Cheatography

Linux cheatsheet Cheat Sheet

by culebrinoo via cheatography.com/122227/cs/22624/

Expansion

`ls $(which cp)` `ls` `` `which cp` ``	Command expansion
`mkdir {2017...2-020}-{01-12}`	Brace expansion
`echo text ~/*.txt {a,b} $USER`	Variable expansion
`echo "text ~/*.txt {a,b} $USER"`	" expansion
`echo 'text ~/*.txt {a,b} $USER'`	' expansion (NONE)

Redirection & Commands

`ls > file.txt`	Standard Out
`ls 2> file.txt`	Standard Error
`ls > file.txt 2>&1` `ls &> file.txt`	Standard Out & Error
`ls | tee file | wc -l`	Read stdin & writes stdout
`cmd1 ; cmd2`	Run cmd1 then cmd2
`cmd1 && cmd2`	Run cmd2 if cmd1 is OK
`cmd1 || cmd2`	Run cmd2 if cmd1 is KO

su / sudo

`su [-[l]] [user]`

> Become another user, `ROOT` by default. If `-` or `-l`, load user envs and working dir.

`su [user] -c 'command'`

> Execute command as user. Default `root`

`sudo [-u user] command`

> Execute command as user. Default `root`

`sudo -ll`

> Which commands I'm allowed to execute

`visudo`

> Edit `/etc/sudoers` file. Example
> `teralco ALL=(root) NOPASSWD: /etc/init.d/jboss`
> `teralco ALL=(jboss) NOPASSWD: /bin/kill`

UFW

`ufw status` `[verbose|numbered]`

> Show status and rules

`ufw default` `deny incoming`
`ufw default` `allow outgoing`

> Deny all incoming traffic by default
> Allow all outgoing traffic by default

`ufw` `[allow|deny]` **`from`** `IP` **`to`** `[any|interface_name]` **`[proto`** `tcp|udp]` **`port`** `PORT`

> Full allow/deny rule

`ufw` `[allow|deny] service_name`

> Allow/deny a service (`ssh www ftp ...`)

`ufw` `[enable|disable]`

`ufw delete` `[rule|number]`

Alt commands

`/var/log/messages & /var/log/-syslog`

> System log files

`script` `file`

> Record session commands in file

`nohup` `command &`

> Keep command running even after close session

`tar -J``xvf file.tar.xz [-C dest_folder]`

> Extract xz (higher compress ratio)

`zip -FF x.zip --out Y.zip && unzip Y.zip`

> Merge zip files (x.zip, x.z01, x.z02)

`ps aux --sort -rss`

> Higher memory consumption processes

`fdisk -l`

> List partition tables

`dd bs=4M if=input.iso of=/de-v/sd? conv=fdatasync`

> Burn iso in device

Searches

`find` `path -name *.log -type f -mtime +5 -exec rm -rvf {} \;`

> Find and delete files older than 5 days

`find` `path -type f -printf "%s-\t%p\n" |` **`sort`** `-rn |` **`head`** `-10`

> Find the 10 biggest files

`grep` `-rlie 'pattern' path`

> Find files with pattern content

`du` `-cks path/* |` **`sort`** `-rn |` **`head`** `-10`

> Find biggest dirs

By **culebrinoo**
cheatography.com/culebrinoo/

Published 4th May, 2020.
Last updated 4th May, 2020.

Cheatography

Linux cheatsheet Cheat Sheet

by culebrinoo via cheatography.com/122227/cs/22624/

Searches (cont)

du *-sh* path

Dir size

Permissions

chmod [u|g|o][+|-|=][rwx] dir_file

Change permissions

chmod **u[+|-]s** file

Set uid. File is always exec as owner user

chmod **g[+|-]s** dir

Set gid. New files in folder are always owned by folder owner

chmod **[+|-]t** dir

Sticky Bit. Files in dir can only be renamed or removed by owner or root

umask xxxx

Set default permissions to dirs

Enviroment

/etc/profile /etc/bash.bashrc	Global env config files
~/.bashrc ~/.profile	User env config file
printenv	Print defined env vars
alias	Show defined aliases
export VAR	Make a VAR available to child process
source script . script	Load a file into current script or shell session

Network

ip addr

Show ips

ifup|**ifdown** *interface_name*

Up or down an interface

/etc/network/interfaces

File interfaces are defined

hostnamectl [set-hostname *hostname*]

Manage hostname (/etc/hostname) without restarting

netstat -tuln

All tcp and udp listening ports

ss -tuln

All tcp and udp listening ports

nc *-vz* host port

Scan port in host

SSH

ssh-keygen [-f /etc/ssh/ssh_host_rsa_key] -t rsa -b 4096

Generate ssh rsa key. By default ~/.ssh/id_rsa

ssh-copy-id [-i ~/.ssh/mykey] user@host

Copy ssh key in remote host (~/.ssh/authorized_keys). By default ~/.ssh/id_rsa.

ssh user@host command

Exec command in host

ssh *-J* hostA hostB

Connect to hostB through hostA (Jumping). Identification in localhost. Can use **ProxyJump** in ~/.ssh/config

SSH (cont)

ssh *-D* port *-fCqN* user@host

Proxy socket (HTTP and HTTPS traffic) through port.

ssh *-nNT -L* 9000:remote_server:80 user@host

Tunneling (Local port forwarding). Map remote_server:80 into localhost:9000 through host

ssh *-nNT -R* 9000:localhost:3000 user@host

Tunneling (Remote port forwarding). Map localhost:3000 into host:9000

By **culebrinoo**
cheatography.com/culebrinoo/

Published 4th May, 2020.
Last updated 4th May, 2020.