

RHCE^{Q&As}

Red Hat Certified Engineer — RHCE

Pass RedHat RHCE Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/rhce.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by RedHat
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

SIMULATION

There were two systems: system1, main system on which most of the configuration take place system2, some configuration here Webpage content modification. Implement website for <http://serverX.example.com/owndir> Create a directory named as "owndir" under the document root of webserver Download <http://station.network0.example.com/pub/rhce/restrict.html> Rename the file into `index.html` The content of the `owndir` should be visible to everyone browsing from your local system but should not be accessible from other location

A. explanation

Correct Answer: A

```
mkdir /var/www/html/owndir
restorecon -Rv /var/www/html
cd /var/www/html/owndir
```

```
wget http://station.network0.example.com/pub/rhce/restrict.html
my restrict.html index.html
```

```
vi/etc/httpd/conf.d/server1.conf
```

(Add this)

```
<Directory "/var/www/html/owndir">
AllowOverride None
Require all Denied
Require local
</Directory>
```

```
systemctl restart httpd
```

QUESTION 2

SIMULATION

There were two systems: system1, main system on which most of the configuration take place system2, some configuration here

NFS server. Configure serverX with the following requirements Share the `/nfsshare` directory within the `example.com` domain clients only, share must be writable Share the `/nfssecure`, enable `krb5p` security to secure access to the NFS share from URL <http://station.network0.example.com/pub/keytabs/serverX.keytab> Create a directory named as `protected` under `/nfssecure` The exported directory should have read/write access from all subdomains of the `example.com` domain Ensure the directory `/nfssecure/protected` should be owned by the user `harry` with read/write permission

A. explanation

Correct Answer: A

```
yum install -y nfs*
```

```
mkdir -p /nfsshare  
chmod 0777 /nfsshare
```

```
vim /etc/exports  
/nfsshare *.example.com(rw)
```

```
systemctl restart nfs-server  
systemctl enable nfs-server  
firewall-cmd --permanent --add-service=nfs  
firewall-cmd --reload
```

```
mkdir -p /nfssecure  
wget -O /etc/krb5.keytab  
http://station.network0.example  
.com/pub/keytabs/serverX.keytab
```

```
vim /etc/sysconfig/nfs  
RPCNFSARGS="-V 4.2"
```

```
systemctl enable nfs-secure-server  
mkdir /nfssecure/protected  
vim /etc/exports  
/nfssecure * .example.com(rw,sec=krb5p, sync)  
grep -i "harry" /etc/passwd  
(If it return nothing, then create the user harry)  
[indent =1] useradd -u 300 harry --- IT SHOULD BE  
nologin or not? [/indent]  
chown harry /nfssecre/protected
```

Best it do like this:

```
setfacl -m u:harry:rwX/nfssecure/protected  
exportfs -r
```

```
semanage fcontext -a -t public_content_rw_t  
"/nfsshare(/.*)?"  
semanage fcontext -a -t public_content_rw_t  
"/nfsshare(/.*)?"  
restorecon -Rv /nfssecure/  
firewall-cmd --permanent --add-service=rpc-bind  
firewall-cmd --permanent --add-service=mountd  
firewall-cmd -reload
```

```
systemctl restart nfs-server  
systemctl restart nfs-secure-server  
systemctl enable nfs-secure-server
```

QUESTION 3

SIMULATION

There are two different networks 192.168.0.0/24 and 192.168.1.0/24. Where 192.168.0.254 and 192.168.1.254 IP Address are assigned on Server. Verify your network settings by pinging 192.168.1.0/24 Network's Host.

A. explanation

Correct Answer: A

```
1. vi /etc/sysconfig/network
```

```
NETWORKING=yes
```

```
HOSTNAME=station?.example.com
```

```
GATEWAY=192.168.0.254
```

```
2. service network restart
```

Or

```
1. vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

```
DEVICE=eth0
```

```
ONBOOT=yes
```

```
BOOTPROTO=static
```

```
IPADDR=X.X.X.X
```

```
NETMASK=X.X.X.X
```

```
GATEWAY=192.168.0.254
```

```
2. ifdown eth0
```

```
3. ifup eth0
```

QUESTION 4

SIMULATION

There were two systems:

system1, main system on which most of the configuration take place

system2, some configuration here

Link aggregation.

Configure your serverX and desktop, which watches for link changes and selects an active port for data transfers.

serverX should have the address as 192.169.X.10/255.255.255.0

desktopX should have the address as 192.168.X.11/255.255.255.0

(Note: where X is your station number)

A. explanation

Correct Answer: A

On Server Machine: Verification and Testing:

```
nmcli con add type team con-name Team1 ifname Team1
        config '{"runner":{"name":"activebackup"}}'

nmcli con modify Team1 ipv4.addresses 192.168.1.10/24
nmcli con modify Team1 ipv4.method manual
nmcli con add type team-slave con-name Team1-slave1 ifname eth1 master Team1
nmcli con add type team-slave con-name Team1-slave2 ifname eth2 master Team1

nmcli con up Team1
nmcli con up Team1-slave1
nmcli con up Team1-slave2
```

```
teamdctl Team1 state
nmcli dev dis eth1 ---> Disconnect device for verification
nmcli con up Team1-slave1
teamnl Team1 ports
teamnl Team1 getoption activeport
teamnl Team1 setoption activeport PORT_NUMBER

ping -I Team1 192.168.1.11
```

On Desktop Machine:

```
nmcli con add type team con-name Team1 ifname Team1 config '{"runner":
{"name": "activebackup"}}'
nmcli con modify Team1 ipv4.addresses 192.168.1.11/24
nmcli con modify Team1 ipv4.method manual
nmcli con add type team-slave con-name Team1 -slave1 ifname eth1 master
Team1
nmcli con add type team-slave con-name Team1 -slave2 ifname eth2 master
Team1

nmcli con up Team1
nmcli con up Team1 -slave1
nmcli con up Team1 -slave2
```

Verification and Testing:

```
teamdctl Team1 state
nmcli dev dis eth1 ---> Disconnect device
for verification
nmcli con up Team1-slave1
teamnl Team1 ports
teamnl Team1 getoption activeport
teamnl Team1 setoption activeport
PORT_NUMBER

ping-I Team1 192.168.1.10
```

QUESTION 5

SIMULATION

Configure the samba server, share /common, which can be browsed. The user harry can only read it. If it is needed, the password for harry is harryuser.

A. explanation

Correct Answer: A

```
# yum install -y samba samba-common samba-client
# chkconfig smb on
# chkconfig nmb on      (nmb is a dependency of smb to resolve netbios)
# service smb start
# service nmb start

# useradd harry
# smbpasswd -a harry
# mkdir /common
# vim /etc/samba/smb.conf
    [common]
        comment = common
        path = /common
        browseable = yes
        valid user = harry
        read only = yes

testparm
# getsebool -a |grep samba_share_nfs
# setsebool -P samba_share_nfs=1
# chcon -R --reference=/var/spool/samba/ /common/
# services smb restart
# mount -t cifs //172.16.30.5/common /mnt -o
username=harry,password=harryuser
# smbclient //172.24.50.5/common -U harry
```

[Latest RHCE Dumps](#)

[RHCE Study Guide](#)

[RHCE Exam Questions](#)