special bit only) |
|  |
| *-If 3 digits are given, 1st is owner, 2nd is group, 3rd is everyone else (all); digits are added from options above* |
| *-If 4 digits are given, 1st is the special bit, 2nd is owner, 3rd is group, 4th is everyone else (all)* |
|  |
| setuid: run exe with same permissions as file’s owner |
| setgid: run exe with same permissions as file’s group |
| *(setuid and setgid are represented as an “s” replacing the “x” in file permissions for exe files and a “S” for non-executable files)* |
| sticky bit: prevents a user from removing or renaming a file in a directory unless they own the file or directory, represented as a “t” replacing the “x” in directory permissions |
| **chmod -R 6754 /var/log** = run executables with permissions of the owning user and group (4+2=6, special bit), give rwx (**4**+**2**+**1**=7) permissions to owner, give rx (**4**+**1**=5) to the owning group, give r (**4**=4) permissions to everyone else (aka “all”); apply these permissions recursively (**-R**) |

**chgrp wheel /home/alice** = change group owner of the /home/alice directory to wheel

**SELinux**

**sestatus -v** = display general SELinux config, verbose **(-v**)

**setenforce 1** = enable SELinux enforcement (**1** for on, **0** for off)

**restorecon -F /file.txt** = forcibly (**-F**) restore SELinux content to specified file or directory

**fixfiles** = check security context database

**getsebool** = get SELinux boolean values

**setsebool** = toggle SELinux boolean values