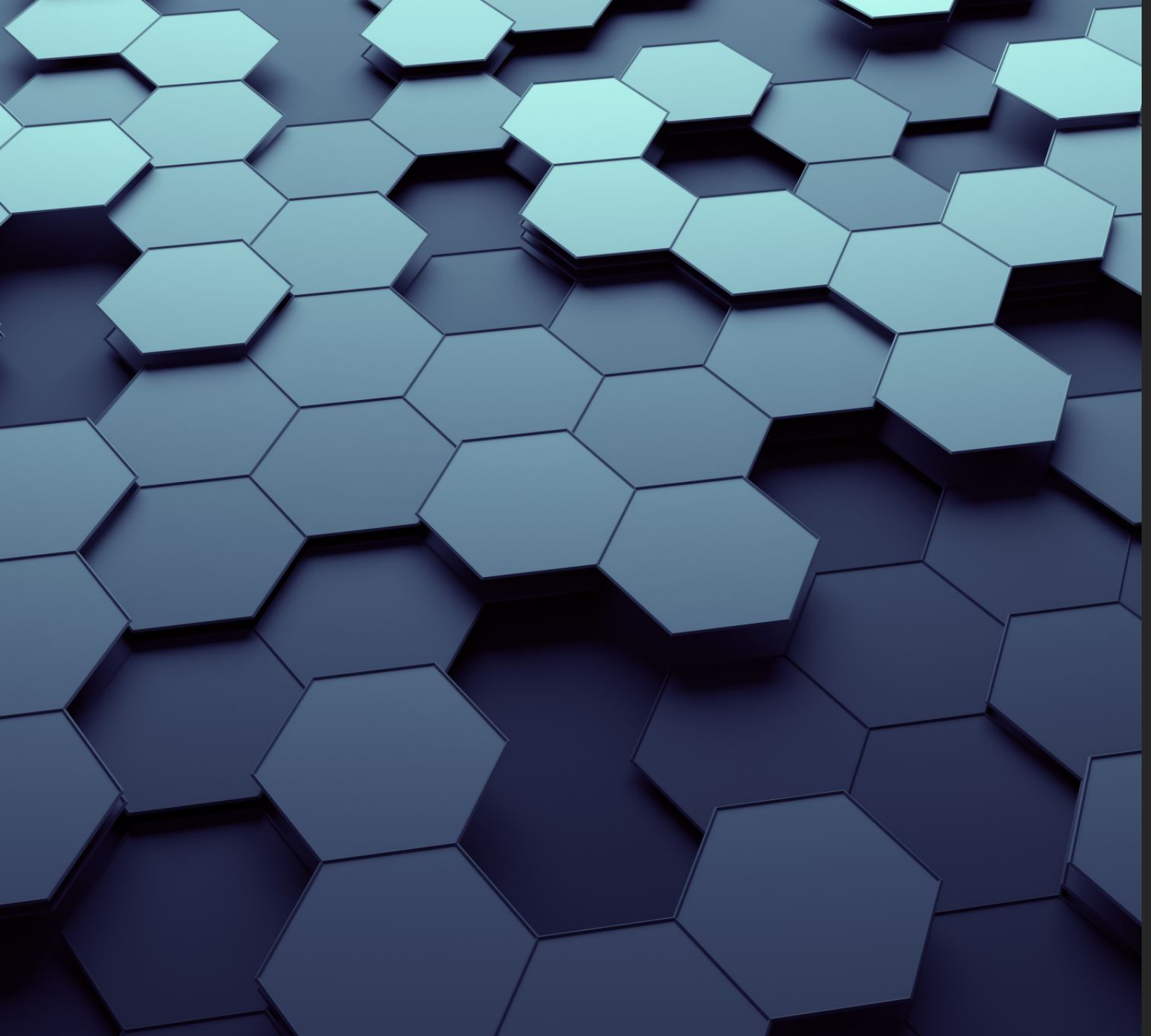


Red Hat Linux System Admin

BY PRAVEEN SINGAMPALLI

Manually set up a repository

We create a .repo file within /etc/yum.repos.d using a text editor. In this example, we will create the repository file for MySQL 5.7

Step1 :
cd /etc/yum.repos.d/

Step2:
vim mysql57-community.repo

```
[mysql57-community]
name=MySQL 5.7 Community Server
baseurl=http://repo.mysql.com/yum/mysql-5.7-community/el/7/$basearch/
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
```

Step3:
yum-config-manager mysql57-community [Validate the yum repository]

Step4:
yum install mysql

YUM CONFIGURTION

- **YUM stands for Yellow Dog Updater Manager.**
- **Yum is the default package management utility in RHEL/Centos.**
- **Yum uses repository to get the necessary rpm files.**
- **A repository is collection of rpm files.**
- **Repository may contain multiple versions of the same RPM package.**
- **Repository may contain different builds for different architectures for example one for i686 and other for x86_64.**
- **A repository can be configured locally or remotely.**

vi /etc/yum.repos.d/rhcelab.repo	As we know repository configuration files are stored in ***/etc/yum.repos.d/*** directory with an extension **.repo**, So we executed this command to create the necessary configuration file for repository.
[rhcerepo]	This is the label of repository. Usually a repository file contains configuration for multiple repositories. In that case label is used as identifier of repository.
name=rhcerepo	This configuration value is used to set the name of repository.
baseurl=file:///rhcelab/repo	This configuration value defines the location of rpm files.
enabled=1	This key defines the state of repository. If value is set to **1** then repository is enabled. If value is set to **0** then repository is disabled.
gpgcheck=0	This key defines whether the integrity of package should be check or not. If value is set to **1**, integrity will be checked. If value is set to **0**, integrity will not be checked.
:wq	We used vi editor to create the file. In vi editor, the command: wq is used to save and quit from file.

CONFIGURING IP NETWORKING WITH NMCLI

The **nmcli** (NetworkManager Command Line Interface) command-line utility is used for controlling NetworkManager and reporting network status.

Step1 : yum install NetworkManager

Step2: systemctl start NetworkManager

Step3: systemctl enable NetworkManager
To make sure it is up 24/7

Step4 : nmcli connection show --active

Step 5: nmcli device status

```
[root@ip-172-31-22-205 yum.repos.d]# systemctl enable NetworkManager
[root@ip-172-31-22-205 yum.repos.d]# nmcli connection show --active
NAME  UUID                                  TYPE      DEVICE
eth0  5a037419-2a20-4bd5-859c-213324d97084  ethernet  eth0
```

```
[root@ip-172-31-22-205 yum.repos.d]# nmcli device status
DEVICE  TYPE      STATE      CONNECTION
eth0    ethernet  connected  eth0
lo      loopback  unmanaged  --
```

nmcli connection add type ethernet ifname eth0

Ifname = interface name

```
[root@ip-172-31-22-205 yum.repos.d]# nmcli connection add type ethernet ifname eth0
Connection 'ethernet-eth0' (41617833-1202-4743-86fa-3e6e68597283) successfully added.
```

nmcli connection show

```
Error: argument 'show' not understood. Try passing --help instead.
[root@ip-172-31-22-205 yum.repos.d]# nmcli connection show
NAME                UUID                                  TYPE      DEVICE
eth0                5a037419-2a20-4bd5-859c-213324d97084  ethernet  eth0
ethernet-enp0s8     0a2bc44b-65c5-42f2-ba48-8c7782e130f6  ethernet  --
ethernet-eth0       41617833-1202-4743-86fa-3e6e68597283  ethernet  --
System eth0         5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  ethernet  --
[root@ip-172-31-22-205 yum.repos.d]#
```

nmcli connection up ethernet-eth0

```
[root@ip-172-31-22-205 yum.repos.d]# ^C
[root@ip-172-31-22-205 yum.repos.d]# nmcli connection up ethernet-eth0
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/2)
```

nmcli connection show --active

```
[root@ip-172-31-22-205 yum.repos.d]# nmcli connection show --active
NAME            UUID                                  TYPE      DEVICE
ethernet-eth0   41617833-1202-4743-86fa-3e6e68597283  ethernet  eth0
[root@ip-172-31-22-205 yum.repos.d]#
```

To Change the Linux system IP ADDRESS

nmcli connection modify ethernet-eth0 ipv4.address 172.31.16.0/20

```
[root@ip-172-31-28-145 ec2-user]#
[root@ip-172-31-28-145 ec2-user]# nmcli connection modify ethernet-eth0 ipv4.address 172.31.16.0/20
```

nmcli connection modify ethernet-eth0 ipv4.method manual

```
[root@ip-172-31-28-145 ec2-user]#
[root@ip-172-31-28-145 ec2-user]# nmcli connection modify ethernet-eth0 ipv4.method manual
```

To bring the connection down and up

```
[root@ip-172-31-28-145 ec2-user]# ^C
[root@ip-172-31-28-145 ec2-user]# nmcli connection down ethernet-eth0
[root@ip-172-31-28-145 ec2-user]# ^C
```

```
[root@ip-172-31-28-145 ec2-user]# ^C
[root@ip-172-31-28-145 ec2-user]# nmcli connection up ethernet-eth0
```

To modify IPV4 Gateway

nmcli connection modify ethernet-eth0 ipv4.gateway “172.31.16.1”

To modify the DNS

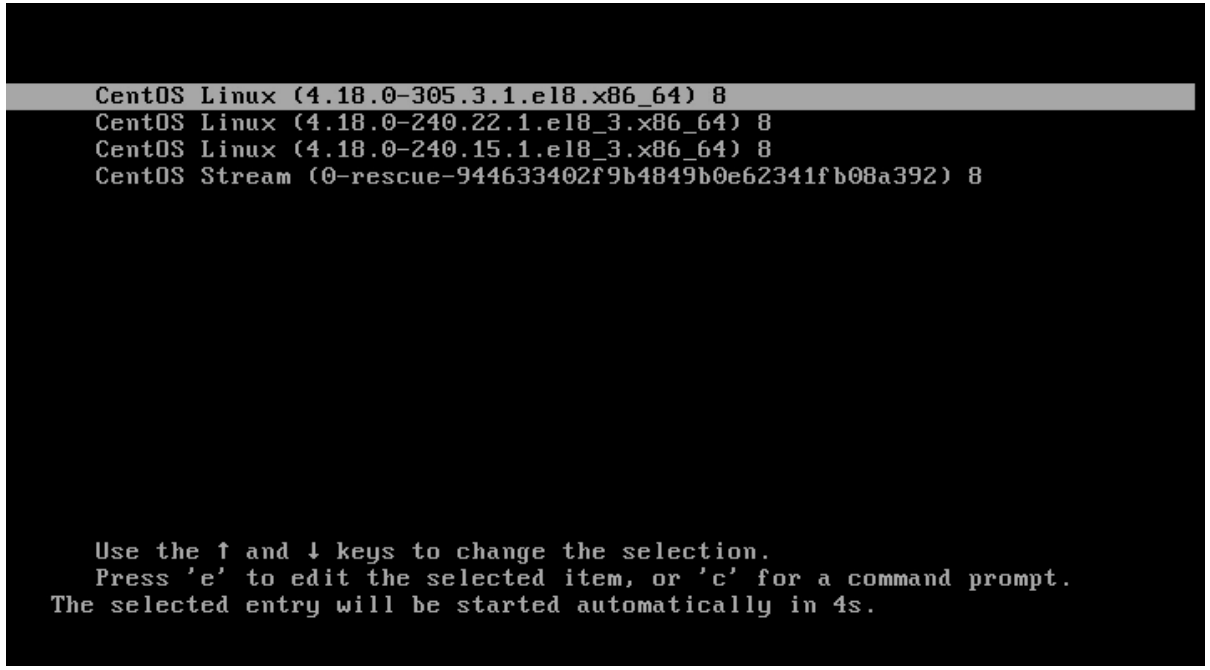
nmcli connection modify ethernet-eth0 ipv4.dns “172.31.16.103”

```
connect     delete     disconnect  help        lldp        modify      monitor     reapply
[root@ip-172-31-22-205 yum.repos.d]# nmcli device show
GENERAL.DEVICE:                         eth0
GENERAL.TYPE:                           ethernet
GENERAL.HWADDR:                         02:B3:C9:CB:32:6D
GENERAL.MTU:                            9001
GENERAL.STATE:                          100 (connected)
GENERAL.CONNECTION:                     ethernet-eth0
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnection/2
WIRED-PROPERTIES.CARRIER:               on
IP4.ADDRESS[1]:                         172.31.22.205/20
IP4.GATEWAY:                            172.31.16.1
IP4.ROUTE[1]:                           dst = 0.0.0.0/0, nh = 172.31.16.1, mt = 100
IP4.ROUTE[2]:                           dst = 172.31.16.0/20, nh = 0.0.0.0, mt = 100
IP4.DNS[1]:                             172.31.0.2
IP4.DOMAIN[1]:                          us-west-1.compute.internal
IP6.ADDRESS[1]:                         fe80::fcd1:22d6:9d30:6273/64
IP6.GATEWAY:
```

Resetting a Root Password in Linux CentOS (If Forgot)

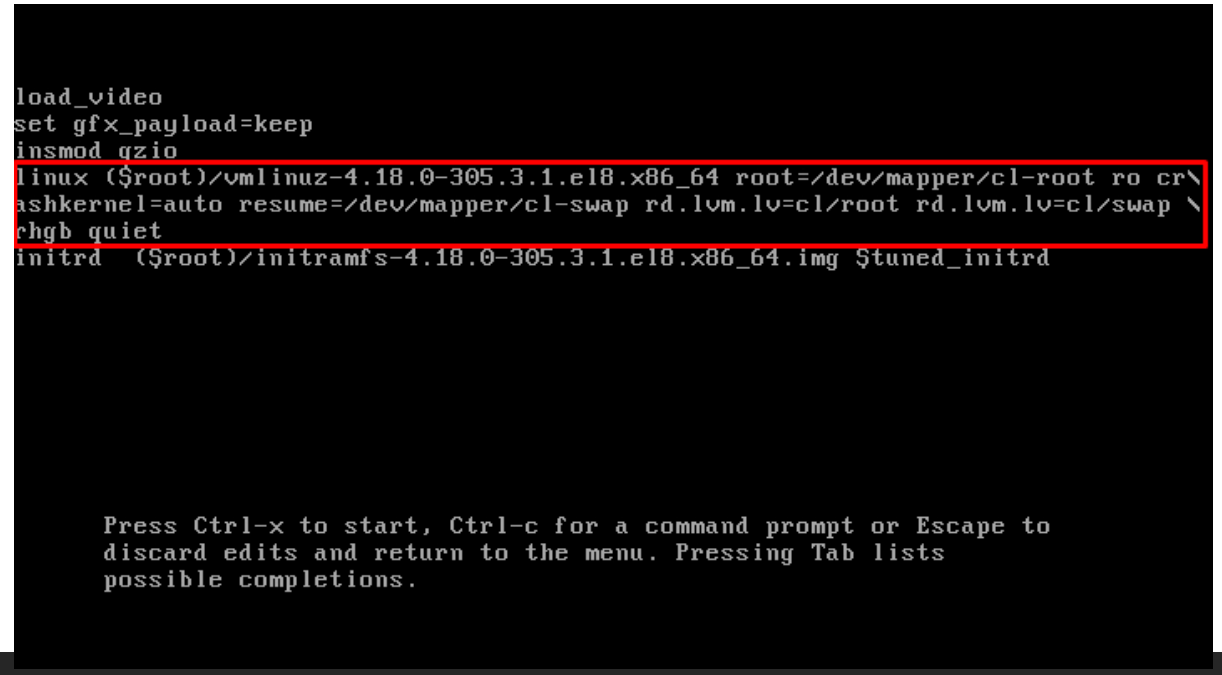
Step 1: Boot to Recovery Mode

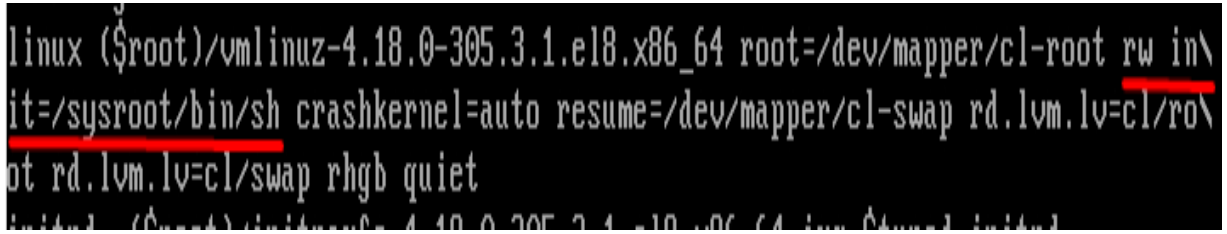
For resetting the root password we need to reboot our computer. When the system restarts, press the "**ESC**" key immediately to interrupt the boot process and select the kernel from the GRUB/Boot menu you want to boot into by pressing the arrow keys.



Step 2 - Pressing 'e' from your keyboard will open the editing menu.

Step 3 - In the editing menu, locate the "**ro**" kernel parameter and replace it with "**rw,**" and add an additional parameter "**init=/sysroot/bin/sh**"





Step 4 - Press **Ctrl + X** to enter into the single-user mode once you are done with the previous step.

Step 5 - Now run the "chroot /sysroot" command to convert the root file system in read and write mode

```
:/# chroot /sysroot
:/#
```

Step 6 – Set a new password for root, input the command (Changing the password for user root)

```
:/# passwd root
Changing password for user root.
New password: _
```

Step 7 – Set a new password for root, input the command

```
:/# passwd root
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
:/#
```

```
[    4.827760] [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log messa
ge.
[    4.837060] [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log messa
ge.
[  OK  ] Stopped target Paths.
[  OK  ] Stopped target System Initialization.
[  OK  ] Stopped target Swap.
[  OK  ] Stopped Create Volatile Files and Directories.
[  OK  ] Stopped target Local File Systems.
[  OK  ] Stopped udev Coldplug all Devices.
[  OK  ] Stopped Apply Kernel Variables.
[  OK  ] Stopped Load Kernel Modules.
         Stopping udev Kernel Device Manager...
[  OK  ] Stopped target Local File Systems (Pre).
[  OK  ] Stopped target Initrd Root Device.
[  OK  ] Stopped udev Kernel Device Manager.
[  OK  ] Started Plymouth switch root service.

Generating "/run/initramfs/rdsosreport.txt"


Entering emergency mode. Exit the shell to continue.
Type "journalctl" to view system logs.
You might want to save "/run/initramfs/rdsosreport.txt" to a USB stick or /boot
after mounting them and attach it to a bug report.


:/#
```

Step 8 - SELinux relabelling (to set the permissions for files or folders)

```
:/# touch /.autorelabel
:/# _
```

Step 9 – Exit from terminal

```
:/# exit
exit
:/# _
```

Step 10 – Hit reboot

```
:/# reboot
:/# _
```

```
[    4.519419] [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log messa
ge.
[    4.529807] [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log messa
ge.
[   28.346627] selinux-autorelabel[817]: *** Warning -- SELinux targeted policy relabel is required.
[   28.347001] selinux-autorelabel[817]: *** Relabeling could take a very long time, depending on fi
le
[   28.347268] selinux-autorelabel[817]: *** system size and speed of hard drives.
[   71.767007] selinux-autorelabel[817]: Warning: Skipping the following R/O filesystems:
[   71.767271] selinux-autorelabel[817]: /sys/fs/cgroup
[   71.768244] selinux-autorelabel[817]: Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts
 /dev/shm /run /sys /sys/fs/cgroup/blkio /sys/fs/cgroup/cpu,cpuacct /sys/fs/cgroup/cpuset /sys/fs/cg
roup/devices /sys/fs/cgroup/freezer /sys/fs/cgroup/hugetlb /sys/fs/cgroup/memory /sys/fs/cgroup/net_
cls,net_prio /sys/fs/cgroup/perf_event /sys/fs/cgroup/pids /sys/fs/cgroup/rdma /sys/fs/cgroup/system
d /sys/fs/pstore /sys/kernel/debug /sys/kernel/tracing
_
```

How to create a tar backup

- tar -cvf backup.tar finaldraft.sh

-c - Create the archive
-v - Show the process verbosely
-f - Name the archive

- create a tar.gz backup

tar -czf backup.tar.gz finaldraft.sh

-c - Create the archive
-v - Show the process verbosely
-f - Name the archive
-z - Compressed gzip archive file

- Exclude files when creating a tar backup

tar --exclude file.txt --exclude file.sh -cvfz backup.tar.gz

- Extract content from a tar (.gz) backup

tar -xvfz backup.tar.gz

-x - Extract the content
-v - Show the process verbosely
-f - Name the archive
-z - compressed gzip archive file

Tuning of Linux Systems****

The profiles provided with **tuned** are divided into two categories: power-saving profiles, and performance-boosting profiles. The performance-boosting profiles include profiles focus on the following aspects:

•low latency for storage and network
•high throughput for storage and network
•virtual machine performance
•virtualization host performance

- yum install tuned
- systemctl enable --now tuned
- yum install tuned-profiles-realtime
- tuned-adm active (Verify that a **TuneD** profile is active and applied)
  tuned-adm verify

```
[admin@vps1 ~]$ tuned-adm list
Available profiles:
- balanced                    - General non-specialized tuned profile
- desktop                     - Optimize for the desktop use-case
- latency-performance         - Optimize for deterministic performance at the cost of increased po
wer consumption
- network-latency             - Optimize for deterministic performance at the cost of increased po
wer consumption, focused on low latency network performance
- network-throughput          - Optimize for streaming network throughput, generally only necessar
y on older CPUs or 40G+ networks
- powersave                   - Optimize for low power consumption
- throughput-performance      - Broadly applicable tuning that provides excellent performance acro
ss a variety of common server workloads
- virtual-guest               - Optimize for running inside a virtual guest
- virtual-host                - Optimize for running KVM guests
Current active profile: virtual-guest
[admin@vps1 ~]$
```

TuneD recommends the most suitable profile for your system

```
# tuned-adm recommend

balanced
```

```
# tuned-adm profile selected-profile
```

```
# tuned-adm profile virtual-guest powersave
```

Create a Group

Need to create groups before creating any account otherwise we have to use existing groups at your system

Command	Description
useradd	Adds accounts to the system.
usermod	Modifies account attributes.
userdel	Deletes accounts from the system.
groupadd	Adds groups to the system.
groupmod	Modifies group attributes.
groupdel	Removes groups from the system.

groupadd [-g gid [-o]] [-r] [-f] groupname

Option	Description
-g GID	The numerical value of the group's ID.
-o	This option permits to add group with non-unique GID
-r	This flag instructs groupadd to add a system account
-f	This option causes to just exit with success status if the specified group already exists. With -g, if specified GID already exists, other (unique) GID is chosen.
Groupname	Actaul group name to be created.

```
$ groupadd developers
```

Modify a Group

To modify a group, use the **groupmod** syntax –

```
$ groupmod –n new_modified_group_name old_group_name
```

To change the developers_2 group name to developer, type –

```
$ groupmod –n developer developer_2
```

Here is how you will change the financial GID to 545 –

```
$ groupmod –g 545 developer
```

```
$ groupdel developer
```

Create an Account

useradd -d /home/singam/ -g testers -s /bin/bash -m singam

Option	Description
- d homedir	Specifies home directory for the account.
-g groupname	Specifies a group account for this account.
-m	Creates the home directory if it doesn't exist.
-s shell	Specifies the default shell for this account.
-u userid	You can specify a user id for this account.
accountname	Actual account name to be created

```
[root@ip-172-31-20-113 ec2-user]# useradd -d /home/singam/ -g testers -s /bin/bash -m singam
```

```
[root@ip-172-31-20-113 ec2-user]# passwd singam
Changing password for user singam.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
```

```
[ec2-user@ip-172-31-20-113 ~]$ sudo su
[root@ip-172-31-20-113 ec2-user]# userdel singam
```

SELINUX SELinux stands for **S**ecurity **E**nhanced **Linux**, which is an access control system that is built into the Linux kernel. It is used to enforce the resource policies that define what level of access users, programs, and services have on a system.

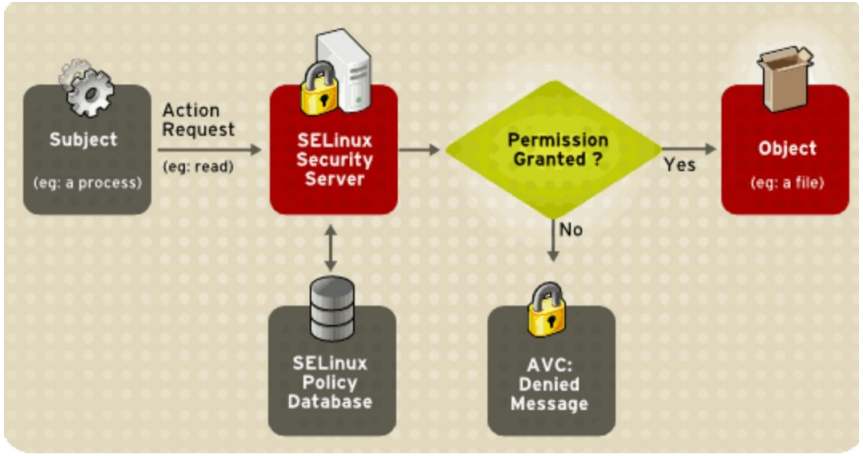
```
-rw-rw-rw-  1 root root 0 Sep 22 13:14 access
dr-xr-xr-x  1 root root 0 Sep 22 13:14 booleans
--w-------  1 root root 0 Sep 22 13:14 commit_pending_bools
-rw-rw-rw-  1 root root 0 Sep 22 13:14 context
-rw-rw-rw-  1 root root 0 Sep 22 13:14 create
--w-------  1 root root 0 Sep 22 13:14 disable
-rw-r--r--  1 root root 0 Sep 22 13:14 enforce
-rw-------  1 root root 0 Sep 22 13:14 load
-r--r--r--  1 root root 0 Sep 22 13:14 mls
-r--r--r--  1 root root 0 Sep 22 13:14 policyvers
-rw-rw-rw-  1 root root 0 Sep 22 13:14 relabel
-rw-rw-rw-  1 root root 0 Sep 22 13:14 user
```

SELINUX=*enforcing|permissive|disabled* — Defines the top-level state of SELinux on a system.

- **enforcing** — The SELinux security policy is enforced.
- **permissive** — The SELinux system prints warnings but does not enforce policy.
- **disabled** — SELinux is fully disabled. SELinux hooks are disengaged from the kernel and the pseudo-file system is unregistered.

SELINUXTYPE=targeted|strict — Specifies which policy SELinux should enforce.

- **targeted** — Only targeted network daemons are protected.
- **strict** — Full SELinux protection, for all daemons. Security contexts are defined for all subjects and objects, and every action is processed by the policy enforcement server.



Step 1: Status of S

```
[root@ip-172-31-20-113 ec2-user]#
[root@ip-172-31-20-113 ec2-user]# sestatus
SELinux status:                 disabled
```

Step 2: Check SELinux

cat /etc/selinux/config

```
SELinux status:                 disabled
[root@ip-172-31-20-113 ec2-user]# cat /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Step 3 : Change SELinux Mode

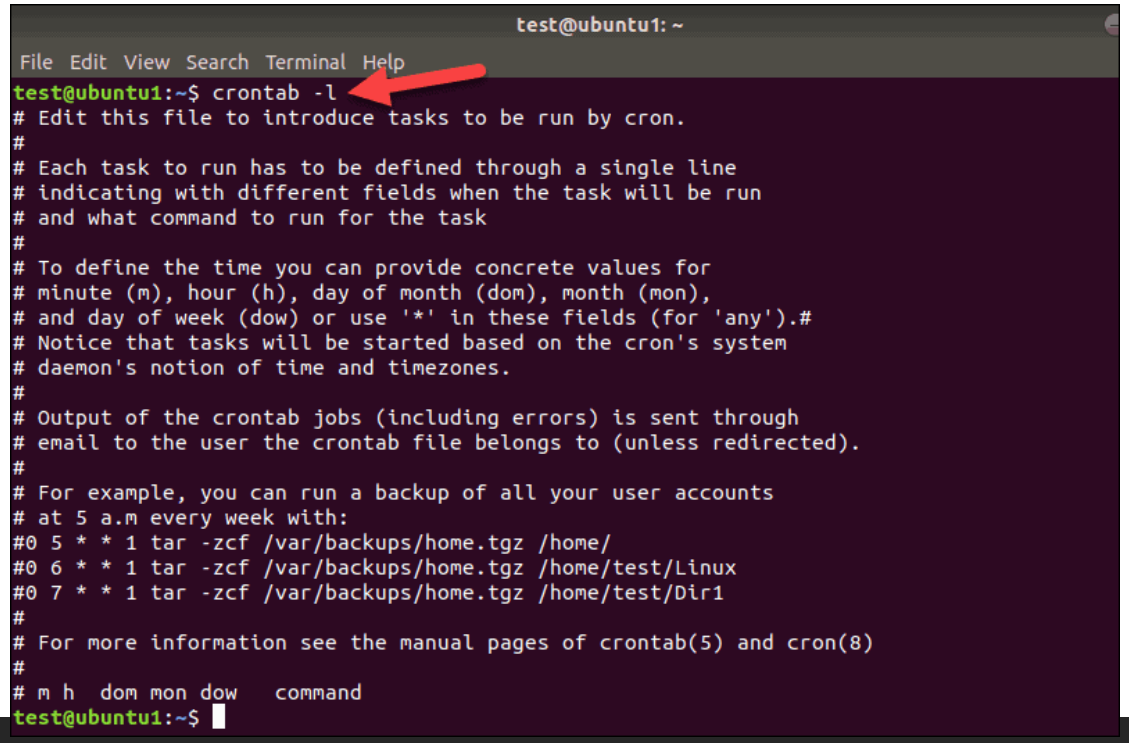
```
[root@server ~]# vi /etc/sysconfig/selinux   <- open the file
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing   <- Update the default value
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted

:wq   <- save the file
[root@server ~]# reboot -f   <- Restart the system
```

Cron Job Time Format

Send email to ShineIncareer team at everyday 5 PM (mail.sh)
CRON → TO RUN A SCRIPT AT A PARTICULAR TIME (crontab -e)

*** * * * * sh /apps/opt/mail.sh**
*** * 8-14,22-30 * ***

Edit the crontab File. crontab –e



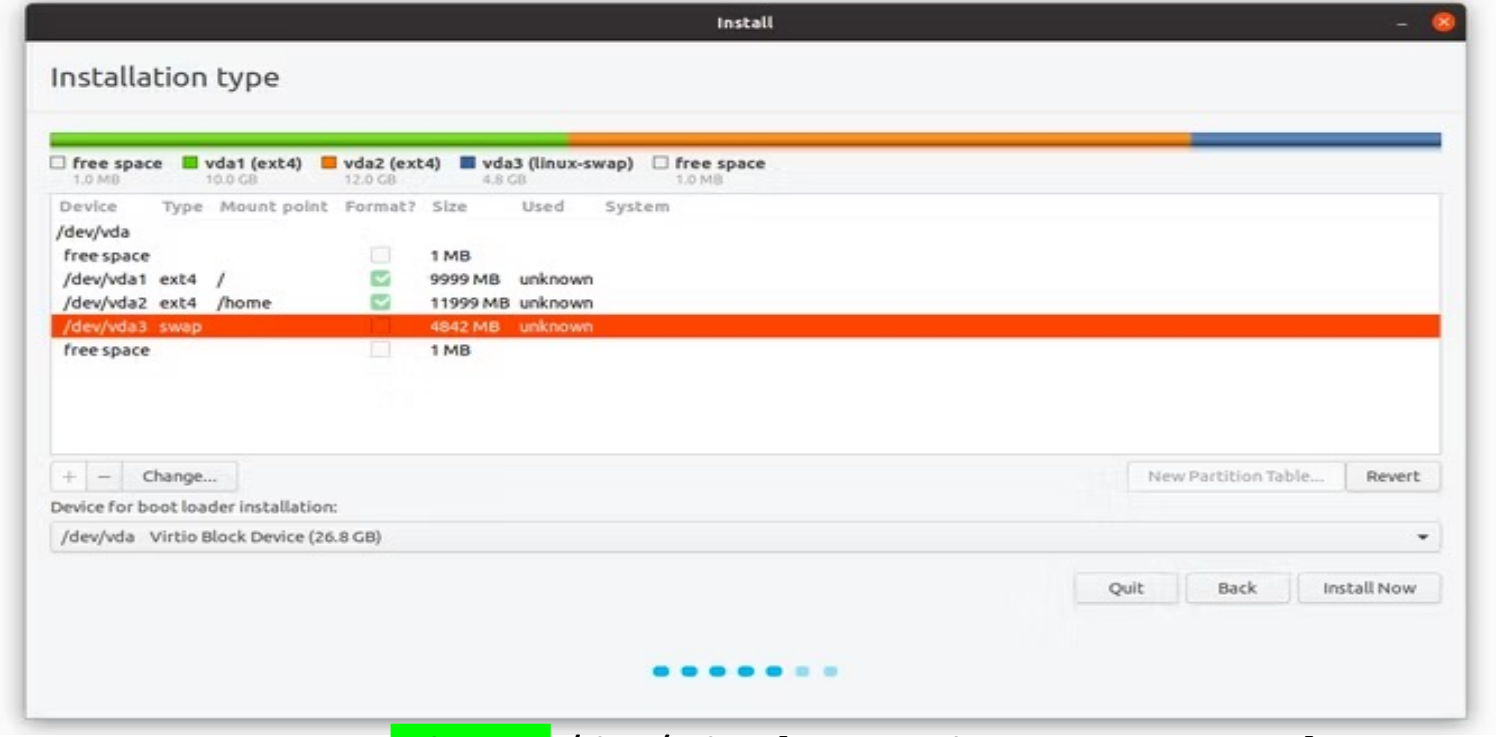

```
* * * * * command to be executed
- - - - -
| | | | |
| | | | ----- Day of week (0 - 7) (Sunday=0 or 7)
| | | ------- Month (1 - 12)
| | --------- Day of month (1 - 31)
| ----------- Hour (0 - 23)
------------- Minute (0 - 59)
```

Cron Job	Command
Run Cron Job Every Minute	** * * * * /root/backup.sh*
Run Cron Job Every 30 Minutes	*30 * * * * /root/backup.sh*
Run Cron Job Every Hour	*0 * * * */root/backup.sh*
Run Cron Job Every Day at Midnight	*0 0 * * * /root/backup.sh*
Run Cron Job at 2 am Every Day	*0 2 * * * /root/backup.sh*
Run Cron Job Every 1st of the Month	*0 0 1 * * /root/backup.sh*
Run Cron Job Every 15th of the Month	*0 0 15 * * /root/backup.sh*
Run Cron Job on December 1st – Midnight	*0 0 0 12 * /root/backup.sh*
Run Cron Job on Saturday at Midnight	*0 0 * * 6 /root/backup.sh*

SWAP PARTITION 82

The swap partition serves as overflow space for your RAM. If your RAM fills up completely, any additional applications will run off the swap partition rather than RAM.

Prioritization and Hibernation are the end goals for using the SWAP



Create a swap partition

fdisk /dev/vda

Press n [N for new]

+512 M

t –> For type of partition 82 number is for SWAP

w [quit]

partprobe /dev/vda3 [To let the kernel know about partition]

mkswap /dev/vda3 [To use the swap partition]

mount –a [To check for errors]

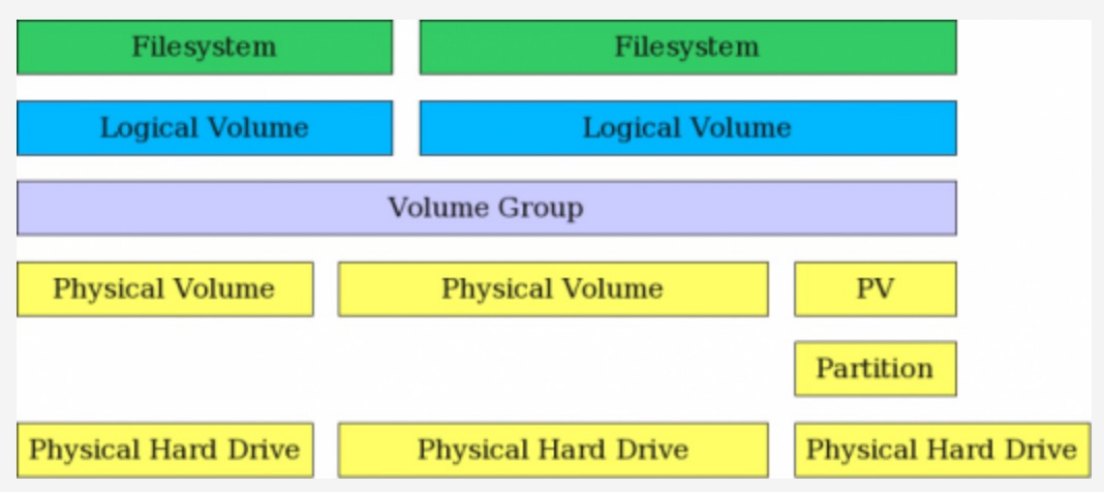
vi /etc/fstab [For permanent mount]

/dev/vda3 swap swap

swapon -s

Logical Volume Management. **********

Logical Volume Management enables the combining of multiple individual hard drives and/or disk partitions into a single volume group (VG). That volume group can then be subdivided into logical volumes (LV) or used as a single large volume.



1. Install a new hard disk drive

1 TB PHD.
+ 1 TB on LINUX

2. Designate Physical Volumes

pvcreate /dev/vda1

D PV1
E PV2
C PV3
F PV4

3. Manage Volume Groups

vgcreate vgname /dev/vda1

VG1

4. Manage Logical Volumes

The VG can be subdivided into one or more Logical Volumes (LVs).

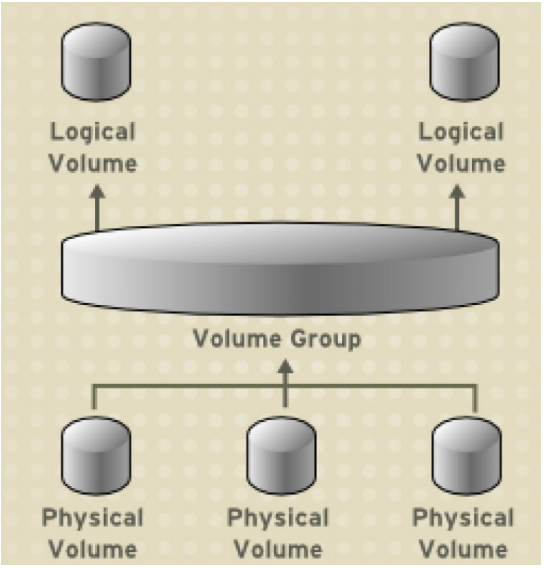
LV1
LV2
LV3

lvcreate -L size -n lvname vgname

LV%
LV^

lvcreate -L 10G -n shineincareer-lv vgname

```
[root@centos7_server ~]# fdisk -l

Disk /dev/vda: 85.9 GB, 85899345920 bytes, 167772160 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x0008ee47

   Device Boot      Start         End      Blocks   Id  System
/dev/vda1   *        2048     1026047      512000   83  Linux
/dev/vda2         1026048   167772159    83373056   8e  Linux LVM

Disk /dev/mapper/centos-root: 53.7 GB, 53687091200 bytes, 104857600 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/centos-swap: 4160 MB, 4160749568 bytes, 8126464 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/centos-home: 27.5 GB, 27455913984 bytes, 53624832 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/vdb: 107.4 GB, 107374182400 bytes, 209715200 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

[root@centos7_server ~]#
```

Logical volumes- 8e

fdisk /dev/vda
n

+500M

t → 8e

:wq

Reboot the VM

pvcreate /dev/vdb

vgcreate –s 16 test /dev/vdb

lvcreate –l 30 –n new test

Mkdir /mnt/storage

MAKE VFAT FILE SYSTEM

A virtual file allocation table (VFAT) is **an extension to the file allocation table (FAT) from Windows 95 and onward for creating, storing and managing files with long names**.

Mkfs.vfat /dev/test/new

Vim /etc/fstab

/dev/test/new /mnt/storage vfat

/dev/test/new

INSTAGRAM/TELEGRAM/TWITTER – SINGAM4DEVOPS

YOUTUBE/LINKEDIN - PRAVEEN SINGAMPALLI