STUDY RHCSA

RH-124-9 – SYSTEM ADMINISTRATOR i

RH-134-8 – SYSTEM ADMINISTRATOR ii

EX200 EXAM GUIDE

RH-124-9

Course objectives

As a result of attending this course, delegates should be able to demonstrate the following skills:

- Introduce Linux and the Red Hat Enterprise Linux ecosystem.
- Run commands and view shell environments.
- Manage, organize, and secure files.
- Manage users, groups and user security policies.
- Control and monitor systemd services.
- Configure remote access using the web console and SSH.
- Configure network interfaces and settings.
- Archive and copy files from one system to another.
- Manage software using DNF.

Course content

Lesson 1: Get started with Red Hat Enterprise Linux	
• Describe and define open source, Linux, Linux distributions, and Red Hat Enterprise Linux.	
Lesson 2: Access the command line	
• Log in to a Linux system and run simple commands from the shell.	
Lesson 3: Manage files from the command line	
• Copy, move, create, delete, and organize files from the Bash shell.	
Lesson 4: Get help in Red Hat Enterprise Linux	
• Resolve problems by using local help systems.	

Lesson 5: Create, view, and edit text files	
• Create, view, and edit text files from command output or in a text editor.	
Lesson 6: Manage local users and groups	
• Create, manage, and delete local users and groups, and administer local password policies.	
Lesson 7: Control access to files	
• Set Linux file-system permissions on files and interpret the security effects of different permission settings.	
Lesson 8: Monitor and Control services and daemons	
• Control and monitor network services and system daemons with the system service.	
Lesson 9: Configure and secure SSH	
• Configure secure command-line services on remote systems with OpenSSH.	
Lesson 10: Analyze and store logs	
• Locate and accurately interpret system event logs for troubleshooting purposes.	
Lesson 11: Manage networking	

• Configure network interfaces and settings on Red Hat Enterprise Linux servers.	
Lesson 12: Archive and transfer files	
• Archive and copy files from one system to another.	
Lesson 13: Install and Update Software Packages	
• Download, install, update, and manage software packages from Red Hat and DNF package repositories…	
Lesson 14: Access Linux file systems	
• Access, inspect, and use existing file systems on storage that is attached to a Linux server.	
Lesson 15: Analyze servers and get support	
• Investigate and resolve issues in the web-based management interface, getting support from Red Hat to help solve problems.	
Lesson 16: Comprehensive review	
• Review tasks from Red Hat System Administration I.	

RH-134-8

Course objectives

As a result of attending this course, delegates should be able to demonstrate the following skills:

- •Install Red Hat Enterprise Linux with scalable methods.
- •Access security files, file systems, and networks
- •Execute shell scripting and automation techniques
- •Manage storage devices, logical volumes, and file systems
- •Manage security and system access
- •Control the boot process and system services
- •Running containers

Course content

Lesson 1: Improve command line productivity	
• Run commands more efficiently by using advanced features of the bash shell, shell scripts, and various utilities provided by Red Hat Enterprise Linux.	
Lesson 2: Schedule future tasks	
• Schedule tasks to execute at a specific time and date.	
Lesson 3: Tune system performance	
• Improve system performance by setting tuning parameters and adjusting scheduling priority of processes.	
Lesson 4: Manage SELinux security	
• Protect and manage the security of a server by using SELinux.	
Lesson 5: Maintain basic storage	

• Create and manage storage devices, partitions, file systems, and swap spaces from the command line.	
Lesson 6: Manage logical volumes	
• Create and manage logical volumes containing file systems and swap spaces from the command line.	
Lesson 7: Access network-attached storage	
• Access network-attached storage with the NFS protocol.	
Lesson 8: Control the boot process	
• Manage the boot process to control services offered and to troubleshoot and repair problems.	
Lesson 9: Manage network security	
• Control network connections to services using the system firewall and SELinux rules.	
Lesson 10: Install Red Hat Enterprise Linux	
• Install Red Hat Enterprise Linux on servers and virtual machines.	
Lesson 11: Run Containers	
• Obtain, run, and manage simple lightweight services as containers on a single Red Hat Enterprise Linux server.	

EX 200 – ADMINISTRATOR – (RHCSA) EXAM

TIME: 3HRS

LAB ENVIRONMENT

PASSMARK: 70%

Study points for the exam

RHCSA exam candidates should be able to accomplish the tasks below without assistance. These have been grouped into several categories.

Understand and use essential tools

- Access a shell prompt and issue commands with correct syntax
- Use input-output redirection (>, >>, |, 2>, etc.)
- Use grep and regular expressions to analyze text
- Access remote systems using SSH
- Log in and switch users in multiuser targets
- Archive, compress, unpack, and uncompress files using tar, star, gzip, and bzip2
- Create and edit text files
- Create, delete, copy, and move files and directories
- Create hard and soft links
- List, set, and change standard ugo/rwx permissions
- Locate, read, and use system documentation including man, info, and files in /usr/share/doc

Create simple shell scripts

- Conditionally execute code (use of: if, test, [], etc.)
- Use Looping constructs (for, etc.) to process file, command line input
- Process script inputs ($1, $2, etc.)
- Processing output of shell commands within a script

Operate running systems

- Boot, reboot, and shut down a system normally
- Boot systems into different targets manually
- Interrupt the boot process in order to gain access to a system
- Identify CPU/memory intensive processes and kill processes
- Adjust process scheduling

- Manage tuning profiles
- Locate and interpret system log files and journals
- Preserve system journals
- Start, stop, and check the status of network services
- Securely transfer files between systems

Configure local storage

- List, create, delete partitions on MBR and GPT disks
- Create and remove physical volumes
- Assign physical volumes to volume groups
- Create and delete logical volumes
- Configure systems to mount file systems at boot by universally unique ID (UUID) or label
- Add new partitions and logical volumes, and swap to a system non-destructively

Create and configure file systems

- Create, mount, unmount, and use vfat, ext4, and xfs file systems
- Mount and unmount network file systems using NFS
- Configure autofs
- Extend existing logical volumes
- Create and configure set-GID directories for collaboration
- Diagnose and correct file permission problems

Deploy, configure, and maintain systems

- Schedule tasks using at and cron
- Start and stop services and configure services to start automatically at boot
- Configure systems to boot into a specific target automatically
- Configure time service clients
- Install and update software packages from Red Hat Network, a remote repository, or from the local file system
- Modify the system bootloader

Manage basic networking

- Configure IPv4 and IPv6 addresses
- Configure hostname resolution
- Configure network services to start automatically at boot
- Restrict network access using firewall-cmd/firewall

Manage users and groups

- Create, delete, and modify local user accounts
- Change passwords and adjust password aging for local user accounts
- Create, delete, and modify local groups and group memberships
- Configure superuser access

Manage security

- Configure firewall settings using firewall-cmd/firewalld
- Manage default file permissions
- Configure key-based authentication for SSH
- Set enforcing and permissive modes for SELinux
- List and identify SELinux file and process context
- Restore default file contexts
- Manage SELinux port labels
- Use boolean settings to modify system SELinux settings
- Diagnose and address routine SELinux policy violations

Manage containers

- Find and retrieve container images from a remote registry
- Inspect container images
- Perform container management using commands such as podman and skopeo
- Build a container from a Containerfile
- Perform basic container management such as running, starting, stopping, and listing running containers
- Run a service inside a container
- Configure a container to start automatically as a systemd service
- Attach persistent storage to a container

As with all Red Hat performance-based exams, configurations must persist after reboot without intervention. Red Hat reserves the right to add, modify, and remove objectives. Such changes will be made public in advance through revisions to this document.

RHCSA 9 - EX 200 – (RHCSA) -- EXAM SAMPLE

--------- VM REQUIREMENTS – 9 DISKS “various size” / 3 NICS --------

Ensure all the tasks are implemented with firewalld and SELinux enabled. Your server should be able to survive a reboot with persistence. Good Luck.
Take note that the ip address 192.168.0.X is your local ip address – please change accordingly to complete this exam sample.

Question 0: (root Passwd)

Interrupt the boot process and reset the root password. Change it to “wander” to gain access to the system make sure that settings do not change make sure that SELinux is enforcing

Question 1: (NMCLI - IPV4)

Configure TCP/IP and “hostname” as following – for ipv4 ...

IP ADDRESS = 192.168.0.(94 or 90) == e.g(172.25.X.11) X is your seat number in exam
NETMASK = 255.255.255.0
GATEWAY = 192.168.0.1 ==== e.g(172.25.X.254)
DNS = 8.8.8.8 ------ e.g(172.25.254.254)
Hostname = serverX.example.com

Question 2: (NMCLI - IPV6)

Add the following secondary IP address statically to your current setup. Do this in a way that doesn’t compromise your existing settings --- **IPV6 ---- fd01::100/64**

Question 3: (REPO)

Configure your repository for installing the packages distribution which is available via YUM / DNF ; Exam can be ftp or file or https for the repos.

Base os url = file:///mnt/repo/BaseOS
App stream url = file:///mnt/repo/AppStream

Question 4: (Local TimeZone)

The system time should be set to your (or nearest to you) timezone

Question 5: (Packet Forwarding)

Enable packet forwarding for ipv4 and ipv6 on your system. This should persist after a reboot

Question 6: (SELINUX)

Configure a basic web server that displays “Welcome to the Jungle” once connected and make it listen on port 82

SELINUX – make sure selinux is in enforcing mode

SELINUX BOOLEAN – ensure the httpd is able to access the user home directory

SELINUX PORT – the system is not able to connect to httpd service port 82 it should be accessible at port 82 and should start at boot time

SELINUX CONTEXT – Ensure that the httpd service is able to access and host files from the /test directory – not from /var/www/html

Question 7: (UMASK)

set the default permission for user alex and for all newly created file and folders

- set the permission for all newly created files == r- - r- -r- -
- set the permission for all newly created directories == r-xr-xr-x

Question 8: (USERS / ACL / SUDOERS)

create the following users, groups, and group membership
- all new users should have a file named **“Welcome”** in their home folder after account creation that says – “welcome to redhat training 101” when logged into account

- all user passwords should expire after 60 days for future user creation and any user created
- a group named "sysadm"
- a user “harry” who belongs to "sysadm” as a secondary group
- a user “natasha” who belongs to "sysadm" as a secondary group
- a user “sarah” who does not have access to an interactive shell & who is not a member of "sysadm" group
- “harry”, “natasha”, and “sarah” should all have the password of password
- “sysadm" group has access to add user in the server
- “harry” user has access to set password for users without asking sudo password

- phil and laura should be part of the “accounting group”
- steward and kevin should be part of the “marketing group”

Question 9: (SUID / SGID / STICKYBIT)

create a collaborative directory /shared/"sysadm" with the following characteristics:

- Group ownership of “/shared/sysadm/” is "sysadm"
- The directory should be readable, writable, and accessible to member of "sysadm", but not to any other user -- (it is understood that root has access to all files and directories on the system)
- Files created in “/shared/sysadm” automatically have group ownership set to the "sysadm" group
- Only members of the accounting group should have access to the “/accounting” directory. Make laura the owner of the this directory. Make the accounting group the group owner of the accounting directory
- Only members of the marketing group should have access to the “/marketing” directory. Make steward the owner of this directory. Make the marketing group the group owner of the “/marketing” directory

Question 10: (CRONS)

Set the following cron jobs for the user “Natasha”
- that should run daily every 1 minutes local time and executes “Ex200 Testing” with logger
- that should run at 14:30 everyday with echo the words : hello world

Question 11: (NFS - AUTOFS)

Configure autofs to automount the home directories of netuserX user. Note the following:
- if you do not have a seperate server you can use your own localhost for this

- netuserX home directory is exported via NFS which is available on “192.168.0.91”
- (192.168.0.91) and your NFS-exports directory is “/netdir” for “netuserX”,
- netuserX home directory is “192.168.0.91:/home/guests/netuserX”
- netuserX home directory should be automounted autofs service
- home directories must be writable by there users
- password for “netuser” is “ablerate”

Question 12: (create archive)

create a tar archive of “/etc/” Directory with .bzip2 extension. Tar archive named “myetcbackup.tar” should be placed in “/root/” directory

Question 13: (file permissions)

Copy the file /etc/fstab/ to /var/tmp. Configure the permissions of /var/tmp/fstab so that
- the file /var/tmp/fstab is owned by the root user
- the file /var/tmp/fstab belongs to the group root
- the file /var/tmp/fstab should not be executable by anyone
- the user “natasha” is able to read and write /var/tmp/fstab
- the user “harry” can neither write nore read /var/tmp/fstab
- all other users (current or future) have the ability to read /var/tmp/fstab

Question 14: (BASH)

Write a script named awesome.sh in the root directory on the system
-- if **“me”** is given as an argument then the script should ouput **“Yes Im Awesome”**
-- if **“them”** is given as an argument then the script should ouput **“Okay they are Awesome”**
-- if the argument is empty or anything else is given then the script should ouput **“Usage ./awesome.sh me|them”**

Question 15: (NTP)

Configure your system to synchronize the time from one or all of the NTP servers
- 0.africa.pool.ntp.org
- 1.africa.pool.ntp.org
- 2.africa.pool.ntp.org
- 3.africa.pool.ntp.org

Question 16: (FIND)

Find all the .txt file extensions and NOT directories for the user “root” with the permission of “rw-r—r--” with a size of more than 1Mb and less than 30Mb and copy it into “/share/txtfiles/” directory

Question 17: (GREP/eGREP)

Find all strings “ich” AND “stratisd” from “/usr/share/dict/words” file and copy that strings in a “/root/lines” file

Question 18: (USERS)

Create a user “unilao” with UID “2334” with password as “ablerate”

- change natasha user to the accounting group

Question 19: (TUNED)

Configure recommended tuned profile

Question 20: (Containers build)

Download containerfile from “http://192.168.0.91/Containerfile”
Containerfile Contents:
“””
FROM docker.io/centos/httpd-24-centos7
LABEL maintainer=”Linux2Cloud”
“””
- Do not make any modification
- Build image with this container

Question 21: (Containers manage)

Configure a container to start automatically

- create a container named mycontainer using the image which you build previously
- configure the service to automatically mount the directory “/opt/file” to container directory “/opt/incoming” and user directory “/opt/processed” to container directory “/opt/output”
- configure to run it as a systemd service that should run from existing user xanadu only
- the service should be named mycontainer and should automatically start at system rebot without any manual intervention.

Question 22: (Disks)

Create a standard xfs partition of 5GB and make it available permanent

Question 23: (SWAP)

Create a swap partition of 400MB and make it available permanent

Question 24: (VDO)

Use the appropriate utility to create a 50Gb thin provisioned volume

Question 25: (LVM CREATE / EXTEND / REDUCE)

Create a new 2Gb volume group name “vgprac” with the size of the PE at 8Mb

- Create a 500mb logical volume name “lvprac” inside the “vgprac” volume group
- Create a logical volume name “lvpracext” with 30 extent inside the “vgprac” volume group
- The “lvprac” logical volume should be formatted with the “xfs” filesystem and mounted persistently on the /mnt/lvprac directory
- The “lvpracext” logical volume should be formatted with the “ext4” filesystem and mounted persistently on the “/mnt/lvpracext” directory
- Extend the “xfs” filesystem on lvprac by 500mb
- Reduce the size of the “ext4” filesystem on lvpracext by 100mb

-make all permanent

Question 26: (STRATIS)

Create a file system from a stratis named “pool1”

- extend the stratis “pool1” by 2Gb
- create a secondary filesystem on “pool1”
- make all permanent