INFINITE
LEARNING

IBM ACADEMY: HYBRID CLOUD & RED HAT
RED HAT CERTIFIED SYSTEM ADMINISTRATOR
TIMEDRILLS EXERCISE

IMPORTANT CONFIGURATION INFORMATION

During the exam you will be working with several virtual systems in addition to the desktop at which you are seated. You do not have root access in the desktop system however you have full root access to the virtual systems.

System Information
You will be working with the following virtual systems for this exam:

System	IP Address
node1.network9.example.com	172.24.9.10
node2.network9.example.com	172.24.9.11

The systems you are working with are members of the DNS domain network network9.example.com. All systems in this domain are in the 172.24.9.0/255.255.255.0 subnet and all systems in that subnet are in network9.example.com.

The IP Addresses listed for these systems are the addresses that **should** be assigned to the system. You may find a necessary to configure the network for one or both of your systems in order to reach it at the address listed above.

Account Information

The **root** password for node1 has been set to **"redhat"**
Unless otherwise specified, this will be the password you use to access other systems and services. Also, unless otherwise specified, you should use this password for any accounts that you create or for any services that require a password be set.

Registry Access
Some of the items in this exam may require container images from a registry.

Container registry server is registry.lab.example.com
Use admin as username and redhat321 as password for container registry

Other Information
You may access your exam systems via SSH or via the console. Note that SSH access may be dependent on your solving for other exam items.

Your domain number = **9**

Before You Begin

Before you do these bootcamp exercise, **please reset** your **virtual labs** first to make sure there is no issues.

As the student user on the workstation machine, use the **timedrills** command to prepare your system for this exercise.

This command prepares your environment and ensures that all required resources are available.

[student@workstation ~] $ timedrills start

Do this in node1.network9.example.com

1. Assign Hostname and IP Address for your virtual machine.
   Hostname node1.network9.example.com
   IP Address 172.24.9.10
   Netmask 255.255.255.0
   Gateway 172.24.9.254
   Nameserver 172.24.9.254

2. Create a repository
   https://mirror.stream.centos.org/9-stream/AppStream/x86_64/os/
   https://mirror.stream.centos.org/9-stream/BaseOS/x86_64/os/

3. Configure the Selinux
   The webserver is running on non-stardard port 82 having a issue serve the web content. Debug and fix the issue:
   a) The web server can serve all the existing HTML file located at /var/www/html directory (Don't alter or remove any files in this directory)
   b) The webserver can serve the content on port 82
   c) Make the content accessible

4. Create the following users, groups and group memberships:
   a) A group named sysadmin.
   b) A user harry who belongs to sysadmin as a secondary group.
   c) A user natasha who belongs to sysadmin as a secondary group.
   d) A user sarah who does not have access to an interactive shell on the system and who is not member of sysadmin.
   e) The users harry, natasha, sarah should all have password of **redhat**

5. Create a collaborative directory /common/sysadmin with the following characteristics:
   a) Group ownership of /common/sysadmin is sysadmin.
   b) The directory should be readable, writable and accessible to members of sysadmin, but not to any other user. (It is understood that root has access to all files and directories on the system.)
   c) Files created in /common/sysadmin automatically have group ownership set to the sysadmin group

6. Configure autofs to automount the home directories of remoteuser9 domain users. Note the following:
   a) utility.network9.example.com (172.24.9.10) NFS -exports /netdir to your system.
   b) remoteuser9 home directory is utility.network9.example.com:/netdir/remoteuser9
   c) remoteuser9 home directory should be auto mounted locally beneath to /netdir as /netdir/remoteuser9.
   d) The home directories must be writable by their users.
   e) remoteuser9's password is ”**redhat**”

7. Configure Crontab
   The user natasha must configure cron job that runs daily at 12:30 local time and execute **/bin/echo "hello"**

8. Configure NTP with **time.cloudflare.com**

9. Locate all the files owned by sarah and make a copy of them in the given path /root/find.user

10. Find a string "home" in /etc/passwd and searching string has been stored in /root/search.txt

11. Create a user account
    a) Create a new user with UID 1326 and user name as alies.
    b) assign the password of **“redhat**”.

12. Create a tar archive file
    Backup the /var/tmp as /root/archive.tgz

13. Build a container image as user **neith**
    a) Using the URL of https://bit.ly/Containerfile to build the container image with name **monitor**.
    b) Do not modify the container file

14. Configure the container as a system start-up service and mount volumes persistently.
    a) Create the container name as ascii2pdf as neith user
    b) Run the container by using image monitor which one was already done in previous
    c) Create the container as a system start-up service, While reboot it will automatically start the service without any human intervention.
    d) The system service should be container-ascii2pdf.
    e) The local directory /opt/files should be persistently mount on container’s /opt/incoming directory.
    f) The local directory /opt/processed should be persistently mount on container’s /opt/outgoing directory.

Note: In working of service starts, any file create/store under the /opt/files automatically creates into pdf on /opt/processed directory.

15. Configure Default permissions
    a) All new creating files for user natasha as -r-------- as default permission.
    b) All new creating directories for user natasha as dr-x------ as default permission.

16. Set the Password expire date
    The password for all new users in node1.network9.example.com should expires after 60 days.

17. Configure sudoers for group sysadmin without pasword

18. Configure the application RHCSA as an alies user, When login it will show the message "Welcome to RHCSA Timedrills"

19. Create a mysearch script file under /usr/local/bin directory, find all file /usr then save the output in /root/myfiles that has file size +30k and -50k with special user id permission.

Do this in node2.network9.example.com

20. Assign root user password as **redhat**

21. Configure repo
    https://mirror.stream.centos.org/9-stream/AppStream/x86_64/os/
    https://mirror.stream.centos.org/9-stream/BaseOS/x86_64/os/

22. Create swap partitons with size of 512MiB

23. Create one logical volume named ‘database’ and it should be on ‘datastore’ volume group with size 50 extent and assign the filesystem as ext3.
    (i). The datastore volume group extend should be 8MiB
    (ii). Mount the logical volume under /mnt/infinite as it’s mount point.

24. Resize the logical volume size of 800M on /mnt/infinite directory.

25. Set the recommend tuned profile for your system

Evaluation

As the student user on the workstation machine, use the **timedrills** command to grade your work.

Correct any reported failures and rerun the command until successful.

```
[ student@workstation ~ ] $ timedrills grade
```

Finish

Reset your lab to finish this timedrills exercise. This step is important to ensure your lab stay clean for your next exercise attempt.