RHCSA / RHCE Practice Exam #01

This Exam:

These tasks are taken from the objectives Red Hat has publicly posted and should therefore approximate the type of tasks one might find on the RHCSA and RHCE exams. It is expressly NOT based on actual contents of actual Red Hat Exams.

For the most authentic experience, this sample exam should be undertaken in a "closed-book" manner – referring to nothing but what is on the system or contained on the Red Hat Enterprise Linux installation tree that will be made available to you. However, because this Sample Exam is intended in part as a learning experience in itself, should you get seriously stuck you may refer to the Study Guide, to online resources, or to assistance from the instructor. Recognize, though, that such a decision may indicate a need for additional preparation before undertaking the Red Hat Exam.

Your Test Environment:

You should configure your physical server and three virtual machines as follows (where <x> is your station number):

Systems Configuration

	Physical Host	vm1	vm2	vm3
Hostname	s<x>host.linux-acc.local	s<x>server.linux-acc.local	s<x>client.linux-acc.local	s<x>untrusted.linux-acc.local
IP Address	192.168.5.<x>0	192.168.5.<x>1	192.168.5.<x>2	DHCP
Subnet	/22 or 255.255.252.0	/22 or 255.255.252.0	/22 or 255.255.252.0	n/a
Def. GW	192.168.4.1	192.168.4.1	192.168.4.1	192.168.4.1
Nameserver	192.168.7.254	192.168.7.254	192.168.7.254	192.168.7.254

Networks:

Local network

192.168.4.0/22 (255.255.252.0), GW 192.168.4.1, DNS 192.168.7.254

Trusted subnet

192.168.5.0/24 (255.255.255.0)

Untrusted subnet

192.168.4.0/24 (255.255.255.0)

An installation tree has been made available to you at ftp://192.168.5.200/pub/rhel6 which can serve as the basis for a yum repository.

Requirements Common to Both Exams

- SELinux must, at the end of the exam, be running in enforcing mode on both the client and server virtual machines after a reboot of each.
- The IPTables firewall must be enabled and configured to permit the types of traffic set forth in these requirements.
- On the untrusted host, use DHCP networking and install/configure only that components that are required for testing prohibited access to the services described below.

RHCSA Requirements

Complete the following in approximately 2 hours:

- Obtain access to your virtual machines (you do not know the root passwords) and reset the root passwords to "linuxacc".
- Ensure that the network configuration matches that in the table above.
- Create users and groups on both your server and client virtual machines:

  Users:

  - tester (UID=1004), password: linuxacc
  - ford (UID=1005), password: linuxacc
  - carter (UID=1006), password: linuxacc
  - reagan (UID=1007), password: linuxacc
  - clinton (UID=1008), password: linuxacc

  Groups:

  - presidents (GID=1000; members=ford, carter, reagan, clinton)
  - republicans (GID=1001; members=ford, reagan)
  - democrats (GID=1002; members=carter, clinton)

- On the server virtual machine, create the following directories:

  `/share/presidents`

  - All four ("presidential") users must be able to write here.
  - This directory must be owned by root and the group presidents.
  - Only users in this group should have any access to the directory.
  - Files created here should be owned by the group presidents.
  - Users should not be able to delete files they did not create.
  - This directory should have an SELinux fcontext that will permit it to be shared by multiple services.

  `/share/presidents/republicans`

  - This directory should be owned by root and the group republicans.
  - Files created here should be owned by the group republicans.
  - Only users in this group should have any access to the directory.
  - Users should not be able to delete files they did not create.
  - This directory should have an SELinux fcontext that will permit it to be shared by multiple services.

  `/share/presidents/democrats`

  - This directory should be owned by root and the group democrats.
  - Files created here should be owned by the group democrats.
  - Only users in this group should have any access to the directory.

    - Users should not be able to delete files they did not create.
    - This directory should have an SELinux fcontext that will permit it to be shared by multiple services.

- The Client Virtual machine should boot into a GNOME desktop
- The Server Virtual machine should boot into runlevel 3 (CLI only), but should provide a desktop for root and for tester through secure VNC.
- Configure static name resolution such that FQDN of each VM resolves correctly (even without DNS) from each of the other VMs.
- Configure each of the following names as aliases for `s<x>server.linux-acc.local`:
    - `pres.s<x>server.linux-acc.local`
    - `rep.s<x>server.linux-acc.local`
    - `dem.s<x>server.linux-acc.local`
- On the Client virtual machine, create a directory `/home/remote`.
- On the Client virtual machine, configure the automounter such that attempts to access locations in `/home/remote/presidents/` cause the nfs share `/share/presidents` from your server to be mounted at `/home/remote/presidents`.
- On the Client virtual machine, install the `slang` package.

RHCE Requirements

Complete the following in approximately 2 hours:

- Ensure that both the Server and Client Virtual machines are obtaining their time from NTP. Your server virtual machine should obtain its time from `ntppub.tamu.edu` and from `ntp.bytestacker.com`. Your client virtual machine should get its time from your server virtual machine.
- SSH connections should be allowed from throughout the `192.168.4.0/22` network.
- For all other services, connections should be allowed from addresses within the trusted network (`192.168.5.0/24`), but disallowed from `192.168.4.0/24`.
- Configure an SMTP server that allows connections from the trusted subnet.
- Connect to the iSCSI target provided by the target portal at `192.168.5.200`.
- Configure `/share/presidents`, `/share/presidents/republicans`, and `/share/presidents/democrats` to be shared via NFS to any system in the trusted subnet. Ensure that root privileges cannot be gained from a remote mount.
- Configure an FTP server to allow anonymous downloads from `/var/ftp/pub` and anonymous uploads to `/var/ftp/pub/inbound` (create this directory and set permissions appropriately). Ensure that uploaded files cannot be viewed or downloaded without admin intervention.
- Configure a Web server to serve the following vhosts:

    Access to `pres.s<x>server.linux-acc.local`
    serves an index page located in `/share/presidents/`

    Access to `rep.s<x>server.linux-acc.local`
    serves an index page located in `/share/presidents/republicans/`

    Access to `dem.s<x>server.linux-acc.local`
    serves an index page located in `/share/presidents/democrats/`

Use filesystem ACLs to resolve any permissions issues you encounter.

Place an index file in each of these locations that indicates which directory it is in and under which name it should be served out.

- Configure Samba to share the `/share/presidents` directory using a share name of presidents. Make it readable for `ford` and `carter` and writable for `reagan` and `clinton`.
- Create a bash script that uses `top` non-interactively to write 2 interations of its report to the file `/root/logs/top_report.txt`. Configure a cron job that performs this task every 20 minutes.
- Configure your Server VM to provide a caching DNS server and to allow queries from the trusted network. Configure your Client VM to obtain its DNS name resolution from your Server VM.
- Tune the kernel behavior of your Server VM so that it will respond to broadcast pings (ICMP ECHO broadcasts). This must persist after a reboot.