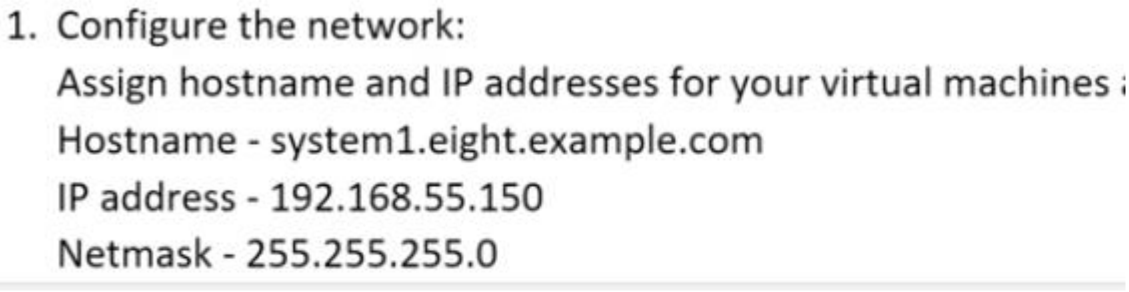
Questions RHCSA 9 (EX 200)



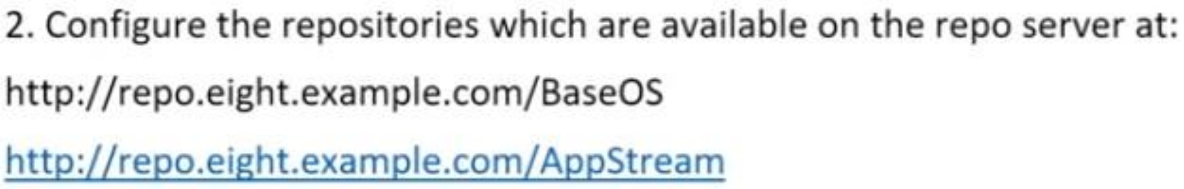
1. Configure the network:

   Assign hostname and IP addresses for your virtual machines

   Hostname - system1.eight.example.com

   IP address - 192.168.55.150

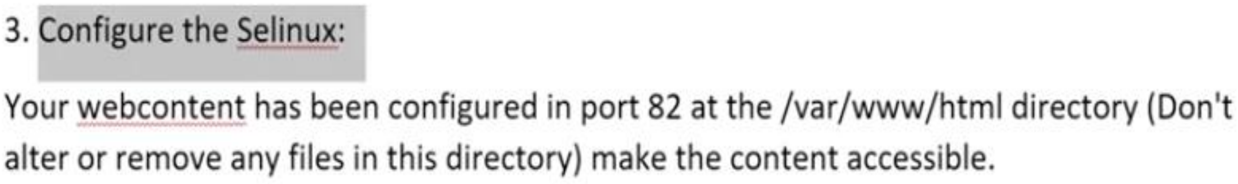
   Netmask - 255.255.255.0



2. Configure the repositories which are available on the repo server at:

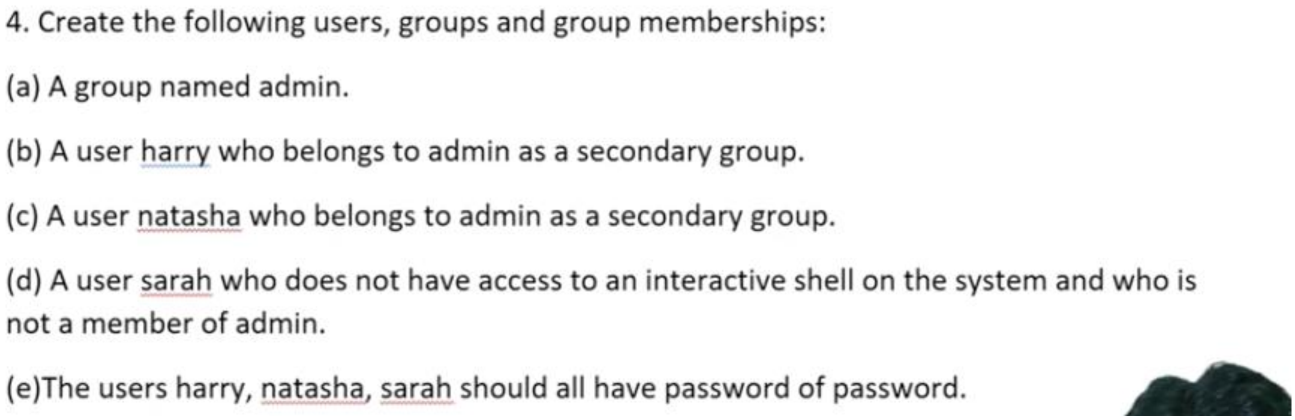
http://repo.eight.example.com/BaseOS

http://repo.eight.example.com/AppStream



3. Configure the Selinux:

Your webcontent has been configured in port 82 at the /var/www/html directory (Don't alter or remove any files in this directory) make the content accessible.



4. Create the following users, groups and group memberships:

(a) A group named admin.

(b) A user harry who belongs to admin as a secondary group.

(c) A user natasha who belongs to admin as a secondary group.

(d) A user sarah who does not have access to an interactive shell on the system and who is not a member of admin.

(e)The users harry, natasha, sarah should all have password of password.

5. Create a collaborative directory /common/admin with the following characteristics:

(a) Group ownership of /common/admin is admin.

(b) The directory should be readable, writable and accessible to members of admin, but not any other user. (It is understood that root has access to all files and directories on the system.)

(c) Files created in /common/admin automatically have group ownership set to the admin group.

6. Configure Autofs:

(a) to automatically mount the below NFS shares on system1.eight.example.com machine at /automount directory:

192.168.55.151:/public & 192.168.55.151:/private

(b) the public nfs share should have read only access for all users.

(c) the private nfs share should have read write access for all users.

(d) both shares should get automatically unmounted if not in use for 30 sec

7. (a) Set a Cron job for harry on 12.30 at noon print "hello" using echo command.

Solution:

```
# crontab -eu harry
30 12 * * * /bin/echo “hello”
# crontab -lu harry #(it should show crontabs of that user) (-l=list, -u=user, -e=edit)
```

(b) Deny the natasha user to create a cronjob in system.

8. Configure ACL permissions:

Copy the file /etc/fstab to /var/tmp. Configure the permission of /var/tmp/fstab so that:

(a) The file /var/tmp/fstab is owned by root user.

(b) The file /var/tmp/fstab belongs to the group root.

(c) The file /var/tmp/fstab should not be executable by anyone.

(d) The user harry is able to read and write by /var/tmp/fstab.

(e) The user natasha can neither read nor write /var/tmp/fstab.

(f) All other users (current/future) have the ability to read /var/tmp/fstab

9. Configure the NTP:

a) Configure your system so that it is an NTP client of *system2.eight.example.com (192.168.55.151)*

10. Locate & copy the Files:

Find all files that greater than 4 MB in the /etc directory & copy them to /find/largefiles directory.

11. (a) Create a new user with UID 1326, user name and password as alies.

Solution:

```
# useradd -u 1326 alies
# echo "alies" | passwd --stdin alies
# tail -1 /etc/passwd
```

11. (b) Create an archive file:

Backup the /var/tmp as /root/test.tar.gz

11. (c) Set the permissions:

(i) All new creating files for user natasha as -r-------- as default permission.

(ii) All new creating directories for user natasha as dr-x------ as default permission.

12. (a) The password for all new users in *system1.eight.example.com* should expires after 20 days.

12. (b) Assign the sudo privilege:

(a) Assign the Sudo Privilege for Group "admin" and Group members can administrate without any password.

13. Create a bash shell script program for:

(a) Create a mysearch script to locate file under /usr/share having size less than 1M.

(b) After executing the mysearch script file and listed (searched) files has to be copied under /root/myfiles.

14. Reset the forgotten root password in *system2.eight.example.com* machine and set it as 'redhat'

15. (a) Create a swap partition 512MB size.

15. (b) Create one logical volume named database and it should be on datastore volume group with size 50 extent and assign the filesystem as ext3. the datastore volume group extend should be 8 MiB (mount the logical volume under mount point /mnt/database.

16. Create the vectra volume using the VDO with the logical size 50 GB and mount under test directory.

17. Resize the logical volume size of +100 extents on /mnt/database directory.

18. Set the recommended tuned profile for your system.

19. Create the container as a system startup service.

(a) Create the container name as logserver with the images rsyslog are stored in docker on paradise user.

(b) The container should be configured as system startup services.

(c) The container directory is container_ journal should be created on paradise user.

20. Configure the Container as persistent storage and create logs for container.

(a) Configure the container with the persistent storage that mounted on /var/log/journal to /home/paradise/container.

(b) The container directory contains all journal files.