RHEL 7 : PRACTICE PAPERS FOR RHCSA & RHCE EXAM

With Answers

PAWAN BAHUGUNA

Table of Contents

Red Hat® Enterprise Linux 7

Practice Papers for RHCSA (EX200) and RHCE (EX300) Exam

V.1.1

By Pawan Bahuguna

This book is dedicated to all RHCSA & RHCE aspirants who want to make their career in Linux System Administration.

PREFACE

If you have purchased this book, you must be aware that Red Hat has now started taking the exam on its latest release Red Hat Enterprise Linux version 7 through certification Exams **EX200 (RHCSA)** and **EX300 (RHCE)**. This is completely performance based exam and no objective questions are there to judge your knowledge and administration skills.

You must prove you have ability to work in a live environment through this exam in a fixed interval of time. RHCSA and RHCE certifications are very valuable and keep you aside from the rest of the administrator who are not certified and I recommend this exam if you are working in a UNIX environment or even if you are a student who has an interest in UNIX/LINUX.

Before reading this book, I assume that you have already taken training from Red Hat certified vendor or institute OR have already gained enough knowledge via various books, videos, CBT etc. to and you are ready to give Red Hat certification Exams. If you haven't, then please do so. This is only practice book and no deep explanations are given.

I have kept this book very simple and it is divided into two parts. 1st section will contain practice papers for Red Hat Certified System Administrator (RHCSA) exam and 2nd section will contain practice papers for Red Hat Certified Engineer (RHCE) exam.

For good practice, I have kept practice papers first and then answers at the last. This will help you in evaluating yourself and if you have any problem with any question you can check answer afterwards.

Know Your Author

Pawan Bahuguna is a Linux system administrator from many years and holds a B.Tech degree in Electronics & Telecommunication. He is ITIL, RHCSA, RHCE and MCP certified.

I have tried to keep this book error free but we all are humans and mistakes happen. So let me know if you find any mistake in the book through comments & email and I will try to rectify it in next version.

For any suggestion and feedback about this book, please reach him at contact@pawanbahuguna.com

SECTION 1

RHCSA

Actual Exam Time: 2.5 Hr EXAM Code: EX200

Note:

1. You have to do all work in virtual machine only (KVM).
2. This is completely performance based exam and not tick-mark questions will be asked.
3. Red hat can ask any questions from RHCSA syllabus, so be prepared.
4. These sample/practice papers are only meant for your practice once you have done your training.
5. Practice is the key to clear this exam.

RHCSA SAMPLE PAPER 1

1. Create users “kavin and aarav” and also create new group called “students”. kavin and aarav should have students as their secondary group. Note their primary group should not change.

2. User aarav has to monitor uptime and load average of the server at 18:15 every day, so schedule a cron job as aarav.

3. Set SELinux to Enforcing mode.

4. Create 250MB partition and format it with EXT4 and mount it permanently at /data.

5. Give /data FS group ownership of students group and set permission so no other member to access it. Also group should have read, write and

execute permission.

6. Copy file /etc/passwd to /var/tmp. Configure permission of /var/tmp/passwd such that no one is allowed to execute it and user kavin is able to read and write. The owner should be root and group ownership should also be with root.

7. Extend the filesystem /data to 500M.

8. Create user david with UID 555 and he should not be able to access the shell.

9. Locate all the files with name “date” and save the output to /tmp/locate.txt

10. Extend the SWAP space with "500" MB, don’t remove the existing swap. It should be available even after reboot.

11. Create softlink of /etc/fstab file as /etc/vtab.

********** END of Practice Paper 1 **********

RHCSA SAMPLE PAPER 2

1. Setup Network and hostname as given below.
    i. IP : 192.168.0.10
    ii. Netmask : 255.255.255.0
    iii. Gateway : 192.168.0.1
    iv. DNS : 192.168.0.254
    v. Hostname: client10.example.com

2. Setup YUM repo as per given yum location http://server.example.com/rhel7

3. Create user “david” with UID 521, and set password as “Pa55w0rd”.

4. Configure your machine as LDAP client. LDAP server and LDAP directory tree information given below.

a. ldapuser10 should be able to log into your system, where X is your station number, but will not have
    i. a home directory until you have completed the autofs requirement.
b. All ldapuser users have a password of password

c. Configure LDAP Search Base DN with: dc=example,dc=com
d. Configure LDAP Server with the URI: ldap://server1.example.com
e. Download CA from Certificate URL: http://server1.example.com/example-ca.crt

f. Configure AUTOFS for the LDAP user so that the home Directory of LDAP USER should be mounted automatically on the Machine. Share location Via NFS from the server server1.example.com:/home/guests/ldapuserX

5. Configure NTP with server server1.example.com

6. Download upgraded kernel package from
    a. ftp://rhcert.server10.ecample.com/pub/x86 The
    b. Upgraded kernel should be the default kernel of your system and the original

kernel should also be there.

7. Locate all uncommented lines in file /etc/ssh/sshd_config and copy the lines in a same order on /root/list file.

8. Make a new lvm in a new volume group. Name your volume group as myvol and lvm as mylvm. The size of lvm should be of 64 extents and base size should be 16MB. Permanently mount the logical volume on /datadir directory as Ext4 filesystem.

9. Create a cron job that reboots your computer at 2:15 p.m. on 1st of every month as root.

10. Create user “don” and “sam” and set password expiry to 60 days of user don and no password expiry of sam.

11. Resize /home to 500MB.

********** END of Practice Paper 1 **********

SECTION 2

RHCE

Actual Exam Time: 3.5 Hr EXAM Code: EX300

Note:

1. You will be given 1 physical machine with 2 virtual machines. You have to do all task in virtual machines only.
2. For practice papers we are taking these virtual machines as client1.example.com and client2.example.com. At your place you can take any.
3. RHCSA syllabus questions can also be asked in RHCE exam.
4. There is not any fixed number of questions and in this sample paper we will include 10 questions or more in each sample paper.
5. Key to clear RHCE exam is practice. More you practice; more are your chances of success.

RHCE SAMPLE PAPER 1

1. Set SELinux to Enforcing mode on both virtual machines.

2. Configure SSH access such that root is not able to login on client1.example.com.

3. Share /datadir through NFS from client1.example.com to client2.example.com and mount at /nfsshare. Changes made should be permanent.

4. Configure Teaming on both the stations using IPv4, both machine should communicate with each other through bonding interface.
   i. On client1.example.com team IP should be 192.168.0.10/24
   ii. On Client2.example.com team IP should be 192.168.0.11/24

5. Enable IP4 routing.

6. Configure firewall to route all traffic from 192.168.0.0/24 through work zone.

7. On client1, Share the **/smbshare** directory via SMB, such that your SMB server must be a member of the **SMBGROUP** workgroup, the share name must be **shared**, the shared share must be available to example.com domain clients only, the shared share must be browseable and user david must have read and execute access to the share.

8. Install MariaDB and secure it with root password "**redhat**" on client1. Remove test database, anonymous user and disallow root login remotely.

9. Configure a simple web server and test it with elinks on client1.example.com

10. Create a command called "**rhcecmd**" with below entry and it should be available to all users in the system.

sar 1 5

**** END of RHCE Practice Paper 1 *****

RHCE SAMPLE PAPER 2

1. Enable IP4 routing, change should be persistent.

2. Configure Teaming on both the stations using IPv4, both machine should communicate with each other through teaming interface with active-backup runner.

i) On client1.example.com team IP should be 192.168.0.10/24

ii) On client2.example.com team IP should be 192.168.0.11/24

3. There is an extra Network connection called team02, as it is not needed, delete it.

4. Share /data-krb through Kerberos enabled NFS from client1.example.com to client2.example.com and mount at /nfsshare-krb. Changes made should be permanent. keytab file can download from

ftp://server.example.com/pub/keytabs/clientX.keyt

5. Set SELinux to Permissive mode on client1.example.com.

6. Set default Zone to public.

7. Configure Firewall such that all traffic of port no 5420 of client1 should be forwarded to port no 80 of 192.168.0.2

8. Client1 should export an ISCSi Disk Called **iqn.2015- 06.com.example:client1.rhcedisk**

   This ISCSI Disk should be 512MB partition and access should be allowed to clients with an IQN of **iqn.2015-06.com.example:client2**
   The name of LUN should be iscsi_disk

9. Access the iscsi disk exported from client1 into the client2 and create a partition of 300MB and permanently mount it under **/iscsi** it should be formatted with "**xfs**" file system

10. Configure Internet Email service on your Client1, so that

    i) Your Email server should accept Email from 192.168.0.0/24 subnet.

ii) It should be acting like an email “Null Client” which relay email through **smtp1.example.com**, using **client2.example.com** as your organization’s domain name on outgoing email.

11. Verify that mail server is working by using an IMAPS-capable mail client to retrieve a test email from **imap1.example.com** (as user and mail recipient **david** with IMAP password **david**)

i) Disable local delivery of emails.

**** END of RHCE Practice Paper 2 *****

RHCE SAMPLE PAPER 3

1. Set target to Multi user mode.

2. Configure Teaming on both the stations using IPv4, both machine should communicate with each other through bonding interface with active-backup runner.

i) On client1.example.com team IP should be 192.168.0.10/24

ii) On client2.example.com team IP should be 192.168.0.11/24

iii) **Configure IPv6 on both the system and they should communicate with IPv6. IPv6 of client1 is 12::2/64 and client2 is 12::3/64.**

3. Configure firewall such that all traffic of port no 22 on client1 should forward to 2222 port of local client1.

4. Configure password less root sftp login between client 1 and client2.

5. Export **/exports/nfs** using from client1 using **NFS version 4** using **kerberos** Authentication.

i) All clients in 192.168.0.0/24 should be able to access the NFS share with RW access.
ii) Permission of **/exports/nfs** should be 1777.
iii) Download keytab file from below location
http://server.example.com/pub/keytabs/client1.keyta

6. Mount the NFS exported Directory from client1 into your client2 machine and make sure it should be available across the reboot.
   i) Download keytab file from below location
http://server.example.com/pub/keytabs/client2.keyta

   ii) Mount the share to **/mnt/nfsshare-krb** and it should be available after reboot.

7. Enable IP forwarding on both the systems.

8. Configure web server by downloading a file from server1 and make it available permanent.

   Deploy the site http://client1.example.com, where 1 is your station number, and then perform the following steps: - Download

   http://server1.example.com/rhcert/station.html

   - Rename the downloaded file to index.html
   - Copy this index.html file to the DocumentRoot of your web server
   - Do NOT make any modifications to the

content of index.html

9. Configure virtual webhosting. /srv/www/virtual

   Virtual host for the site http://www1.example.com, then perform the following steps:
   - Set the DocumentRoot to /srv/www/virtual – Download http://server1.example.com/rhcert/www.html

   - Rename the downloaded file to index.html
   - Place this index.html in the DocumentRoot of the virtual host
   - Do NOT make any modifications to the content of index.html
   - Ensure that harry is able to create content in /srv/www/virtual

10. Extend url of your web server and make it under /var/www/html/secret

    http://server1.example.com/rhcert/secret.html
    This web site should be accessible as sub domain to your Default website by pointing your web browser to- http://client1.example.com/secret

11. Install MariaDB and secure it with root

password “**redhat**” on client1.example.com.
i) Remove test database, anonymous user and disallow root login remotely.
ii) Create mysql user “rhceroot” with password “redhat”.
iii) Restore database from location http://server10.example.com/rhcert/inventory.dump
iv) Grant **SELECT** privilege to user “rhceroot” on database inventory database.

12. Create Script which prints “**RHCE**” when given “**RHCSA**” and vice-versa. If nothing is given it should print “**Error: Usage RHCE|RHCSA**”.

**** END of RHCE Practice Paper 3 *****

Answer RHCSA Practice Paper 1

1. # useradd kavin

   # useradd aarav

   # groupadd students

   # usermod –aG students kavin

   # usermod –aG students aarav

   Confirmation: # groups kavin;groups aarav

2. # crontab –u aarav –e

Press “i” for insert mode and enter below values

15 18 * * * /usr/bin/uptime

Now Esc and **:wq!** to save.

Confirmation: # crontab -l -u aarav

3. # vi /etc/selinux/config

   SELINUX=enforcing

   :wq!

4. # fdisk /dev/sda

   Press ‘n’,

   Select (default p): l

   Adding logical partition 5

   First sector (188416-20971519, default 188416): Press

<Enter Key>

Using default value 188416

Last sector, +sectors or +size{K,M,G} (188416-20971519, default 20971519): +250M

Partition 5 of type Linux and of size 250 MiB is set

Now press “t” for changing partition type.

Hex code: 8e

Press ‘p’ to confirm partition.

w

partprobe /dev/sda or partx -a /dev/sda

Tip: If you are creating partition 1st time, create it as extended partition for all the available space and then from it you can create more different partition.

pvcreate /dev/sda5

vgcreate datavg

lvcreate –L 250M –n datalv datavg

#mkfs.ext4 /dev/datavg/datalv

vi /etc/fstab

/dev/datavg/datalv /data ext4 defaults 0 0

5. # chown :students /data or # chgrp students /data

chmod 770 /data or # chmod g+rwx,o-rwx /data

6. # cp /etc/passwd /var/tmp

   # chmod –x /var/tmp/passwd

   # setfacl –m u:kavin:rw- /var/tmp/passwd

   # chown root:root /var/tmp/passwd

7. Create one partition of 250M as explained above with hex ID for 8e for LVM and perform below commands. /data is already 250M so we have to increase only 250M to make it 500M.

   # pvcreate /dev/sda6

   # vgextend datavg /dev/sda6

   # lvextend –L +250M /dev/datavg/datalv datavg

   # resize2fs /dev/datavg/datalv

   # df –h /data

8. # useradd –u 555 –s /sbin/nologin david
9. # locate date >>/tmp/locate.txt
10. # fdisk /dev/sda

    p (Print partition table)

    n

    (Create new partition: press e to create extended partition, press p to create the main partition, and the extended

partition is further divided into logical partitions) Enter

+500M

t

Choose hex code 82 for swap

w

partprobe /dev/sda or you can even reboot

# mkswap /dev/sda7
# swapon /dev/sda7
# swapon -s
# blkid /dev/sda7 (Copy UUID)
# vim /etc/fstab
UUID=XXXXX swap swap defaults 0 0

swapon –s (To verify)

11. # ln –s /etc/fstab /etc/vtab

Answer RHCSA Practice Paper 2

1. # vim /etc/sysconfig/network-scripts/ifcfg-eno16777736
   (Configure IP Address, Gateway and DNS)
   IPADDR0=192.168.0.10
   GATEWAY=192.168.0.1
   DNS1=”192.168.0.254”
   ONBOOT=yes

   # systemctl restart network.service

   To set hostname:
   # nmtui-hostname
   client10.example.com
   OR
   # vi /etc/hostname

   Graphical Interfaces (Configure IP Address, Netmask, Gateway)
   Application->Sundry->Network Connections
   # service network restart (Will work on RHEL 7 also)
   OR
   # systemctl restart network.service

Verify: - # hostnamectl or hostname

cat /etc/hostname

2. # cd /etc/yum.repos.d/

   # rm –rf * .

   # vi yum.repo

   [Repo]

   name=Repo Name

   baseurl=http://server.example.com/rhel7

   gpgcheck=0

yum repolist

3. # useradd –u 521 david

   # passwd david

   OR

   # echo Pa55w0rd |passwd --stdin david

4. # yum install authconfig-gtk -y
   # system-config-authentication
   LDAP Server: ldap//server.example.com (In domain form, not write IP)

   OR

yum groupinstall directory-client (1.krb5-workstation 2.pam-krb5 3.sssd)
system-config-authentication
i.User Account Database: LDAP
ii.LDAP Search Base DN: dc=example,dc=com
iii.LDAP Server: ldap://server1.example.com (In domain form, not write IP)
iv.Check: **use TLS to encrypt connection** and give certificate URL by clicking
Download CA Certificate
v. Authentication Method: LDAP password
vi. Apply

systemctl enable sssd
systemctl start sssd
systemctl status sssd

getent passwd ldapuser10
Above command will give information about ldapuser10 with its home DIR, note that, it will help in completing autofs requirement.

vi /etc/auto.master
/home/guest /etc/auto.ldap

vi /etc/auto.ldap
ldapuser10 -rw
server1.example.com:/home/guests/ldapuser10

systemctl enable autofs
systemctl start autofs
systemctl status sutofs
su – ldapuser10
Should get home dir now.

5. # vi /etc/chrony.conf

   Comment all the lines under

   "# Use public servers from the pool.ntp.org project."
   And enter below line

   server server1.example.com iburst

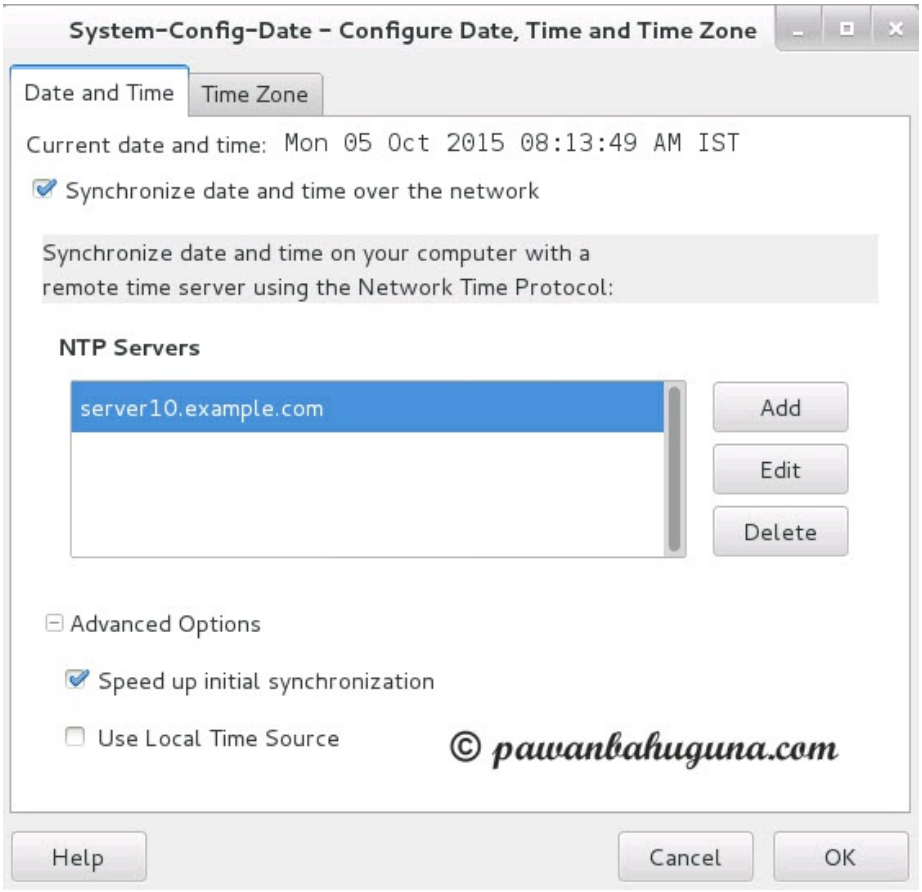
systemctl restart chronyd.service

chronyc sources –v (For verification)

OR

yum install ntp system-config-date –y

system-config-date



#systemctl enable ntpd

systemctl restart ntpd

systemctl status ntpd

firewall-cmd --permanent --add-service=ntp

firewall-cmd --reload

6. Download kernel and firmware from the link given.

   # wget ftp://rhcert.server10.ecample.com/pub/x86_64/rhcsa/*

   # rpm -Uvh linux-firmware-20140911-0.1.git365e80c.el7.noarch.rpm

rpm –ivh kernel-3.10…(tab)

grub2-mkconfig > /boot/grub2/grub.cfg

systemctl reboot

If latest kernel does not come on top, do following after checking position of kernel in /boot/grub2/grub.cfg. I have always seen latest kernel come on first place at grub menu.

vi /etc/defaults/grub

GRUB_DEFAULT=position

grub2-mkconfig > /boot/grub2/grub.cfg

systemctl reboot

uname –r (Verify)

7. grep -v '^[#;]' /etc/ssh/sshd_config >/root/list

8. Given : 64 extents and 16MB base size

   Partition =PExLE = 64x16=1024MB

   Take around 200MB extra space, so create partition with 1200MB

   # pvcreate /dev/sda5

   # vgcreate –s 16M myvol /dev/sda5

   # lvcreate -l 64 -n mylvm myvol

   # mkfs.ext4 /dev/myvol/mylvm

   # vi /etc/fstab

/dev/myvol/mylvm /datadir ext4 defaults 0 0

mount –a

df -hT /datadir

9. # crontab –e

Press “i” for insert mode and enter below values

15 14 1 * * systemctl reboot

10. # useradd don;useradd sam

chage -M 60 don

chage -M -1 sam

11. This may be a tricky question. First you will have to see what is the current size of filesystem i.e. /home.

If size is more than 500MB then you will have to reduce /home and if size is less than 500M, you will have to increase the size.

So in this case, suppose we have /home of 1G, so we will reduce /home to 500M.

umount /home

e2fsck –f /dev/vg1/homelv

resize2fs /dev/vg1/homelv 500M [This command should not give any error, If there is error read and do

accordingly.]

lvreduce –L -500M /dev/vg/homelv

e2fsck –f /dev/vg1/homelv

mount /home or mount -a

Answer RHCE Practice Paper 1

1. # vi /etc/selinux/config

   SELINUX=enforcing

   :wq!

2. On client1.example.com

   # vi /etc/ssh/sshd_config

   And change "#PermitRootLogin yes" to "PermitRootLogin no"

   Now restart ssh daemon to make this change effective.

   # systemctl restart sshd.service

3. On Client1.example.com

   # yum install nfs-utils

   # mkdir /datadir

   # chown nfsnobody /datadir

   # vi /etc/exports

   /datadir client2.example.com(rw,sync)

   # exportfs –r

   # exportfs –v

   # systemctl start nfs-server

systemctl enable nfs-server

systemctl start rpcbind

systemctl enable rpcbind

firewall-cmd --permanent --add-service=nfs

firewall-cmd --reload

On client2.example.com

mkdir /nfsshare

systemctl start rpcbind

systemctl enable rpcbind

mount –t nfs client1:/datadir /nfsshare

vi /etc/fstab

Client1.example.com:/datadir /nfsshare nfs defaults 0 0

mount -a

4. # rpm -qa |grep -i NetworkManager
   If network manager is not installed, install it.
   # yum –y install NetworkManager
   # nmcli con add type team con-name team0 ifname team0 config '{"runner": {"name": "activebackup"}}'
   # nmcli con mod team0 ipv4.addresses 192.168.0.10/24
   # nmcli con mod team0 ipv4.method manual

   # nmcli con add type team-slave con-name team0-eth0

ifname **eno16777736** master team0

nmcli con add type team-slave con-name team0-eth1 ifname **eno33554960** master team0

nmcli con up team0-eth0

nmcli con up team0-eth1

teamdctl team0 state

Perform above steps in Client2 also and replace the IP 192.168.0.11/24

Note: **ifname** is name of your interface, put accordingly. GUI method will be shown on other question.

5. **echo 1 > /proc/sys/net/ipv4/ip_forward**

   Note: This is not for permanent

6. # firewall-cmd --permanent --zone=work --add-source=192.168.0.0/24

   To verify use below command

   # firewall-cmd --get-active-zones

7. On Client1

   # yum install samba* -y

   # vi /etc/samba/smb.conf

workgroup = SMBGROUP

hosts allow = 127. 192.168.0. .example.com

- Make below entry at last of smb.conf file.

[shared]

comment = Shared Stuff

path = /smbshare

public = no

browseable = yes

valid users = david

mkdir /smbshare

systemctl enable smb.service

systemctl start smb.service

systemctl status smb.service

setsebool -P samba_share_nfs=1 samba_export_all_ro=1 samba_export_all_rw=1

chcon -R -t samba_share_t /smbshare

systemctl restart smb.service

smbpasswd -a david

setfacl -m user:david:r-x /smbshare

firewall-cmd --permanent --add-service=samba

firewall-cmd –reload

testparm

Testing

smbclient //client1/shared -U david

Password

You should be able to see content in the share as below.

```
[root@client1  ~]# smbclient //client1/shared -U david
Enter david's password:
Domain=[SMBGROUP] OS=[Unix] Server=[Samba 4.1.1]
smb: \> ls
  .                                   D        0  Mon Sep 21 00:41:12 2015
  ..                                  D        0  Mon Sep 21 00:16:21 2015
  test.txt                            N        5  Mon Sep 21 00:41:12 2015

                55672 blocks of size 262144. 41075 blocks available
smb: \>
```

8. On Client1, enter below commands.

   # yum groupinstall "mariadb" -y

   # firewall-cmd --permanent --add-service=mysql

   # firewall-cmd --permanent --add-port=3306/tcp

   # firewall-cmd --reload

   Enable, start and check status of MariaDB

   # systemctl enable mariadb

   # systemctl start mariadb

   # systemctl status mariadb

   Enter below command to set password, remove test

DB, anonymous user etc. Give "Yes" to all option

mysql_secure_installation

9. # yum install httpd* -y

   # systemctl enable httpd

   # systemctl start httpd

   # systemctl status httpd

   # firewall-cmd --permanent --add-service=http

   # firewall-cmd –reload

   # vi /etc/hosts

   192.168.0.10 client1 client1.example.com

   # yum install elinks –y

   # elinks client1.example.com or elinks <IP of the client1>

   This should display a test page. If not, you have don't something wrong.

10. # vi /bin/rhcecmd

    sar 1 5

    # chmod a+x /bin/rhcecmd

    # chmod u+s /bin/rhcecmd

    Verify by running command rhcecmd on terminal.

```
# rhcecmd
```

Answer RHCE Practice Paper 2

1. **echo 1 > /proc/sys/net/ipv4/ip_forward**

For Permanent make file called ipfwd.conf under /etc/sysctl.d/

net.ipv4.ip_forward = 1

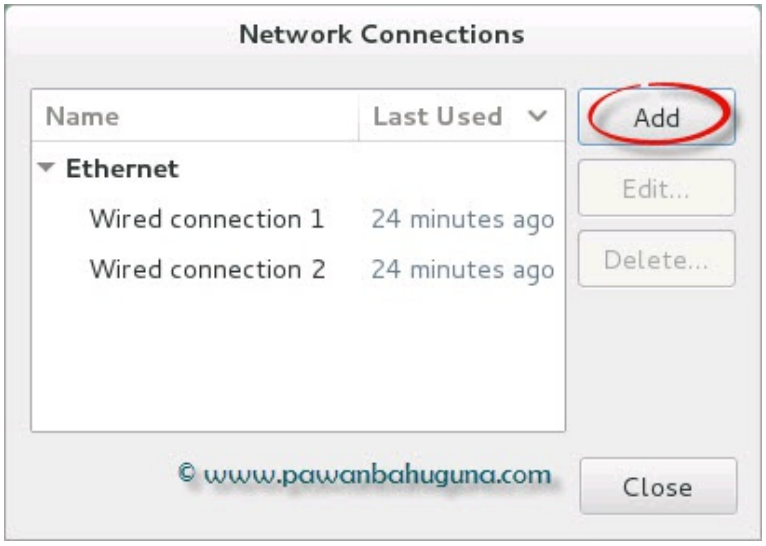
Or make entry to **/etc/sysctl.conf** and then type **sysctl –p**

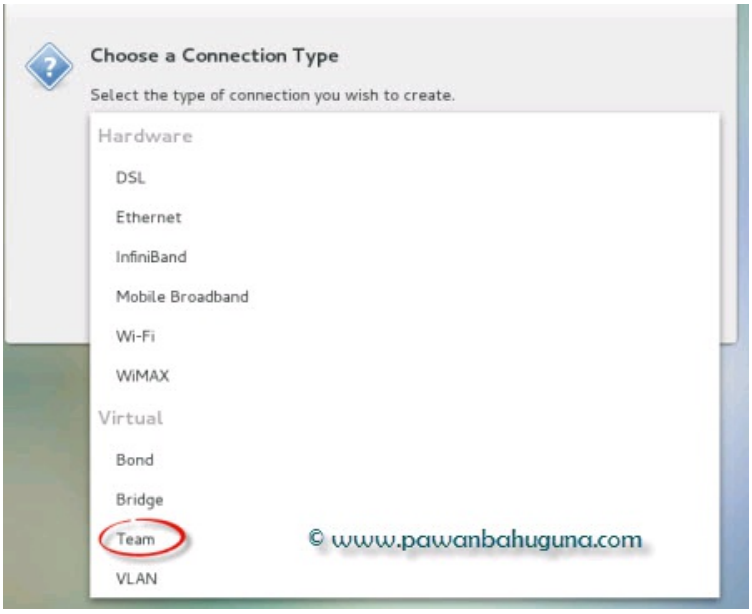
2. This question will be answered using GUI method.

   # nm-connection-editor

   OR click on network connection on right top. 

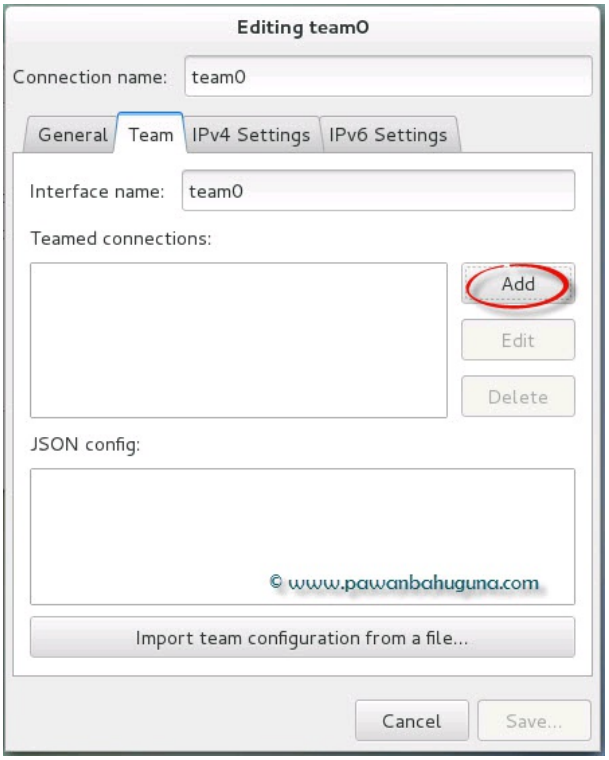
- Click on Add and then choose **team** as shown below.





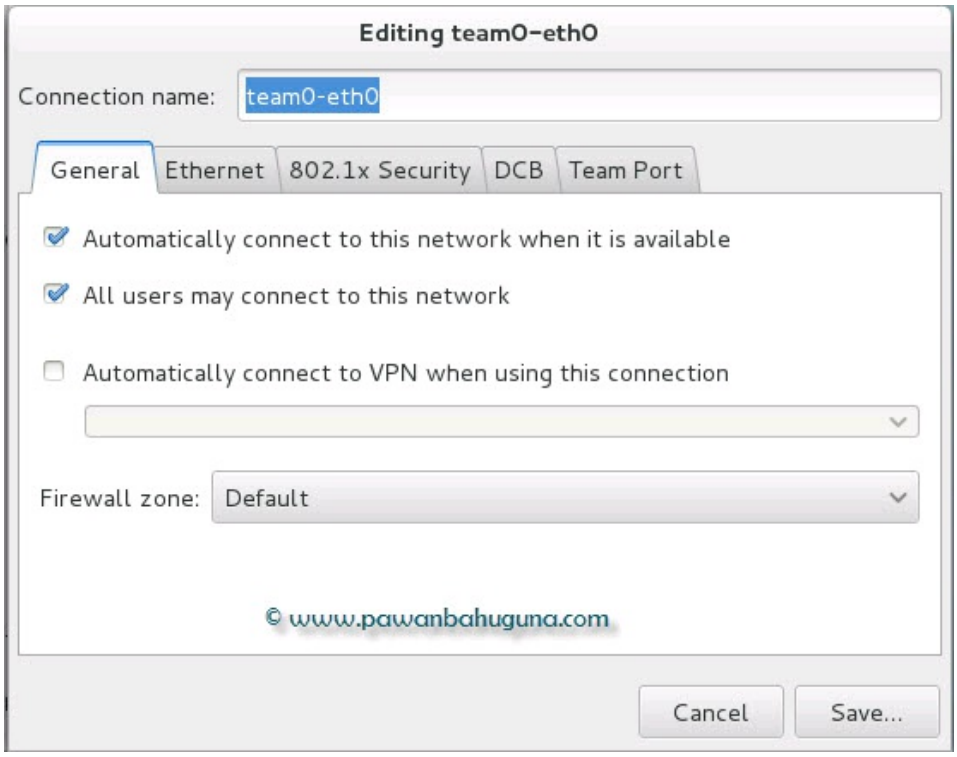
After choosing Team, click **create**.

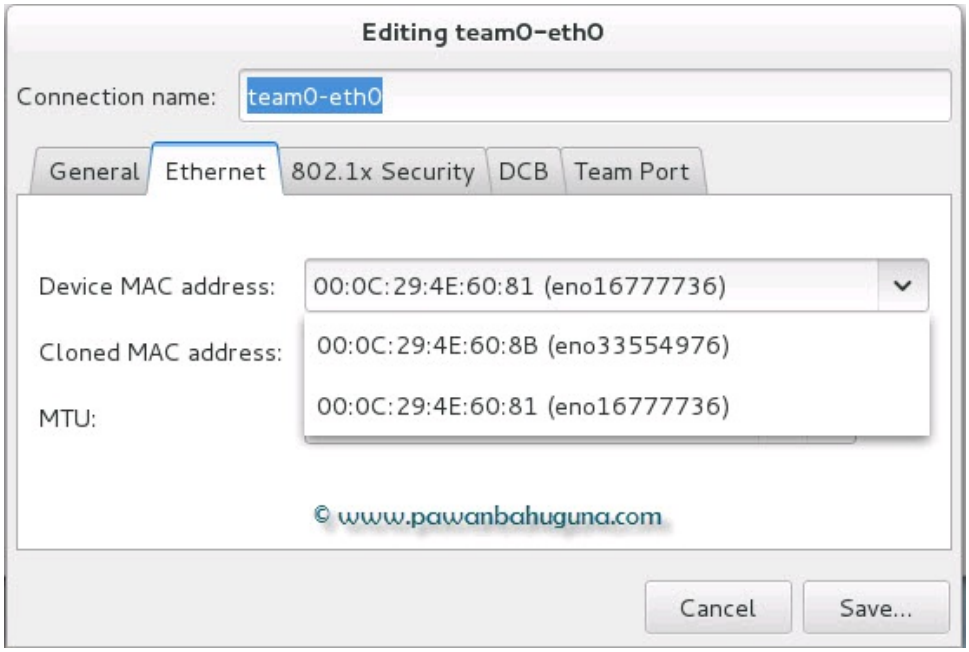
- Change interface name as desired and Click on Add.


Editing team0
Connection name:
team0
General
Team
IPv4 Settings
IPv6 Settings
Interface name:
team0
Teamed connections:
Add
Edit
Delete
JSON config:
© www.pawanbahuguna.com
Import team configuration from a file...
Cancel
Save...

- Now, choose Ethernet connection and click **create**.

Now do setting as shown below.

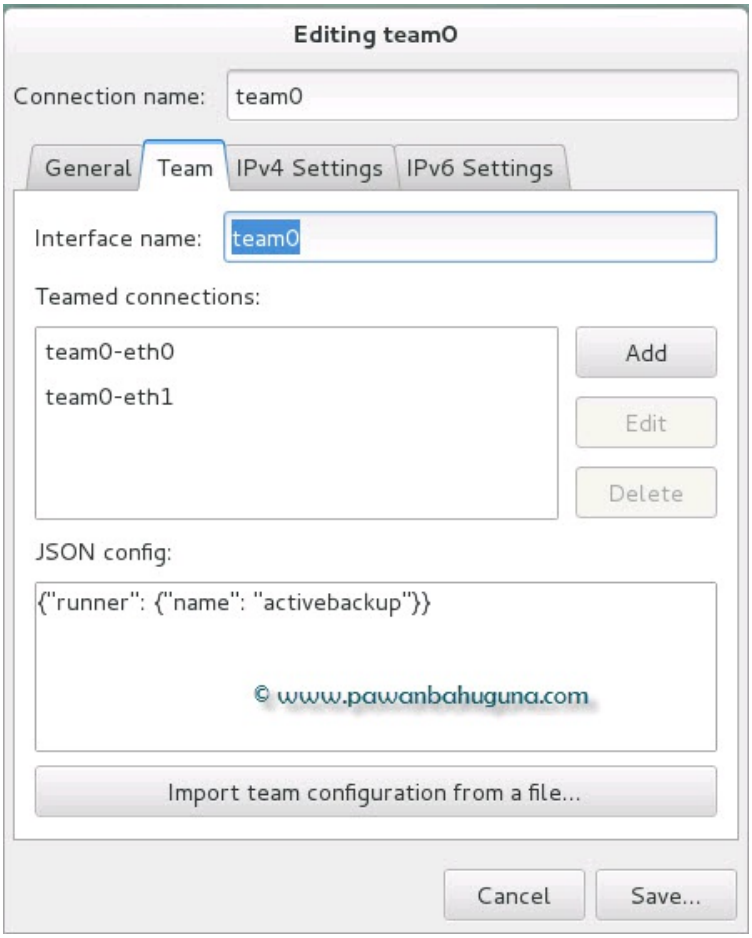




Choose any network card MAC address, be sure not choose same on next connection.

- Similarly do all above steps for other salve device.

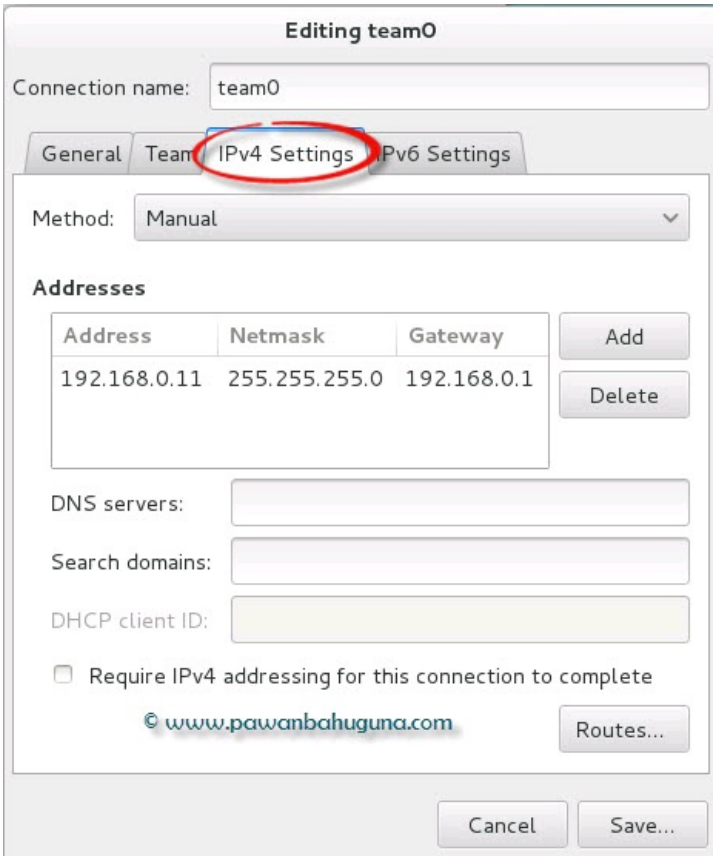
Now your team0 connection should look like below image.



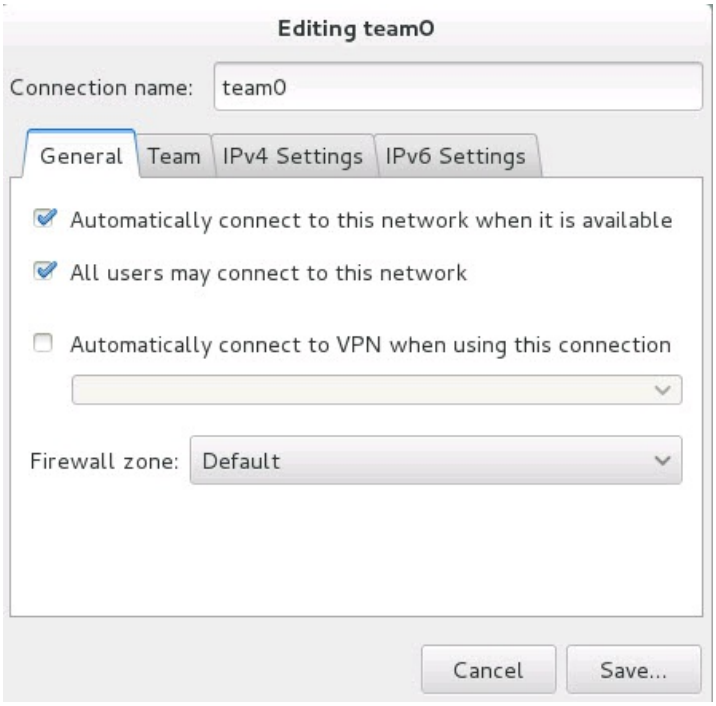
In JSON config put below lines for active backup connection.

{"runner": {"name": "activebackup"}}

Now, set IPv4 for your new team0 connection. For this go to IPv4 settings.



General setting should look like below unless any special need is to be met.



systemctl restart network.service; nmcli con show

Should look like below.

```
[root@client11 Desktop]# nmcli con show
NAME        UUID                                  TYPE            DEVICE
team0       ba35b5e4-7149-4927-a487-86dae46262f3  team            team0
team0-eth0  4e53abd4-6cd0-4d77-8215-4e5ca151fe21  802-3-ethernet  eno16777736
team0-eth1  09891019-ef7f-4106-837c-c3634918a2da  802-3-ethernet  eno33554976
[root@client11 Desktop]#
```

If it's giving error try to check configuration file at /etc/sysconfig/network-scripts/ or reboot your client machine.

Do same configuration on other server and try to ping both.

3. # nmcli con show [Verify Connection]

   # nmcli con del team2

4. On Client1.example.com

   # yum install nfs-utils

   # systemctl start nfs-server.service

   # systemctl enable nfs-server.service

   # wget –0 /etc/krb5.keytab ftp://server.example.com/pub/keytabs/client1.keytab

   # systemctl enable nfs-secure-server

   # systemctl start nfs-secure-server

   # systemctl status nfs-secure-server

firewall-cmd --permanent --add-service=nfs

firewall-cmd --reload

Note: If keytab file is not there in /etc dir, nfs-secure-server will not start.

mkdir /data-krb

vi /etc/exports

/data-krb client2.example.com(sec=krb5p,rw)

exportfs –r

At client2.example.com

wget –0 /etc/krb5.keytab ftp://server.example.com/pub/keytabs/client2.keytab

systemctl enable nfs-secure

systemctl start nfs-secure

systemctl status nfs-secure

Note: If nfs-secure is not there first install **nfs-utils** package.

mkdir /nfsshare-krb

mount –o sec-krb5p client1.example.com:/data-krb /nfsshare-krb

For Permanent mounting

vi /fstab

client1.example.com:/data-krb /nfsshare-krb nfs sec=krb5p 0 0

5. # vi /etc/selinux/config

SELINUX=permissive

6. First check default zone.

   # firewall-cmd --get-default-zone

   If output is other than public, set as below.

   # firewall-cmd --set-default-zone=public

7. # firewall-cmd --zone=external --permanent --add-forward-port=port=5420:proto=tcp:toport=80:toaddr=192.168.0.2

   # firewall-cmd –reload

   For verification

   # firewall-cmd --list-forward-ports --zone=external

8. On Client1.

   # yum install targetcli –y

   # systemctl enable target

   # systemctl start target

   # systemctl status target

   # firewall-cmd --permanent --add-port=3260/tcp

   # firewall-cmd –reload

   Now create a 512MB partition with id “8e” for LVM and create lv with it.

pvcreate /dev/sdb1

vgcreate iscsivg /dev/sdb1

lvcreate -L +512M -n iscsilv iscsivg

targetcli

/> /backstores/block create **iscsi_disk** /dev/iscsivg/iscsilv

/> /iscsi create iqn.2015-06.com.example:client1.rhcedisk

/> /iscsi/iqn.2015-06.com.example:client1.rhcedisk/tpg1/acls create iqn.2015-06.com.example:client2

/> /iscsi/iqn.2015-06.com.example:client1.rhcedisk/tpg1/luns create /backstores/block/iscsi_disk

/> /iscsi/iqn.2015-06.com.example:client1.rhcedisk/tpg1/portals create **192.168.0.10**

exit

systemctl restart target.service

Note: IP given above is client1 IP

9. # yum install iscsi-initiator-utils -y

systemctl enable iscsi.service

systemctl start iscsi.service

vi /etc/iscsi/initiatorname.iscsi

InitiatorName=iqn.2015-06.com.example:client2

iscsiadm -m discovery -t st -p 192.168.0.10 –discover

You will get iqn number like below. Copy it.

192.168.0.10:3260,1 **iqn.2015-06.com.example:client1.rhcedisk**

iscsiadm -m node -T **iqn.2015-06.com.example:client1.rhcedisk** -p 192.168.0.10 –login

Verify newly added disk

dmesg |tail

Now create new LVM partition with this disk of 300M. (You can also directly use the disk and format it using xfs.)

fdisk /dev/sdb

pvcreate /dev/sdb

vgcreate vgint /dev/sdb1

lvcreate -L +300M -n lvint vgint

mkfs.xfs /dev/vgint/lvint

mkdir /iscsi

blkid /dev/vgint/lvint [copy UUID]

vi /etc/fstab

UUID=054a3ba6-3a1d-4caa-9480-4a315d8db30c /iscsi xfs _netdev 0 0

mount –a

df –h /iscsi

iscsiadm -m node -T **iqn.2015-06.com.example:client1.rhcedisk** -p 192.168.0.10 --logout

10. On Client1.

yum install postfix* -y

firewall-cmd --permanent --add-service=imaps

firewall-cmd --permanent --add-service=smtp

firewall-cmd --permanent --add-port=25/tcp

firewall-cmd --reload

 # vim /etc/postfix/main.cf (append below lines)

- relayhost =[smtp1.example.com]
- inet_interfaces = loopback-only
- mynetwroks=127.0.0.1/8 [::1]/128 192.168.0.0/24
- myorigin = client2.example.com
- mydestination=

- local_transport=error: local delivery disabled (save and exit)

systemctl enable postfix.service

systemctl restart postfix.service

11. # yum install mutt –y

    Now send a test email.

    # mail –s “Test Email” david@client2.example.com

    Test Email

    .

    EOT

    # **mutt –f imaps://imap1.example.com**

    User name at imap1.exmaple.com: **david**

    Password for david@imap1.example.com: **david**

    Check the message and quit.

Answer RHCE Practice Paper 3

1. # systemctl set-default multi-user.target

2. Check Answer 4 of RHCE practice paper1 or Answer 2 of RHCE practice paper 2 for teaming.

   IPV6

   On Client1

   # nmcli connection modify team0 ipv6.addresses 12::2/64

   # nmcli connection modify team0 ipv6.method static

   # systemctl restart network

   On Clinet2

   # nmcli connection modify team0 ipv6.addresses 12::3/64

   # nmcli connection modify team0 ipv6.method static

   # systemctl restart network

   Now try to ping each other or SSH, both system should ping each other.

   # ping6 12::3

   # ping6 12::2

3. # firewall-cmd --zone=external --permanent --add-forward-port=port=22:proto=tcp:toport=2222

   # firewall-cmd --reload

   To verify

   # firewall-cmd --list-forward-ports --zone=external

4. On client1.example.com

   # ssh-keygen

   And press enter for default option's, do not put any password.

   # ssh-copy-id client2 or ssh-copy-id <IP of Client2>

   Will ask for root password of client2, enter.

   Now verify.

   # ssh client2 [Should not ask any password]

5. On Client1.example.com

yum install nfs-utils

systemctl start nfs-server.service

systemctl enable nfs-server.service

wget –0 /etc/krb5.keytab http://server.example.com/pub/keytabs/client1.keytab

systemctl enable nfs-secure-server

systemctl start nfs-secure-server

systemctl status nfs-secure-server

firewall-cmd --permanent --add-service=nfs

firewall-cmd --reload

Note: If keytab file is not there in /etc dir, nfs-secure-server will not start.

vi /etc/sysconfig/nfs

RPCNFSDARGS="-v 4.2"

mkdir /exports/nfs

chmod 1777 /exports/nfs

vi /etc/exports

/exports/nfs 192.168.0.0/24 (sec=krb5p,rw,sync)

exportfs –r

6. **At client2.example.com**

wget –0 /etc/krb5.keytab ftp://server.example.com/pub/keytabs/client2.keytab

systemctl enable nfs-secure

systemctl start nfs-secure

systemctl status nfs-secure

Note: If nfs-secure is not there first install **nfs-utils** package.

mkdir /nfsshare-krb

mount –o sec-krb5p client1.example.com:/data-krb /nfsshare-krb

For Permanent mounting

vi /fstab

client1.example.com:/data-krb /nfsshare-krb nfs sec=krb5p 0 0

7. # vi /etc/sysctl.conf

net.ipv4.ip_forward=1

sysctl –p

8. # yum install httpd* -y

systemctl enable httpd

systemctl start httpd

systemctl status httpd

firewall-cmd --permanent --add-service=http

firewall-cmd –reload

vi /etc/hosts

192.168.0.10 client1 client1.example.com

cd /var/www/html

wget http://server1.example.com/rhcert/station.html

mv station.html index.html

restorecon -RF *

vim /etc/httpd/conf.d/a.conf

<VirtualHost 192.168.0.10>

ServerName client1.example.com

DocumentRoot /var/www/html

DirectoryIndex index.html

</VirtualHost>

<Directory /var/www/html>

Order allow,deny

Allow from 192.168.0.0/24

</Directory>

:wq! [Save the file]

Now, Check syntax using below command.

httpd –t

systemctl restart httpd

9. # mkdir /srv/www/virtual

cd /srv/www/virtual

wget http://server1.example.com/rhcert/www.html

mv www.html index.html

cd

restorecon -RFv /srv/www/virtual/*

setfacl -m u:harry:rwx /srv/www/virtual

#vim /etc/httpd/conf.d/b.conf

<VirtualHost 192.168.0.10>

ServerName www1.example.com

DocumentRoot /srv/www/virtual

DirectoryIndex index.html

VirtualHost>

<Directory /srv/www/virtual >

require all granted

</Directory>

:wq!

httpd -t (to check syntax, it should be ok)

systemctl restart httpd.service

10. # mkdir –p /var/www/html/secret

cd /var/www/html/secret

wget http://server1.example.com/rhcert/secret.html

mv secret.html index.html

restorecon -RFv *

vim /etc/httpd/conf.d/a.conf (Append below lines)

<Directory /var/www/html/secret>

Allowoverride none

Order allow,deny

allow from client1.example.com

</Directory> (save and exit)

httpd -t (to check syntax, it should be ok)

systemctl restart httpd.service

11. # yum groupinstall "mariadb" -y

firewall-cmd --permanent --add-service=mysql

firewall-cmd --permanent --add-port=3306/tcp

firewall-cmd --reload

Enable, start and check status of MariaDB

systemctl enable mariadb

systemctl start mariadb

systemctl status mariadb

Enter below command to set password, remove test DB, anonymous user etc. Give "**Yes**" to all option

mysql_secure_installation

mysql -u root -p'redhat'

> CREATE USER 'rhceroot'@'%' IDENTIFIED BY 'redhat';

> create database inventory;

> GRANT SELECT on inventory.* to rhceroot@'%';

> flush privileges;

> exit

wget http://server10.example.com/rhcert/inventory.dump

mysql -u root -p inventory <inventory.dump

12. # vi script1.sh

#!/bin/bash

Author: Pawan Bahuguna

if [-z "$1"]; then

echo "Error: Usage RHCE|RHCSA"

fi

if ["$1" = "RHCE"]; then

```
echo "RHCSA"
elif [ "$1" = "RHCSA" ]; then
echo "RHCE"
fi
exit
```

Save the script using :wq!

chmod +x script1.sh

Test as below

./script1.sh RHCSA

./script1.sh RHCE

./script1.sh

Output should look like below

```
[root@client1 /]# ./script1.sh RHCSA
RHCE
[root@client1 /]# ./script1.sh RHCE
RHCSA
[root@client1 /]# ./script1.sh
Error: Usage RHCE|RHCSA
[root@client1 /]#
```

How to Break Root Password and Login to machine

In Red Hat exam, you may also ask to set root password in the starting. But as you don't have actual root password you will have to break it and enter to machine. So you should know how to do that.

1. On grub screen press any key and then press "**e**" to edit.

2. Go to line which start with "**linux16 / vmlinuz**", and add **rd.break** at last of line or in middle and press **ctrl+x**.

3. Now server will start in emergency mode. Follow below steps.

mount –o remount,rw /sysroot

chroot /sysroot

sh-# **passwd**

Enter root password which you need to set.

touch /.autorelabel

exit

exit or reboot

I will request you to watch below video to understand

better.

https://www.youtube.com/watch?v=5KtVtrbTgTk

Thank You

Table of Contents