RHCE Sample Exam 1

Start with the preconfigured RHEL 7 system described in Appendix A. Make sure that system is currently powered down. As discussed in Appendix A, a current repository of the installation DVD is available from an FTP server configured on the local system. SELinux should be set to enforcing mode. You'll have three and a half hours to complete the following tasks:

1. Configure an SSH server on server1.example.com with access limited to the hosts on the 192.168.122.0/24 network. Create local users named katie and dickens. Limit SSH access on the server only to user katie.
2. Configure a Samba server. Share a directory named /food with user dickens. Share a second directory named /book limited to users tim and stephanie.
3. Set up a local NTP server, accessible to the local network.
4. Configure an NFS server on server1.example.com to share the /home directory in read-write mode with the physical host system.
5. Configure Apache on server1.example.com with two secure virtual hosts. Call those virtual hosts shost1.example.com and shost2.example.com. Create and configure an appropriate SSL self-signed certificate for those websites. Set up two default web pages with shost1 and shost2 as the content, respectively.
6. Block access to the Apache web server running on server1 from outsider1.example.net. All the other hosts must be able to connect to the web server.
7. Create a script named /usr/local/bin/backup.sh that takes a directory as an argument and backs up all files in that directory in a tar-gzipped archive in the current directory. If no argument is specified, the script should display the following error message:

   ```
   Usage: backup.sh <DIRECTORY>
   ```

   Configure the script to run automatically at 2:00 a.m. every day, to create a backup of the /home directory in the /tmp filesystem.
8. Configure IPv4 and IPv6 forwarding on server1.example.com.

9. Set up the IPv6 address 2001:db8:1::1/64 on the eth0 interface of server1.example.com and 2001:db8:1::2/64 on the eth0 interface of tester1.example.com. Ensure that the two system can “ping” each other.

10. Configure an iSCSI target on server1.example.com. Create a 500MB logical volume to be used as a backstore for a new LUN with IQN iqn.2015-01.com.example:server1-lun1. Set an ACL to grant access to tester1.example.com only.

11. Configure tester1.example.com as an iSCSI initiator with IQN iqn.2015-01.com.example:tester1. Discover and mount the LUN from server1.example.com and create a partition with an XFS filesystem. Ensure that the volume is mounted at boot on the /mnt/iscsi directory.

12. Set up system activity reports to run the related accounting tool every minute.

13. Set up a MariaDB database named “exam” in MariaDB. Create a table named “marks” with an integer ID column as a primary key, and the columns “name,” “date,” and “mark.” Use the appropriate type value for each column. Insert the following records into the table:

```
tim, 2015-03-21, 70
alex, 2015-07-05, 60
mike, 2015-04-25, 85
```

14. Add a MariaDB user named examuser with a password of pass123. The user examuser must have full access to the exam database. Set the password of the MariaDB root user to pass456. Ensure that MariaDB accepts connections only from the localhost.