RHCE EXAM PAPER:-

Your system1 is having ip 172.24.X.50 & Syatem2 ip 172.24.X.60 from dhcp. Your nameserver is running
on server.networkX.example.com 172.24.254.254.
your system1 have name system1.networkX.example.com
your system2 have name system2.networkX.example.com

Password for root is wakennym.

1). Create a user environment

- Create user environment qstat on system1 and system2 command is /bin/ps -Ao
  pid,tt,user,fname,stat,rsz & available for present user and future user.

Ans:- alias qstat='/bin/ps -Ao pid,tt,user,fname,stat,rsz'

2). Port forwarding

Configure Port forwarding in your machine system1 such that forward all incoming connection on port
5909/tcp on the firewall to port 80/tcp on the machine with the 172.26.1.0/255.255.255.0.

3). Configure link Aggregation

- Configure link Aggregation b/w system1 & system2 using eth1 & eth2 on both machine
- system1 ip 172.16.X.65/255.255.255.0
- system2 ip 172.16.X.75/255.255.255.0
- link Aggregation in backup mode if one down another up
- link should be ping able after reboot

4). Provide ipv6

- provide ipv6 to eth0 on system1 and system2

- system1 ip fd00:ba5e:ba11:X::1/64
- system2 ip fd00:ba5e:ba11:X::1/64

- should be pingable in fd00:ba5e:ba11/64
- ipv6 remain after reboot and ipv4 also remain on eth0 and should be accessible.

5). Configure mail service

- configure mail service on both system1 & system2
  your system should not connect to external source
  your mail ser don't contain any mail and pass it on server.networkX.example.com
  your mail shoud be originate from neteorkX.example.com
- send mail user hal from system1 and system2, mail should be able on given link

6). Share NFS directory

- export nfs directory /public
- export should be in read mode
- all user with in network networkX.example.com have read access on directory
- Mount export on /mnt/nfsmount on system2

7). Share secure NFS

- export nfs /private in read and write mode using Kerberos protocol
- /private having subdirectory protect

- Kerberos keytab path for system1
  http://host.networkX.example.com/materials/nfs system1.keytab

- Kerberos keytab path for system1
  http://host.networkX.example.com/materials/nfs system2.keytab

- Directory protect owned by user varuna and user varuna should be access
  with read write permission on export directory and its remain after reboot.
- mount export on /mnt/nfssecure.

8). Samba share Directory

- share a samba directory /common for your domain its access by your domain
- share name common and must be browseable
- user harry having read permission on samba share.
- all users in networkX.example.com have access the share directory

9). Samba multiuser Directory

- Share a samba directory /devfas for your domain its access by your domain.

• directory /devfas have Share name devfas and share must be browseable.
• user magneter having a read permission and password is wakennym.
• user wolfryen having read and write permission on share and password is wakennym.
• all users in networkX.example.com have access the share directory
• Share mount on /mnt/smbashare on system2 using credential wolfryen.
• share must be accessable after reboot.

10). Configure iscsi disk export

• System1 provide 3G lv backstore iscsi_data
• Using the iscsi provide a backstore disk for system2 by using iqn.2015-07.com.example.networkX:system1
from system1.

11). configure iscsi initiator

• A iscsi disk provide by system1 for iqn.2015-07.com.example.networkX:system2 from system2
• The partition size should be 1900 Mib. the disk having file system ext4 and mount on /mnt/data.
it will remain after reboot.

12). web server

•Configure a web server for the site http://system1.networkX.example.com then perform the following steps:-
download file from http://server.networkX.example.com/materials/station.html on document root of your web server.
Rename the downloaded file to index.html.Do NOT make any modifications to the content of index.html.
it should be accessable by your network networkX.example.com and not accessible by my133t.org

13). Virtual hosting

•Configure web server to include a virtual host for the site http://www.networkX.example.com,
perform The following steps:

•Create a virtual directory in document root of your web server Download page from
http://server.networkX.example.com/materials/www.html.
Rename the downloaded file to index.html.

Place this index.html in the Document Root of the virtual host.
Do NOT make any modifications to the content of index.html. Ensure that sarah is able to create
content in /var/www/virtual.

The original web site http://system1.networkX.example.com must still accessible.

DNS resolution for the hostname www.networkXexample.com is already provided
by the name server.

14). Restrict web servers

- Restrict your web server for site http://system1.networkX.example.com. Configure such that restrict directory
in this document root is access by your system only. Create index.html in restrict directory. Previous website
remains same.

15). Configure web server to include a virtual host for the site http://webapp.networkX.example.com,
perform The following steps:

- Download page from
http://server.networkX.example.com/materials/webapp.wsgi.
on document root of your web server.

16). configure SSH service

- Configure SSH on both system1 and system2 that all network comes under networkX.example.com
can SSH your system and network comesunder my133t.org could not SSH.

17). create script
- Create A script name /root/script.sh such that
- when an argument “foo” is pass in front of script.sh then o/p comes “bar”
- when “bar” pass o/p comes “foo”
- When noting b/w bar & foo passes o/p come /roo/script.sh foo|bar.

18). configure mariadb
- Configure & Install MariaDB Server and set mariadb root password ‘wakennym’.

- Mariadb access by only localhost
- create a user “luigi” which should be able to login locally using password ‘wakennym’.
- user "luigi" have access on the database.
- Create a mariadb database Contacts and Download a database file from
  http://server.networkX.example.com/materials/User_contact.dump
  and restore dump in contact database

19). mariadb query

- search first name of user in database Contact who has password "troocase".

20). selinux

- Set selinux must be in enforcing mode on both system