RHCSA EXAM-200 DUMPS QUESTION & SOLUTION

Setup an Ip address for node1 virtual machine

hostname: nodea.lab.example.com or localhost.localdomain
Password: redhat
IP: 172.25.250.10/24
GW: 172.25.250.254
DNS: 172.25.250.254
NB: All partition should be created on /dev/vdb

00 Password Break >>>>
Method -01: Send key >> Clrt + Alt + Delete>> for reboot vm server

```
#vim /etc/default/grub/
        GRUB_TIMEOUT=10
        :wq!
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

reboot >> up Arrow button for freez >> linux.... >>>> press end button or cltr+e >>
rd.break console=tty1 rw >>> cltr+x
chroot /sysroot/
passwd or echo "redhat" | passwd --stdin root
man selinux >>Show details
touch /.autorelabel
exit
exit OR cltr+d

Method -02:
Linux >> rw init=/bin/bash >>> cltr+x [mount -o remount,rw / >> rw dite vule gele]
[# ls # cat /etc/mtab]
passwd or echo "redhat" | passwd root --stdin
man selinux >> Show details
touch /.autorelabel
/usr/sbin/reboot -f

00 Network Configuration >>>
hostnamectl hostname node2.lab.example.com
Or # hostnamectl set-hostname node2.lab.example.com

ifconfig or ip a s [To check your physical or virtual interface name: here is: eth0 /ens160]
lsattr /etc/resolv.conf
chattr -i /etc/resolv.conf
nmcli connection show
namcli connection delete "Wired connection 1"
nmcli connection add con-name lan1 ifname eth0 type ethernet ipv4.method manual ipv4.addresses 172.25.250.11/24 ipv4.gateway 172.25.250.254 ipv4.dns 172.25.250.254 autoconnect yes
nmcli connection up lan1
nmcli device show

chattr +i /etc/resolv.conf
lsattr /etc/resolv.conf
====Extra==========
yum whatprovides ifconfig
ifconfig or # ip a x or ip a s
route - n [show getway]
cat /resolv.conf [dns]
[# man chattr
chattr +i alex [add attrivute imuateble]
ll
chattr -i alex
cat /etc/resolv.conf]
yum whatprovides nmcli

01: SElinux Must be Running in Enable.

Ans: # getenforce
# setenforce 1 or # setenforce 0 [To change the selinux policy on runtime. So, you should change the config file]
# vim /etc/selinux/config
selinux=enforcing
To change the sestatus from config file then reboot your system.

02: Yum repository configuration on node1 machine:
Packages are available at: url1= http://content.example.com/rhel8.0/x86_64/dvd/AppStream/
Packages are available at: url2= http://content.example.com/rhel8.0/x86_64/dvd/BaseOS/

Ans: #vim /etc/yum.repos.d/appstream.repo
[appstream_any_name_you_can_assign_but_no_space_here]
name=any name or if specify any name in the exam
baseurl=http://content.example.com/rhel8.0/x86_64/dvd/BaseOS/
gpgcheck=0
Test: #yum clean all #yum repolist all
##BaseOS is same:

03: Configure a cron job on Primary machine:
a. The user natasha must configure a cron job that runs daily at 14:23 local time & executes /bin/echo "hi alex"

Ans: cronie package is already installed in the exam if doesn't install you have to installed.
userdd natasha
#passwd natasha >>> redhat
yum install cronie
systemctl enable crond
systemctl start crond
crontab -eu natasha
23 14 * * * /bin/echo "hi alex" [For live demo # 23 14 * * * echo "hi Aleex" >> test.txt]
verification: crontab -u -l natasha or tail -f /var/spool/cron/natasha
watch ls # tail -f test.txt #tail -f /var/log/cron

b. The user harry must configure a cron job that runs daily at every 3-minute local time & executes /bin/echo I got RHCSA Certificate.
Ans: #useradd harry
passwd harry >> redhat
crontab -eu harry
*/3 * * * * /bin/echo "I got RHCSA Certificate."
cd /var/spool/cron/ */20
cat natasha harry

11: Deny cronjob for user susan so that other user for this system is not affected for this cronjob.

Ans: # useradd susan
vim /etc/cron.deny
susan
:wq!
#cat /etc/cron.deny
#su susan #crontab -e #crontab -l [for validation]

04: Debug Selinux:
Fixed the HTTP service, the page isn't provived nodea machine by this link=http://172.25.250.10:82 | SELinux must be running in the Enforcing mode.

[Note: first you install HTTP service on node1 machine & configure the Main Configuration File: /etc/httpd/conf/httpd.conf
Now, set the Listen port is:2658. 2nd step:Create a file name index.html to Document Root: /var/www/html & write it to "I got RHCSA Certificate."]

Ans: # yum install httpd
systemctl enable httpd
systemctl restart httpd

vim /etc/httpd/conf/httpd.conf
listen on 2658

vim /var/www/html/index.html
I got RHCSA Certificate.

This part is already done in the exam & document root is aslo set.
Frist you check the service is running or not, # systemctl status httpd
or you can restart the service. Then it's show [journalctl -xe]

journalctl -xe [you can check the log.]
semanage port -l | grep http [Check the port is here or not.] [iF command not working >> # yum install policycoreutils* -y]
man semanage port [For manual to see the example & simply copy the example & change the port no:]
semanage port -a -t http_port_t -p tcp 2658
curl http://172.25.250.10:2658 [first check it servera or nodea]

Then check it from serverb or nodeb if you can't found the page then check firewall.

firewall-cmd --list-all
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-port=2658/tcp
firewall-cmd --reload
systemctl restart httpd
#curl http://172.25.250.10:2658

05: Create the following users, groups, and group memberships:
- A group named sysadmin
- A user natasha who belongs to sysadmin as a secondary group.
- A user sarah who also belongs to sysadmin as a secondary group.
- A user harry who does not have access to an interactive shell on the system & who is not a member of sysadmin. natasha, sarah & harry should all have the password of password.

Ans: A group named sysadmin
groupadd sysadmin
cat /etc/group | grep sysadmin
A user natasha who belongs to sysadmin as a secondary group.
useradd natasha
usermod -aG sysadmin natasha
Or # useradd natasha -G sysadmin
A user sarah who also belongs to sysadmin as a secondary group.
useradd sarah
usermod -aG sysadmin sarah (-G = Second Group, -g = Primary)
A user harry who does not have access to an interactive shell on the system & who is not a member of sysadmin.
Or # useradd sarah -G sysadmin
usermod -s /sbin/nologin harry
Or # useradd harry -s /sbin/nologin
natasha, sarah & harry should all have the password of password.
passwd sarah
passwd harry
passwd natasha
Or # # echo password | passwd --stdin natasha

06: Create a collaborative directory "/common/admin" with the following characteristics:
- Group ownership of "/common/admin/" is sysadmin.
- The directory should be readable, writable & accessible to members of sysadmin, but not to any other users. (It is understood that root has access to all files & directories on the system.)
- Files created in "/common/admin/" automatically have group ownership set to the sysadmin.

Ans: # mkdir /common/admin -p
Group ownership of "/common/admin/" is sysadmin.
chgrp sysadmin /common/admin
The directory should be readable, writable & accessible to members of sysadmin, but not to any other users. (It is understood that root has access to all files & directories on the system.)
Files created in "/common/admin/" automatically have group ownership set to the sysadmin.
chmod 2770 /common/admin

or
chmod o-rwx /common/admin/
chmod g+s /common/admin/
verification: # getfacl /common/admin/
ls -ld /com mon/admin
#touch /common/admin/file1.txt
ls -ltr /common/admin/file1.txt [check details]
[Will file be create in /common/admin??]

07: Configure ACL Permission:
Copy the file "/etc/passwd" to "/var/tmp". Configure the permissions of "/var/tmp /passwd" so that:
- The file "/var/tmp/passwd" is owned by the root user.
- The file "/var/tmp/passwd" belong to the group root.
- The file "/var/tmp/passwd" should not be executable by anyone.
- The user harry is able to read and write "var/tmp/passwd". [ACL]
- The user sarah can neither write nor read "/var/tmp/passwd".
[Note that: all other users (current or future) have the ability to read "/var/tmp/passwd".]

Ans: #cp /etc/passwd /var/tmp
The file "/var/tmp/passwd" is owned by the root user.
The file "/var/tmp/passwd" belong to the group root.
The file "/var/tmp/passwd" should not be executable by anyone.
getfacl /var/tmp/passwd
The user harry is able to read and write "var/tmp/passwd". [ACL]
setfacl -m u:harry:rw- /var/tmp/passwd
The user sarah can neither write nor read "/var/tmp/passwd". [Note that: all other users (current or future) have the ability to read "/var/tmp/passwd".]
setfacl -m u:sarah:--- /var/tmp/passwd
verification: #getfacl /var/tmp/passwd
08: Syncronise your system time with the classroom.example.com or Configure NTP in your system so that it is an NTP client of 3.in.pool.ntp.org

Ans: #yum install chrony -y
vim /etc/chrony.conf
server classroom.example.com iburst
systemctl restart chronyd
systemctl enable chronyd
verification: # chronyc tracking
or # chronyc sources -v # timedatectl status

09. Configure AutoFS.
All remote users home directory is exported via NFS, which is available on workstation.lab.example.com or 172.25.250.9 and your NFS-exports directory is /home/guests/ for remote5.
- Remote home directory is workstation.lab.example.com:/home/guests/
- Remote home directory should be automount autofs service.
- Home directories must be writable by their users.
-when you are able to log in as remote5 user it's found home directory as /home/guests/remote5.
- Ensure that remote5 user can read, write on his home directory but remote10 only can read privileges.

Ans-1: **Server Part**

```
# yum install nfs-utils -y
# systemctl start nfs-server.service
# systemctl enable nfs-server.service

# mkdir /home/guests/ [-p]
# useradd -u 2001 remote5 -d /home/guests/remote5
# echo "redhat" | passwd --stdin remote5
# useradd -u 2002 remote10 -d /home/guests/remote10
# echo "redhat" | passwd --stdin remote10

# vim /etc/exports
/home/guests/remote5 192.168.194.0/24(rw,sync)
/home/guests/remote5 192.168.194.0/24(rw,sync)

# systemctl restart nfs-server.service

# firewall-cmd --permanent --add-service={nfs,rpc-bind,mountd}
# firewall-cmd --reload

# chmod 777 /home/guests/
# setfacl -R -m u:nobody:rwx /home/guests/
# setfacl -m u:remote5:rwx /home/guests/remote5

# exportfs -avr
[Verify]
# su - remote5 >> df -hT >> touch file.txt >> ls
```

Client Part

```
# yum install autofs -y
# systemctl enable autofs.service
# systemctl restart autofs.service

# showmount -e 192.168.194.131

# vim /etc/auto.master.d/nfs.atuofs
/-        /etc/auto.master.d/nfs.txt

# vim /etc/nfs.txt
/remoteuser     -rw,sync         192.168.194.131:/home/guests/

# systemctl restart autofs
[Verify]
# cd /remoteuser/remote5 >> df -hT >> touch file.txt  >> ls
```

Ans-2: SERVERA OR NODEA

```
# yum install nfs-utils -y                    [package is already installed]
# systemctl status nfs-server.service         [start & enable]
```

```
# mkdir /ourhome/nfsuser -p
# cd /ourhome/nfsuser
# mkdir user1
# touch user.txt
# vim /etc/exports
/ourhome/nfsuser        172.25.250.0/24(rw,sync)

# systemctl restart nfs-server.service
Or # exportfs -avr

# showmount -e
# setfacl -m u:nobody:rwx /ourhome/nfsuser [cat /etc/passwd | grep nobody >> show ID]
# firewall-cmd --permanent --add-service={nfs,mountd,rpc-bind}
# firewall-cmd –reload

Or [# firewall-cmd --permanent --add-service=nfs
# firewall-cmd --permanent --add-service=mountd
# firewall-cmd --permanent --add-service=rpc-bind
# firewall-cmd –reload]

SERVERB OR NODEB
# rpm -qa autofs
# yum install autofs -y
[# mkdir /data >> if needed]

Edit the Master map file (/etc/auto.master.d):
First method:   # vim /etc/auto.master.d/nfs.autofs
/data     /etc/auto.master.d/user

# vim /etc/auto.master.d/user
remoteuser      172.25.250.10:/ourhome/nfsuser

Second method:
# vim /etc/auto.master.d/nfs.autofs
/-          /etc/auto.master.d/user

# vim /etc/auto.master.d/user
/data     172.25.250.10:/ourhome/nfsuser
Or /data  -fstype=nfs,rw,sync 172.25.250.10:/ourhome/nfsuser
# systemctl restart autofs.service
# df -HT
```

NOTE: ##Direct map support >> Direct maps in autofs provide a mechanism to automatically mount file systems at arbitrary points in the file system hierarchy. A direct map is denoted by a mount point of /- in the master map. Entries in a direct map contain an absolute path name as a key (instead of the relative path names used in indirect maps).

##Multiple master map entries per autofs mount point. One thing that is frequently used but not yet mentioned is the handling of multiple master map entries for the direct mount point /-. The map keys for each entry are merged and behave as one map

10: Create a backup.tar.(bz2 and gz) of /etc directory in /home location.

Ans: # tar -cvjf /home/backup.tar.bz2 /etc
file /home/backup.tar.bz2

tar -cvzf /home/backup.tar.gz /etc
file /home/backup.tar.gz

12: Find all files owned by user brain and put them into /root/brain.

Ans: # useradd brain
echo “redhat” | passwd brain –stdin
mkdir /root/brain
find / -user brain -exec cp -av {} /root/brain \;
cd /root/brain/
ll >> ll -al
[# find / -user brain -exec cp -frvp {} /root/brain/ \;]

13: Download a file word.dict from http://content.example.com & put it to "/root". Copy all the lines from /root/word.dict files that contains the word "mail" and put those lines in /root/sorted.dict

Ans: # cd /root
wget http://classroom.example.com/content/word.dict
grep “mail” /root/word.dict > /root/sorted.dict
cat /root/sorted.dict [for check]

[Or # wget -O /root/word.dict http://classroom.example.com/content/word.dict

grep mail word.dict > /root/sorted.dict]

NodeB

0: First crack password of node2 Machine & set it to the instruction is above instructions:

Setup an ip address for node2 virtual machine:

hostname: node2.lab.example.c om
Password: TombigSmall
IP: 172.25.250.11/24
GW: 172.25.250.254
DNS: 172.25.250.254

Ans: #reboot the vm. press ESC then select boot loader, press 'e' to enter grub mode.
then type: rd.break console=tty1 rw
Press Ctrl + x to start:
chroot /sysroot/
passwd root
give the password and re-type it.
touch /.autorelabel

exit
exit [To logout.]

if we mount readonly then we can use this:
switch_root:/# mount -o remount,rw /sysroot/
switch_root:/# chroot /sysroot

FILE LABELING
All files, directories, devices ... have a security context/label associated with them. These contexts are stored in the extended attributes of the file system. Problems with SELinux often arise from the file system being mislabeled. This can be caused by booting the machine with a non SELinux kernel. If you see an error message containing file_t, that is usually a good indicator that you have a serious problem with file system labeling. The best way to relabel the file system is to create the flag file /.autorelabel and reboot. system-config-selinux, also has this capability. The restorecon/fixfiles commands are also available for relabeling files.

Network connection:
hostnamectl set-hostname node2.lab.example.com

ifconfig or ip a s [To check your physical or virtual interface name: here is: enp1s0]
nmcli connection show
nmcli connection add con-name lan1 ifname enp2s0 type ethernet ipv4.method manual ipv4.addresses 172.25.250.11/24 ipv4.gateway 172.25.250.254 ipv4.dns 172.25.250.254 autoconnect yes
nmcli connection up lan1

or, we can create a new config file or modify existing config file
vim /etc/sysconfig/network-scripts/ifcfg-lan1

01: SElinux Must be Running in Enable.

02: Yum repository configuration on node1 machine:
Packages are available at: url1= http://content.example.com/rhel8.0/x86_64/dvd/AppStream/
Packages are available at: url2= http://content.example.com/rhel8.0/x86_64/dvd/BaseOS/

03: Set a recommended tuning profile for your system. (Profile already available).

Ans: # rpm -qa tuned to check package is installed or not.
yum install tuned -y
systemctl start tuned.service
systemctl enable tuned.service
tuned-adm active [To see the active profile]
tuned-adm list [check how many profiles are available]
tuned-adm recommend [check which profile recommend to your system]
tuned-adm profile virtual-guest [set the profile]
tuned-adm active [To see the active profile]

04: Create a SWAP partition of 250 megabyte & make available at next reboot.

Ans: # fdisk /dev/vdb

Hex code (type L to list all codes): 82

Changed type of partition 'Linux' to 'Linux swap / Solaris'.
lsblk
fdisk -l
partprobe [To update partition table. if the partition shows # fdisk -l comman but not # lsblk then we can use # partprobe or just reboot the system.]
mkswap /dev/vdb1
blkid
/dev/vdb1: UUID="b2337e16-691e-4a2a-92d1-35d5c1be3f18" TYPE="swap" PARTUUID="d8f3c21a-01"
# vim /etc/fstab
UUID="b2337e16-691e-4a2a-92d1-35d5c1be3f18" swap swap defaults 0 0
# swapon -av
verification: # swapon -s # free -h

05: Create the volume group with name myvolume with 8MiB P.E. and create the lvm name mydatabase with the 100P.E. format this lvm with ext4 and create a directory /database & mount this lvm permanently on /database.

Ans: # fdisk /dev/vdb
Last sector, +sectors or +size{K,M,G,T,P} (514048-10485759, default 10485759): +850M
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'.
lsblk
fdisk -l
pvcreate /dev/vdb2
Physical volume "/dev/vdb2" successfully created.
pvdisplay or, # pvs

vgcreate myvolume -s 8M /dev/vdb2
Volume group "myvolume" successfully created
vgdisplay or, # vgs

lvcreate -n mydatabase -l 100 myvolume
lvdisplay or, lvs

mkfs.ext4 /dev/myvolume/mydatabase or, # mkfs.ext4 /dev/mapper/myvolume-mydatabase
blkid
/dev/mapper/myvolume-mydatabase: UUID="a747660c-8d14-4943-a227-a1320a31e943" TYPE="ext4"

# vim /etc/fstab +
UUID="a747660c-8d14-4943-a227-a1320a31e943" /database ext4 defaults 0 0

mkdir /database
mount -av

06: Extend or Resize the LVM partition /dev/myvolume/mydatabase into 500 MiB from the current size and mount the LVM /dev/myvolume/mydatabase to a mount point /database. The extended partition size must be within approximately 450MiB to 550MiB.

Ans: # lvresize -r -L 500M /dev/myvolume/mydatabase
df -HT

07: You have been provided with a disk drive attached to your system /dev/vdX. Make use of it to create a VDO. VDO device name is myvdo1 with a logical size of 100GiB & format this vdo storage as xfs & create a mount point /vdostorage & mount it permanently.

Ans: Step 1: Install the VDO in RHEL 8:
rpm -qa vdo kmod-kvdo
yum install kmod-kvdo vdo
systemctl restart vdo.service
systemctl enable vdo.service

Step 2: Create a VDO Volume in RHEL 8:
man vdo [to see the manual simply copy an example] # vdo create --name=vdo0 --device=/dev/sdb1 --vdoLogicalSize=10T
lsblk
vdo create --name=myvdo1 --device=/dev/vdb --vdoLogicalSize=100G

>> create --This initiates the creation of the VDO volume.
>> --name=myvdo1 --This gives the volume a label known as myvdo1.
>> --device=/dev/sdX --The device option specifies the disk on which the volume will be created.
>> --vdoLogicalSize=100G --This indicates the effective volume capacity to be used by the operating system, in this case, 100G.
blkid
/dev/vdb: UUID="9a19fe3d-0000-442b-aea9-840be34f22bb" TYPE="vdo"
lsblk
fdisk /dev/mapper/myvdo1

lsblk
fdisk -l
fdisk -l /dev/mapper/myvdo1
/dev/mapper/myvdo1-part1 256 26214399 26214144 100G 83 Linux

mkfs.xfs /dev/mapper/myvdo1 -K -f
blkid
/dev/mapper/myvdo1: UUID="5f4fbb6e-9f31-4b66-b6c3-c87df039db7f" TYPE="xfs"
/dev/vdb: UUID="9a19fe3d-0000-442b-aea9-840be34f22bb" TYPE="vdo"

# vim /etc/fstab
UUID="5f4fbb6e-9f31-4b66-b6c3-c87df039db7f" /vdostorage xfs defaults,x-systemd.requires=vdo.service 0 0

mkdir /vdostorage

mount -av
NOTE: ##Usually, when a filesystem is created, a trim operation is carried out on the device. This is undesirable in the case of the VDO. When formating using the mkfs command, use the -K option to instruct the command not to discard blocks during the creation to the filesystem.

ls -l /dev/mapper/myvdo1 [We can use the ls command as shown to investigate file permissions & ownership.]

vdostats --hu [vdostats command to retrieve statistics on the size and the usage of the volume.]
vdostats --verbose /dev/mapper/myvdo1 | grep -B6 'saving percent'
>>The vdostats command can be used with the --verbose flag to retrieve more detailed information as shown.

08: Configure the rhcsa application so that when run as "pandora" it shows below message "Labla lbal lahs ksbhs".

Ans: # vim /etc/bashrc
```
pandora ()
{
        (echo "Labla lbal lahs ksbhs")
}
```
save & exit
source /etc/bashrc
pandora

Or # vim /usr/bin/pandora
```
        #!/bin/bash
        echo "Labla lbal lahs ksbhs"
        :wq!
```
chmod +x /usr/bin/pandora
pandora

Or # useradd alex
su – alex
vim .bashrc
```
        Pandora()
        {
                echo "Labla lbal lahs ksbhs"
        }
        :wq!
```
source .bashrc
pandora

09: Customize user environment:

- Create a command called starton on your server.
- It should able to execute the following command (ps -eo pid,tid,class,rtprio,ni,pri,psr,pcpu, stat, comm).

Ans: # vim /etc/bashr
```
starton ()
{
```

```
        (ps -eo pid,tid,class,rtprio,ni,pri,psr,pcpu,stat,comm)
};
# source /etc/bashrc    [Reload file]
# starton
-----------------------------------------------
Or # vim /bin/bash/starton
        #!/bin/bash
        (ps -eo pid,tid,class,rtprio,ni,pri,psr,pcpu,stat,comm)
        :wq!
# chmod a+x /bin/bash/starton
# starton
-----------------------------------------------
Or # su – alex
# vim .bashrc
        Starton()
        {
                (ps -eo pid,tid,class,rtprio,ni,pri,psr,pcpu,stat,comm)
        }
        :wq!
# source .bashrc
# starton
```

10: Configure your system so that; All the new user's password will be valid of maximum 30 days. But all the previous user will be default days.

Ans: # vim /etc/login.defs
PASS_MAX_DAYS 30
:wq!
useradd new
chage -l new

11: Container / Docker:
A. Build image [NAME pdfconvert] from those url = https://content.example.com/container/Containerfile | - Run a container named monitor using the newly created image.

B. Create a container using the image pdfconvert which have been created in question no:1. Run container named pdfconverter. Attche the volume /opt/input/ and /opt/processed/ with container /action/incoming/ and /action/outgoing/ respectively.
- Create a service container-pdfconverter.service
Ensure that container-pdfconverter.service will run automatically at system boot

Ans: Root User >>
[yum install wget -y]
yum install podman -y
systemctl start podman
systemctl enable podmanq
systemctl status podman.service
useradd alex
passwd alex or echo "redhat" | passwd --stdin alex
loginctl enable-linger alex

loginctl show-user alex

[Question 2 start here]
---
mkdir /opt/input -p
mkdir /opt/processsed -p
setfacl -m u:alex:rwx /opt/input/
setfacl -m u:alex:rwx /opt/processsed/
man semanage fcontext
semanage fcontext -a -t container_file_t "/opt/input(/.*)?"
semanage fcontext -a -t container_file_t "/opt/processed(/.*)?"
restorecon -Rv /opt/processed
restorecon -Rv /opt/input

Alex user or local user >>>
ssh alex@localhost
wget https://content.example.com/container/Containerfile
----------OR----------
vim Containerfile
FROM docker.io/openviewdev/pdfconverter
:wq!
systemctl restart podman.service [For root end]
---
podman build . -t pdfconvert -f Containerfile [podman build . -t <demo or imagename> -f <File name>]
podman images
podman run -dit --name monitor localhost/pdfconvert:latest
podman ps
podman exec -it monitor /bin/bash
exit

[Question 2 start here]
---
podman run -dit --name pdfconverter -v /opt/input/:/action/incoming/ -v /opt/processed/:/action/outgoing/ localhost/pdfconvert:latest
podman ps
mkdir .config/systemd/user -p
cd .config/systemd/user/
ls
podman generate systemd pdfconverter -f -n
ls
systemctl --user daemon-reload
systemctl --user start container-pdfconverter.service
systemctl --user enable container-pdfconverter.service
systemctl --user status container-pdfconverter.service
podman ps
reboot
[For Verify]
systemctl --user stop container-pdfconverter.service
systemctl --user status container-pdfconverter.service

Delete Container | If Needed
---
podman rmi -a -f
podman ps
podman images

xx. Create a container logserver from an image rsyslog in nodeb from: registry.lab.example.com
- Configure the container with systemd services by an existing user "Walhalla".
- Service name should be container-logserver and configure it to start automatically across reboot.

xx.Configure your host journal to store all journal across reboot.
- Copy all *.journal from /var/log/journal and all subdirectories to /home/Walhalla/container _logserver.
- Configure automount /var/log/journal from logserver (container) to /home/walhalla/container _logserver. when container starts.