```
================================================================================
================================
# 1. You will have two VMs with CLI as servera.lab.example.com &
serverb.lab.example.com (Minimal Server)
# 2. One of the VM's password need to reset that is
servera.lab.example.com
# 2. You need to break "root" password and then password as ablerate  on
servera.lab.example.com
# 3. You need to set "hostname" according to questions.
# 4. You Need to set static IP address/Netmask/Gateway/DNS  according to
questions.
================================================================================
================================
You need to fill the form with your name / address / email and  accept
Rules Agreement and than submit.

================================================================================
================================
Note: you will get 3 disks
1.  /dev/vda - OS Installed
2.  /dev/vdb - To create partition (Pre-created partitions available)
3.  /dev/vdc - for Stratis/VDO pool,filesystem and snapshots
================================================================================
================================

Your Exam is begin from here ......!

.............................Perform Task on servera.lab.example.com
machine.....................................

Question 1: Configure TCP/IP and "hostname" as follwing:


        IP ADDRESS      = 172.25.250.11
        NETMASK         = 255.255.255.0
        GATEWAY         = 172.25.250.254
        DNS                   = 172.25.250.254
        Hostname        = servera.lab.example.com

Solution: nmtui
           |_ edit a connection
                 |_ enter
                       |_ ipv4.method : manual
                       |_ ipv4 configuration : 172.25.250.11/24
                       |_ gateway : 172.25.250.254
                       |_ nameserver: 172.25.250.254
                                          |_ ok
                 |_ quit
           |_ activate a connection
                 |_ enter | enter *
                       |_ back
           |_ set hostname
                 |_ servera.lab.example.com
```

```
           quit

# vim /etc/selinux/config
SELINUX=enforcing

# reboot


--------------------------------------------------------------------------------
-------------------------------------------
Q.2 Configure Your servera VM repository installed the packages
distribution is available via YUM:
           baseos url =
http://classroom.example.com/content/rhel8.0/x86_64/dvd/BaseOS
       appstream url=
http://classroom.example.com/content/rhel8.0/x86_64/dvd/AppStream

solution:

# vim /etc/yum.repos.d/client.repo
[BaseOS]
name = base server
enabled = true
gpgcheck = false
baseurl = http://classroom.example.com/content/rhel8.0/x86_64/dvd/BaseOS
[AppStream]
name = app server
enabled = true
gpgcheck = false
baseurl =
http://classroom.example.com/content/rhel8.0/x86_64/dvd/AppStream

# yum repolist

--------------------------------------------------------------------------------
-------------------------------------------

Q.3 SELINUX PORT
      -  Your system httpd service having some issues service is not
running on port 82.
      - In your system httpd service have some files in /var/www/html (do
not change or alter files)
      - solve the port issue.

solution:
# systemctl status httpd
# semanage port -l | grep http
# semanage port -at http_port_t -p tcp 82
# firewall-cmd --permanent --add-port=82/tcp
# firewall-cmd --reload
# systemctl restart httpd
# curl http://localhost:82
```


Q.4 Create the following users, groups, and group membership:
- A group named sysadm.
- A user "harry" who belongs to sysadm as a secondary group.
- A user "natasha" who belongs to sysadm as a secondary group.
- A user "sarah" who does not have access to an interactive shell & who is not a member of sysadm group.
- "harry", "natasha", and "sarah" should all have the password of password.

solution:
```
# groupadd sysadm
# useradd harry -G sysadm
# useradd natasha -G sysadm
# useradd sarah -s /sbin/nologin
# echo harry:password | chpasswd
# echo natasha:password | chpasswd
# echo sarah:password | chpasswd

# su - harry
# su - natasha
# su - sarah
#
```


Q.5 create a collaborative directory /shared/sysadm with the following characteristics:

- Group ownership of /shared/sysadm is sysadm.
- The directory should be readable, writable, and accessible to member of sysadm, but not to any other user.
(It is understood that root has access to all files and directories on the system.)
- Files created in /shared/sysadm automatically have group ownership set to the sysadm group.

solution:
```
# mkdir -p /shared/sysadm
# chgrp sysadm /shared/sysadm
# chmod 2770 /shared/sysadm
# touch /shared/sysadm/file
# ll /shared/sysadm
```


Q.6 the user natasha must confire a cron job that runs daily at 5:30PM localtime and print hello message with logger.

solution:
```
# crontab -e -u natasha
42    14    *     *     *     logger -p user.info "hello"

# crontab -l -u natasha
# cat /var/log/messages
```

Q.7 Configure autofs to automount the home directories of netuserX user. Note the following:

- netuserX home directory is exported via NFS, which is available on classsroom.example.com:/home/netuserX (172.25.254.254) and your NFS-exports directory is /netdir for netuserX,
- netuserX's home directory is classroom.example.com:/home/netuserX , where X is your station number
- /rhome directory should be automounted autofs service.
- home directories must be writable by their users.
- password for netuser is ablerate.

solution:

```
# showmount -e classroom
# yum install autofs -y
# vim /etc/auto.misc
netuser2    -fstype=nfs workstation.lab.example.com:/netdir
# vim /etc/auto.master
/rhome     /etc/auto.misc
# systemctl restart autofs
# systemctl enable autofs
# cd /rhome/netuser2
```

Q 8

a. backup /usr/share director to /root/usr.tar.gz
b. backup /usr/share directory to /root/usr.tar.bz2
c. backup /usr/share directory to /root/usr.tar.xz

solution:

```
    tar czf  /root/usr.tar.gz     /usr/share
   tar cjf  /root/usr.tar.bz2      /usr/share
   tar cJf  /root/usr.tar.xz      /usr/share
```

Q.9 Copy the file /etc/fstab to /var/tmp. Configure the permissions of /var/tmp/fstab so that:

- the file /var/tmp/fstab is owned by the root user
- the file /var/tmp/fstab belong to the group root
- the file /var/tmp/fstab should not be executable by anyone
- the user "natasha" is able to read and write /var/tmp/fstab
- the user "harry" can neither write nor read /var/tmp/fstab
- all other users (current or future) have the ability to read /var/tmp/fstab

solution:

```
[root@servera ~]# setfacl -m u:natasha:rw /var/tmp/fstab
[root@servera ~]# setfacl -m u:harry:--- /var/tmp/fstab
```

```
[root@servera ~]# setfacl -m o::r- /var/tmp/fstab
[root@servera ~]# getfacl /var/tmp/fstab
```

Q.10 Configure your system to syncronize the time from form "classroom.example.com".

Solution :

```
[root@servera ~]# vim /etc/chrony.conf
server classroom.example.com iburst
[root@servera ~]# systemctl restart chronyd
[root@servera ~]# timedatectl
```

Q.11 Find all files and directories which is created by a user "natasha" in to this system and copy it into a "/root/natasha.found" directory.

Solution:

```
[root@servera ~]# mkdir /root/natasha.found
[root@servera ~]# find / -user natasha -exec cp -rfp {}
/root/natasha.found/ \;
[root@servera ~]# ll -a /root/natasha.found
```

Q.12 Find all strings "ich" from "/usr/share/dict/words" file and copy that strings in a /root/lines file.

Solution:

```
[root@servera ~]#  grep -i "ich" /usr/share/dict/words >  /root/lines
[root@servera ~]# grep -i 'ich' /root/lines
```

Q.13 Create a user "unilao" with UID "2334" with password as "ablerate".

Solution:

```
[root@servera ~]#  useradd -u 2334 unilao
[root@servera ~]#  passwd unilao
ablerate
ablerate
```

```
# reboot [servera]
```

.....

serverb.lab.example.com

.....

Question 1: Set "root" password to "ablerate"

> reboot
> press 'tab' to pause menu entry
> press 'e' to edit kernel
> goto line 'linux' press 'end' key , then type
console=tty1 rd.break

```
> ctrl x

> mount -o remount,rw /sysroot
> chroot /sysroot
> passwd root
ablerate
ablerate
> touch /.autorelabel
> ctrl d
> ctrl d
```

Q.14 Configure Your serverb VM repository installed the packages distribution is available via YUM:
baseos url = http://classroom.example.com/content/rhel8.0/x86_64/dvd/BaseOS
appstream url= http://classroom.example.com/content/rhel8.0/x86_64/dvd/AppStream
Solution:

```
[root@servera ~]#  vim /etc/yum.repos.d/client.repo
[BaseOS]
name = base server
enabled = true
gpgcheck = false
baseurl = http://classroom.example.com/content/rhel8.0/x86_64/dvd/BaseOS
[AppStream]
name = app server
enabled = true
gpgcheck = false
baseurl =
http://classroom.example.com/content/rhel8.0/x86_64/dvd/AppStream


[root@servera ~]# yum repolist
```

Q.15 Create an LVM name wshare from wgroup volume group. Note the following:
- PE size should be 8MB
- LVM size should be 70 extents
- Format with "vfat" file system and mount it under /mnt/wshare.

And it should auto mount after next reboot

```
# fdisk /dev/vdb
# n
# enter | enter | last sector : +1G
# t
# 3
# 8e
# w

# pvcreate /dev/vdb3
# vgcreate -s  8M  wgroup /dev/vdb3
```

```
# lvcreate -l 70 -n wshare wgroup
# mkfs.vfat /dev/wgroup/wshare
# mdkir /mnt/wshare
# vim /etc/fstab
/dev/wgroup/wshare /mnt/wshare  vfat   defaults 0 0
# mount -a
# df -h
# reboot
```

Q.16 Create a swap partition of 400 MB and make it available permanent.

Q.17 Resize your existing "vo" logical volume, it should be approx 300MB(note -> only size accepted from 290mb to 310mb).

```
# lvs
                 # vo  : 200M
#  lvextend -L +100M /dev/vg/vo
# df   -Th
# xfs_growfs     /mnt/vo                # xfs
or
# resize2fs /mnt/vo                # ext3,2
# df  -Th
```

Q.18 Configure Stratis as following
- create stratis pool
- create filesystem
- take snapshot

or

Q.18 create the VDO volume vdo1 and set logical size to 50GB
mount the volume vdo1 on /mnt/vdo1 with the xfs file system so that it persists across reboots.

Solution:

```
   vdo create --name vdo1  --vdoLogicalSize 50G --device /dev/vdc
   mkdir /mnt/vdo1
   mkfs.xfs -K /dev/mappper/vdo1
   vim /etc/fstab
   /dev/mapper/vdo1   /mnt/vdo1   xfs d efaults,x-
systemd.requires=vdo.service 0 0
  # mount -a
  # df -h

  # reboot
```

Q 19 . Configure recommended tuned profile

```
# tuned-adm recommend
# tuned-adm profile virtual-guest
# tuned-adm active
```

20. Configure a container to start automatically.

- Create a container named logserver using the rsyslog image that is available from your registry.
- Configure it to run as a systemd service that should run from the existing user blackhorse only.

Solution

```
    1 podman images
    3  podman ps
    4  mkdir ~/.config/containers
    5  cp /etc/containers/registries.conf .config/containers/
    6  podman search ubi
    7  podman login registry.redhat.io
    2  podman run -d --name logserver rsyslog
    8  podman ps
    9  mkdir -p ~/.config/systemd/user
   10  cd ~/.config/systemd/user
   15  podman generate systemd --name logserver --files --new
   16  podman ps
   17  podman stop logserver
   18  podman rm logserver
   20  systemctl --user daemon-reload
   21  systemctl --user enable --now container-logserver
   22  podman ps
   24  systemctl --user stop container-logserver
   25  podman ps
   26  systemctl --user start container-logserver
   27  podman ps
   28  loginctl enable-linger blackhorse
   29  loginctl show-user blackhorse
```

21. Extend the service from previous task in this way
- Configure the host system journal to preserve its data after reboot and restart the logging service.
- Copy all *.journal files from the host /var/log/journal directory and subdirectories into the directory /home/blackhorse/container_journal.
- Configure the service to automatically mount the directory /home/blackhorse/container_journal under /var/log/journal on the container when it starts.

Solution:

```
    1  # mkdir /var/log/journal
    2  # chown root:systemd-journald /var/log/journal
    3  # vim /etc/systemd/journald.conf
    4  # [journal]
    5  # storage=persistent
    6  # systemctl restart systemd-journald
    7  # systemctl enable systemd-journald
    8  # reboot
    9  cp -rfp
/var/log/journal/499c2280d57f44e29f3cd55514af59f7/*.journal
/home/blackhorse/container_journal
   10  cd .config/systemd/user/
```

```
   11  podman run -d --name journal -v
/home/blackhorse/container_journal:/var/log/journal:Z rsyslog
   12  podman ps
   13  podman generate systemd --name journal --files --new
   14  ls
   15  podman stop journal
   16  podman rm journal
   17  podman ps
   18  systemctl --user daemon-reload
   19  systemctl --user enable container-journal
   20  podman ps
   21  systemctl --user start container-journal
   22  podman ps

$ loginctl enable-linger
$ loginctl show-user xanadu
```