4th February 2016

RHCE 7 exam point of view question and Answer | RHCE 7 dums

Note:- This only for the practice purpose. Know the exam set-up and clear your RHCE 7 in first attempt. Wish you all the best.

O Additional information -----> Click this to know following information

Domain Name:
System1: system1.district10.example.com use as Server
System2: system2.district10.example.com use as Client
IP Address:
System1:172.24.10.110/24
System1:172.24.10.120/24
Name Server: 172.24.10.250
Gateway:172.24.10.254
Root password : zaldebro
Your Domain: district10.example.com
Your Subnet : 172.24.10.0/255.255.255.0
Yum path ***http://station.district0.example.com/content/rhel7.0/x86_64/dvd***

Note:(for this subnetmask CIDR value is /24)

ssh -X root@ [mailto:root@system1.district10.example.com] system1.district10.example.com
(or)
#ssh -X root@172.24.10.110
Password:zaldebro
[root@system1 ~]#iptables -F
[root@system1 ~] # systemctl mask iptables.service
[root@system1 ~] # systemctl mask ip6tables.service
[root@system1 ~] # systemctl mask ebtables.service

ssh -X root@system2.district10.example.com [mailto:root@system1.district10.example.com]
(or)
#ssh -X root@172.24.10.120
Password:zaldebro

[root@system1 ~]#iptables -F
[root@system2 ~] # systemctl mask iptables.service
[root@system2 ~] # systemctl mask ip6tables.service
[root@system2 ~] # systemctl mask ebtables.service

1. Enable Selinux on enforcing method

Do This on Both Server and Client
server side: (System1)
[root@system1 ~]# getenforce
[root@system1 ~]# vim /etc/sysconfig/selinux
Set SELINUX = enforcing
:wq
[root@system1 ~]#setenforce 1
[root@system1 ~]#init 6
[root@system1 ~]# getenforce
Enforcing

Client Side: (System2)
[root@system2 ~]# getenforce
[root@system2 ~]# vim /etc/sysconfig/selinux
Set SELINUX = enforcing
:wq
[root@system2 ~]#setenforce 1
[root@system2 ~]#init 6
[root@system2 ~]# getenforce
Enforcing
[root@ system2 ~]#

Yum Client Configuration

2.Configure repository. Create a Repository for your virtual machines. The URL is

http://station.district0.example.com/content/rhel7.0/x86_64/dvd

Do This on Both Server and Client
System1 :
[root@ system1 ~]# cd /etc/yum.repos.d/

[root@ system1 ~]# vim system1.repo

[system1]
name=server
*baseurl=**http://station.district0.example.com/content/rhel7.0/x86_64/dvd***
enabled=1
gpgcheck=0

[root@ system1 ~]# yum clean all

[root@ system1 ~]# yum repolist all

System 2:

[root@ system2 ~]# cd /etc/yum.repos.d/

[root@ system2 ~]# vim system1.repo

[system2]
name=client
*baseurl=**http://station.district0.example.com/content/rhel7.0/x86_64/dvd***
enabled=1
gpgcheck=0

[root@ system2 ~]# yum clean all

[root@ system2 ~]# yum repolist all

3. SSH Configuration.
-Clients within my133ilt.org should NOT have access to ssh on your systems
-Clients with domain district10.example.com should be able to access the systems

in case you my133ilt.org has ***(172.25.70.0/255.255.0.0)***

Ans:

Do This on Both Server and Client

[root@ system1 ~]# vim /etc/hosts.allow
sshd: *.district10.example.com *(**Note** sshd:space *.given domain nam)*
:wq
(or)

[root@ system1 ~]# vim /etc/hosts.allow
sshd: 172.25.10.0/255.255.255.0 *(**Note** sshd:space *.given domain address)*

[root@ system1 ~]# vim /etc/hosts.deny
*sshd: *.my133ilt.org (**Note** sshd:space *.given domain name)*
:wq

[root@ system1 ~]# vim /etc/hosts.deny
*sshd: 172.25.70.0/255.255.255.0 (**Note** sshd:space *.given domain address)*

4. Port forwarding.
-Configure system1 to forward traffic incoming on port 80/tcp from source network 172.24.X.0/255.255.255.0 to port on 5243/tcp

Ans:

Server side

client:(to verify in your local environment ask me if not working)
server5.example.com:5243

[root@ system1 ~]# firewall-cmd - -permanent - -add-rich-rule 'rule family=ipv4 source address=172.24.10.0/24 forward-port port=5243 protocol=tcp to-port=80'

[root@ system1 ~]# firewall-cmd - -reload

[root@ system1 ~]# firewall-cmd - -list-rich-rules

(or)

Configure serverX to forward traffic incoming on port 80/tcp from source network 172.25.X.0/255.255.255.0 to port on 5243/tcp.

[root@ system1 ~]# ***firewall-config***

Configuration : Permanent

Select → Rich Rule Tab

click →Add

Family : ipv4
Check Elements → forward-port [Click this tab]
|
|
V
protocol ***:*** *tcp*
Port / Port Range: 5243

Destination
check ***Local forwarding***
Port / Port Range: 80

*click [**ok**]*
Source :172.24.10.0/24
click ***[OK]***
click option *→reload Firewalld (in terminal put* ***# firewall-cmd - -list-rich-rules*** *)*

5. User Environment.

-Create a command called qstat on both system1 and system2. It should able to execute the following command(ps eo pid,tid,class,rtprio,ni,pri,psr,pcpu,stat,wchan:14,comm)
The command should be executable by all users..

Ans:

Server side :
[root@ system1 ~]# vim /bin/qstat

ps eo pid,tid,class,rtprio,ni,pri,psr,pcpu,stat,wchan:14,comm

:wq

[root@ system1 ~]#chmod a+x /bin/qstat

[root@ system1 ~]#qstat

PID	TID	CLS	RTPRIO	NI	PRI	PSR	%CPU	STAT	WCHAN	COMMAND
1271	1271	TS	-	0	19	0	0.0	Ss+	poll_schedule_	Xorg
1502	1502	TS	-	0	19	0	0.0	Ss+	n_tty_read	agetty
1632	1632	TS	-	0	19	0	0.0	Ss	wait	bash
29595	29595	TS	-	0	19	0	0.0	S+	wait	bash
29596	**29596**	**TS**	-	**0**	**19**	**0**	**0.0**	**R+**	-	**ps**

Client side :
[root@ system1 ~]# vim /bin/qstat

ps eo pid,tid,class,rtprio,ni,pri,psr,pcpu,stat,wchan:14,comm

:wq

[root@ system1 ~]#chmod a+x /bin/qstat

[root@ system1 ~]#qstat

PID	TID	CLS	RTPRIO	NI	PRI	PSR	%CPU	STAT	WCHAN	COMMAND
1271	1271	TS	-	0	19	0	0.0	Ss+	poll_schedule_	Xorg
1502	1502	TS	-	0	19	0	0.0	Ss+	n_tty_read	agetty
1632	1632	TS	-	0	19	0	0.0	Ss	wait	bash
29595	29595	TS	-	0	19	0	0.0	S+	wait	bash
29596	29596	TS	-	0	19	0	0.0	R+	-	ps

_

6.IPV 6 Connection
-Configure eth0 with a static ipv6 addresses as follows.
-configure a static IPV6 address in system1 as fddb:fe2a:ab1e::c0a8:64/64.
-configure a static IPV6 address in system2 as fddb:fe2a:ab1e::c0a8:02/64.
-Both machines are able to communicate within the network fddb:fe2a:able/64
-The changes should be permanent even after the reboot
Ans :
Server Side:

*[root@ system1 ~]#**nmcli connection show***

```
NAME        UUID                                  TYPE           DEVICE
System eth0  5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  802-3-ethernet  eth0
```

*[root@ system1 ~]#**nmcli device status***

```
DEVICE  TYPE      STATE         CONNECTION
eth0    ethernet  connected     System eth0
eno1    ethernet  disconnected  --
eno2    ethernet  disconnected  --
lo      loopback  unmanaged     --
```

*[root@ system1 ~]# **nmcli connection modify "System eth0" ipv6.addresses fddb:fe2a:ab1e::c0a8:64/64 ipv6.method manual***

*[root@ system1 ~]# **nmcli connection up "System eth0"***

Client Side:

*[root@ system2 ~]# **nmcli connection show***

```
NAME        UUID                                  TYPE           DEVICE
System eth0  5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  802-3-ethernet  eth0
```

*[root@ system2 ~]# **nmcli device status***

```
DEVICE  TYPE      STATE         CONNECTION
eth0    ethernet  connected     System eth0
eno1    ethernet  disconnected  --
eno2    ethernet  disconnected  --
lo      loopback  unmanaged     --
```

*[root@ system2 ~]# **nmcli connection modify "System eth0" ipv6.addresses fddb:fe2a:ab1e::c0a8:02/64 ipv6.method manual***

*[root@ system2 ~]# **nmcli connection up "System eth0"***

Client Side:-

*[root@ system2 ~]# **ping6 fddb:fe2a:ab1e::c0a8:64***

Server Side:-
*[root@ system1 ~]# **ping6 fddb:fe2a:ab1e::c0a8:02** **(do this on both side if packet transmited & received same means correct other wise wrong)***

–

7. Link aggregation Configure your system1 and system2, which watches for link changes and selects an active port for data transfers. System1 should have the address as 172.24.10.10/255.255.255.0. System2 should have the address as 172.24.10.20/255.255.255.0

*[root@ system1 ~]# **nmcli connection show***

```
NAME        UUID                                  TYPE           DEVICE
System eth0  5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  802-3-ethernet  eth0
```

*[root@ system1 ~]# **nmcli device status***

```
DEVICE  TYPE      STATE         CONNECTION
eth0    ethernet  connected     System eth0
```

```
eno1    ethernet   disconnected  --
eno2    ethernet   disconnected  --
lo      loopback   unmanaged     --
```

System1 Side:

```
[root@ system1 ~]# nmcli connection add type team ifname team config '{"runner": {"name": "activebackup"}}'
[root@ system1 ~]# nmcli connection modify team-team ipv4.addresses 172.24.10.10/24 ipv4.method manual
[root@ system1 ~]# nmcli connection show

NAME        UUID                                  TYPE           DEVICE
System eth0  5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  802-3-ethernet  eth0
team-team    e10a27c3-bd4a-431a-a284-50375a3c4717  team           team

[root@ system1 ~]# nmcli connection add type team-slave ifname eno1 master team
[root@ system1 ~]# nmcli connection add type team-slave ifname eno2 master team
[root@ system1 ~]# nmcli connection up team-team
[root@ system1 ~]# teamdctl team state
setup:
 runner: activebackup
ports:
 eno1
   link watches:
     link summary: up
     instance[link_watch_0]:
       name: ethtool
       link: up
 eno2
   link watches:
     link summary: up
     instance[link_watch_0]:
       name: ethtool
       link: up
runner:
 active port: eno2
```

Client Side :

```
[root@ system2 ~]# nmcli connection show

NAME        UUID                                  TYPE           DEVICE
System eth0  5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  802-3-ethernet  eth0

[root@ system2 ~]# nmcli device status

DEVICE  TYPE      STATE         CONNECTION
eth0     ethernet   connected     System eth0
eno1    ethernet   disconnected  --
eno2    ethernet   disconnected  --
lo      loopback   unmanaged     --
```

System2 Side:

```
[root@ system2 ~]# nmcli connection add type team ifname team config '{"runner": {"name": "activebackup"}}'
[root@ system2 ~]# nmcli connection modify team-team ipv4.addresses 172.24.10.20/24 ipv4.method manual
[root@ system2 ~]# nmcli connection show

NAME        UUID                                  TYPE           DEVICE
System eth0  5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  802-3-ethernet  eth0
team-team    e10a27c3-bd4a-431a-a284-50375a3c4717  team           team

[root@ system2 ~]# nmcli connection add type team-slave ifname eno1 master team
```

[root@ system2 ~]# ***nmcli connection add type team-slave ifname eno2 master team***
[root@ system2 ~]# ***nmcli connection up team-team***
[root@ system2 ~]# ***teamdctl team state***

```
setup:
 runner: activebackup
ports:
 eno1
   link watches:
     link summary: up
     instance[link_watch_0]:
       name: ethtool
       link: up
 eno2
   link watches:
     link summary: up
     instance[link_watch_0]:
       name: ethtool
       link: up
runner:
 active port: eno2
```

server side:-
#ping -I team-team 172.25.10.20

---

8. SMTP Configuration. Configure the SMTP mail service on system1 and system2 which relay the mail
only from local system through station.network0.example.com, all outgoing mail have their sender domain as district10.example.com. Verify the mail server is working by sending mail to a local user clarke.
Check the mail on both system1 and system2 with the below URL

http://rhcert.district0.example.com

System1

[root@ system1 ~]# ***yum install postfix* -y***

[root@ system1 ~]# ***firewall-cmd –permanent –add-service=smtp***

[root@ system1 ~]# ***firewall-cmd –reload***

[root@ system1 ~]# ***systemctl restart postfix.service***

[root@ system1 ~]# ***systemctl enable postfix.service***

[root@ system1 ~]# ***vim /etc/postfix/main.cf***

Line No 99 : (Remove #) myorigin = district10.example.com

Line No 116 : inet_interfaces = loopback-only

Line No 164 : mydestination =

Line No 317 : (Remove #) relayhost = [station.network0.example.com]

[root@ system1 ~]# ***systemctl restart postfix.service***

[root@ system1 ~]# ***mail -s “HAI” clarke***

This is test mail

.

EOT

To Verify

Click the above Links

System2

[root@ system2 ~]# ***yum install postfix* -y***

[root@ system2 ~]# ***firewall-cmd –permanent –add-service=smtp***

[root@ system2 ~]# ***firewall-cmd –reload***

[root@ system2 ~]# ***systemctl restart postfix.service***

[root@ system2 ~]# ***systemctl enable postfix.service***

[root@ system2 ~]# ***vim /etc/postfix/main.cf***

Line No 99 : (Remove #) myorigin = district10.example.com

Line No 116 : inet_interfaces = loopback-only

Line No 164 : mydestination = “”

Line No 317 : (Remove #) relayhost = [station.network0.example.com]

[root@ system2 ~]# ***systemctl restart postfix.service***

[root@ system2 ~]# ***mail -s “HAI” clarke***

This is test mail

.

EOT

To Verify

Click the above Links

9. NFS server

- Configure system1 with the following requirements.
- Share the /nfsshare directory within the district10.example.com domain clients only, share must not be writable.

Ans:

[root@ system1 ~]# ***yum install nfs* -y***

[root@ system1 ~]# ***systemctl start nfs-server***

[root@ system1 ~]# ***systemctl enable nfs-server***

[root@ system1 ~]# ***mkdir /nfsshare***
(Note : Here no need to give nfsnobody permission for read only share)

[root@ system1 ~]# ***vim /etc/exports***

/nfsshare *.district10.example.com(ro,sync)

:wq

[root@ system1 ~]# ***exportfs -a***
[root@ system1 ~]# ***exportfs -r***
[root@ system1 ~]# ***exportfs***

[root@ system1 ~]# ***systemctl restart nfs-server***

[root@ system1 ~]# ***firewall-cmd --permanent --add-service=nfs***

[root@ system1 ~]# ***firewall-cmd --permanent --add-service=rpc-bind***
t
[root@ system1 ~]# ***firewall-cmd --permanent –add-service=mountd***

[root@ system1 ~]# ***firewall-cmd –reload***

[root@ system1 ~]# ***showmount -e 172.24.10.110***
Export list for server2:
/nfsshare *. district10.example.com

Nfs mount

-Mount /nfsshare directory on system2 under /public directory persistently at system boot time.
Ans:

[root@ system2 ~]# ***mkdir /public***

[root@ system2 ~]# ***yum install nfs-utils* -y***

[root@ system2 ~]# ***vim /etc/fstab***

172.24.10.110:/nfsshare /public nfs defaults 0 0

:wq

[root@ system2 ~]# ***mount -a***
[root@ system2 ~]# ***df -h***

```
Filesystem              Size  Used  Avail  Use%  Mounted on
/dev/vda1               10G   3.1G  7.0G   31%   /
devtmpfs                906M  0     906M   0%    /dev
tmpfs                   921M  140K  921M   1%    /dev/shm
tmpfs                   921M  17M   904M   2%    /run
tmpfs                   921M  0     921M   0%    /sys/fs/cgroup
172.24.10.110:/nfsshare 10G   3.6G  6.5G   36%   /public
```

[root@ system2 ~]# ***cd /public***

Read Only share Output:

[root@ system2 ***public]# touch nfs.txt***

touch: cannot touch '777': Read-only file system

NFS KERBEROS

NFS Secure:

-Share the /nfssecure, enable krb5p security to secure access to the NFS share from URL ***http://station.network0.example.com/pub/keytabs/system1.keytab***

Create a directory named as protected under /nfssecure The exported directory should have read/write access from all subdomains of the distric10.example.com domain. Ensure the directory

/nfssecure/protected should be owned by the user harry with read/write permission..

*[root@ system1 ~]# **yum install nfs* krb5* -y (we already installed nfs package for previous*

normal share he we just install krb5 packages only)

*[root@ system1 ~]# **wget -O /etc/krb5.keytab***
http://server1.domain70.example.com/pub/keytabs/system1.keytab
[http://server1.domain70.example.com/pub/keytabs/server25.keytab]

Saving to: '/etc/krb5.keytab'

100%
[==========>] 1,242 --.-K/s in 0s

2015-12-15 13:06:28 (137 MB/s) - '/etc/krb5.keytab' saved [1242/1242]
*[root@ system1 ~]# **systemctl start nfs-server***

*[root@ system1 ~]# **systemctl start nfs-secure***

*[root@ system1 ~]# **systemctl start nfs-secure-server***

*[root@ system1 ~]# **systemctl enable nfs-server***

*[root@ system1 ~]# **systemctl enable nfs-secure***

*[root@ system1 ~]# **systemctl enable nfs-secure-server***

*[root@ system1 ~]# **mkdir -p /nfssecure/protected***

*[root@ system1 ~]# **firewall-cmd --permanent --add-service=nfs***

*[root@ system1 ~]# **firewall-cmd --permanent --add-service=rpc-bind***

*[root@ system1 ~]# **firewall-cmd --permanent - -add-service=mountd***

*[root@ system1 ~]# **firewall-cmd - -reload***

*[root@ system1 ~]# **chown harry /nfssecure/protected***

*[root@ system1 ~]# **vim /etc/exports***

/nfssecure *.district10.example.com(rw,sync,sec=krb5p)

:wq

*[root@ system1 ~]# **systemctl restart nfs-secure-server***

*[root@ system1 ~]# **showmount -e 172.24.10.110***
Export list for server2:
/nfsshare *.district10.example.com
/nfssecure *.district10.example.com

NFS Secure Client:

Mount /nfssecure/protected with krb5p secured share on system2 beneath /secure/protected provided with keytab http://station.network0.example.com/pub/keytabs/system2.keytab
The user harry able to write files on /secure directory

```
#  yum install nfs-utils* krb5*  -y

# mkdir /secure/protected

# setfacl -m u:harry:rwx /secure/

# wget  -O  /etc/krb5.keytab   http://station.network0.example.com/pub/keytabs/system2.keytab

# systemctl start nfs-secure

# systemctl enable nfs-secure

# vim /etc/fstab

172.24.10.110:/nfsshare   /public nfs     defaults       0       0
172.24.10.110:/nfssecure/protected   /secure/protected nfs     defaults, sec=krb5p       0       0

:wq

# mount -a
```

```
# df -h

Filesystem                    Size        Used     Avail    Use%     Mounted on
/dev/vda1                    10G         3.1G     7.0G     31%     /
devtmpfs                  906M       0      906M     0%     /dev
tmpfs                     921M       140K     921M     1%     /dev/shm
tmpfs                     921M       17M      904M     2%     /run
tmpfs                     921M       0      921M     0%     /sys/fs/cgroup
172.24.10.110:/nfsshare          10G        3.6G     6.5G     36%     /public
172.24.10.110:/nfssecure/protected    10G        3.3G  6.8G     33%     /secure/protected

# ssh -X harry@system2.district10.example.com [mailto:ldapuser25@desktop25.example.com]
  password:

# df -h

Filesystem                    Size        Used     Avail    Use%     Mounted on
/dev/vda1                    10G         3.1G     7.0G     31%     /
devtmpfs                  906M       0      906M     0%     /dev
tmpfs                     921M       140K     921M     1%     /dev/shm
tmpfs                     921M       17M      904M     2%     /run
tmpfs                     921M       0      921M     0%     /sys/fs/cgroup
172.24.10.110:/nfsshare          10G        3.6G     6.5G     36%     /public
172.24.10.110:/nfssecure/protected    10G        3.3G  6.8G     33%     /secure/protected
```

Read/Write Share Output:

[harry@system2 ~] # cd /secure/protected

[harry@system2 secure/protected] # touch one; mkdir two

[harry@system2 secure] # ls
one two

SAMBA :

11. SMB access.
Share the /sambadir directory via SMB on system1 Your SMB server must be a member of the STAFF workgroup The share name must be data .The data share must be available to district10.example.com domain clients only The data share must be browseable .Susan must have read access to the share, authenticating with the same password "password", if necessary

[root@ system1 ~]# ***yum install samba* -y***

[root@ system1 ~]# ***systemctl start smb nmb***

[root@ system1 ~]# ***systemctl enable smb nmb***
ln -s '/usr/lib/systemd/system/smb.service' '/etc/systemd/system/multi-user.target.wants/smb.service'
ln -s '/usr/lib/systemd/system/nmb.service' '/etc/systemd/system/multi-user.target.wants/nmb.service'

[root@ system1 ~]# ***firewall-cmd --permanent --add-service=samba***
success

[root@ system1 ~]# ***firewall-cmd --reload***
success

[root@ system1 ~]# ***mkdir /sambadir***

[root@ system1 ~]# ***semanage fcontext -a -t samba_share_t '/sambadir(/.*)?'***

[root@ system1 ~]# ***restorecon -Rv /sambadir/***
restorecon reset /sambadir context unconfined_u:object_r:default_t:s0->unconfined_u:object_r:samba_share_t:s0

[root@ system1 ~]# ***ll -Zd /sambadir/***

drwxr-xr-x. root root unconfined_u:object_r:samba_share_t:s0 /sambadir/

(all the samba user will be added in our machine because it all are domain users)

[root@ system1 ~]# ***smbpasswd -a Susan***
New SMB password:password
Retype new SMB password:password
Added user Susan.

[root@ system1 ~]# ***smbpasswd -a frankenstein***
New SMB password:SaniTago
Retype new SMB password:SaniTago
Added user frankenstein.

[root@ system1 ~]# ***smbpasswd -a martin***
New SMB password:SaniTago
Retype new SMB password:SaniTago
Added user martin.

[root@ system1 ~]# ***ll -d /sambadir/***
drwxr-xr-x. 2 root root 6 Dec 16 10:12 /sambadir/

[root@ system1 ~]# ***vim /etc/samba/smb.conf***

Line No 89 : workgroup = STAFF

Line No end of the Document:

[data]
path=/sambadir
hosts allow=172.24.10.
browseable=yes
valid users=susan
read list=susan

:wq

[root@ system1 ~]# ***systemctl restart smb nmb***

[root@ system1 ~]# ***smbclient -L //172.24.10.110***

Enter root's password: (just enter)
Anonymous login successful
Domain=[STAFF] OS=[Unix] Server=[Samba 4.1.1]

Sharename	Type	Comment
data	Disk	
IPC$	IPC	IPC Service (Samba Server Version 4.1.1)

Anonymous login successful
Domain=[STAFF] OS=[Unix] Server=[Samba 4.1.1]

Server	Comment
SYSTEM1	Samba Server Version 4.1.1

Workgroup	Master
STAFF	

[root@ system1 ~]# ***smbclient //172.24.10.110/data -U Susan***
Enter susan's password:
Domain=[STAFF] OS=[Unix] Server=[Samba 4.1.1]

smb:** \> **ls
.** **D** **0** **Wed Dec 16 10:12:30 2015
..** **D** **0** **Wed Dec 16 10:12:30 2015

40913 blocks of size 262144. 27465 blocks available
***smb:** \>*

12.SAMBA Mount

Share /opstack with SMB share name must be cluster.
The user frankenstein has readable,writeable,accesseable to the /opstack SMB share. The user martin has read access to the /opstack SMB share. Both users should have the SMB passwd "SaniTago".

The share must be browseable

Mount the samba share /opstack permanently beneath /mnt/smbspace on system2 as a multiuser mount. The samba share should be mounted with the credentials of martin.

*[root@ system1 ~]# **mkdir /opstack***

*[root@ system1 ~]# **ll -Zd /opstack/***
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 /opstack/

*[root@ system1 ~]# **semanage fcontext -a -t samba_share_t '/opstack(/.*)?'***

*[root@ system1 ~]# **restorecon -Rv /opstack/***
restorecon reset /opstack context unconfined_u:object_r:default_t:s0->unconfined_u:object_r:samba_share_t:s0

*[root@ system1 ~]# **ll -lZd /opstack/***
drwxr-xr-x. root root unconfined_u:object_r:samba_share_t:s0 /opstack/

*[root@ system1 ~]# **chmod 775 /opstack/***
*[root@ system1 ~]# **chgrp frankenstein /opstack/***

*[root@ system1 ~]# **vim /etc/samba/smb.conf***

Line No 89 : workgroup = STAFF

Line No end of the Document:

[data]
path=/sambadir
hosts allow=172.24.10.
browseable=yes
valid users=Susan
read list=Susan

[cluster]
path=/opstack
valid users=@frankenstein,martin
read list=martin
write list=@frankenstein

:wq

```
[root@server2 ~]# systemctl restart smb.service nmb.service
```

```
[root@server2 ~]# smbclient -L //172.24.10.110
Enter root's password:  (just enter)
Anonymous login successful
Domain=[STAFF] OS=[Unix] Server=[Samba 4.1.1]

   Sharename       Type      Comment
   ---------       ----      -------
   data            Disk
   cluster         Disk
   IPC$            IPC       IPC Service (Samba Server Version 4.1.1)
Anonymous login successful
Domain=[STAFF] OS=[Unix] Server=[Samba 4.1.1]

   Server               Comment
   ---------            -------
   SYSTEM1              Samba Server Version 4.1.1

   Workgroup            Master
   ---------            -------
   STAFF

[root@server2 ~]# smbclient //172.24.10.110/cluster -U frankenstein
Enter frankenstein's password:
Domain=[STAFF] OS=[Unix] Server=[Samba 4.1.1]
smb: \> mkdir test
.                   D        0  Wed Dec 16 10:32:03 2015
..                  D        0  Wed Dec 16 10:32:03 2015

        40913 blocks of size 262144. 27466 blocks available
smb: \> exit

[root@server2 ~]# smbclient //172.24.10.110/cluster -U martin
Enter martin's password:
Domain=[STAFF] OS=[Unix] Server=[Samba 4.1.1]
smb: \> ls
.                   D        0  Wed Dec 16 10:32:03 2015
..                  D        0  Wed Dec 16 10:32:03 2015

        40913 blocks of size 262144. 27466 blocks available
smb: \> exit
```

SAMBA Client :

12. Smb mount.

-mount the samba share /opstack permanently beneath /mnt/smbspace on system2 as a multiuser mount.
-the samba share should be mounted with the credentials of martin.

```
[root@desktop2 ~]# yum install cifs-utils* -y

[root@desktop2 ~]# mkdir /mnt/smbspace
```

MultiUser Mount

```
[root@desktop2 ~]# vim /etc/fstab

//172.25.2.11/cluster /mnt/smbspace   cifs    credentials=/root/credential.txt,multiuser     0      0

:wq

[root@desktop2 ~]# vim /root/credential.txt

username=martin
password=SaniTago( press enter)
:wq

[root@desktop2 ~]# mount -a
[root@desktop2 ~]# df -h
Filesystem                      Size     Used    Avail    Use%    Mounted on
/dev/vda1                       10G     3.1G     6.9G     31%    /
devtmpfs                       906M     0     906M      0%     /dev
tmpfs                          921M     80K    921M      1%       /dev/shm
tmpfs                          921M    17M    904M      2%    /run
tmpfs                          921M    0    921M      0%    /sys/fs/cgroup
//172.25.2.11/cluster            10G              3.3G     6.8G     33%   /mnt/smbspace
172.24.70.25:/nfsshare           10G              3.6G     6.5G     36%     /public
172.25.70.25:/nfssecure/protected    10G              3.3G  6.8G      33%     /secure/protected
[root@desktop2 ~]# cd /mnt/smbspace/
[root@desktop2 smbspace]# touch samba.txt
read only file system touch cannot allow
```

WEB SERVER

Normal :

– *Implement a webserver for the site* ***http://system1.district10.example.com***
– *Download the webpage from*
http://station.district0.example.com/pub/rhce/rhce.html
– *rename the downloaded file in to* ***index.html.***
– *copy the file into the document root.*
– *Do not make any modification with the content of the index.html.*
– *Webserver must be available to clients with domain* ***district10.example.com***
– *Clients within* ***my22ilt.org*** *should NOT access the webserver on your systems*

```
[root@system1 ~]# systemctl start httpd
[root@system1 ~]#  systemctl enable httpd
ln -s '/usr/lib/systemd/system/httpd.service' '/etc/systemd/system/multi-user.target.wants/httpd.service'
[root@system1 ~]#  firewall-cmd --permanent --add-service=http
success
[root@system1 ~]#  firewall-cmd --reload
success
```

[root@system1 ~]# cd /var/www/html/
[root@system1 html]# wget http://station.district0.example.com/pub/rhce/rhce.html [http://classroom.example.com/pub/rhce/rhce.html]

[root@system1 html]# ls
rhce.html
[root@system1 html]# mv rhce.html index.html
[root@system1 html]# ls
index.html
[root@system1 html]# mv rhce.html index.html
[root@system1 html]# ls
index.html
[root@system1 html]# systemctl restart httpd.service
[root@system1 html]# vim /etc/httpd/conf/httpd.conf

<virtualhost *:80>
servername system1.district10.example.com
documentroot /var/www/html
</virtualhost>

[root@system1 html]# httpd -t
Syntax OK
[root@system1 html]# systemctl restart httpd.service
[root@system1 html]# cd

[root@system1 ~]# vim /etc/hosts.deny
[root@system1 ~]# cat /etc/hosts.deny
#
 # hosts.deny This file contains access rules which are used to
 # deny connections to network services that either use
 # the tcp_wrappers library or that have been
 # started through a tcp_wrappers-enabled xinetd.
#
 # The rules in this file can also be set up in
 # /etc/hosts.allow with a 'deny' option instead.
#
 # See 'man 5 hosts_options' and 'man 5 hosts_access'
 # for information on rule syntax.
 # See 'man tcpd' for information on tcp_wrappers
#
#
sshd: *.my133ilt.org
httpd: *.my22ilt.org

:wq

[root@ system1 ~]# vim /etc/hosts.allow
sshd: *.district10.example.com
httpd: *.district10.example.com

:wq

[root@system1 ~]# systemctl restart httpd.service
[root@system1 ~]#

use firefox

address : http://server70.example.com/ [http://server2.example.com/]

this normal webpage

[root@system1 ~]# yum install elinks -y*

[root@system1 ~]# elinks system1.example.com

this normal webpage

client side

[root@system1 ~]# elinks system1.example.com

this normal webpage

Secure Web Page Hosting

Secured webserver
– configure the website https://system1.district10.example.com with TLS
– SSLCertificate file http://classroom.example.com/pub/rhce/tls/certs/system1.networkX.crt
– SSLCertificatekeyfile
http://classroom.example.com/pub/rhce/tls/private/system1.networkX.key
– SSL CA certificate file http://classroom..example.com/pub/exampleca.crt
[http://classroom.example.com/pub/example-ca.crt]

[root@system1 ~]# yum install httpd mod_ssl* -y*

[root@system1 ~]# vim /etc/httpd/conf.d/ssl.conf

Line No 56: <VirtualHost _default_:443>
Line No 59: DocumentRoot "/var/www/html"
Line No 60:ServerName https://system1.district10example.com:443
Line No 70:SSLEngine on
Line No 75:SSLProtocol all -SSLv2
Line No 80:SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5
Line No 93:(remove #)SSLHonorCipherOrder on

Line No 100: SSLCertificateFile /etc/pki/tls/certs/system1.network10.crt (change local host to your system hostname)

Line No 107: SSLCertificateKeyFile /etc/pki/tls/private/system1.network10.key (change local host to your system hostname)

Line No 122 : SSLCACertificateFile /etc/pki/tls/certs/exampleca.crt

</virtualhost>

[root@system1 ~]# cd /etc/pki/tls/certs/
[root@system1 certs]# wget http://classroom.example.com/pub/tls/certs/system1.network10.crt

[root@system1 certs]# wget http://classroom.example.com/pub/exampleca.crt
[http://classroom.example.com/pub/example-ca.crt]

[[root@system1 certs]# cd /etc/pki/tls/private/

[root@system1 private]# wget http://classroom.example.com/pub/tls/private/system1.network10.key

[root@system1 private]# cd
[root@system1 ~]# systemctl restart httpd.service

[root@system1 ~]# firewall-cmd --permanent --add-service=https
success

[root@system1 ~]# firewall-cmd --reload
success
[root@system1 ~]#

use firefox

address : https://system1.example.com/ [http://server2.example.com/]

this normal webpage

Confidential Web Hosting

webpage content modification.

Implement website for http://system1.district10.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
User harry can edit the contents of the directory

[root@system1 ~]# cd /var/www/html/

[root@system1 html]# mkdir owndir

[root@system1 html]# cd owndir/

[root@system1 owndir]# wget http://station.district0.example.com/pub/rhce/restrict.html

[root@system1 owndir]# ls

restrict.html

[root@system1 owndir]# mv restrict.html index.html

[root@system1 owndir]# ls

index.html

[root@system1 owndir]# vim /etc/httpd/conf/httpd.conf

[root@system1 owndir]# chown harry /var/www/html/owndir/

<virtualhost *:80>
servername system1.district10.example.com
documentroot /var/www/html
</virtualhost>

<directory /var/www/html/owndir>
order deny,allow
deny from all
allow from 172.24.10.110
</directory>

[root@system1 ~]# systemctl restart httpd.service

firefox:

http://system1.district10.example.com/owndir/ [http://server2.example.com/owndir/]

this restricted page

client :

[root@system2 ~]# firefox

http://system1.district10.example.com/owndir/ [http://server2.example.com/owndir/]

1. ***Forbidden***

You don't have permission to access /owndir on this server.

Virtual hosting.

– Setup a virtual host with an alternate document root .
– Extend your web to include a virtual for the site http://www.district10.example.com
– Set the document root as /usr/local/vhost
– Download http://station.network0.example.com/pub/rhce/vhost.html
– rename it as index.html place this document root of the virtual host
– Note: The other websites configures for your server must still accessible.
vhosts.networkX.example.com is already provide by the name server on example.com

[root@system1~]# mkdir /usr/local/vhost

[root@system1~]# cd /usr/local/vhost

[root@system1 vhost]# wget http://station.network0.example.com/pub/rhce/vhost.html

[root@*system1* vhost]# semanage fcontext -a -t httpd_sys_content_t ' /usr/local/SIT (/.*)?'

[root@*system1* vhost]# restorecon -Rv /usr/local/SIT/
restorecon reset /usr/local/vhost context unconfined_u:object_r:usr_t:s0->unconfined_u:object_r:httpd_sys_content_t:s0
restorecon reset /usr/local/vhost/vhost.html context unconfined_u:object_r:usr_t:s0->unconfined_u:object_r:httpd_sys_content_t:s0

[root@*system1* vhost]# ls
vhost.html

[root@*system1* vhost]# mv vhost.html index.html

[root@*system1* SIT]# ls
index.html

[root@*system1* SIT]# vim /etc/httpd/conf/httpd.conf

<virtualhost *:80>
servername *www.district10.example.com*
documentroot /usr/local/vhosts
</virtualhost>

<directory /usr/local/vhosts>
require all granted
</directory>

[root@system1 ~]# vim /etc/hosts

172.25.10.110 www.district10.example.com
:wq

firefox
http://www.district10.example.com/ [http://vhosts2.example.com/]

this is virtual web page

client side :
(In our Examination no need to put hosts entry , if “hosts entry” entered also no issuses)

[root@system2 ~]# vim /etc/hosts

172.25.10.110 www.district10.example.com

:wq

firefox
http://www.district10.example.com/ [http://vhosts2.example.com/]

this is virtual web page

Dynamic Webpage configuration.

-configure website http://dynamic.district10.example.com:8899 on system1 with the document root /var/www/scripts
-site should executes webapp.wsgi
-page is already provided on *http://station.district0.example.com/pub/*webapp.wsgi
-content of the script should not be modified.

[root@system1 [mailto:root@system1] ***~]# mkdir -p /var/www/scripts***

[root@system1 [mailto:root@system1] ***~]# yum install mod_wsgi* -y***

[root@system1~]# cd /var/www/scripts

[root@system1~]# semanage fcontext -a -t httpd_sys_script_exec_t '/var/www/scripts(/.*)?'

[root@system1~]# semanage port -a -t http_port_t -p tcp 8899

[root@system1 [mailto:root@system1] ***~]# firewall-cmd - -permanent - -add-port=8899/tcp***

[root@system1 [mailto:root@system1] ***~]# firewall-cmd - -reload***

[root@system1 [mailto:root@system1] ***~]#*** **wget**
http://station.district0.example.com/pub/**webapp.wsgi**

[root@server70 ~]# restorecon -Rv /var/www/scripts

restorecon reset /var/www/scripts context unconfined_u:object_r:var_t:s0->unconfined_u:object_r:httpd_sys_script_exec_t:s0
restorecon reset /var/www/scripts/webapp.wsgi context unconfined_u:object_r:var_t:s0->unconfined_u:object_r:httpd_sys_script_exec_t:s0

[root@server70 ~]# vim /etc/httpd/conf/httpd.conf

listen 8899
<virtualhost *:8899>
servername dynamic.district10.example.com
documentroot /var/www/scripts
WSGIScriptAlias / /var/www/scripts/webapp.wsgi
</virtualhost>

<directory /var/www/scripts>
require all granted
</directory>

[root@system1 ~]# vim /etc/hosts

172.25.10.110 dynamic.district10.example.com
:wq

O/P

Goto Firefox

Address: dynamic.distrcit10.example.com:8899

UNIX EPOCH time is now: 1450238773.24
(if you press F5 time time will be automatically changed)

18. Script 1

-create a script on serverX called /root/random with following details.
-When run as /root/random user, should bring the output as kernel
-When run as /root/random kernel, should bring the output as user
-When run with any other arguments or without argument,
should bring the stderr as /root/random user|kernel

[root@server2 ~]# vim /root/random
read a
case $a in
user) echo "kernel";;
kernel) echo "user";;
***) echo "/root/random user|kernel" >> stderr**
esac

[root@server2 ~]# chmod a+x /root/random
[root@server2 ~]# /root/random

```
user
kernel
[root@server2 ~]# /root/random
kernel
user
[root@server2 ~]# /root/random
f
[root@server2 ~]# ls
anaconda-ks.cfg  random  stderr
[root@server2 ~]# cat stderr
/root/random user|kernel
[root@server2 ~]#
```

19. Script 2

-Create a script on serverX called /root/createusers
-When this script is called with the testfile argument, it should add all the users from the file
-Download the file from http://station.district0.example.com/pub/rhce/testfile
-All users should have the login shell as /bin/false, password not required.
-When this script is called with anyother arguments, it should print the message as Input File Not Found
-When this script is run without any arguments, it should display Usage: /root/createusers
Note: If the users are added no need to delete.

```
[root@server2 ~]# wget http://station.district0.example.com/pub/testfile
[http://classroom.example.com/pub/rhce/testfile]

[root@server2 ~]# cat testfile
arul
john
david

[root@server2 ~]# vim /root/createusers

a=""
case "$@" in
testfile       )       for i in `cat /root/testfile`
do
useradd -s      /bin/false      $i
done;;
$a)echo "Input File Not Found";;
*)echo  "Usage: /root/createusers";;
esac

[root@server2 ~]# chmod a+x /root/createusers

[root@server2 ~]# /root/createusers
Usage: /root/createusers

[root@server2 ~]# /root/createusers 111
Input File Not Found

[root@server2 ~]# tail -n 5 /etc/passwd
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:993:991::/run/gnome-initial-setup/:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
```

[root@server2 ~]# /root/createusers testfile

[root@server2 ~]# tail -n 5 /etc/passwd
tcpdump:x:72:72::/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
arul:x:1001:1001::/home/arul:/bin/false
john:x:1002:1002::/home/john:/bin/false
david:x:1003:1003::/home/david:/bin/false

MARIADB :

22.MaridDB Configuration

Configure a MariaDB on System1 with a database name Contacts.

The Database must be accessible locally only.

The root password must be zaldebro.

Apart from root, only the user Zyuichi must be able to query the Contacts Database.

Zyuichi must be identified by zaldebro.

Restore a database on system1 from the backup file

http://station.district0.example.com/pub/rhce/backup.mdb

23.MariaDB Query

Find the first name of user with password "ecosystem"

MariaDB [student]> use mysql

MariaDB [mysql]> show tables;

MariaDB [mysql]> show grants for john@'172.25.5.%';

MariaDB [mysql]> select * from tables_priv;

[root@server2 ~]# yum groupinstall mariadb mariadb-client -y

[root@server2 ~]# systemctl start mariadb

[root@server2 ~]# systemctl enable mariadb

ln -s '/usr/lib/systemd/system/mariadb.service' '/etc/systemd/system/multi-user.target.wants/mariadb.service'

[root@server2 ~]# firewall-cmd --permanent --add-service=mysql

success

[root@server2 ~]# firewall-cmd --permanent --add-port=3306/tcp

success

[root@server2 ~]# firewall-cmd --reload

success

[root@server2 ~]# vim /etc/my.cnf

[mysqld]

datadir=/var/lib/mysql

socket=/var/lib/mysql/mysql.sock

skip-networking=1 (this line) {note if skip-networking=1 means deny remote login

skip-networking=0 means allow remote login)

[root@server2 ~]# mysql_secure_installation

Enter current password for root (enter for none): (if fresh installation means just enter)

Set root password? [Y/n] Y

New password: zaldebro

Re-enter new password: zaldebro

Password updated successfully!

Reloading privilege tables..

... Success!

Remove anonymous users? [Y/n] y
... Success!

Disallow root login remotely? [Y/n] y
... Success!

Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!
Reload privilege tables now? [Y/n] y
... Success!

[root@server2 ~]# mysql -u root -p
Enter password: zaldebro

Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 10
Server version: 5.5.35-MariaDB MariaDB Server

Copyright (c) 2000, 2013, Oracle, Monty Program Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
```
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
3 rows in set (0.00 sec)
```

MariaDB [(none)]> create database Contacts;

MariaDB [(none)]> show databases;
```
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
```

```
| performance_schema |
| Contacts           |
+--------------------+
4 rows in set (0.00 sec)

MariaDB [(none)]> exit
Bye

[root@server2 ~]# wget http://station.district0.example.com/pub/rhce/backup.mdb
--2015-12-16 12:24:49-- http://station.district0.example.com/pub/rhce/backup.mdb
Resolving c (c)... 172.25.254.254
Connecting to c (c)|172.25.254.254|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3785 (3.7K)
Saving to: 'backup.mdb'

100%
[==========================================================================
==================================>] 3,785       --.-K/s   in 0s

2015-12-16 12:24:49 (460 MB/s) - 'backup.mdb' saved [3785/3785]

[root@server2 ~]# ls
anaconda-ks.cfg  backup.mdb

[root@server2 ~]# mysql -u root -p Contacts < backup.mdb
Enter password: zaldebro

[root@server2 ~]# mysql -u root -p
Enter password: zaldebro

MariaDB [(none)]> use  Contacts

Database changed
MariaDB [Contacts]> show tables;
+-------------------+
| Tables_in_student |
+-------------------+
| category          |
| manufacturer      |
| product           |
+-------------------+
3 rows in set (0.00 sec)

MariaDB [Contacts]> describe product;
+-----------------+--------------+------+-----+---------+----------------+------------
| Field                | Type          | Null | Key | Default  | Extra                |
+-----------------+--------------+------+-----+---------+----------------+-----------------
| id                  | int(11)               | NO   | PRI | NULL    | auto_increment |
| name                | varchar(100)        | NO   |       | NULL    |                 |
| price               | double          | NO   |       | NULL    |                       |
| stock               | int(11)         | NO   |       | NULL    |                      |
| id_category         | int(11)         | NO   |       | NULL    |                       |
| id_manufacturer     | int(11)         | NO   |       | NULL    |                       |
+-----------------+--------------+------+-----+---------+----------------+
6 rows in set (0.00 sec)

MariaDB [student]> help grant
  example:

CREATE USER 'jeffrey'@'localhost' IDENTIFIED BY 'mypass';
GRANT ALL ON db1.* TO 'jeffrey'@'localhost';
GRANT SELECT ON db2.invoice TO 'jeffrey'@'localhost';
```

GRANT USAGE ON *.* TO 'jeffrey'@'localhost' WITH MAX_QUERIES_PER_HOUR 90;

MariaDB [student]> create user 'Zyuichi'@'localhost' identified by 'zaldebro';
Query OK, 0 rows affected (0.00 sec)

MariaDB [student]> grant all on student.product to 'Zyuichi'@'localhost';
Query OK, 0 rows affected (0.00 sec)

MariaDB [student]> Select first name from tablename where password=”echosystem”;

Client :
[root@desktop2 ~]# yum groupinstall mariadb-client* -y

[root@desktop2 ~]# mysql -u root -p -h 172.25.2.11

Enter password:

ERROR 1045 (28000): Access denied for user 'root'@'desktop2.example.com' (using password: YES)

[root@desktop13 ~]# mysql -u Zyuichi -p -h 172.25.13.11

Enter password: zaldebro

ERROR 1130 (HY000): Host 'desktop13.example.com' is not allowed to connect to this MariaDB server

[root@desktop13 ~]#

17) script:1

--->create a script on serverX called /root/random with the following details
--->when run as /root/random Postconf, should bring the output as "Postroll"
--->when run as /root/random Postroll, should bring the output as "Postconf"
--->when run with only other argument or wihout argument, should bring the stderr as "/root/random Postconf | Postroll"

$@ is to refer argument as a separate word
case Stating this is conditioned structure to reduce difficulties from a normal statement like if/then/elif/then/else
“” To disabled meaning of special characters

```
#vim /root/random
case $@ in
postconf ) echo "Postroll";;
Postroll ) echo "postconf";;
      *) echo "/root/random postconf | Postroll";;
esac

#chmod a+x /root/random
```

18) script 2:

--->create a script on serverX called /root/createusers
--->when this script is called with the test file argument, it should add all the users from the file
--->downloaded the fire from http://station.network0.example.com/pub/testfile
--->all user should have the login shell as /bin/false, passwd not required.
--->when this script is called wih anyother argument, it should print the message "Input File Not Found"
--->When this script is run without any argument, it should dissplay "Usage "/root/createuser"
Note:- If the users are added no need to delete.

Ans:
#wget http://classroom.example.com/pub/testfile

#vim /root/createusers

```
a=""
case $@ in
testfile ) for b in `cat testfile`
do
useradd -s /bin/false $b;
done;;
$a ) echo "Usage:/root/createusers";;
* ) echo "Input file Not Found";;
esac
```

#chmod a+x /root/createusers

21. ISCSI Storage.

- **Create a new 3GB target on your system1.district10.example.com.**
- **The logical block name should be lvm The server should export an iscsi disk called iqn.2015-12.com.example.district10:system1**
- **This target should only be allowed only be allowed to system2**

[root@server2 ~]# yum install target* -y

[root@server2 ~]# systemctl start target

[root@server2 ~]# systemctl enable target

ln -s '/usr/lib/systemd/system/target.service' '/etc/systemd/system/multi-user.target.wants/target.service'

[root@server2 ~]# firewall-cmd --permanent --add-port=3260/tcp

success

[root@server2 ~]# firewall-cmd --reload

success

[root@server2 ~]# fdisk -l

[root@server2 ~]# fdisk /dev/vda

Command (m for help): p

Device Boot Start End Blocks Id System

/dev/vda1 * 2048 472143871 236070912 83 Linux

/dev/vda2 472143872 488396799 8126464 82 Linux swap / Solaris

Command (m for help): n

Partition type:

p primary (0 primary, 0 extended, 4 free)

e extended

Select (default p): e

Partition number (1-4, default 1):

First sector (2048-20971519, default 2048):

Using default value 2048

Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519):

Using default value 20971519

Partition 1 of type Extended and of size 10 GiB is set

Command (m for help): n

Partition type:

p primary (0 primary, 1 extended, 3 free)

l logical (numbered from 5)

Select (default p): l

Adding logical partition 5

First sector (4096-20971519, default 4096):

Using default value 4096

Last sector, +sectors or +size{K,M,G} (4096-20971519, default 20971519): +4G

Partition 5 of type Linux and of size 4 GiB is set

Command (m for help): t

Partition number (1,5, default 5): 5

Hex code (type L to list all codes): 8e

Changed type of partition 'Linux' to 'Linux LVM'

Command (m for help): w

The partition table has been altered!

Calling ioctl() to re-read partition table.

Syncing disks.

[root@server2 ~]# partprobe /dev/vda

[root@server2 ~]# pvcreate /dev/vda5

Physical volume "/dev/vda5" successfully created

[root@server2 ~]# vgcreate one /dev/vdb5

Volume group "one" successfully created

[root@server2 ~]# lvcreate -L +3G -n two /dev/mapper/one

Logical volume "two" created

[root@server2 ~]# targetcli

/> /backstores/block create lvm /dev/mapper/one-two

Created block storage object lvm using /dev/mapper/one-two.

/> /iscsi create iqn.2015-12.com.example.district10:system1

Created target iqn.2015-12.com.example.district10:system1.

Created TPG 1.

/> /iscsi/iqn.2015-12.com.example.district10:system1/tpg1/acls create iqn.2015-12.com.example.district10:system2

Created Node ACL for iqn.2015-12.com.example.district10:system2

/> /iscsi/iqn.2015-12.com.example.district10:system1/tpg1/luns create /backstores/block/lvm

Created LUN 0.

Created LUN 0->0 mapping in node ACL iqn.2015-12.com.example.district10:system2

/> /iscsi/iqn.2015-12.com.example.district10:system2/tpg1/portals create 172.24.10.110

Using default IP port 3260

Created network portal 172.24.10.110:3260.

/> saveconfig

Last 10 configs saved in /etc/target/backup.

Configuration saved to /etc/target/saveconfig.json

/> exit

Global pref auto_save_on_exit=true

Last 10 configs saved in /etc/target/backup.

Configuration saved to /etc/target/saveconfig.json

[root@server2 ~]# systemctl restart target.service

ISCSI Initiator

-The system1 provides an iscsi port(3260).
-connect the disk with system2.district10.example.com and configure filesystem with the following requirements.
-Create 2040 MB partition on ISCSI block device and assign the filesystem as ext3.
-Mount the volume under /mnt/initiator at the system boot time.

Client :

[root@desktop2 ~]# yum install iscsi-initiator-utils* -y

[root@desktop2 ~]# vim /etc/iscsi/initiatorname.iscsi

InitiatorName=iqn.2015-12.com.example.district10:system2

:wq

[root@desktop2 ~]# systemctl restart iscsi iscsid.service

[root@desktop2 ~]# systemctl enable iscsi iscsid.service

ln -s '/usr/lib/systemd/system/iscsid.service' '/etc/systemd/system/multi-user.target.wants/iscsid.service'

[root@desktop2 ~]# iscsiadm -m discovery -t st -p 172.25.2.11

172.25.2.11:3260,1 iqn.2015-12.com.example.district10:system1

[root@desktop2 ~]# iscsiadm -m node -T iqn.2015-12.com.example.district10:system1 -p 172.25.2.11

[root@desktop2 ~]# iscsiadm -m node -T iqn.2015-12.com.example.district10:system1 -p 172.25.2.11 -l

Logging in to [iface: default, target: iqn.2015-12.com.example.district10:system1, portal: 172.25.2.11,3260] (multiple)

Login to [iface: default, target: iqn.2015-12.com.example.district10:system1, portal: 172.25.2.11,3260] successful.

[root@desktop2 ~]# lsblk

NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT

sda 8:0 0 3G 0 disk

vda 253:0 0 10G 0 disk

└─vda1 253:1 0 10G 0 part /

vdb 253:16 0 10G 0 disk

[root@desktop2 ~]# fdisk /dev/sda

Command (m for help): p

Device Boot Start End Blocks Id System

Command (m for help): n

Partition type:

p primary (0 primary, 0 extended, 4 free)

e extended

Select (default p): p

Partition number (1-4, default 1):

First sector (8192-6291455, default 8192):

Using default value 8192

Last sector, +sectors or +size{K,M,G} (8192-6291455, default 6291455): +2048M

Partition 1 of type Linux and of size +2048MBs set

Command (m for help): p

Device Boot Start End Blocks Id System

/dev/sda1 8192 1646591 819200 83 Linux

Command (m for help): w

[root@desktop2 ~]# partprobe /dev/sda

[root@desktop2 ~]# mkfs.ext3 /dev/sda1

[root@desktop2 ~]# mkdir /mnt/initiator

[root@desktop2 ~]# vim /etc/fstab

/dev/sda1 /mnt/initiator ext3 _netdev 0 0

:wq

[root@desktop2 ~]# mount -a

[root@desktop2 ~]# df -h

Filesystem	Size	Used	Avail	Use%	Mounted on
//172.25.2.11/OPENGROUP	*10G*	*3.3G*	*6.8G*	*33%*	*/mnt/smbspace*
172.24.70.25:/nfsshare	*10G*	*3.6G*	*6.5G*	*36%*	*/public*
172.25.70.25:/nfssecure/protected	*10G*	*3.3G*	*6.8G*	*33%*	*/secure/protected*
/dev/sda1	*2024M*	*33M*	*1998M*	*5%*	*/mnt/initiator*

Posted 4th February 2016 by muthu kumar

8 View comments

1st January 2016

RHCE 7 QUESTIONS and Answer

Domain Name:

System1: system1.district10.example.com

System2: system2.district10.example.com

IP Address:

System1:172.24.10.110/24

System1:172.24.10.120/24

Name Server: 172.24.10.250

Gateway:172.24.10.254

Root password : zaldebro

1.Configure selinux. Configure your systems that should be running in Enforcing.

2.Configure repository. Create a Repository for your virtual machines. The URI is http://station.district0.example.com/content/rhel7.0/x86_64/dvd [http://station.district0.example.com/content/rhel7.0/x86_64/dvd]

3. SSH configuration.

Clients within my133ilt.org should NOT have access to ssh on your systems

Clients with domain district10.example.com should be able to access the systems

4. Port forwarding

Configure system1 to forward traffic incoming on port 80/tcp from source network 172.24.X.0/255.255.255.0 to port on 5243/tcp

5. User Environment.

Create a command called qstat on both system1 and system2. It should able to execute the following command(ps eo pid,tid,class,rtprio,ni,pri,psr,pcpu,stat,wchan:14,comm)

The command should be executable by all users.

6. Ipv6 network.

Configure eth0 with a static ipv6 addresses as follows.

Configure a Static IPv6 address in system1 as fddb:fe2a:ab1e::c0a8:64/64.

Configure a Static IPv6 address in system2 as fddb:fe2a:ab1e::c0a8:02/64.

Both machines are able to communicate within the network fddb:fe2a:able/64

The changes should be permanent even after the reboot

7. Link aggregation Configure your system1 and system2, which watches for link changes and selects an active port for data transfers. System1 should have the address as 172.24.10.10/255.255.255.0. System2 should have the address as 172.24.10.20/255.255.255.0

8. SMTP Configuration. Configure the SMTP mail service on system1 and system2 which relay the mail only from local system through station.network0.example.com, all outgoing mail have their sender domain as example.com. Verify the mail server is working by sending mail to a local user clarke.

Check the mail on both system1 and system2 with the below URL

http://rhcert.district0.example.com [http://rhcert.district0.example.com/]

9. NFS server.

Configure system1 with the following requirements.

Share the /nfsshare directory within the example.com domain clients only, share must not be writable. Share the /nfssecure, enable krb5p security to secure access to the NFS share from

URIhttp://station.network0.example.com/pub/keytabs/system1.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.

10. Nfs mount

Mount /nfsshare directory on system2 under /public directory persistently at system boot time. Mount /nfssecure/protected with krb5p secured share on system2 beneath /secure/protected provided with keytab http://station.network0.example.com/pub/keytabs/system2.keytab

The user harry able to write files on /secure directory

11. Smb access

Share the /sambadir directory via SMB on system1 Your SMB server must be a member of the STAFF workgroup The share name must be data .The data share must be available to district10.example.com domain clients only The data share must be browseable .Susan must have read access to the share, authenticating with the same password “password”, if necessary

12.SAMBA Mount

Share /opstack with SMB share name must be cluster.

The user frankenstein has readable,writeable,accessible to the /opstack SMB share. The user martin has read access to the /opstack SMB share. Both users should have the SMB passwd "SaniTago".

The share must be browseable

Mount the samba share /opstack permanently beneath /mnt/smbspace on system2 as a multiuser mount. The samba share should be mounted with the credentials of martin.

13. Webserver.

Implement a webserver for the site http://system1.district10.example.com

Download the webpage fromhttp://station.district0.example.com/pub/rhce/rhce.html

Rename the downloaded file in to index.html.

copy the file into the document root.

Do not make any modification with the content of the index.html.

Webserver must be available to clients with domain district10.example.com

Clients within my22ilt.org should NOT access the webserver on your systems

14) Secured webserver

configure the websitehttps://system1.example.comwith TLS

SSLCertificate file http://classroom.example.com/pub/rhce/tls/certs/system1.networkX.crt

SSLCertificatekeyfile
http://classroom.example.com/pub/rhce/tls/private/system1.networkX.key

SSL CA certificate filehttp://classroom.example.com/pub/exampleca.crt

15) Webpage content modification.

Implement website for http://system1.district10.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

User harry can edit the contents of the directory

16) Virtual hosting

Setup a virtual host with an alternate document root. Extend your web to include a virtual for the sitehttp://www.district10.example.com

Set the document root as /usr/local/vhosts

Downloadhttp://station.network0.example.com/pub/rhce/vhost.html

Rename it as index.html place this document root of the virtual host

Note: The other websites configures for your server must still accessible.
vhosts.networkX.example.com is already provide by the name server on example.com

17. Dynamic Webpage Configuration.

Configure websitehttp://dynamic.district10.example.com:8899 on system1 with the documentroot /var/www/scripts Site should executes webapp.wsgi.

Page is already provided on http://station.district0.example.com/pub/webapp.wsgi Content of the script should not be modified.

18) Script1

Create a script on system1 called /root/random with following details. When run as /root/random user, should bring the output as "user" When run as /root/random kernel, should bring the output as "user" When run with any other argument or without argument, should bring the stderr as "/root/random user|kernel"

19) Script2

Create a script on system1 called /root/createusers When this script is called with the argument, it should add all the users from the file Download the file from http://station.district0.example.com/pub/testfile

All users should have the login shell as /bin/false, password not required.

When this script is called with anyother argument, it should print the message as "Input File Not Found" When this script is run without any argument, it should display "Usage:

/root/createusers"

20. ISCSI Storage

Create a new 3GB target on your system1.district10.example.com. The logical block name should be lvm The server should export an iscsi disk called iqn.2015-12.com.example.district10:system1. This target should only be allowed to system2

21. ISCSI Initiator

The system1 provides an iscsi port(3260).

connect the disk with system2.district10.example.com and configure filesystem with the following requirements.

Create 2040 MB partition on ISCSI block device and assign the filesystem as ext3.

Mount the volume under /mnt/initiator at the system boot time.

22.MaridDB Configuration

Configure a MariaDB on System1 with a database name Contacts.

The Database must be accessible locally only.

The root password must be zaldebro.

Apart from root, only the user Zyuichi must be able to query the Contacts Database.

Zyuichi must be identified by zaldebro.

Restore a database on system1 from the backup file
http://station.district0.example.com/pub/rhce/backup.mdb
[http://station.district0.example.com/pub/rhce/backup.mdb]

23.MariaDB Query

Find the first name of user with password “ecosystem”

Posted 1st January 2016 by muthu kumar

4 View comments