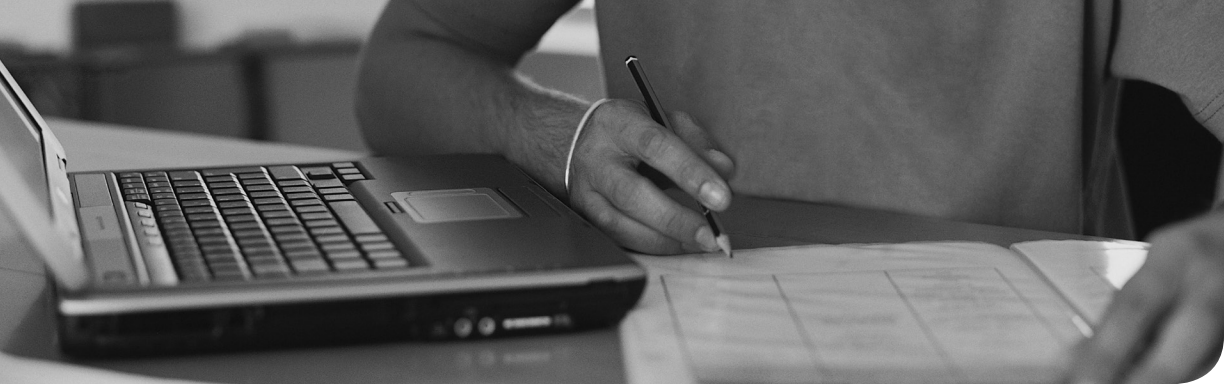

Answers to the "Do I Know This Already" Quizzes and "Review Questions"

Answers to the "Do I Know This Already" Quizzes

Chapter 1

1. A. Explanation: Fedora is an experimental/enthusiast version containing many components that may or may not make it into the RHEL distribution tree and onto the exams.
2. D. Explanation: All RHEL software updates are made available in CentOS as well.
3. A. Explanation: In particular, in Chapter 10, "Working with Virtual Machines," you'll be happy to have a GUI at your disposal.
4. C. Explanation: XFS is used as the default file system. When Red Hat decided which file system to use as the default file system, Btrfs was not stable enough yet.
5. A. Explanation: The size of an XFS file system cannot be reduced.
6. C. Explanation: The Fedora project tries to make a stable distribution as well. There are many Fedora users around the globe who use Fedora as a production distribution.
7. D. Explanation: The Troubleshoot an Existing Installation option is available when booting from disk, not on the Installation Summary screen.
8. D. Explanation: You are allowed to use an unsecure password; you just have to confirm it twice.
9. D. Explanation: Language settings can be changed after installation. This is done easily through the Settings option in the graphical interface.
10. B. Explanation: Even if it makes sense having /home on a dedicated partition, this is not part of a default installation.

Chapter 2

1. B. Explanation: Answer B shows the correct syntax. The **2** redirects error messages, and **&1** makes sure that the same is done for STDOUT.
2. A and B. Explanation: /etc/profile is the file that is processed for all users who are starting a login shell.
3. C. Explanation: On Linux, the current directory is not set in the PATH variable.
4. D. Explanation: A pipe is used to process the output of the first command and use it as input of the second command.
5. A. Explanation: The command **history -c** removes the in-memory state from the history file of current history. Remove ~/.bash_history also to make sure that all history is removed.
6. D. Explanation: **Ctrl+X** is not a valid history command.
7. D. Explanation: Bash completion works for commands, files, and variables and other names if configuration for that has been added (like hostnames for the SSH command).
8. A. Explanation: You need the command **:%s/old/new/** to replace all instances of *old* with *new*. **%** means that it must be applied on the entire file. **s** stands for substitute. The **g** option is used to not apply the command to only the first occurrence in a line (which is the default behavior) but on all occurrences.
9. B. Explanation: The /etc/motd file contains messages that are displayed after user login on a terminal session.
10. C. Explanation: The **man -k** command goes through a database to find the keywords you are looking for. On RHEL 7, this database is updated with the **mandb** command. The previously used **makewhatis** command is removed from RHEL 7.

Chapter 3

1. D. Explanation: Program files that are not required to boot a system are typically stored in a subdirectory below the /usr directory.
2. C. Explanation: The /var directory is used on Linux to store files that may grow unexpectedly.
3. A. Explanation: The /etc/directory contains configuration files that are needed while your server boots. Putting /etc on a dedicated device would make your server unbootable.
4. C. Explanation: The **df -h** command shows mounted devices and the amount of disk space currently in use on these devices. The **-T** option helps in

recognizing real file systems (as opposed to kernel interfaces) because it shows the file system type as well.

5. C. Explanation: The option **-a** shows hidden files, **-l** gives a long listing, **-t** sorts on modification time which by default shows newest files first, and **-r** reverts the sorting so that newest files are shown last.
6. C. Explanation: To copy hidden files as well as regular files, you need to put a **.** after the name of the directory the files are in. Answer A copies hidden files as well, but it creates a subdirectory $USER in the current directory.
7. A. Explanation: The **mv** command enables you to move files but also to rename files.
8. D. Explanation: In hard links, no difference exists between the first and subsequent hard links.
9. C. Explanation: The option **-s** is used to create a symbolic link. While creating a link, you first have to specify the source, and next you specify the destination.
10. C. Explanation: Use the option **-r** to add one single file to an archive you have created with tar.

Chapter 4

1. A. Explanation: The **head** command by default shows the first 10 lines in a text file.
2. D. Explanation: The **wc** command shows the number of lines, words, and characters in a file.
3. D. Explanation: When using less, the G key brings you to the end of the current file.
4. A. Explanation: The **-d** option is used to specify the field delimiter that needs to be used to distinguish different fields in files while using **cut**.
5. A . Explanation: The **sort** command can sort files or command output based on specific keys. If no specific key is mentioned, sorting happens based on fields. The option **-k3** will therefore sort the third field in the output of the **ps aux** command.
6. D. Explanation: When used in a regular expression, the ^ sign in front of the text you are looking for indicates that the text has to be at the beginning of the line.
7. A. Explanation: The ? regular expression is used to refer to zero or one of the previous characters. This makes the previous character optional, which can be useful. If the regular expression is 'colou?r', for example, you would get a match on 'color' as well as 'colour'.

8. B. Explanation: The . is used as a regular expression to refer to any single character.
9. D. Explanation: The **awk** command first needs to know which field separator should be used. This is specified with the **-F :** option. Then, it needs to specify a string that it should look for, which is **/user/**. To indicate that the fourth field of a matching file should be printed, you need to include the **{ print $4 }** command.
10. B. Explanation: Use **grep -v** to exclude lines containing the regular expression from the results.

Chapter 5

1. B. Explanation: The console is the screen you are working from. On the console, a terminal is started as the working environment. In the terminal, a shell is operational to interpret the commands you are typing.
2. A. Explanation: The console is the screen you are working from. On the console, a terminal is started as the working environment. In the terminal, a shell is operational to interpret the commands you are typing.
3. C. Explanation: The console is the screen you are working from. On the console, a terminal is started as the working environment. In the terminal, a shell is operational to interpret the commands you are typing.
4. B. Explanation: The six virtual consoles that are available on Linux by default are numbered /dev/tty1 through /dev/tty6. The device /dev/pts/6 is used to refer to the sixth pseudo terminal, which is created by opening six terminal windows in a graphical environment.
5. A and C. Explanation: A pseudo terminal device is created when opening new terminals using SSH or from the graphical interface.
6. D. Explanation: Typically, a server reboot is only necessary after making changes to the kernel and kernel modules that are in use. Changing the network configuration does not normally require a reboot, because it is possible to just restart the network service.
7. C. Explanation: Windows has no native support for SSH. You need to install PuTTY or similar software to remotely connect to Linux using SSH.
8. D. Explanation: Key fingerprints of hosts that you have previously connected to are stored in your home directory, in the subdirectory .ssh in a file with the name known_hosts.
9. C. Explanation: The ForwardX11 option in the /etc/ssh/ssh_config file enables support for graphical applications through SSH.

10. C. Explanation: To initiate key-based remote authentication, you should copy the public key to the remote server. The most convenient way to do so is using the **ssh-copy-id** command.

Chapter 6

1. C. Explanation: Privileged users are opposed to unprivileged users. A privileged user can execute tasks in kernel space, without any further restriction. By default, only the user root exists as privileged user.
2. D. Explanation: In the sudo configuration file, all members of the group wheel by default get access to all administrator tasks.
3. B. Explanation: The **runas** command does not exist on Linux.
4. B. Explanation: The hashed user passwords are stored in /etc/shadow.
5. C. Explanation: The file /etc/default/useradd is read for default settings when new user accounts are created.
6. A. Explanation: The **chage** command enables you for managing password properties.
7. B. Explanation: There is no file /etc/.profile.
8. C. Explanation: Security was not a goal in the original design of LDAP, and has to be applied separately.
9. A. Explanation: The system-config-authentication tool was used in RHEL 6 and no longer exists in RHEL7. It has been replaced with authconfig, which comes in a command-line version, a TUI (text user interface) version, and a GTK (graphical) version.
10. D. Explanation: Unprivileged users should be able to set up LDAP authentication, which is why no admin name is needed to configure LDAP login.

Chapter 7

1. C. Explanation: The **newgrp** command is used to set the effective primary group, which will effect default group ownership on new files until the current shell session is ended. The **chgrp** command is used to set the group owner of an existing file. **Chgrp** is not related to any user account and it affects newly created files only.
2. A. Explanation: The **find / -user linda** command searches all files that are owned by user linda. Notice that **find** also has a **-uid** option that allows you to locate files based on a specific UID setting. This does not allow you to search files based on a username, but it will let you find files based on the UID of a specific user.

3. C. Explanation: **chgrp myfile sales** does not set group ownership for the file myfile. The order in this command is wrong; **chgrp** first needs the name of the group, followed by the name of the owner that needs to be set.
4. C. Explanation: When used in relative mode, the three digits are used to specify user, group, and others permissions. The value 6 is used to apply read and write.
5. C. Explanation: The **chmod g+s /dir** command adds (+) the SGID permission to /dir. Answer A (**chmod u+s**) adds SUID to the directory, with **chmod g-s** the SGID permission would be removed, and the 1 in **chmod 1770 /dir** would set sticky bit and not SGID.
6. D. Explanation: ACL support is not offered by default on all file systems. If you get an "operation not supported" error message, make sure to add the **acl mount** option and remount the file system.
7. B. Explanation: Although answers A and B will both set default ACLs, answer B is better because it adds x to the permissions. Without x, members of the group sales will have no way to enter the directory using the **cd** command.
8. A. Explanation: The umask is a systemwide setting and cannot be used to apply to specific directories only. Use a default ACL as shown in answer A to perform this task.
9. C. Explanation: In a umask, 0 in the first position gives all permissions to the file owner. 2 in the second position ensures that members of the group owner can read files, and 7 in the third position takes away all permissions for others.
10. C. Explanation: The **lsattr** command shows current attribute settings to files. The **ls** command is not capable of showing file attributes, and the other commands that are mentioned do not exist.

Chapter 8

1. D. Explanation: Based on the /27 subnet mask, the networks are 192.168.4.0, 192.168.4.64, 192.168.4.128, and 192.168.4.192. That means that IP addresses II, III, and IV belong to the same network.
2. B. Explanation: The 169.254.0.0 network address does not belong to the private address ranges, which are 10.0.0.0/8, 172.168.0.0/12, and 192.168.0.0/16.
3. C. Explanation: By default, the network device names are based on the device type, location, and identification.
4. D. Explanation: Use of the **ifconfig** command is deprecated; use the **ip** command instead. The **ip addr show** command shows information about the state of the interface as well as the current IP address assignment.
5. A. Explanation: The network service should not be used anymore in RHEL 7.

6. B. Explanation: The nmcli-examples man page was created to make working with the long commands in nmcli a bit easier.
7. C. Explanation: On RHEL 7, nmtui is the default utility to set and modify the network interface. Notice that RHEL 7 does not have system-config utilities anymore for configuring networking that were available in earlier versions of RHEL.
8. D. Explanation: When the connection is added, you use **ip4** and **gw4** without a V.
9. A. Explanation: You should not set the DNS servers directly in /etc/resolv.conf, because the /etc/resolv.conf file is automatically written by the NetworkManager service.
10. C. Explanation: The name of the configuration file that contains the hostname is /etc/hostname. Notice that on earlier versions of RHEL the file /etc/sysconfig/network was used for this purpose.

Chapter 9

1. B and D. Explanation: There are two different types of processes that each request a different management approach. These are shell jobs and daemons. A cron job and a thread are subdivisions of these generic categories.
2. B. Explanation: The **Ctrl+Z** command temporarily freezes a current job, after which the **bg** command can be used to resume that job in the background.
3. A. Explanation: The **Ctrl+C** command cancels the current job. **Ctrl+D** sends the EOF character to the current job, which can result in a stop if this allows the job to complete properly. The difference with **Ctrl+C** is that when using **Ctrl+C** the job is canceled with no regard to what it was doing. The **Ctrl+Z** keystroke freezes the job.
4. A and B. Explanation: Individual threads cannot be managed by an administrator. Using threads makes working in a multi-CPU environment more efficient because one process cannot be running on multiple CPUs simultaneously, unless the process is using threads.
5. A. Explanation: The **ps ef** command shows all processes, including the exact command that was used to start them.
6. C. Explanation: To increase process priority, you need a negative nice value. -20 is the lowest value that can be used.
7. C. Explanation: Use the **renice** command to change priority for currently running processes. To refer to the process you want to renice, use the **-p** option.
8. B. Explanation: **mkill** is not a current command to send signals to processes.

9. A. Explanation: The SIGKILL signal sends the famous signal with number 9 to a process, which forces the process to stop.
10. A. Explanation: To change the process priority from top, use **r** for renice.

Chapter 10

1. B. Explanation: KVM virtual machines run directly on top of the KVM hypervisor module and are not depended on the availability of the management program.
2. B. Explanation: The libvirtd process provides the management interface to access KVM virtual machines.
3. A. Explanation: Hardware virtualization support needs to be present in your computer hardware. If it is not you cannot use KVM virtualization. On some computers, the feature is available, but not switched on by default. Switch it on through your computer BIOS setup.
4. C and D. Explanation: Look for the **vmx** flag in /proc/cpuinfo to verify the availability of hardware virtualization support or for the **svm** flag (for AMD cpus). The **lscpu** command shows the hypervisor mode a host is offering, and if used on a virtual machine it shows which type of virtualization platform this machine is used on.
5. A. Explanation: The **modprobe kvm** command loads the KVM kernel module and all its dependencies. Do not use **insmod kvm**; that command will not load the kernel module dependencies as well.
6. C. Explanation: The virtual machine disk files by default are stored in /var/lib/libvirt/images.
7. D. Explanation: Virtual machine configuration files by default are stored in the directory/etc/libvirt/qemu.
8. C. Explanation: Automatic virtual machine startup can be enabled easily using the Virtual Machine Manager Boot options interface.
9. C. Explanation: The **virsh list** command lists all virtual machines. Add **--all** to also show virtual machines that are not currently active.
10. D. Explanation: The **virsh destroy** command is like pulling the power plug. It halts a virtual machine immediately with all the possible bad consequences of that.

Chapter 11

1. D. Explanation: The gpgcheck= line indicates whether to check the integrity of packages in the repository using a GPG key. Although useful, this is not mandatory.
2. B. Explanation: If an RHEL system is not registered with RHEL, no repositories are available.
3. C. Explanation: Use baseurl to specify which URL to use. If the URL is based on the local file system, it uses the URI file:// followed by the path on the local file system, which in this case is /repo, which explains why there are three slashes in the baseurl.
4. D. Explanation: GPG package signing is used to set a checksum on packages, so that altered packages can easily be recognized. The main purpose of signing packages is to make it easy to protect packages on internet repositories. For internal repositories that cannot be accessed by Internet users, the need to add GPG package signatures is less urgent.
5. D. Explanation: Both the commands "**yum provide**s and **yum whatprovides** can be used to search for files within a specific package. The file pattern must be specified as */filename or as a full path, which is why answer D is the only correct answer. Without the */ in front of the file name, you may get a match that is based on the package description, not on the filename.
6. C. Explanation: The **yum list all** command shows installed packages and packages that are available in the repositories. The question was how to show installed packages (not all packages), which is why answer C is the correct answer.
7. D. Explanation: The **yum history** command reads the /var/log/yum.log file and shows recent yum history. In this list, every event is marked with a history number that can be used with the **yum history undo** command.
8. A. Explanation: The **yum install** command installs individually downloaded RPM files while looking for package dependencies in the current repositories. This is better than using **rpm -ivh**, which does not consider the yum repositories. In earlier versions of RHEL, the **yum localinstall** command was used to install packages that were downloaded to the local file system, but this command is now deprecated.
9. C. Explanation: Use the **rpm -qf** command to find which RPM package a specific file comes from.
10. C. Explanation: The **--scripts** option checks whether there are scripts in an RPM package. If you want to query the package file and not the database of installed RPMs, you need to add the **-p** option to the **-q** option, which is used to perform RPM queries.

Chapter 12

1. B. Explanation: The **systemctl** command on RHEL 7 is used to manage services. If used with the status option, the current state of the service is checked, and recent log messages about the service are displayed as well.
2. C. Explanation: The fields in cron timing are minute, hour, day of month, month, and day of week. Answer C matches this pattern to run the task on the seventh day of the week at 11 a.m.
3. A. Explanation: To launch a job from Monday through Friday, you should use **1-5** in the last part of the time indicator. The minute indicator ***/5** will launch the job every 5 minutes.
4. A and D. Explanation: You cannot modify user cron files directly, but have to go through the crontab editor. This editor is started with the **crontab -e command**.
5. B. Explanation: The /etc/cron.d directory is used to store cron files for individual services that need tasks to be executed through cron. This directory is mostly filled by installing RPM files that contain cron jobs.
6. A. Explanation: Although cron jobs that are added to /etc/crontab will be executed, the /etc/crontab file is considered a system file that should not be modified directly.
7. D. Explanation: anacron is a service that takes care of executing jobs on a regular basis where it is not necessary to specify a specific time.
8. D. Explanation: By default, the cron.allow file does not exist. If it exists, a user must be listed in it in order to program cron jobs.
9. B. Explanation: The **Ctrl+D** key sequence sends the end-of-file (EOF) character to the at shell and closes it.
10. C. Explanation: The **atq** command queries the at service and provides an overview of jobs currently scheduled for execution.

Chapter 13

1. C. Explanation: journald is not a replacement of rsyslogd. It is an additional service that logs information to the journal. In RHEL 7, they are integrated to work together to provide you with the logging information you need.
2. D. Explanation: Most messages are written to the /var/log/messages file, but authentication-related messages are written to /var/log/secure.
3. C. Explanation: SELinux events are logged through the audit service, which maintains its log in /var/log/audit/audit.log.
4. A. Explanation: The rsyslogd configuration file is /etc/rsyslog.conf.

5. D. Explanation: The /etc/sysconfig/rsyslog file is the default location to change rsyslogd startup parameters.
6. C. Explanation: Rsyslogd destinations often are files. For further processing, however, log information can be sent to an rsyslogd module. If this is the case, the name of the module is referred to as :modulename:.
7. D. Explanation: The local facilities local0 through local7 can be used to configure services that do not use rsyslog by default to send messages to a specific rsyslog destination, which needs to be further configured in the rsyslog.conf file.
8. A. Explanation: Logrotate can rotate files based on the maximal file size. To configure this, the recommended way is to drop a file in /etc/logrotate.d containing parameters for this specific file.
9. D. Explanation: The journal is stored in /run/log/journal.
10. A. Explanation: To make the journald journal persistent, you have to create a directory /var/log/journal and set the appropriate permissions to that directory.

Chapter 14

1. A. Explanation: In GPT, there is no longer a need to differentiate between primary, extended, and logical partitions; in fact, it is not even possible. Using logical partitions is not an advantage due to the limited number of primary partitions available on MBR disks.
2. B. Explanation: 1 pebibyte (PiB) is 1024 x 1024 x 1024 x 1024 x 1024 bytes.
3. C. Explanation: Partition type 83 is normally used to create Linux partitions.
4. C. Explanation: KVM virtual machines use the virtio driver to address hard disks. This driver generates the device /dev/vda as the first disk device.
5. C. Explanation: A disk can have one partition table only. For that reason, it is not possible to have MBR and GPT partitions on the same disk.
6. B. Explanation: XFS is used as the default file system; partitions can still be formatted with other file systems, like Ext4.
7. D. Explanation: The **blkid** command shows all file systems, their UUID, and if applicable, their label also.
8. D. Explanation: To mount a file system based on its UUID, use UUID=nnnn in the /etc/fstab device column.
9. B and D. Explanation: To check a file system upon boot, but only after the root file system has been checked successfully, put a 2 in the sixth column in /etc/fstab.

10. B. Explanation: The **_netdev** mount option is used to specify that the file system depends on the network to be present before it can be mounted.

Chapter 15

1. B. Explanation: It is common to create a file system on top of a logical volume, but this is not a requirement. For instance, a logical volume can be used as a device that is presented as a disk device for a virtual machine.
2. C. Explanation: Copy on write is a feature that is offered by modern file systems, such as Btrfs. It copies the original blocks a file was using before creating a new file, which allows users to easily revert to a previous state of the file. Copy on write is not an LVM feature.
3. D. Explanation: On GPT disk, LVM partitions must be flagged with the partition type 8e00.
4. C. Explanation: The **lvcreate** command is used to create logical volumes. Use **-n name** to specify the name. The **option -l 50%FREE** will assign 50% of available disk space, and **vgdata** is the volume group it will be assigned from.
5. B and C. Explanation: The **pvdisplay** command is used to show extensive information about physical volumes. The **pvs** command shows a summary of essential physical volume properties only.
6. A and B. Explanation: When marking a partition as a physical volume, it should be flagged with partition type 8e / 8e00. Raw disks can be used as physical volumes also. A physical volume is not dependent on any file system, and any storage device can be used as a physical volume, including LUNs on a SAN.
7. C. Explanation: The **vgcreate** command is followed by the name of the volume group you want to create, after which you need to specify the complete device name of the device you want to add to the volume group.
8. B. Explanation: The extent size is set on the volume group, not on the physical volume or the logical volume.
9. A Explanation: In LVM naming, three different types of volume names can be used. /dev/vgdata-lvdata is not one of them.
10. B. Explanation: The **lvresize** command can be used with two arguments to specify size. To add a specific amount of disk space, use **-L**, followed by a **+** and next specify how much disk space to add. The **-r** option resizes the file system that is used on top of the logical volume.

Chapter 16

1. A. Explanation: A tainted kernel is caused by drivers that are not available as open source drivers. Using these may have impact on the stability of the Linux operating system, which is why it is good to have an option to recognize them easily.
2. B. Explanation: The dmesg utility shows the contents of the kernel ring buffer. This is the area of memory where the Linux kernel logs information to and gives a clear overview of recent kernel events.
3. A. Explanation: The **uname -r** command shows the current kernel version. The **uname -v** command gives information about the hardware in your computer, and the **procinfo** command does not exist.
4. C. Explanation: The /etc/redhat-release version contains information about the current version of RHEL you are using, including the update level.
5. A. Explanation: On a systemd-based operating system such as RHEL 7, the systemd-udevd process takes care of initializing new hardware devices.
6. B. Explanation: Default rules for hardware initialization are in the directory /usr/lib/udev/rules.d; custom rules should be stored in /etc/udev/rules.d.
7. C. Explanation: The **modprobe** command is the only command that should be used for managing kernel modules, as it considers kernel module dependencies as well. Use **modprobe** to load a kernel module and **modprobe -r** to unload it from memory.
8. C. Explanation: The **lspci -k** command lists devices that are detected on the PCI bus and supporting kernel modules that have been loaded for those devices. Alternatively, **lspci -v** shows more verbose information about modules that are currently loaded.
9. C. Explanation: The files /etc/modules.conf and modprobe.conf were used for this purpose in the past. On RHEL 7, kernel module parameters are passed through /usr/lib/modprobe.d if it is for operating system managed permanent parameters. The /etc/modprobe.d directory is used for files that create custom configurations.
10. C and D. Explanation: Kernels are not updated, they are installed, and you can use either yum update kernel or yum install kernel to do so. There are no additional requirements, which makes Answers C and D both false.

Chapter 17

1. A. Explanation: The httpd package contains the core components of the Apache web server. It can be installed using **yum install httpd**.
2. A. Explanation: The default Apache configuration file is in /etc/httpd/conf/httpd.conf.
3. C. Explanation: The **DocumentRoot** parameter specifies where the Apache web server will look for its contents.
4. A. Explanation: The **ServerRoot** parameter defines where Apache will look for its configuration files. All file references in the httpd.conf configuration file are relative to this directory.
5. B. Explanation: The /etc/http/conf directory contains the main Apache configuration file httpd.conf.
6. D. Explanation: The /etc/httpd/modules.d directory contains configuration files that are used by specific Apache modules.
7. C. Explanation: The /etc/httpd/conf.d directory is used by RPMs that can drop files in that directory without changing the contents of the main Apache configuration file.
8. A. Explanation: The NameBased virtual host is used as the default virtual host type. It allows multiple virtual hosts to be hosted on the same IP address.
9. A. Explanation: The **VirtualHost** parameter is used to open a virtual host definition. * refers to all IP addresses, and :80 defines the port it should listen on.
10. C. Explanation: No additional packages need to be installed to enable virtual hosts. Virtual hosts are supported through the default httpd RPM package.

Chapter 18

1. A. Explanation: The **--type=service** argument shows all currently loaded services only.
2. C. Explanation: Wants are specific to a particular system and for that reason are managed through /etc/systemd/system.
3. D. Explanation: Masking a service makes it impossible to enable it.
4. D. Explanation: Running(dead) is not a valid status for systemd services.
5. A. Explanation: The required statement is **AllowIsolate**. All other statements mentioned here are invalid.
6. B. Explanation :udev is not a valid systemd unit type. All others are.

7. B. Explanation: Answers A and B are very similar, but answer A uses the wrong command. You have to use the **systemctl** command, not the **systemd** command.
8. D. Explanation: Changes to GRUB 2 need to be applied to /etc/default/grub, not to /boot/grub2/grub.cfg. The /boot/grub2/grub.cfg file cannot be edited directly, you'll have to apply changes to /etc/default/grub and run the **grub2-mkconfi**g command to write them to the appropriate configuration file.
9. B. Explanation: The **grub2-mkconfig** command enables you to regenerate the GRUB 2 configuration. The result, by default, is echoed to the screen. Use redirection to write it to a file.
10. A. Explanation: The word order is wrong. It should be **systemctl start unit**, not **systemctl unit start**.

Chapter 19

1. C. Explanation: During the boot procedure, the GRUB 2 boot loader gets loaded first. From here, the kernel with the associated initramfs are loaded, and once that has completed, systemd can be loaded.
2. B. Explanation: The **Ctrl+X** key sequence leaves the GRUB 2 shell and continues booting.
3. B. Explanation: The /etc/dracut.conf file is used for managing the initramfs file system.
4. D. Explanation: The **rd.break** boot option enters at the end of the initrd phase. The root file system has not been mounted on / yet, which allows for easy troubleshooting.
5. A and C. Explanation: The **rhgb** and **quiet** boot options make it impossible to see what is happening while booting.
6. B. Explanation: The emergency.target systemd target gives just a root shell and not much more than that. All other options that are mentioned also include the loading of several systemd unit files.
7. C. Explanation: If you do not get a GRUB 2 boot prompt, you cannot select any alternate startup mechanism. This is why his situation requires you to use a rescue disk so that GRUB can be reinstalled. If the kernel or initramfs cannot load successfully, you might need to use a rescue disk also, but in many cases an alternate kernel is provided by default.
8. C. Explanation: The **mount -o remount,rw /** option remounts the / file system in read/write mode.
9. A. Explanation: Because the error occurs before the GRUB 2 menu is loaded, the only option to fix this is by using a rescue disk.

10. C. Explanation: The **kpartx** command is used to create device nodes for devices that are found in a block device. The **-a** option adds device nodes for all devices, and the **-v** option does that in a verbose way.

Chapter 20

1. B. Explanation: CIFS is not supported as an installation server.
2. A and B. Explanation: If you do not want to boot from the network, you need to provide a boot image on a local medium. The boot.iso image is a perfect solution to do that. Alternatively, you could choose to start the installation from an installation disk.
3. D. Explanation: The tftpd service is started through xinetd. Make sure that the xinetd service is enabled for automatic starting using **systemctl enable xinetd**. The further configuration is done through the /etc/xinetd.d/tftp configuration file, where you have to change the disabled parameter to enabled.
4. C. Explanation: The DHCP server communicates to the TFTP server and specifies which file from the TFTP server should be handed out for booting installable clients.
5. B. Explanation: The TFTP server is defined through xinetd. Xinetd works with configuration files in /etc/xinetd.d. Each service that is managed through xinetd has its own configuration file.
6. A. Explanation: The syslinux package contains everything that is needed to provide a boot menu through PXE.
7. B. Explanation: To use a Kickstart file while installing, use the **ks=** boot argument, followed by the location of the Kickstart file (which is typically on an installation server).
8. C. Explanation: The /root/anaconda-ks.cfg file is created while installing an RHEL server and can be used as a Kickstart file to install other servers.
9. B. Explanation: The system-config-kickstart file is used to create Kickstart files manually. Notice that this is one of the few system-config utilities that still remains from a past where many system-config utilities were available to make configuration tasks easier.
10. D. Explanation: The system-config-kickstart utility is old and has not been updated for a long time, which is why all of the above cannot be configured using system-config-kickstart.

Chapter 21

1. D. Explanation: Enabled is not a valid mode that can be set using **setenforce** or the /etc/sysconfig/selinux configuration file.

2. A. Explanation: The **getenforce** command is used to request the current SELinux mode.
3. A. Explanation: For basic SELinux configuration, you need to make sure that the appropriate context type is set. User and role are for advanced use only.
4. D. Explanation: SELinux security can be applied to users, files and ports.
5. C. Explanation: The **-Z** option displays SELinux-related information and can be used with many commands.
6. D. Explanation: **chcon** should be avoided at all times. Answer D is the only answer that provides correct usage information about **semanage**.
7. B. Explanation: When moving a file, the original file context it moved with the file. To ensure that the file has the context that is appropriate for the new file location, you should use **restorecon** on the file.
8. B. Explanation: To change Booleans, use **setsebool**; to make the change persistent, use **-P**.
9. A. Explanation: SELinux messages are logged by auditd, which writes the log messages to /var/log/audit/audit.log
10. D. Explanation: SELinux log messages always contain the text *avc*.

Chapter 22

1. A. Explanation: On a default configuration, there is no untrusted zone in firewalld.
2. C. Explanation: Netfilter is the name of the firewall implementation in the Linux kernel. Different toolsets exist to manage netfilter firewalls. Iptables has been the default management interface for a long time, and in Red Hat Enterprise Linux 7, firewalld has been added as an alternative solution to manage firewalls.
3. D. Explanation: Firewalld and iptables are mutually exclusive.
4. C. Explanation: The **firewall-cmd --get-services** command shows all services that are available in firewalld.
5. C. Explanation: The name of the GUI tool that can be used to manage firewall configurations is firewall-config.
6. A. Explanation: Answer A shows the correct syntax.
7. A. Explanation: The trusted zone is provided for interfaces that need minimal protection.

8. D. Explanation: Configuration that is added with the **--permanent** option is not activated immediately and needs either a restart of the firewalld service or the command **firewall-cmd --reload**.
9. B. Explanation: The **--list-all** command without further options shows all configurations for all zones.
10. A. Explanation: When working with firewall-config, you need to choose between the run-time and the permanent mode.

Chapter 23

1. B. Explanation: In the default configuration, NFS share access is based on UID matching between the client and server. To enable anonymous user access, you need to specify the **sec=none** mount option.
2. D. Explanation: You do not have to enable the Kerberos service on the client to configure a Kerberos-enabled NFS mount. The Kerberos service should be enabled on the NFS server.
3. B. Explanation: The **krb5i** mount option guarantees that the message has not been tampered with but does not add encryption.
4. D. Explanation: Showmount is using the NFS portmapper, which is using random UDP ports to make the connection. Portmapper traffic is not automatically allowed when the nfs service is added to the firewall because RPC ports that are needed by showmount are blocked by the firewall.
5. A. Explanation: To authenticate to a Samba share, you need to use the **-o username=sambauser** option to specify the username.
6. D. Explanation: To avoid having to put a username and password in clear text in the /etc/fstab file, you can use a credentials file.
7. D. Explanation: You do not have to set any permissions on the local file system for automount to be effective.
8. B. Explanation: Automount mounts are not performed by a user but by the autofs service.
9. C. Explanation: There is no need to create an FTP anonymous user; the FTP user is used for this purpose by default.
10. A. Explanation: An SMB share is mounted with the **cifs fstype** option. The name of the server and share should start with a colon, as is the case for all devices that are mounted through automount of which the name starts with a /.

Chapter 24

1. C. Explanation: When booting, a server reads the hardware time and sets the local time according to hardware time.
2. D. Explanation: Hardware time on Linux servers typically is set to UTC, but local administrators may chose to make an exception to that general habit.
3. D. Explanation: The **timedatectl** command has been introduced as a new solution in RHEL 7 that allows you to manage many aspects of time.
4. C. Explanation: Atomic clocks can be used as a very accurate alternative to the normal hardware clock.
5. D. Explanation: The /etc/chrony.conf file.
6. C. Explanation: The **-s** option is used to set the current time, and to do so, military time format is the default.
7. A. Explanation: To translate epoch time into human time, you need to put an @ in front of the epoch time string.
8. C. Explanation: The **hwclock -c** command opens an interface that is refreshed every 10 seconds and shows the current hardware time, system time, and the difference between the two of them.
9. D. Explanation: When used without arguments, **timedatectl** gives a complete overview of current time settings on your server.
10. D. Explanation: The graphical tool to manage time can be accessed directly from the graphical desktop but also by running the system-config-date utility from the command line.

Chapter 25

1. B. Explanation: One of the essential things in Kerberos is that at no time passwords are sent over the network.
2. B. Explanation: The DNS name is not a part of a principal name. Instead of a DNS name, the instance part is used. This can be a DNS name, but it can also be another type of identifier for the host.
3. A. Explanation: Kerberos passwords are stored in the keytab file. This file uses the default name /etc/krb5.keytab.
4. D. Explanation: Kerberos is an authentication service, which is used on top of account information services such as LDAP to guarantee secure authentication.
5. C. Explanation: NIS is a legacy service used for managing identities and authorization, and is not used much anymore on current Linux versions.

6. C. Explanation: The /etc/sysconfig/authconfig file contains information about the authentication backend service that should be used.
7. D. Explanation: The LDAP client looks for the CA certificate in the /etc/openldap/cacerts file.
8. C. Explanation: USEPAMACCESS specifies that PAM should be used for authentication. It is not related to the authentication backend that is used.
9. D. Explanation: Systems that do not use sssd for authentication normally use the nslcd service to authenticate.
10. C. Explanation: You can use the **realm** command to join an Active Directory domain. It relies on the realmd service, which in current state is still in an early development stage.

Chapter 26

1. C. Explanation: Special file systems like GFS2 ensure that multiple nodes can access SAN storage simultaneously, because they'll synchronize cache between nodes.
2. D. Explanation: The iSCSI target can be configured to share any storage device.
3. C. Explanation: In a resilient SAN topology, you need to make sure that networking is set up in a redundant way. The multipath driver helps doing that.
4. A. Explanation: The LUN is the iSCSI configuration that is created for the backend storage device that makes sure the device can be shared through the iSCSI target process.
5. C. Explanation: The targetcli utility is used to configure the LIO iSCSI target.
6. C. Explanation: Before configuring anything, you need to make sure the backend storage is available.
7. C. Explanation: The iSCSI target by default is listening on port 3260.
8. C. Explanation: The initiatorname is stored in the file /etc/iscsi/initiatorname.iscsi.
9. A. Explanation: iSCSI discovery is a mandatory process that ensures that the iSCSI target name is stored locally.
10. A. Explanation: To get details about each of the iSCSI modes, the **-P** option can be used. A higher number as an argument to **-P** gives more detail. Session details are requested in the session mode, which has 3 as the highest detail level.

Chapter 27

1. B. Explanation: The us number indicates the percentage of time the CPUs spend handling processes in user space.
2. D. Explanation: To show one line for each CPU (core) in top, press 1 from the top interface.
3. C. Explanation: Cache is used for memory optimization. If the memory currently used for cache is needed for other purposes, the cache memory is automatically liberated.
4. A. Explanation: From a running top, press f to show fields that can be selected for display.
5. C. Explanation: The W key is used to write current top settings to the top configuration file.
6. D. Explanation: The pidstat utility shows detailed performance statistics for specific processes.
7. C. Explanation: The option **-d** is used for device usage statistics only. The numeric arguments are used to first specify the interval and next the number of polling loops.
8. D. Explanation: The vmstat utility gives detailed memory usage information, which includes information about the number of blocks being moved between RAM and swap space.
9. C. Explanation: The **sar** command works on data that has been collected in the /var/log/sa directory. If the sysstat package has just been installed, there will not be any data yet to show results.
10. C. Explanation: Startup parameters for the sysstat processes sa1 and sa2 are set in /etc/sysconfig/sysstat.

Chapter 28

1. B. Explanation: It is not a good idea to focus on one tool only while analyzing performance parameters. The tool you are using might be outdated and showing wrong information. So, you better try gathering performance parameters with as many tools as possible (or get the performance information directly from /proc).
2. C. Explanation: The /proc/sys directory contains tunable settings. In this directory, the ipv4/ip_forward file is used to enable packet forwarding. Make sure that this file contains a 1 if you want your server to be able to forward packets between interfaces.

3. B. Explanation: The /proc/sys/vm directory contains memory tunables. VM in the directory stands for virtual memory.
4. A. Explanation: The /proc/meminfo file contains detailed information about current system memory usage. The /proc/memory file does not exist. /proc/iomem has information specifically about io related memory, and /proc/kcore is the raw memory image that the kernel is using.
5. B. Explanation: Answer A blocks all ICMP packets, not just ping. Answers C and D do not refer to valid filenames in /proc.
6. D. Explanation: Swap handling is related to memory management and for that reason can be found in /proc/sys/vm. The correct filename is swappiness.
7. A and C. Explanation: The /etc/sysctl.d is the preferred location for applying changes to the sysctl configuration. You should not make modifications to /usr/lib/sysctl.d, which is for. Answer A is deprecated, but also works.
8. B. Explanation: The **sysctl -a** command prints all current **sysctl** settings. This command is very useful in combination with grep to find the correct settings.
9. A. Explanation: The **sysctl -p** command reads the sysctl configuration and applies changes to the runtime configuration.
10. A. Explanation: The **sysctl -w** command writes a new value to a sysctl parameter without updating the configuration files (which makes it of limited use).

Chapter 29

1. D. Explanation: There are no specific modules for rsyslog that are used to connect rsyslog to firewalling.
2. D. Explanation: The **InputFileSeverity** parameter is used to specify which severity should be used.
3. B. Explanation: The imfile module is used to have rsyslogd process messages that are written to files.
4. A. Explanation: The first argument when addressing the mysql output module is the name of the server that runs the database.
5. B. Explanation: The imjournal rsyslog module is now the preferred module to use for reception of logging information from journald in rsyslogd.
6. C. Explanation: The /etc/systemd/journald.conf file contains several parameters, including **ForwardToSyslog**, which can be used to switch off the feature that forwards messages to rsyslogd.
7. A. Explanation: Even if a remote log server is used, a local rsyslogd process is still required to forward messages to the remote log server.

8. A. Explanation: To configure remote logging, port 514 is used. Either a TCP or a UDP port can be configured.
9. C. Explanation: Old syslog implementations support sending messages to a log server only over port 514 UDP.
10. B. Explanation: The **InputTCPServerRun** allows messages to be accepted through TCP. This statement needs to start with a $ and have the port name as its argument.

Chapter 30

1. A. Explanation: The roundrobin, loadbalance, and the lacp runners all load balance workload between the interfaces that are involved. Of these three, the roundrobin runner is the most simple runner that does not need any additional support on the hardware that is involved.
2. B. Explanation: The graphical NetworkManager applet offers no support for configuring teaming. nmcli and nmtui do offer this support and write the configuration to the /etc/sysconfig/network-scripts directory.
3. A. Explanation: The IP configuration in a teaming environment is set in the team configuration.
4. C. Explanation: No specific configuration file defines the interface that is used on a specific device. The ifcfg-team-slave configuration file is used for that purpose.
5. A. Explanation: By starting the team interface, port interfaces are *not* automatically started.
6. B. Explanation: In a link-local address, the network prefix fe80/64 is used, which is followed by the MAC address with fffe inserted in the middle of the MAC address.
7. C. Explanation: The ff02::1 IPv6 address is the all nodes IPv6 address. Use %eth0 to specify that the network connected to interface eth0 must be addressed.
8. C and D. Explanation: When adding new configuration to an interface, **ip6**, **gw6**, **ip4,** and **gw4** should be used. When modifying existing configuration, use **ipv6**, **ipv4**, **gwv6**, and **gwv4**.
9. D. Explanation: The first argument to nmcli is **con**, to refer to the connection that should be modified. This is followed by the action that is performed on that interface (in this case, **mod**, to modify the interface configuration). Then the name of the interface follows, which is followed by **ipv6.method** that needs to be set to **manual**.

10. B. Explanation: The **/proc/sys/net/ipv4/ip_forward** parameter is set to 1 to enable packet forwarding on RHEL 7.

Chapter 31

1. B. Explanation: The first line of a bash shell script contains the shebang. This defines the subshell that should be used for executing the script code.
2. A. Explanation: The **exit 0** statement at the end of a script is an optional statement to inform the parent shell that the script code was executed successfully. It is optional.
3. C. Explanation: The **read** statement stops a script, which allows a user to provide input. If **read** is used with a variable name as its argument, the user input is stored in this variable.
4. D. Explanation: The first argument is referred to as $1. To store $1 in a variable with the name NAME, use the command **NAME=$1**. Make sure that no spaces are included. In Answer A, for instance, the name of the variable that is defined is **"NAME "** and not **"NAME"**.
5. D. Explanation: Both $@ as $* can be used to refer to all arguments that were provided when starting a script. $@ is the preferred method though, because it enables the script to distinguish between the different individual arguments, where $* refers to all the provided arguments as one entity.
6. D. Explanation: A conditional loop that is started with **if** is closed with **fi**.
7. C. Explanation: If within an **if** loop a new conditional check is opened, this conditional check is started with **elif**.
8. B. Explanation: After stating the condition in a for loop, **do** is used to start the commands that need to be started when the condition is true.
9. D. Explanation: The **mail** command needs its subject specified with the **-s** option. The **mail** command normally waits until a dot is entered on an empty line to start sending the message. This dot can be fed to the mail command using STDIN redirection, using < .
10. A. Explanation: In a **case** statement, the different options are proposed with a) behind them. *) refers to all other options (not specifically specified in the script).

Chapter 32

1. A. Explanation: The iptables, ebtables, and ip6tables services should be disabled when running firewalld. For firewalld compatibility, there is no reason to disable the network service as well.

2. C. Explanation: Custom port allocations can be created by modifying service files; all other features listed can be configured only by using rich rules.
3. A. Explanation: Direct rules go before anything else, and then port forwarding/masquerading, logging, allow, and deny rules are processed.
4. C. Explanation: Examples of firewalld rich rules are in man 5 firewalld.richlanguage.
5. A. Explanation: Answer A shows correct syntax. To create a rich rule, always use **ipv4** and not **ip4**, always use **rule family**, and do not forget **address=** if you want to refer to an address.
6. A. Explanation: Answer A shows the correct syntax.
7. C. Explanation: If port forwarding to another host is configured, the return packets must be taken care of by using masquerading.
8. A. Explanation: Answer A is the only answer that does not contain errors.
9. A. Explanation: Masquerading can be used only on a router.
10. C. Explanation: Custom firewalld service files should be stored in /etc/firewalld/services.

Chapter 33

1. C. Explanation: The .htaccess file can be used to specify directory access. This is a convenient way to configure access restrictions on directories, but it does have a relatively high performance price.
2. D. Explanation: The Options Indexes directive shows a list of files in a directory where no index.html file exists. Notice that from a security perspective this is better avoided. All other answers refer to nonexisting options.
3. B. Explanation: The /etc/httpd/modules.conf.d directory is used for snap-in configuration files that come from Apache modules. The /etc/httpd/conf.d directory contains generic Apache configuration files, and the other two files are not used by Apache web servers.
4. C. Explanation: The hpptd_unified Boolean applies, when set to off, default security restrictions that make Apache more secure.
5. A and B. Explanation: The genkey and the openssl utilities can be used to create a public key certificate. Because openssl is difficult because of its many command-line utilities, it is recommended to use the genkey utility.
6. B. Explanation: The default location where the private key is stored is in /etc/pki/tls/private. Of course, it is up to the discretion of the system administrator to store this key in another location.

7. A. Explanation: After installing the mod_tls package that contains all that is needed for setting up a TLS secured host, the SSLEngine is already set to on. The other parameters mentioned here must be changed to match the server configuration.
8. A and D. Explanation: Using mod_php or running the script as a CGI script are both valid solutions. Answers A and D will not work.
9. A. Explanation: To access a local database, no additional configuration is required. To allow Apache to access remote databases, you may have to set both the httpd_can_network_connect_db as the httpd_can_network_connect Booleans.
10. B. Explanation: The **htpasswd** command is used for adding Apache users to a server. The **-c** option is required once only. It creates the authentication file and adds the user to it. Do *not* use it while adding additional users, because it will overwrite the old configuration file!

Chapter 34

1. A. Explanation: To do DNS lookups, only one DNS server needs to be contacted. Only if the first DNS name server is not available is the next DNS name server contacted.
2. C. Explanation: Resource records are not bound to a specific DNS name server.
3. B. Explanation: The PTR (pointer) resource record is used to match an IP address to a host name. PTR resource records can be used for IPv4 and IPv6.
4. C. Explanation: Unreal is a game, not a DNS caching-name server.
5. B. Explanation: The **unbound-checkconf** command enables you to check for errors in the unbound configuration file.
6. B. Explanation: The **trust-anchor** parameter is used for specific DNS domains that have been configured with DNSSEC but which cannot be verified all the way back to the root domain. The **interface** and **access-control** parameters must be changed because otherwise no connections will be accepted. It is highly recommended to configure a **forward-zone** also.
7. A. Explanation: The **domain-insecure** parameter is used to specify the name of a domain that is not configured with DNSSEC security settings.
8. A. Explanation: The command to use the DNSKEY to be used as the trust anchor in unbound.conf is **dig +dnssec DNSKEY example.com**.
9. D. Explanation: The **unbound-control dump_cache** command dumps the current contents of the unbound cache to a file.

10. C. Explanation: Dig shows the NXDOMAIN in the answer section when the requested DNS name cannot be found.

Chapter 35

1. C. Explanation: The **mysql_secure_installation** command goes through a few steps to set up basic security settings.
2. A. Explanation: By default, MariaDB listens on the loopback address only. Set the bind address to :: to enable MariaDB on IPv4 as well as on IPv6.
3. C. Explanation: The default administrative user for mysql is root; use **-p** to prompt for a password.
4. A. Explanation: The **describe users;** command gives information about information currently stored in the users table.
5. C. Explanation: Commands need to be closed with a semicolon. All values that need to be inserted in tables need to be put between single quotes.
6. A. Explanation: Read this command as "select all records from the user table where the name field contains the value johnson."
7. D. Explanation: To create something, you need to tell what you want to create, hence **create user**. You then need to specify where you want to create the user, hence **lisa@localhost**. Last, you need to set the password using **identified by 'password';**. In this last part, it is important to put the password between single quotes and to close the command with a semicolon.
8. B. Explanation: A physical backup is just a backup of database files. It does not perform any queries on the database.
9. D. Explanation: To make a backup, you need to authenticate as user root and have MariaDB prompt for a password. You then specify the name of the database you want to back up. You need **--databases** to make clear what it needs to back up and you need to redirect the output to a specific file.
10. A. Explanation: To create a snapshot, you need to specify the options **-s** for snapshot and **-L** to specify the size. You also need a complete path reference to the original logical volume. Specifying a name for the snapshot is optional, but if you want to do it, you have to use **-n** followed by the name you want to use.

Chapter 36

1. C. Explanation: To configure a Kerberized NFS setup, you need to get Kerberos credentials for the NFSv4 server, which is accomplished by providing a keytab file. The second step is that the user needs to get Kerberos credentials as well.

2. A. Explanation: In Kerberos, servers need to authenticate against the Kerberos server. If users want to authenticate, they send a username and password. The alternative for a user to do the same is to use a keytab file that contains the server credentials. The client that needs to access the Kerberized NFS share needs to do this by using a keytab that is specific for the host on which they are and needs to get credentials for the user as well, which means that the user authentication procedure has to be Kerberized as well.
3. C. Explanation: The /etc/exports file is the default file where NFS shares are created. Alternatively, on RHEL 7, you can create snap-in files that define the export settings and put these files in the directory /etc/exports.d.
4. B. Explanation: There is no default security setting; it needs to be configured using the appropriate options in the export.
5. A. Explanation: Port 2049 gives access to the NFS server. It does not allow old utilities such as showmount, which use RPC calls, to traverse the firewall. To allow them, you need to add the mountd as well as the rpc-bind services to the firewall also, which open ports 111 and 20048 also.
6. C. Explanation: The **showmount** command uses RPC calls, and for these to be successful, ports 2049, 111, and 20048 need to be allowed through the firewall. It is a common mistake that these ports have not been enabled, which will cause **showmount** to fail. In that case, to test the availability of the export, it is easiest to just mount the export.
7. D. Explanation: For anything on RHEL 7 where the most secure solution is needed, use SELinux. The **nfs_export_all_rw** Boolean will shut off all read/write access to NFS shares.
8. C. Explanation: In NFS 4.2, the client respects SELinux settings on the server.
9. B. Explanation: On earlier versions of RHEL, the **_netdev mount** option needed to be used to mount remote file systems from /etc/fstab. In RHEL 7, this is no longer a requirement because of the event-driven nature of systemd. You need to make sure that the remote-fs.target is enabled on the client, though.
10. D. Explanation: Any service that uses Kerberos for added security needs access to a keytab file. The name of this file by default is /etc/krb5.keytab, and it contains credentials for the local server and all Kerberized services that are running on that server. These credentials are required; without them, the service cannot get the mandatory Kerberos ticket.

Chapter 37

1. B. Explanation: To install a Samba server, install the samba package. The cifs-utils and samba-client RPMs contain client functionality.

2. D. Explanation: The **workgroup** setting is used to specify the name of the workgroup and the domain name.
3. B. Explanation: If the **writable** parameter is used, users who have write access to the Linux file system will be able to write files. If the write list parameter is set, users listed will have write access, even if writable is not set to yes. This works only if the users also have write access on the Linux file system.
4. C. Explanation: By default, all users have browse access to the share and further access is based on Linux permissions. To limit which users can access a share, use the valid users parameter.
5. B. Explanation: By default, RHEL 7 Samba uses user-based security.
6. A. Explanation: When using smbpasswd without further arguments, the current Samba password for an existing user will be changed. Use **-a** to add a new user account.
7. A. Explanation: When you use **samba_share_t**, the Samba service automatically has read access and write access to the share.
8. C. Explanation: The **use_samba_home_dirs** Boolean is used to use Samba home directories on remote servers.
9. B. Explanation: The **smbclient -L** command lists Samba shares that are available on a Samba server.
10. C. Explanation: **cifscreds** is the command that Samba users use for accessing a Samba multiuser share and is not used as a **mount** option.

Chapter 38

1. A. Explanation: The **inet_interfaces** parameter specifies the IP addresses on the local host where Postfix should offer its services.
2. B. Explanation: The **relayhost** parameter is used to specify which host should be used as a relay host. If you use this parameter, the Postfix process on your server will not address other mail servers directly.
3. C. Explanation: The message transfer agent (MTA) uses SMTP to find the mail server that is responsible for message reception of the addressed recipient.
4. D. Explanation: The /etc/postfix/main.cf file contains most of the Postfix parameters.
5. C. Explanation: Postfix is a collection of different processes that are each dedicated to a specific task. The Postfix process is not part of these. The name sendmail is a historic thing caused by Postfix trying to be compatible with the then-popular sendmail MTA.

6. C. Explanation: The **postqueue -f** command flushes all messages in the queue. This means that all messages currently waiting in the queue will be sent immediately.
7. B. Explanation: The /var/log/maillog file is used as the default destination to log messages about success and failure of email delivery. This is a default setting in the rsyslog configuration.
8. B. Explanation: The **postconf -e** command enables you to change values in the Postfix configuration. Do not forget to reload the Postfix service after doing this to make the changes effective!
9. C. Explanation: On the receiving mail server, the mail server needs to know which domains it should receive messages for. To do this, set the **mydestination** parameter to include at least the current domain.
10. A. Explanation: The **mail** command needs a dot at the end of the command to indicate that the end of the message has been reached. In Answer A, this dot is fed into the system by using input redirection.

Chapter 39

1. A. Explanation: Disabling X11 forwarding is a useful option to prevent remote users from using potentially vulnerable graphical applications remotely, but it does not help against brute-force attacks.
2. C. Explanation: The **AllowUsers** parameter is used to limit SSH server access to specific users only. The names of these users are provided as a space separated list.
3. D. Explanation: The **semanage port** command is used to change SELinux context labels on port. Use **-a** to add a new port, and use **-t ssh_port_t** to set the **ssh_port_t** type. The port itself is specified using **-p tcp 2022**.
4. B. Explanation: Blocking access to a user account in an SSH environment leads to a denial of service situation. This option starts logging failed attempts after reaching half of the number that is specified here.
5. D. Explanation: SSH failed login attempts are logged to the syslog AUTHPRIV facility. This facility by default is configured to send information about failed attempts to the /var/log/secure file.
6. C. Explanation: The UseDNS option looks up the IP address of incoming client connections so that a hostname verification can be done. In test environments, where DNS is not always set up, this might significantly slow down the authentication procedure, and for that reason, this option should be switched off in test environments.

7. D. Explanation: The UseDNS option may speed up creating the connection, but it does not help in keeping the connection alive. The other three options mentioned do.
8. B. Explanation: The optional ~/.ssh/config file is used to set connection options for individual clients. The /etc/ssh/ssh_config is used to set options for all clients.
9. C. Explanation: The **ssh-agent /bin/bash** command starts the ssh-agent, which takes care of caching passphrases. After starting ssh-agent, you need to add the passphrase using **ssh-add**. You must repeat this procedure each time a new session is created.
10. A. Explanation: The command needs to be specified as follows: **LocalPort:localhost:remotePort root@remoteServer**.

Chapter 40

1. B and D. Explanation: In Kerberos, authentication tickets are handed out. These authentication tickets depend on time being correctly synchronized, and only a limited difference between clocks is accepted. The same is true for database synchronization.
2. B. Explanation: IPA uses an integrated ntpd time server. chronyd normally is the default service on RHEL. Answers A and C are incorrect because **timedatectl** and **hwclock** are commands to manage time, not services.
3. D. Explanation: chronyd is the default service to synchronize time on RHEL 7.
4. B. Explanation: A server that has established successful synchronization with an Internet time server typically would show a low stratum, somewhere between 2 and 5. Not 1, because that is for servers that are directly connected to a very reliable clock. Not 7, because that means there are many other servers between this server and the time source. Not 10, because that is the default stratum for a server that uses its local clock for synchronization.
5. D. Explanation: The name of the chrony configuration file is /etc/chrony.conf.
6. D. Explanation: The **local stratum 10** statement can be enabled in /etc/chrony.conf to enable synchronization with the local reference clock. Notice that this line does not need to include the word *server*.
7. A. Explanation: The clock that chrony currently is synchronized with is indicated with a # is used for a source to which connectivity has been list, + is another acceptable source, and x is used for an unreliable clock.
8. D. Explanation: The **chronyc sources** command shows which servers chrony currently is using to synchronize with.

9. C. Explanation: The **chronyc tracking** command shows detailed information about the current system time and how it differs from the time that is offered by the time sources.
10. B. Explanation: The **chronyc sourcestat** command gives detailed information about drift rate and offset of the time sources that currently are used.

Answers to the "Review Questions"

Chapter 1

1. CentOS
2. 32-bit RHEL does not support virtualization.
3. 512MB
4. By default, updates and installation of additional software packages requires Internet connectivity.
5. Use an ISO image.
6. To manage virtualization in an easy way, you need virrt-manager, which is a GUI utility.
7. XFS
8. You can. But you cannot register with RHN, so you will not have access to any repositories after the installation has finished.
9. Repository access
10. Minimal

Chapter 2

1. A placeholder that contains a specific value and that can be used in scripts to work with dynamic contents
2. **man -k**
3. /etc/bashrc
4. Use **pinfo**.
5. ~/.bash_history
6. **mandb**
7. Use **u**.
8. **2> /dev/null**
9. **echo $PATH**
10. **Ctrl+r, dog**

Chapter 3

1. /etc
2. **ls -alt** (**-a** also shows files that have a name that starts with a dot.)
3. **mv myfile yourfile**
4. **rm -rf /directory**
5. **ln -s /tmp ~**
6. **cp /etc/[abc]* .**
7. **ln -s /etc ~**
8. Use **rm symlink**. If **rm** is aliased to **rm -i** and you do not want to answer yes for every individual file, use **\rm** instead.
9. **tar zcvf /tmp/etchome.tgz /etc /home**
10. **tar xvf /tmp/etchome.tgz /etc/passwd**

Chapter 4

1. **ps aux | less**
2. **tail -n 5 ~/samplefile**
3. **wc ~/samplefile**. You might use -w to show only the number of words.
4. Use **Ctrl+C.**
5. **grep -v -e '^#' -e '^;' filename**
6. ?
7. **grep -i text file**
8. **grep -A5 'PATH' filename**
9. **sed -n 9p ~/samplefile**
10. **sed -i 's/user/users/g' ~/samplefile**

Chapter 5

1. Typically, the main screen on a Linux server
2. **Ctrl+Alt+F1**
3. **w** or **who**
4. /dev/pts/0
5. **ssh -v**
6. **ssh -X**

7. **~/.ssh/ssh_config**
8. **scp /etc/hosts lisa@server2:/tmp**
9. **~/.ssh/authorized_keys**
10. **ssh-keygen**

Chapter 6

1. 0
2. /etc/sudoers
3. **visudo**
4. /etc/default/useradd and /etc/login.defs
5. None, groups are created in /etc/group
6. wheel
7. **vigr**
8. **passwd** and **chage**
9. /etc/shadow
10. /etc/group

Chapter 7

1. **chown :groupname filename or chown .groupname filename**
2. **find / -user username**
3. **chmod -R 770 /data**
4. **chmod +x file**
5. **chmod g+s /directory**
6. **chmod +t /directory**
7. **setfacl -m g:sales:r ***
8. Use two commands: **setfacl -R -m g:sales:rx /dir** and **setfacl -m d:g:sales:rx /dir**.
9. Make sure that the last digit in the umask is a 7.
10. **chattr +i myfile**

Chapter 8

1. 213.214.215.96
2. **ip link show**

3. NetworkManager
4. /etc/hostname
5. **hostnamectl**
6. **nmcli con reload**
7. /etc/hosts
8. **ip route show**
9. **systemctl status NetworkManager**
10. **nmcli con mod "static" ipv4.addresses "10.0.0.20/24" 10.0.0.100**

Chapter 9

1. **jobs**
2. **Ctrl+Z, bg**
3. **Ctrl+C**
4. Use process management tools such as ps and kill.
5. **ps fax**
6. Use **ps -nn -p 1234**, where **nn** is a value between -1 and -19.
7. **killall dd**
8. **pkill mycommand**
9. **k**
10. **nice -5** command. Use -5 to start with and determine whether that gives your process sufficient priority.

Chapter 10

1. kvm, as well as kvm_intel on Intel hardware, or kvm_amd on AMD hardware
2. vmx on Intel or vms on AMD
3. Press the left **Ctrl** and **Alt** keys at the same time.
4. **arch**
5. cat /proc/cpuinfo
6. **virsh start vmname**
7. libvirtd
8. /var/lib/libvirt/images
9. **virsh list --all**
10. **virsh destroy vm1**

Chapter 11

1. **createrepo**
2. [some-label]
   name=some-name
   baseurl=http://server.example.com/repo
3. **yum repolist**
4. **yum provides */useradd**
5. **yum group list,** next use **yum group info "Security Tools"**
6. **yum install**
7. **rpm -q --scripts packagename**
8. **rpm -qd name-of.rpm**
9. **rpm -qf /path/to/file**
10. **repoquery**

Chapter 12

1. As a specific cron file in /etc/cron.d, or tied to a user account using **crontab -e -u** username
2. **0 14 1,15 * ***
3. **0/2 * * * ***
4. **0 0 19 9 4**
5. **Sun, 0, 7**
6. **crontab -e -u lisa**
7. Create the file /etc/cron.deny and make sure that it includes username boris.
8. Specify the job in /etc/anacrontab and make sure that the anacron service is operational.
9. The atd service; use **systemctl status atd** to verify.
10. Use **atq**

Chapter 13

1. /etc/rsyslog.conf
2. /var/log/secure
3. 5 weeks (1 week for the current file, 4 weeks for old files that are rotated away)
4. **logger -p user.notice "some text"**

5. Create a file in /etc/rsyslog.d. The name does not really matter. Give it the following contents: "*.=info /var/log/messages.info
6. /etc/systemd/journald.conf
7. **journalctl -f**
8. **journalctl _PID=1 --since 9:00:00 --until 15:00:00**
9. **journalctl -b**
10. **mkdir /var/log/journal; chown root:systemd-journal /var/log/journal; chmod 2755 /var/log/journal; killella -USR1 systemd-journald**

Chapter 14

1. gdisk
2. fdisk
3. XFS
4. /etc/fstab
5. noauto
6. mkswap
7. mount -a
8. Ext2
9. mkfs.ext4 or mkfs -t ext4
10. blkid

Chapter 15

1. 8e00
2. **vgcreate vggroup -s 4MiB /dev/sdb3**
3. **pvs**
4. Just type **vgextend vggroup /dev/sdd**. You do not have to do anything on the disk device itself.
5. Use **lvcreate -L 6M -n lvvol1 vgname**. Notice that this works only if you have created the volume group with a 2 MiB physical extent size.
6. **lvextend -L +100M /dev/vgname/lvvol1**
7. Add the disk space to the volume group using **vgextend**.
8. **-r**

9. **lvs**
10. Just use **fsck**. It does not matter that the file system was created on a logical volume; just the file system needs checking.

Chapter 16

1. **uname -r**
2. /etc/redhat-release
3. **lsmod**
4. **modinfo modulename**
5. **modprobe -r**
6. Use lsmod to find out which other kernel modules currently need this kernel module and unload these kernel modules first. Notice that this will not always work, especially not if the considered hardware currently is in use.
7. Use modinfo.
8. Create a file in /etc/modules.d.
9. **options cdrom debug=1**
10. **yum upgrade kernel**

Chapter 17

1. "Basic Web Server"
2. **systemctl enable httpd**
3. /etc/httpd/conf.d
4. **elinks**
5. /etc/httpd/conf/httpd.conf
6. /var/www/html
7. index.html
8. **systemctl status httpd or ps aux| grep http**
9. /etc/httpd/conf.d
10. /etc/httpd

Chapter 18

1. A unit is a thing that is started by systemd. There are different types of units, such as services, mounts, sockets, and many more.
2. Use **systemctl mask**.

3. /etc/default/grub
4. **systemctl --type=service**
5. By using systemctl enable on that service
6. By using systemctl isolate rescue.target
7. There are two types of targets: targets that can run independently and targets that cannot. Check the target unit file to find out more about this.
8. **systemctl list-dependencies --reverse**
9. /etc/default/grub
10. **grub2-mkconfig > /boot/grub2/grub.cfg**

Chapter 19

1. **e**
2. An error in /etc/fstab prevents the **fsck** command on that file system to finish successfully.
3. **systemd.unit=rescue.target**
4. Start from a rescue system
5. **systemctl list-units**
6. **rd.break**
7. **load_policy -i**
8. **chcon -t shadow_t /etc/shadow**
9. Use **grub2-mkimage > /boot/grub2/grub.cfg**
10. systemd.unit.emergency.target

Chapter 20

1. /root/anaconda-ks.cfg
2. system-config-kickstart
3. LVM logical volumes, firewalld firewall configuration, and individual packages
4. While the boot menu shows, press Tab. This opens the GRUB 2 prompt. On the GRUB 2 prompt, add **ks=http://server.example.com/kickstart.cfg**.
5. An online repository, a TFTP server that provides the boot image, a DHCP server that indicates where the boot image can be found
6. xinetd. Use **systemctl start xinetd** and **systemctl enable xinetd** to make it available.

7. In the TFTP root directory, create a directory pxelinux.cfg and in this directory create the file default that contains specific bootloader options.
8. syslinux
9. Download boot.iso from RHN.
10. /var/lib/tftpboot

Chapter 21

1. **setenforce 0**
2. **getenforce -a** or **semanage boolean -l**
3. Use the **sepolicy manpage** command.
4. setroubleshoot-server
5. **semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"** followed by **restorecon**
6. Never!
7. /etc/sysconfig/selinux
8. /var/log/audit/audit.log
9. **man -k _selinux | grep ftp**
10. Use **setenforce 0** to temporarily switch SELinux to permissive mode and try again.

Chapter 22

1. firewalld
2. **firewall-cmd --add-port=2345/udp**
3. **firewall-cmd --list-all-zones**
4. **firewall-cmd --remove-service=vnc-server**
5. **--reload**
6. **--list-all**
7. **firewall-cmd --add-interface=eno1 --zone=public**
8. The default zone
9. **firewall-cmd --permanent --add-source=192.168.0.0/24**
10. **firewall-cmd --get-services**

Chapter 23

1. A keytab file. This file typically has the name /etc/krb5.keytab.
2. **showmount -e server1**. Notice that the **showmount** command does not get through a firewall.
3. **mount [-t nfs] server1:/share /somewhere**
4. **smbclient -L**
5. cifs-utils
6. **mount -t cifs -o guest //server1/data /mnt**
7. Use a credentials file that contains at least the username and password that need to be used. Specify all mount options and use **creds=/somewhere/credentials.file** in the mount options column.
8. The name should end in autofs, and it should contain the name of the directory on which the automount is performed, as well as the file that contains further specifics on the mount.
9. If you want to perform the mount on a directory that is already existing
10. /etc/vsftpd/vsftpd.conf

Chapter 24

1. **date -s 16.24**
2. hwclock --systohc
3. **date -d '@nnnnnnn'**
4. **hwclock --hctosys**
5. chronyd
6. **timedatectl set-ntp 1**
7. /etc/chrony.conf
8. **timedatectl list-timezones**
9. **timedatectl set-timezone ZONE**
10. **timedatectl set-time TIME**

Chapter 25

1. authconfig-gtk
2. The nslcd service is used instead of the sssd service.
3. Add the **ldap_tls_reqcert = never** option to the [domain/default] section in /etc/sssd/sssd.conf.

4. /etc/sysconfig/authconfig
5. Make sure the realmd package is installed and run **realm join mydomain.example.com**.
6. /etc/krb5.conf
7. **kinit <username>**
8. /etc/nsswitch.conf
9. /etc/ldap.conf
10. /etc/krb5.keytab

Chapter 26

1. **lsscsi** provides useful information (but other commands are available also).
2. Do not refer to the device directly, but use a UUID instead and use the **_netdev** mount option.
3. **targetcli**
4. To make sure that the iSCSI target information is stored locally and is made accessible before logging in to the target
5. /var/lib/iscsi
6. /etc/iscsi/initiatorname.iscsi
7. iscsid, which is started with iscsi.service
8. **iscsiadm --mode session -P 3**
9. The target portal group
10. It should be : and not . to separate the com.example part from the myserver part.

Chapter 27

1. Use the < and > keys to move to the left or right and select a different sorting column. Alternatively, you can use Shift-M.
2. It depends on other performance indicators so it is impossible to say just based on this single parameter. You should at least look at the number of CPU cores in your system to say more about this.
3. It depends on the amount of memory that is currently in use by buffers and cache. If a memory shortage occurs, memory can be freed from the buffers and cache area.
4. Remove ~/.toprc

5. vmstat
6. pidstat
7. iostat
8. The sa1 and sa2 data gathering processes might not be started.
9. Set an alias for sar to make sure it is always started with the **LANG=C** setting, adding **sar="LANG=C sar"** in /etc/bashrc or ~/.bashrc.
10. cifsiostat

Chapter 28

1. /proc/<PID>/environ
2. /proc/partitions
3. /proc/meminfo
4. **echo 1 > /proc/sys/net/ipv4/ip_forward**
5. Create a file in /etc/sysctl.d. Make sure that the file name ends in .conf and put the following line in it: **net.ipv4.ip_forward = 1**
6. **sysctl -a**
7. net.ipv4.icmp_echo_ignore_all
8. systemd-sysctl
9. kernel.hostname
10. **sysctl -p /etc/sysctl.d/net.conf**

Chapter 29

1. imjournal
2. imuxsock
3. **$OmitLocalLogging on**
4. /etc/systemd/journald.conf
5. **ForwardToSyslog=yes**
6. imfile
7. ommysql
8. **$ModLoad imupd and $UDPServerRun 514**
9. **firewall-cmd --add-port=514/tcp and firewall-cmd --add-port=514/tcp --permanent**
10. ***.* @logserver.example.com:514**

Chapter 30

1. lacp
2. **teamdctl teamname state**
3. nmcli-examples(5)
4. **TEAM_MASTER**
5. **teamnl teamname ports**
6. Anything starting with fe80
7. **ping6 fe02::1%eth0**
8. The network address, the associated netmask, the gateway, and the metric
9. /etc/sysconfig/network-scripts/route-eno1
10. Create a file in /etc/sysctl.d that has a name ending in .conf, and give it the contents net.ipv4.ip_forward = 1.

Chapter 31

1. The script will be interpreted by the same shell as the parent shell.
2. **test -z $VAR or [-z $VAR]**
3. Use **$#**.
4. $@
5. Use **read SOMEVAR.**
6. [-f filename] || echo file does not exist
7. [-e filename]
8. A **for** statement is typically used in such cases.
9. You do not; it is a part of the if statement which is closed with a **fi**.
10. ;;

Chapter 32

1. Use **systemctl mask** iptables to prevent it from ever being started.
2. In /etc/firewalld/services
3. <port protocol=tcp port=2022>
4. **firewall-cmd --get-services**
5. Direct rules. Note that use of these is not recommended.
6. **firewall-cmd --add-rich-rule='rule family=ipv4 source address=10.0.0.0/24 port port=7900-7905 protocol=tcp accept' --zone=dmz**

7. **firewall-cmd --add-rich-rule='rule service name=http log limit value=3/m accept' --zone=dmz**
8. Network Address Translation is generic terminology that is used when a firewall is configured to change either port or IP addresses. Masquerading is the specific solution that is used to allow hosts on a private network to access hosts on the Internet, using the public IP address of the NAT router.
9. **firewall-cmd --add-forward-port=port=4404:proto:tcp:toport=22:toaddr10.0.0.10**
10. **firewall-cmd --permanent --zone=public--add-masquerade**

Chapter 33

1. Require All Denied
2. httpd_unified set to on
3. httpd_sys_content_t
4. /etc/pki/tls
5. **SSLCertificateKeyFile**
6. /etc/httpd/conf.d/ssl.conf
7. **genkey**
8. WSGIScriptAlias /webapp/ /opt/webapp/app.py
9. It will create a new file, with the result that all old users no longer exist!
10.
```
<Directory /var/www/html/secret>
                AuthType Basic
                AuthName "secret files"
                AuthUserFile /etc/httpd/htpasswd
                Require user valid-user
        </Directory>
```

Chapter 34

1. AAAA
2. MX
3. **dig MX example.com**
4. **dig -x 192.168.4.122**
5.
```
forward-zone:
name: "."
forward-addr: 10.0.0.100
```

6. Include access-control: 192.168.122.0/24
7. domain-insecure: rhatcert.com
8. The **interface** parameter
9. Use **unbound-checkconf.**
10. Use **unbound-control dump_cache.**

Chapter 35

1. mysql_secure_installation
2. In my.cnf, set the **bind-address** to :: and make sure that **skip-networking** is set to 0.
3. **/usr/libexec/mysqld --help --verbose**
4. **SHOW TABLES;**
5. **USE addressbook;**
6. **LIST tables;**
7. **DESCRIBE addressbook;**
8. **SELECT * from addressbook;**
9. **lvcreate -s -n name-of-snapshot -L 1G /dev/vgname/ lvname-of-original-volume**
10. Type **FLUSH TABLES WITH READ LOCK**;. Do not forget to use **UNLOCK TABLES**; later to make the database accessible again!

Chapter 36

1. /etc/exports
2. Nothing. On previous versions of RHEL, the nfs-secure service needed to be started, but this is no longer required.
3. nfs-server. The nfs-secure-server that needed to be started on RHEL 7 is now no longer needed.
4. 2049, 111, 20049
5. public_content_t
6. On previous versions of RHEL, that would have been the **_netdev** mount option. On RHEL 7, usage of this mount option is no longer required.
7. krb5

8. Make the user nfsnobody owner of the NFS share and use **all_squash** on the share. This ensures that all users have access according to the permissions on the share on nfsnobody.
9. /etc/sysconfig/nfs
10. 4.2

Chapter 37

1. [data]
   path = /data
2. Just use **writable = yes** or **read only = no** in the share definition.
3. Do no include **writable = yes**, but do include the write list parameter and specify the group whose members can write to the share, adding **@groupname** or **+groupname**
4. Use **samba_enable_homedirs**.
5. Use the **hosts_allow parameter** and specify the network part of the IP address, as in 192.168.10.
6. **pdbedit -L**
7. Log in as that user and use **cifscreds add servername**.
8. Use **mount -o multiuser,sec=ntlmssp,username=lisa //server/sambashare /mnt/multiuser**.
9. Create a credentials file with the **username=** and **password=** contents, store it in a secure location, and mount it through fstab by using **creds=/root/credentialsfile**.
10. **smbclient -L //servername**

Chapter 38

1. **inet_interfaces**
2. **myorigin**
3. **mydestnation**
4. **inet_protocols**
5. **relayhost=[smtp.example.com]**
6. **postconf**
7. Type **postqueue -f**.
8. /var/log/maillog

9. On a default configuration, no SELinux contexts/Booleans need to be changed to guarantee successful Postfix operation.
10. On a server that handles incoming mail, make sure that the smtp service is enabled in the firewall.

Chapter 39

1. **ssh-agent /bin/bash; ssh-add**
2. Use **AllowUsers lisa**. This will only allow access for user lisa and exclude all other users, including root.
3. Include the Port line twice, each line mentioning a specific port.
4. Use -fN in the ssh command.
5. It is not stored; it is copied to a secured area in RAM.
6. **ssh -fNL 5555:localhost:80 root@server2.example.com**
7. **ssh -fNR 80:localhost:8088 user@server.somewhere.com**
8. **semanage port -a -t ssh_port_t -p tcp 2022**
9. **firewall-cmd --add-port=2022/tcp --permanent,** followed by **firewall-cmd --reload**
10. **GatewayPorts yes**

Chapter 40

1. Because data can be stored in different replicas. To see whether other replicas have newer data, the modifications have a time stamp.
2. Kerberos tickets are valid for a limited time only. To see whether a Kerberos ticket is still valid, the time needs to be synchronized between the different servers that are involved.
3. chronyd
4. 10
5. NTP uses UDP port 123, no matter if it is configured as a server or as a peer.
6. Local stratum, which is followed by the stratum number, which is typically 10
7. 16
8. **chronyc sources**
9. **chronyc tracking**
10. **chronyc sourcestats**