RHCE EXAM (Passing - 210/300 , Duration 3.5Hrs)

Physical Machine - root user (password is provied)

Virtual Machines-
Domain:- station0
system1:-
IP ADDR: 172.25.0.11(server)
HOSTNAME: (system1.network0.example.com)server0.example.com
system2:-
IP ADDR: 172.25.0.10(client)
HOSTNAME: (system2.network0.example.com)desktop0.example.com

Additional Information:
IP ADDR - 172.25.254.250
NETMASK- 255.255.255.0
GATEWAY - 172.25.254.254
DNS - 172.25.254.254
root psswd - <postroll>
YUM Server <URL> (http://content.example.com/rhel7.0/x86_64/dvd/
Deny domain- my133t.org
centralised server- server.network0.example.com(classroom.example.com)

---

1. Selinux should be in enforcing mode permanantly on your both systems.

Ans: set selinux to enforcing mode
#sestatus
#setenforce 1
vim /etc/selinux/config
insert
SELINUX=enforcing
:wq
#sestatus

---

2. Configure SSH access on your both systems as follows.
a. Users should have SSH access on your systems from remotely.
b. Clients within my133t.org should not have SSH access on your systems.

Ans: #systemctl enable sshd ; systemctl start sshd

#vim /etc/hosts.deny
insert
sshd: .my133t.org
:wq
#systemctl restart sshd

---

3. Create a new customized environment for your users on both systems.
a. Create a new custom command called "qstat" whos output should be similar to "/bin/ps -Ao pid,tty,user,fname,rsz"
b. Make sure "qstat" command should available by-default for all users on both systems.

Ans: #vim /etc/bashrc
shift G
insert
alias qstat="ps -Ao pid,tty,user,fname,rsz"
:wq

#source /etc/bashrc
#qstat [cross verify ur output]

---

4. Configure port forwarding on your system1.
a. The traffic coming from system2 on port 443/tcp should be forwarded to port 22/tcp on your system1.

Ans: # systemctl start sshd
systemctl enable sshd
firewall-cmd --permanent --add-service=ssh
firewall-cmd --permanent --add-rich-rule 'rule family=ipv4 source address=172.25.0.10 forward-port port=443 protocol=tcp to-port=22'

OR

firewall-cmd --permanent --add-rich-rule 'rule family=ipv4 source address=172.25.0.0/24 forward-port port=443 protocol=tcp to-port=22'

firewall-cmd --reload

Now check from both system2,
#ssh -p 443 system1.network0.example.com

OR

b. The traffic coming from system2 on port 5423/tcp should be forwarded to port 80/tcp on your system1.

Ans: # yum install httpd
systemctl start httpd
systemctl enable httpd
firewall-cmd --permanent --add-service=http --add-service=https
firewall-cmd --permanent --add-rich-rule 'rule family=ipv4 source address=172.25.0.10 forward-port port=5423 protocol=tcp to-port=80'
firewall-cmd --reload
semanage port -a -t http_port_t -p tcp 5423
vim /etc/httpd/conf/httpd.conf
Listen 80
(add new lines)
Listen 5423

```
     # systemctl restart httpd
```

5. Configure a link aggregation on both systems
     a. Both systems has a network interfaces "eno1" and "eno2"
     b. These two interface should be Slaved for new teaming device called "team1". (Make sure "team1" should remain active even if one of the interfaces goes down)
     c. Assign the given IP address for "team1" on 1st system - 172.25.XX.50
     d. Assign the given IP address for "team1" on 2nd system - 172.25.XX.60

Ans: on system1,

```
       #nmcli con add type team con-name team0 ifname team0 config '{"runner": {"name": "activebackup"}}'
     #nmcli con mod team0 ipv4.addresses '172.25.0.50'
     #nmcli con mod team0 ipv4.method manual
     #nmcli con add type team-slave con-name team0-port1 ifname eth1 master team0
     # nmcli con add type team-slave con-name team0-port2 ifname eth2 master team0
     #teamdctl team0 state
```

on system2,

```
       #nmcli con add type team con-name team0 ifname team0 config '{"runner": {"name": "activebackup"}}'
     #nmcli con mod team0 ipv4.addresses '172.25.0.60'
     #nmcli con mod team0 ipv4.method manual
     #nmcli con add type team-slave con-name team0-port1 ifname eth1 master team0
     # nmcli con add type team-slave con-name team0-port2 ifname eth2 master team0
     #teamdctl team0 state

     #ping -I team0 172.25.0.60 ----from system1
     #ping -I team0 172.25.0.50 ----from system2
```

6. Configure the following IPV6 ip address for interface eth0 on your both systems.
     a. IPV6 address for system1 - "fddb:fe2a:ab1e::c0a8:1/64"
     b. IPV6 address for system2 - "fddb:fe2a:ab1e::c0a8:fe/64"

Ans: on system1,

```
       # nmcli con add con-name eth0 type ethernet ifname eth0 ip4 "fddb:fe2a:ab1e::c0a8:1/64"
       # nmcli con mod eth0 ipv4.method manual connection.Autoconnect yes
       # nmcli con down eth0
       # nmcli con up eth0
```

on system2,

nmcli con add con-name eth0 type ethernet ifname eth0 ip4 "fddb:fe2a:ab1e::c0a8:fe/64"
nmcli con mod eth0 ipv4.method manual connection.Autoconnect yes
nmcli con down eth0
nmcli con up eth0

---

7. Implement a web server for the site http://serverX.example.com,
Then perform the following steps:
- Download http://classroom.example.com/pub/server.html
- Rename the downloaded file to index.html
- Copy this index.html to the DocumentRoot of your web server
- Do NOT make any modifications to the content of index.html
(attend all http questions at a time)

Ans:
```
# yum install httpd-manual mod_ssl mod_wsgi -y
# cd /var/www/html
# wget http://classroom.example.com/pub/server.html
# mv server.html index.html
# cd /etc/httpd/conf.d
# vim webhost.conf

 Listen 5423
<VirtualHost server0.example.com:80>
 DocumentRoot "/var/www/html"
 ServerName server0.example.com
 CustomLog "/var/log/httpd/server0.example.com-access_log" combined
</VirtualHost>

<Directory "/var/www/html">
 Require all granted
</Directory>

# Restorecon -RFv /var/www
# systemctl restart httpd
```

---

8. Extend your web server to include a virtual host for the site
http://wwwX.example.com
then perform the following steps:
- where X would be replaced by domain number.
- Set the DocumentRoot to /var/www/virtual
- Download http://classroom.example.com/pub/www.html
- Rename the downloaded file to index.html
- Copy this index.html to 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 /var/www/virtual

Ans:

```
            # mkdir -p /var/www/virtual
            # cd /var/www/virtual
            # wget http://classroom.example.com/pub/www.html
            # mv www.html index.html
            # cd /etc/httpd/conf.d/
            # vim webhost.conf
            <VirtualHost www0.example.com:80>
             DocumentRoot "/var/www/virtual"
             ServerName www0.example.com
             CustomLog "/var/log/httpd/www0.example.com-access_log"
combined
            </VirtualHost>


            <Directory "/var/www/virtual">
             Require all granted
            </Directory>

            # restorecon -Rfv /var/www
            # systemctl restart httpd
```

---

9. Secure web service.

a)- Configure TLS encryption for the web server "https://serverX.example.com"
- A signed certificate for web server is available at http://classroom.example.com/pub/tls/certs/serverX.crt
- Required key for this certificate file is available at http://classroom.example.com/pub/tls/private/serverX.key
- The certificate for signing authority is provided at http://classroom.example.com/pub/example-ca.crt

Ans:

```
        # mkdir -p /srv/www0/www
        # cd /srv/www0/www
        # cat > index.html
          This is a from https_TLS

        # cd /etc/httpd/conf.d
        # vim tls.conf
          Listen 443 https

<VirtualHost _default_:443>
ServerName www.example.com
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5
SSLHonorCipherOrder on
SSLCertificateFile /etc/pki/tls/certs/server0.crt
SSLCertificateKeyFile /etc/pki/tls/private/server0.key
SSLCertificateChainFile /etc/pki/tls/certs/example-ca.crt
DocumentRoot /srv/www0/www
</VirtualHost>
```

```
<Directory "/srv/www0/www">
            Require all granted
           </Directory>

           # restorecon -Rfv /srv/
           # systemctl restart httpd
```

OR

b)- Configure your web server to display the dynamic web contents.
- Dynamic content is provided by a virtual host named as http://dynamic.example.com
- This host should listen on port no 8877
- Download a copy of script from http://172.25.254.250/pub/webapp.wsgi and place it on appropriate location for virtual host so that it generates dynamic web contents.
- Do not make any changes in webapp.wsgi file
- Clients connecting to https://dynamic.example.com:8877 should get the output of dynamic web content

- This virtual host must be accessible to all the systems in example.com.
- A signed certificate for web server is available at http://classroom.example.com/pub/tls/certs/serverX.crt
- Required key for this certificate file is available at http://classroom.example.com/pub/tls/private/serverX.key
- The certificate for signing authority is provided at http://classroom.example.com/pub/example-ca.crt

Ans:

```
        # mkdir -p /srv/webapp0/www
        # cd /srv/webapp0/www
        # wget http://172.25.254.250/pub/webapp.wsgi

        # cd /etc/httpd/conf.d
        # vim wsgi.conf
          Listen 8877 https

<VirtualHost dynamic.example.com:8877>
ServerName  dynamic.example.com
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5
SSLHonorCipherOrder on
SSLCertificateFile /etc/pki/tls/certs/server0.crt
SSLCertificateKeyFile /etc/pki/tls/private/server0.key
SSLCertificateChainFile /etc/pki/tls/certs/example-ca.crt
WSGIScriptAlias / /srv/webapp/www/webapp.wsgi
</VirtualHost>


<Directory "/srv/webapp0/www">
            Require all granted
```

```
            </Directory>

            # restorecon -Rfv /srv/
            # systemctl restart httpd
```

---

10. Create a directory named as secret in default DocumentRoot of your default web server.
- Download a file - http://classroom.example.com/pub/private.html to secret directory.
- Rename this file as index.html
- The secret directory should be only available to localhost.

Ans:

```
            # cd /var/www/html
            # mkdir secret
            # cd /var/www/html/secret
            # wget http://classroom.example.com/pub/private.html
            # mv private.html index.html

            # vim /etc/httpd/conf.d/webhost.conf
               <Directory "/var/www/html/secret">
                order deny,allow
                deny from all
                allow from server0.example.com
               </Directory>
            # systemctl restart httpd
            # restorecon -RFv /var/www
```

---

11. Configure NFS on system1 as follow
- export /public directory with read only acess to network0.example.com domain.
- export /protected directory with read write acess to network0.example.com domain
- Acess to /protected is authenticate by using Kerborse. You can use keytab file from http://classroom.example.com/pub/keytabs/serverX.keytab
- Create a secure directory inside the /protected directory
- User smith have read and write acess on secure directory

Ans: lab nfskrb5 setup

```
            # yum install nfs* -y
            # systemctl start nfs-server
            # systemctl enable nfs-server
            # wget -o /etc/krb5.keytab
http://classroom.example.com/pub/keytabs/server0.keytab
            # systemctl start nfs-secure-server
            # systemctl enable nfs-secure-server
            # mkdir /public
            # mkdir /protected
            # chmod -R 777 /protected
```

```
# vim /etc/exports
  /public  *.example.com(ro.sync)
  /protected *.example.com(rw,sec=krb5p)
# exportfs -r
# showmount -e
# firewall-cmd --permanent --add-service=nfs
# firewall-cmd --reload
# systemctl restart nfs-server
# systemctl restart nfs-secure-server
```

---

12. Configure NFS client on system2 as follow
- /public share should be mount on /mnt/nfs directory with only read permission.
- /protected directory should be mount on /mnt/nfssecure with krb5p authentication and write permission to client.
- You can use keytab file from http://classroom.example.com/pub/keytabs/desktopx.keytab

Ans: lab nfskrb5 setup

```
# yum install nfs-utils -y
# wget -O /etc/krb5.keytab
http://classroom.example.com/pub/keytabs/desktop0.keytab
# mkdir -p /mnt/nfs
# mkdir -p /mnt/nfssecure
# mount -o ro,sync server0.example.com:/public  /mnt/nfs
# mount -o rw,sec=krb5p server0.example.com:/protected
/mnt/nfssecure
# vim /etc/fstab
  server0.example.com:/public  /mnt/nfs  nfs  defaults,ro,sync   0 0
  server0.example.com:/protected  /mnt/nfssecure  nfs
defaults,rw,sec=krb5p  0 0
# systemctl restart nfs-secure
```

---

13. Share /common directory via smb from your system1
- Share name must be smbshare.workgroup should be TEAM.
- Samba share must browseable.
- Members of the marketing group have a read and write permissions on the smbshare.
- User natasha should have read access on it and authenticate with the password "postroll"
- sarah should have read and write access on share and she is also member of marketing team,authenticate with the "postroll" .

Ans:

```
# yum install samba samba-client -y
# systemctl start smb nmb
# systemctl enable smb nmb
# mkdir /common
# cd /common
# cat> smbtest
  this is a samba share file
# vim /etc/samba/smb.conf
```

```
  WORKGROUP = TEAM
  at the end of file,
  [ smbshare ]
  path = /common
  write list = @marketing
  browseable = yes
# testparm

# useradd -s /sbin/nologin sarah
# useradd -s /sbin/nologin natasha
# smbpasswd -a sarah
# smbpasswd -a natasha
# systemctl restart smb nmb
# groupadd marketing
# usermod -G marketing sarah
# chgrp marketing /common
# chmod -R 755 /common
# semanage fcontext -a -t samba_share_t '/common(/.*)?'
# Restorecon -RFv /common
# firewall-cmd --permanent --add-service=samba
# firewall-cmd --reload
```

---

14. - The samba share must be permanently mounted on system2 machine on /mnt/multiuser directory with multiuser mount option.
- The smb share is mounted with credentials file by using username sarah.
- This share must allow anyone who can authenticate as sarah.

Ans:
```
# yum install cifs-utils -y
# mkdir /mnt/multiuser
# vim /root/smb-multiuser.txt
  username=sarah
  password=postroll
# vim /etc/fstab
  //server0.example.com/smbshare  /mnt/multiuser  cifs
credentials=/root/smb-multiuser.txt,multiuser, sec=ntlmssp    0 0
# mount -a
#su - sarah
#cifscreds add server0
# cd /mnt/multiuser
# vi smbtest
Also check by natasha user for read only access
```

---

15. Configure iscsi target on ServerX machine.
- iscsi disk name is iqn.2014-06.com.example:serverX.Iscsi
- iscsi should use default port as 3260.
- target should use 3G backing volume nameing as iscsi_vol.
- target should available to only system2 machine.

Ans:
```
# yum install targetd targetcli -y
# systemctl start target
```

```
        # systemctl enable target
        # fdisk /dev/vdb
        # select p
        create partion 4G with id code 8e it will show,

         /dev/vdb1    LINUX LVM
        # partprobe /dev/vdb
        # pvcreate /dev/vdb1
        # vgcreate iscsi_vg /dev/vdb1
        # lvcreate -L 3G -n iscsi_vol iscsi_vg
        # lvdisplay
        # targetcli
        # /backstores/block/ create server0.Iscsi /dev/iscsi_vg/iscsi_vol
        # /iscsi create iqn.2014-06.com.example:serverX.Iscsi
        # /iscsi/iqn.2014-06.com.example:serverX.Iscsi/tpg1/acls create
iqn.2014-06.com.example:desktop0.Iscsi
        # /iscsi/iqn.2014-06.com.example:serverX.Iscsi/tpg1/luns
create /backstores/block/server0.Iscsi
        # /iscsi/iqn.2014-06.com.example:serverX.Iscsi/tpg1/portals
create 172.25.0.11
        # ls
        # exit
        # firewall-cmd --permanent --add-port=3260/tcp
        # firewall-cmd -reload
```

---

16. Configure system2 machine for iscsi intiator.

- Iscsi device should be automatically mounted at booting time.
- Iscsi should contain a block of 200MB and should have xfs file system on it.
- The partion must be mounted on /mnt/iscsi and it should be automatically mounted.

```
        # yum install iscsi-initiator-utils -y

        # vim /etc/iscsi/initiatorname.iscsi
           InitiatorName=iqn.2014-06.com.example:desktop0.Iscsi
        # systemctl start iscsi
        #systemctl enable iscsi
        # iscsiadm -m discovery -t st -p 172.25.0.11 ---after this cmd you
will get iqn
        # iscsiadm -m node -T iqn.2014-06.com.example:serverX.Iscsi -l
        # lsblk
        # tailf /var/log/messges
        in above cmd output it will show attached disk,/dev/sda
        # fdisk /dev/sda
          create normal partition of 200MB size /dev/sda1
        # partprobe /dev/sda
        # mkfs -t xfs /dev/sda1
        # mkdir /mnt/iscsi
        # mount /dev/sda1  /mnt/iscsi
        # blkid /dev/sda1  -------now u will get UUID of /dev/sda1
        # vim /etc/fstab
          UUID=xxxxxxxxxxxx  /mnt/iscsi   xfs  defaults,_netdev  0 0
```

```
        # df -hT
          /dev/sda1    200M    /mnt/iscsi

        # iscsiadm -m session –u
```

17. Configure local mail service
- In exam do it on both systems
- The system1 do not accept incoming email from external sources.
- Any mail send locally on system1 is automatically routed from server.network0.example.com(smtpx.example.com)
- You may test your configuration by sending email to the local user 'ali'.The system2 has been configured to drop mail for this user info

http://system2.network0.example.com/receivedmail/1(http://desktop0.example.com/receivedmail/1)

Ans:
```
# yum install postfix -y
# systemctl start postfix
# systemctl enable postfix
# vim /etc/postfix/main.cf
  inet_interfaces = loopback-only
  myorigin = desktop0.example.com
  relayhost = [smtp0.example.com]
  mydestination =
  mynetworks = 172.25.0.0/24,127.0.0.0/8
# systemctl restart postfix
# firewall-cmd --permanent --add-service=smtp
# firewall-cmd --reload
# mail -s "null client" ali@desktop0.example.com
  null client test
  EOT
```

18. Make a following Scripts
- script1
- Create a script myusers.sh for creating users from userlist file.
- file downloaded from http://classroom.example.com/pub/userlist path.
- when userlist as first argument provided it will be created all the users as per users name specify in userlist file and all users should be appear /bin/false login shell. If other argument provided it will display "Invalid file name" output.
- if not providing any argument it will display "Invalid Argument"

Ans:
```
# vim script1.sh
 #!/bin/bash
if [ $# == 0 ]; then
```

```
            echo "Invalid Argument"
            exit
            elif [ $1 == userlist ]; then
            for i in `more /root/userlist`
            do
            useradd -s /bin/false "$i"
            done
            else
            echo "Invalid output file"
            fi
```

- Script2
- Create a script /root/script.sh with executable by all such a manner
- with input "print" output should be "python"
- with input "python" output should be "print"
- with input any value output should be "python|print"
- with no input, output should be "Invalid Argument"

Ans:

```
#!/bin/bash
if [ $# == 0 ]; then
echo "Invalid Argument"
elif [ $1 == python ]; then
echo  "print"
elif [ $1 == print ]; then
echo "python"
else
echo "python|print"
fi
```

---

19. Mariadb Database

create a "contacts" database and accept connections only from local clients.

root password should be "postroll"

For creating complete backup download backup file from http://classroom.example.com/pub/mydb.dump.Also create user john for accept connection from localhost with all privileges and another user steve for accept connection from any host for insert,update,delete and select privileges.

Ans:

```
# yum groupinstall mariadb mariadb-client -y
# systemctl start mariadb
# systemctl enable mariadb
# ss -tunlp | grep mysql
its showing, LISTEN  *:3306
# vim /etc/my.cnf
  in section [mysqld], add the below line
skip-networking=1
# systemctl restart mariadb
again check by cmd, # ss -tunlp | grep mysql   ----------this cmd should now return nothing

# mysql_secure_installation ------------set password postroll
# mysql -u root -p
```

```
      > show databases;
      > create database contact;
      > exit;
    # wget http://classroom.example.com/pub/mydb.dump
    # mysql -u root contact < /root/mydb.dump

  now check by connecting again to mariadb,

    # mysql -u root -p
    # use contact;
    # show tables;
    # create user john@localhost identified by 'postroll';
    # create user steve@'%' identified by 'postroll';
    # grant all privileges on contact.* to john@localhost;
    # grant insert,update,delete,select on contact.* to steve@'%';
    # flush privileges;
    #exit;
Now connect with user john and steve for vrify privileges.
```

---

20. Use above specified database and fire query for user mobius. Insert query such that searching all details like username,password,email id for user "mobius".

Ans:

```
    # mysql -u root -p
    # use contact;
    # show tables;
    # select username,password,email id from <table name> where user
= 'mobius';
```