OpenRHCE

A Creative Commons Courseware for RHCE Preparation

Course Outline

Contents

Session One: Introduction

Introductions: Your Instructor

Scott Purcell

scott@texastwister.info

http://www.linkedin.com/in/scottpurcell

http://twitter.com/texastwister

http://www.facebook.com/Scott.L.Purcell

Introductions: Your Instructor

Qualifications:

- RHCSA, RHCE #110-008-877 (RHEL6)
- Also: CTT+, CLA, CLP, CNI, LPIC1, Linux+
- Curriculum Developer and Trainer for a major computer manufacturer for going on 11 years
- Linux Enthusiast since 2000

Personal:

- Husband, father, disciple and
- Fun: Part-time Balloon Entertainer

Introductions: Fellow Students

Please Introduce Yourselves

- Name
- Where you work or what you do.
- What Linux experience do you already have?
- What goals do you have for this class?
- Something fun about yourself.

Introductions: The Course

Expectations

- Should I be able to pass the RHCE on this class alone?

  A stunning number of seasoned professionals taking Red Hat's own prep courses fail to pass on first attempt.

- Planning for more than one attempt is prudent.
- Maximizing your out-of-class preparation time is prudent.

Preparation Recommendations

- Practice/Study Environment
  - 2 or 3 systems or VMs, networked together. Virtualized hosting providers may be an alternative.
  - RHEL 6 (eval), CENTOS 6 (when available), or Fedora (Fedora 13 will be closest to RHEL 6)
  - Red Hat docs at:

    http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/index.htm
  - RHCE Objectives and other information at:

    http://www.redhat.com/certification/
  - Take initiative -- form a study group.
  - Practice, practice, practice!

The Red Hat Certification Landscape

- RHCSA

  RHCSA is new, replacing the RHCT. It is the "core" sysadmin certification from Red Hat. To earn RHCE and other system administration certs will require first earning the RHCSA.

- RHCE

  RHCE is a senior system administration certification. It is an eligibility requirement for taking any COE exams and is thus a requirement for the upper-level credentials as well.

- Certificates of Expertise

  COEs are incremental credentials demonstrating skills and knowledge in specialized areas. They are worthy credentials in their own right, but also the building blocks of the upper level credentials.

- RHCSS, RHCDS, RHCA

  These upper level credentials recognize those who have achieved expertise in several related specialized areas. Each one requires multiple COEs.

RHCSA Objectives

RHCSA Objectives: Understand & 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 and VNC
- Log in and switch users in multi-user runlevels
- Archive, compress, unpack and uncompress files using tar, star, gzip, and bzip2

RHCSA: ...Essential Tools... (cont)

- 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 .

  [Note: Red Hat may use applications during the exam that are not included in Red Hat Enterprise Linux for the purpose of evaluating candidate's abilities to meet this objective.]

RHCSA: Operate Running Systems

- Boot, reboot, and shut down a system normally
- Boot systems into different runlevels manually
- Use single-user mode to gain access to a system
- Identify CPU/memory intensive processes, adjust process priority with renice, and kill processes
- Locate and interpret system log files
- Access a virtual machine's console
- Start and stop virtual machines
- Start, stop and check the status of network services

RHCSA: Configure Local Storage

- List, create, delete and set partition type for primary, extended, and logical partitions
- Create and remove physical volumes, assign physical volumes to volume groups, create and delete logical volumes
- Create and configure LUKS-encrypted partitions and logical volumes to prompt for password and mount a decrypted file system at boot
- Configure systems to mount file systems at boot by Universally Unique ID (UUID) or label
- Add new partitions, logical volumes and swap to a system non-destructively

RHCSA: Create and Configure File Systems

- Create, mount, unmount and use ext2, ext3 and ext4 file systems
- Mount, unmount and use LUKS-encrypted file systems
- Mount and unmount CIFS and NFS network file systems
- Configure systems to mount ext4, LUKS-encrypted and network file systems automatically
- Extend existing unencrypted ext4-formatted logical volumes
- Create and configure set-GID directories for collaboration
- Create and manage Access Control Lists (ACLs)
- Diagnose and correct file permission problems

RHCSA: Deploy, Configure & Maintain

- Configure networking and hostname resolution statically or dynamically
- Schedule tasks using cron
- Configure systems to boot into a specific runlevel automatically
- Install Red Hat Enterprise Linux automatically using Kickstart
- Configure a physical machine to host virtual guests
- Install Red Hat Enterprise Linux systems as virtual guests
- Configure systems to launch virtual machines at boot
- Configure network services to start automatically at boot
- Configure a system to run a default configuration HTTP server
- Configure a system to run a default configuration FTP server
- Install and update software packages from Red Hat Network, a remote repository, or from the local filesystem
- Update the kernel package appropriately to ensure a bootable system
- Modify the system bootloader

RHCSA: 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 a system to use an existing LDAP directory service for user and group information

RHCSA: Manage Security

- Configure firewall settings using system-config-firewall or iptables
- Set enforcing and permissive modes for SELinux
- List and identify SELinux file and process context
- Restore default file contexts
- Use boolean settings to modify system SELinux settings
- Diagnose and address routine SELinux policy violations

RHCE Objectives

RHCE: System Configuration and Management

- Route IP traffic and create static routes
- Use iptables to implement packet filtering and configure network address translation (NAT)
- Use /proc/sys and sysctl to modify and set kernel run-time parameters
- Configure system to authenticate using Kerberos
- Build a simple RPM that packages a single file
- Configure a system as an iSCSI initiator that persistently mounts an iSCSI target
- Produce and deliver reports on system utilization (processor, memory, disk, and network)
- Use shell scripting to automate system maintenance tasks
- Configure a system to log to a remote system
- Configure a system to accept logging from a remote system

RHCE: Network Services

Network services are an important subset of the exam objectives. RHCE candidates should be capable of meeting the following objectives for each of the network services listed below:

- Install the packages needed to provide the service
- Configure SELinux to support the service
- Configure the service to start when the system is booted
- Configure the service for basic operation
- Configure host-based and user-based security for the service

RHCE candidates should also be capable of meeting the following objectives associated with specific services:

RHCE: HTTP/HTTPS

- Install the packages needed to provide the service
- Configure SELinux to support the service
- Configure the service to start when the system is booted
- Configure the service for basic operation
- Configure host-based and user-based security for the service
- Configure a virtual host
- Configure private directories
- Deploy a basic CGI application
- Configure group-managed content

RHCE: DNS

- Install the packages needed to provide the service
- Configure SELinux to support the service
- Configure the service to start when the system is booted
- Configure the service for basic operation
- Configure host-based and user-based security for the service
- Configure a caching-only name server
- Configure a caching-only name server to forward DNS queries
- Note: Candidates are not expected to configure master or slave name servers

RHCE: FTP

- Install the packages needed to provide the service
- Configure SELinux to support the service
- Configure the service to start when the system is booted
- Configure the service for basic operation
- Configure host-based and user-based security for the service
- Configure anonymous-only download

RHCE: NFS

- Install the packages needed to provide the service
- Configure SELinux to support the service
- Configure the service to start when the system is booted
- Configure the service for basic operation
- Configure host-based and user-based security for the service
- Provide network shares to specific clients
- Provide network shares suitable for group collaboration

RHCE: SMB

- Install the packages needed to provide the service
- Configure SELinux to support the service
- Configure the service to start when the system is booted
- Configure the service for basic operation
- Configure host-based and user-based security for the service
- Provide network shares to specific clients
- Provide network shares suitable for group collaboration

RHCE: SMTP

- Install the packages needed to provide the service
- Configure SELinux to support the service
- Configure the service to start when the system is booted
- Configure the service for basic operation
- Configure host-based and user-based security for the service
- Configure a mail transfer agent (MTA) to accept inbound email from other systems
- Configure an MTA to forward (relay) email through a smart host

RHCE: SSH

- Install the packages needed to provide the service
- Configure SELinux to support the service
- Configure the service to start when the system is booted
- Configure the service for basic operation
- Configure host-based and user-based security for the service
- Configure key-based authentication
- Configure additional options described in documentation

RHCE: NTP

- Install the packages needed to provide the service
- Configure SELinux to support the service
- Configure the service to start when the system is booted
- Configure the service for basic operation
- Configure host-based and user-based security for the service
- Synchronize time using other NTP peers

Operating a System: Boot, Reboot, Shutdown

- GRUB Menu
- Display Manager Screen
- Gnome or KDE
- Terminal commands: shutdown, halt, poweroff, reboot, init

Operating a System: Runlevels

- Default
- From GRUB Menu

Operating a System: Single User Mode

- Password Recovery

Note: SELinux bug prevents password changes while set to "Enforcing".

Operating a System: Log Files

`/var/log/*`

View with `cat`, `less` or other tools

Search with `grep`

Operating a System: Start/Stop Virtual Machines

- Using virt-manager
- Using virsh commands

Operating a System: Virtual Machine Consoles

- virt-manager
- virt-viewer

Operating a System: Virtual Machine Text Console

With libguestfs-tools installed and the VM in question shut-down, from the host:

```
# virt-edit {VMname} /boot/grub/menu.lst
```

There, append to the kernel line:

```
console=tty0 console=ttyS0.
```

After saving, the following commands should allow a console based view of the boot process and a console login:

```
# virsh start {VMname} ; virsh console {VMname}
```

Operating a System: Start, stop, and check the status of network services

Operating a System: Modify the system bootloader

Session 2 Storage and filesystems

"Filesystem" - Disambiguation

Several meanings for the term:

- The way files are physically written to storage devices, as in the ext3, Fat-32, NTFS filesystems, or etc.
- The unified directory structure which logically organizes files
- The standard which defines how directories should be structured and utilized in Linux

Linux Filesystem Hierarchy

The directory structure of a Linux system is standardized through the Filesystem Hierarchy Standard (explained at http://www.pathname.com/fhs)

The Linux Manual system has an abbreviated reference:

```
$ man 7 hier
```

Red Hat has a more complete description, along with RedHat-specific implementation decisions in their **Deployment Guide** at http://www.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/html/Deployment_Guide/ch

Disk and Filesystem tools

- `fdisk` or `parted` -- Used to partition hard disks or other block devices
- `mkfs` and variants -- Used to create filesystems on block devices (actually a front-end for a variety of FS-specific tools)
- `fsck` and variants -- Used to run filesystem checks (a front-end to FS specific tools)
- `mount` -- Used to mount a filesystem to a specific location in the directory structure
- `/etc/fstab` -- Configuration file used to describe the filesystems that should be persistently mounted
- `blkid` -- used to identify filesystems or other in-use devices by UUID or filesystem labels.
- `df` -- used to display the capacity and utilization % of mounted filesystems.
- `partx` -- used to force implementation of a new partition table on an in-use device w/o the need to reboot.

Local Storage: Working with Partitions

Overview of process for using Basic Storage Devices:

- Install the device or otherwise make it available to the system.
- Partition it with `fdisk` or `parted`.
- Create a filesystem on the partition with mkfs or other tools.
- Choose or create a directory to serve as a mount point.
- Mount the partition.
- Add an entry to `/etc/fstab` to make it persistent.

Local Storage: Working with Logical Volume Management

Overview of process for using Logical Volume Management:

- Install the device or otherwise make it available to the system.
- Create a type `8e` partition with `fdisk` or `parted`.
- Initialize the partition as a physical volume with `pvcreate`.
- Add the storage of the PV to a volume group with `vgcreate`.
- Allocate storage from the volume group to a logical volume with `lvcreate`.
- Create a filesystem on the logical volume with mkfs or other tools.
- Choose or create a directory to serve as a mount point.
- Mount the partition.
- Add an entry to `/etc/fstab` to make it persistent.

Local Storage: Commands to Know

fdisk

- Always use -u and -c for best compatibility with newer storage devices
- Can't create partitions >= 2TB, use parted with GPT instead

mkfs

- Used to create filesystems on devices
- Front-end for other filesystem-specific tools (usually named mkfs.<fstype>)

blkid

- Shows device name, Fileystem Labels, and UUID of detected block devices.
- May not show block devices until a filesystem is created on them.
- May not show block devices used in non-standard ways (for example, a filesystem on a whole disk instead of on a partition)

mount

- used to make a new filesystem available

Local Storage: Working with LUKS encrypted storage

Overview of process for using LUKS encryption:

- Create a new partition
- Encrypt it with `cryptsetup luksFormat /dev/<partition>`
- Open the encrypted device and assign it a name with `cryptsetup luksOpen /dev/<partition> <name>`
- Create a filesystem on the named device (/dev/mapper/<name>)
- Create a mountpoint for the device
- Mount the device

To lock the volume:

- unmount it
- Use `cryptsetup luksClose <name>` to remove the decryption mapping

Local Storage: Persistent mounting of LUKS devices

To persistently mount it:

- Create an entry in /etc/crypttab:

```
<name> /dev/<partition> <password (none|<blank>|<path/to/file/with/password>)>
```

- If the password field is "none" or left blank, the system will prompt for a password.
- Create an entry in /etc/fstab

Local Storage: Working with SWAP

Overview of process for adding SWAP space using a partition:

- Create a type 82 partition
- Initialize as swap with `mkswap /dev/<partition>`
- Identify the UUID with `blkid`
- Add an `/etc/fstab` line:

```
UUID=<UUID> swap swap defaults 0 0
```

- Activate the new swap space with: `swapon -a`

Local Storage: Using a file for SWAP

Overview of process for adding SWAP space using a file:

- create a pre-allocated file of the desired size:

```
dd if=/dev/zero of=/path/to/<swapfile> bs=1M count=<size in MB>
```

  - Initialize as swap with `mkswap /path/to/<swapfile>`
  - Add an `/etc/fstab` line:

```
/path/to/<swapfile> swap swap defaults 0 0
```

  - Activate the new swap space with: `swapon -a`

Local Storage: Using UUIDs and Filesystem Labels

Configure systems to mount file systems at boot by Universally Unique ID (UUID) or label

Local Storage: Adding New Storage

Add new partitions, logical volumes, and swap to a system non-destructively

File systems: Working with Common Linux Filesystems

Create, mount, unmount and use ext2, ext3 and ext4 file systems

Extend existing unencrypted ext4-formatted logical volumes

Filesystem Permissions: Basic Permissions

Linux permissions are organized around:

- Three sets of permissions -- User, Group, and Other
- Three types of permissions -- Read, Write, and Execute
- Three extended attributes -- SUID, SGID, and Stickybit

Three Sets of Permissions:

Any given file or directory can be owned by one (and only one) user and one (and only one) group. Three different sets of permissions can be assigned.

- User -- User permissions apply to the individual user who owns the file or directory.
- Group -- Group permissions apply to any user who is a member of the group that owns the file or directory.
- Other -- Other permissions apply to any user account with access to the system that does not fall into the previous categories.

Three Types of Permissions:

- Read ("r")
  - On a file, allows reading
  - On a directory, allows listing
- Write ("w")
  - On a file, allows editing
  - On a directory, allows creation and deletion of files
- Execute ("x")
  - On a file, allows execution if the file is otherwise executable (script or binary)
  - On a directory, allows entry or traversal (`# cd {dirname}`)

Three Extended Attributes:

- **SUID (Set User ID)**

  On an executable, runs a process under the UID of the file owner rather than that of the user executing it.

- **SGID (Set Group ID)**

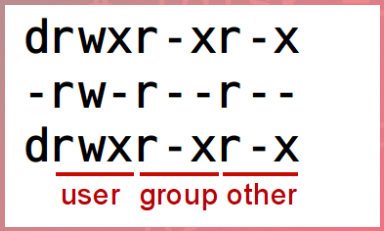
  On a directory, causes any files created in the directory to belong to the group owning the directory.

- **"Stickybit"**

  On a directory, ensures that only the owner of a file or the owner of the directory can delete it, even if all users or other members of a group have write access to the directory.

Viewing Permissions

Permissions are displayed with positions 2-10 of a "long" filelisting:



Setting Permissions

The `chmod` command is used to set permissions on both files and directories. It has two modes -- one using symbolic options and one using octal numbers.

`chmod [option] [ugoa...][+-=][rwxst] filename`

where ugo are user, group, other, or all and rwxst are read, write, execute, s{u/g}id, stickybit.

`chmod [option] XXXX filename`

where XXXX is a number representing the complete permissions on the file.

Setting Permissions with Numeric Options

	User			G		Other			
Permissions	r	w	x	r	w	x	r	w	x
Numeric Value	4	2	1	4	2	1	4	2	1
Sum	0-7			0-7	0-7				

example.txt	User			G		Other			
Permissions	r	w	x	r	-	x	-	-	x
Numeric Value	4	2	1	4	0	1	0	0	1
Sum	7			5	1				

```
# chmod 751 myfile.txt
```

Setting Extended Attributes with Numeric Options

chmod numeric options are actually 4 digits (not three). Missing digits are assumed to be leading zeroes.

The leftmost place is for extended attributes:

Attribute	SUID	SGID	Stickybit
Value	4	2	1

Example: `$ chmod 3775 MySharedDir`

Setting Extended Attributes with Symbolic Values:

`chmod +t {filename}`

Sets the sticky bit

`chmod u+s {filename}`

Sets suid

`chmod g+s {filename}`

Sets sgid

Extended Attributes in Directory Listings

-rwxrwxrwx	Normal Permissions, All permissions granted
-rwSrwxrwx	Indicates SUID set
-rwsrwxrwx	Indicates SUID and execute permission set
-rwxrwSrwx	Indicates SGID set
-rwxrwsrwx	Indicates SGID and execute permission set
-rwxrwxrwT	Indicates Stickybit set
-rwxrwxrwt	Indicates Stickybit and execute permission set

Umask

- The umask value determines the permissions that will be applied to newly created files and directories.
- As a "mask" it is subtractive -- representing the value of the permissions you DO NOT want to grant.
- Execute rights are automatically withheld (w/o regard for the umask) for *files* but not for *directories*.
- Extended attributes are not addressed -- even though a umask is four characters.
- The default umask value is set in /etc/bashrc and can be modified (non-persistently!) with the bash built-in command `umask`.

Umask Examples

- Umask of 0002 yields permissions of 0775 on new directories and 0664 on new files
- Umask of 0022 yields permissions of 0755 on new directories and 0644 on new files

Filesystem Permissions: Use case -- Collaborative Directories

- Create a Group for Collaboration
- Add users to the group
- Create a directory for collaboration
- Set its group ownership to the intended group
- Set its group permissions appropriately
- Recursively set the SGID and sticky bits on the directory

This ensures that:

All files created in this directory will be owned by the intended group (SGID effect)

All files created in this directory can only be deleted by the user who owns the file or the user who owns the directory (stickybit effect)

Filesystems Permissions: File Access Control Lists

- Provide more granular control of permissions.
- Filesystem must be mounted with the 'acl' option or be compiled with that option by default

getfacl

setfacl

getfacl

Example of "getfacl acldir"

```
# file: acldir
# owner: frank
# group: frank
user::rwx
user:bob:-wx
user:mary:rw-
group::rwx
mask::rwx
other::r-x
```

Example of `ls -l acldir`:

```
drwxrwxr-x+ 2 frank frank 4096 2009-05-27 14:15 acldir
```

..Create and manage File Access Control Lists

Network Storage: Working with CIFS network file systems

Will be covered in more detail later.

Mount and unmount CIFS network file systems

Network Storage: Working with NFS file systems

Mount and unmount NFS file systems

Network Storage: iSCSI Devices

Package: iscsi-initiator-utils

Allows a system to access remote storage devices with SCSI commands as though it were a local hard disk.

Terms:

- iSCSI initiator: A client requesting access to storage
- iSCSI target: Remote storage device presented from an iSCSI server or "target portal"
- iSCSI target portal: A server providing targets to the initiator
- IQN: "iSCSI Qualified Name" -- a unique name. Both the initiator and target need such a name to be assigned

Network Storage: Accessing iSCSI Devices

- Install the iscsi-initiator-utils package
- Start the `iscsi` and `iscsid` services (and configure them persistently on)
- Set the initiator IQN in /etc/iscsi/initiatorname.iscsi
- Discover targets with:

```
iscsiadm -m discovery -t st-p <targetportal IP address>
```

- Log in to the target using the name displayed in discovery:

```
iscsiadm -m mode -T <discovered IQN> -p <targetportal IP address> -l
```

- Identify the SCSI device name with `dmesg`, `tail /var/log/messages` or `ls -l /dev/disk/by-path/*iscsi*`
- Use the disk as though it were a local hard disk

Important

Be certain to use UUIDs or labels for persistent mounts in `/etc/fstab`. Also, provide `_netdev` as a mount option so that this device will not be mounted until the network is already up.

Network Storage: Disconnecting from iSCSI Devices

- Ensure the device is not in use
- Unmount the device
- Remove its `/etc/fstab` entry
- Logout from the target:

```
iscsiadm -m node -T <IQN> -p <portal IP> -u
```

- Delete the local record:

```
iscsiadm -m node -T <IQN> -p <portal IP> -o delete
```

Additional References

r 4 of the Storage Administration Guide for
ocs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Storage_Administration_Guide/in
the usage of parted.

- Man pages for fdisk(8), fstab(5), mkfs(8), blkid(8), partprobe(8), mount(8), parted(8), cryptsetup(8), and crypttab(5)

Session 3 Managing software, processes, kernel attributes, and users and groups

Managing Software: RHN

The primary delivery mechanism for installable software, updates, errata and bug fixes and systems management functions for an installation of RHEL 6 is the Red Hat Network or RHN.

The "cost" of RHEL 6 is really a subscription to this support network.

These commands are using in managing an RHN subscription:

```
# man -k rhn
rhn-profile-sync     (8)  - Update system information on Red Hat Network
rhn_check            (8)  - Check for and execute queued actions on RHN
rhn_register         (8)  - Connect to Red Hat Network
rhnplugin            (8)  - Red Hat Network support for yum(8)
rhnplugin.conf [rhnplugin] (5)  - Configuration file for the rhnplugin(8) yum(8) plugin
rhnreg_ks            (8)  - A program for non interactively registering systems to Red Hat Network
rhnsd                (8)  - A program for querying the Red Hat Network for updates and information
```

Managing Software: RHN Subscription Activation

A new user of RHEL6 should receive information similar to this:

```
Red Hat subscription login:
    Account Number       : *******
    Contract Number      : *******
    Item Description     : Red Hat Enterprise Linux ***Edition***
    RHEL Subscription Number : ******************
    Quantity             : #
    Service Dates        : 12-JUN-10 through 11-JUN-11
    Customer Name : ********************************
    Account Number: ************
    Log into the new portal here: access.redhat.com
    Login: *************
    Password: **************
    Email address: ***************************
```

That information can then be used with `rhn_register` to activate a new subscription

Managing Software: Repositories

These are other repositories of installable software, updates, or bugfixes. The `yum` command can be configured to use them in addition to or instead of the RHN.

Configuration of repositories other than the RHN is accomplished through text configuration files located in the directory: `/etc/yum.repos.d/`

Managing Software: Repo Configuration

- A configuration file for each repository (or group of related repos) should be created in `/etc/yum.repos.d/`
- The name of each repo config file should end in ".repo".
  - Tip: This allows repos to be easily temporarily disabled simply by renaming the file to something like: `myrepo.repo.disabled`

Mandatory options:

```
[repositoryid]
name=Some name for this repository
baseurl=url://path/to/repository/
```

Related man pages:

```
# man -k yum
qreposync             (1)  - synchronize yum repositories to a local directory
rhnplugin             (8)  - Red Hat Network support for yum(8)
rhnplugin.conf [rhnplugin] (5)  - Configuration file for the rhnplugin(8) yum(8) plugin
yum                   (8)  - Yellowdog Updater Modified
yum [yum-shell]       (8)  - Yellowdog Updater Modified shell
yum-groups-manager    (1)  - create and edit yum's group metadata
yum-utils             (1)  - tools for manipulating repositories and extended package management
yum.conf [yum]        (5)  - Configuration file for yum(8)
```

Managing Software: Using yum

Commond commands:

- `yum help`
- `yum list`
- `yum search KEYWORD`
- `yum info PACKAGENAME`

Managing Software: Using rpm

Managing Software: Building RPMs

Managing Software: Signing and Publishing RPMs

Managing Software: Updating the kernel package

Manage Processes and Services: Configure network services to start automatically at boot

Manage Processes and Services: Configure systems to boot into a specific runlevel automatically

Manage Processes and Services: Monitoring, prioritizing, and controlling processes

Manage Processes and Services: Schedule tasks using cron

Manage system performance

- Use /proc/sys and sysctl to modify and set kernel run-time parameters
- Produce and deliver reports on system utilization (processor, memory, disk, and network)
- Use shell scripting to automate system maintenance tasks

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 a system to use an existing LDAP directory service for user and group information
- Configure system to authenticate using Kerberos

Session 4 Networking and routing

o Networking & Routing + * Configure networking and hostname resolution statically or dynamically + * Route IP traffic and create static routes

Session 5 Firewalls and SELinux

o IPTables + * Configure firewall settings using system-config-firewall or iptables o SELinux + * Set enforcing and permissive modes for SELinux + * List and identify SELinux file and process context + * Restore default file contexts + * Use boolean settings to modify system SELinux settings + * Diagnose and address routine SELinux policy violations

Session 6 Virtualization

o KVM Virtualization + * Configure a physical machine to host virtual guests + * Install Red Hat Enterprise Linux systems as virtual guests + * Configure systems to launch virtual machines at boot + * Install Red Hat Enterprise Linux automatically using Kickstart

Session 7 Logging and remote access

o + - Remote Logging + * Configure a system to log to a remote system + * Configure a system to accept logging from a remote system o + - Remote Access + SSH # * Install the packages needed to provide the service # * Configure SELinux to support the service # * Configure the service to start when the system is booted # * Configure the service for basic operation # * Configure host-based and user-based security for the service # * Configure key-based authentication # * Configure additional SSH options described in documentation + VNC # * Install the packages needed to provide the service # * Configure SELinux to support the service # * Configure the service to start when the system is booted # * Configure the service for basic operation # * Configure host-based and user-based security for the service

Session 8 Network Time Protocol

o NTP + * Install the packages needed to provide the service + * Configure SELinux to support the service + * Configure the service to start when the system is booted + * Configure the service for basic operation + * Configure host-based and user-based security for the service

Session 9 HTTP and FTP

Session 10 NFS and Samba

Session 11 DNS and SMTP

Session 12 Finish uncompleted topics, Review, or Practice Exam