APPENDIX B

Memory Tables

Chapter 2

Table 2-2 Standard Input, Output, and Error Overview

Name	Default Destination	Use in Redirection	File Descriptor Number
	Computer keyboard	< (same as 0<)	0
	Computer monitor	> (same as 1>)	1
STDERR		2>	2

Table 2-3 Common Bash Redirectors

Redirector	Explanation
(same as 1>)	Redirects STDOUT. If redirection is to a file, the current contents of that file are overwritten.
(same as 1>>)	Redirects STDOUT. If output is written to a file, the output is appended to that file.
	Redirects STDERR.
	Redirects STDERR to the same destination as STDOUT. Notice that this has to be used in combination with normal output redirection, as in **ls whuhiu > errout 2>&1**.
(same as 0<)	Redirects STDIN.

Table 2-4 **vim** Essential Commands

vim Command	Explanation
	Switches from input mode to command mode. Press this key before typing any command.
	Switches from command mode to input mode at (**i**) or after (**a**) the current cursor position.
	Opens a new line below the current cursor position and goes to input mode.
	Writes the current file and quits.
	Quits the file without applying any changes. The **!** forces the command to do its work. Add the **!** only if you really know what you are doing.
	Writes the current file with a new filename.
	Deletes the current line.
	Copies the current line.
	Pastes the current selection.
	Enters visual mode, which allows you to select a block of text using the arrow keys. Use **d** to cut the selection or **y** to copy it.
	Undoes the last command. Repeat as often as necessary.
	Redoes the last undo.
	Goes to the first line in the document.
	Goes to the last line in the document.
	Searches for *text* from the current cursor position forward.
	Searches for *text* from the current cursor position backward.
	Goes to the first position in the current line.
	Goes to the last position in the current line.
	Adds the output of **ls** (or any other command) in the current file.
	Replaces all occurrences of *old* with *new*.

Chapter 3

Table 3-2 FHS Overview

Directory	Use
/	
/boot	

Directory	Use
/dev	
/etc	
/home	
/media, /mnt	
/opt	
/proc	
/root	
/run	
/srv	
/sys	
/tmp	
/usr	
/var	

Chapter 4

Table 4-2 Essential Tools for Managing Text File Contents

Command	Explanation
	Opens the text file in a pager, which allows for easy reading
	Dumps the contents of the text file on the screen
	Shows the first ten lines of the text file
	Shows the last ten lines of the text file
	Used to filter specific columns or characters from a text file
	Sorts the contents of a text file
	Counts the number of lines, words, and characters in a file

Table 4-3 Most Significant Regular Expressions

Regular Expression	Use
	Matches line that starts with specified text.
	Matches line that ends with specified text.
	Wildcard. (Matches any single character.)
	Matches *a*, *b*, or *c*.
	Matches zero to an infinite number of the previous character.
	Matches exactly two of the previous character.
	Matches a minimum of one and a maximum of three of the previous character.
	Matches zero or one of the previous character. This makes the previous character optional, which in this example would match both *color* and *colour*.

Table 4-4 Most Useful **grep** Options

Option	Use
	Not case sensitive. Matches upper- and lowercase letters.
	Shows only lines that do *not* contain the regular expression.
	Searches files in the current directory and all subdirectories.
	Searches for lines matching more than one regular expression.
	Shows <number> of lines after the matching regular expression.
	Shows <number> of lines before the matching regular expression.

Chapter 5

Table 5-2 Common **ssh** Options

Option	Use
	Verbose; shows in detail what is happening while establishing the connection
	Enables support for graphical applications
	Used to connect to an SSH service that is not listening on the default port 22

Table 5-3 Common **rsync** Options

Option	Use
	Synchronizes the entire directory tree
	Also synchronizes symbolic links
	Preserves symbolic links
	Performs only a dry run, not actually synchronizing anything
	Uses archive mode, thus ensuring that entire subdirectory trees and all file properties will be synchronized
	Uses archive mode, and in addition synchronizes ACLs
	Synchronizes SELinux context as well

Chapter 6

Table 6-2 Methods to Run Tasks with Elevated Permissions

Method	Description
	Opens a subshell as a different user, with the advantage that commands are executed as root only in the subshell
	Enables you to set up an environment where specific tasks are executed with administrative privileges
	Enables you to set up graphical utilities to run with administrative privileges

Chapter 7

Table 7-2 Use of Read, Write, and Execute Permissions

Permission	Applied to Files	Applied to Directories
Read		
Write		
Execute		

Table 7-3 Numeric Representation of Permissions

Permission	Numeric Representation
Read	
Write	
Execute	

Table 7-4 Working with SUID, SGID, and Sticky Bit

Permission	Numeric Value	Relative Value	On Files	On Directories
SUID			User executes file with permissions of file owner.	No meaning.
SGID			User executes file with permissions of group owner.	Files created in directory get the same group owner.
Sticky bit			No meaning.	Prevents users from deleting files from other users.

Table 7-5 umask Values and Their Result

Value	Applied to Files	Applied to Directories
0		Everything
1	Read and write	
2	Read	
3		Read
4	Write	
5	Write	
6	Nothing	
7		Nothing

Chapter 8

Table 8-2 Binary-Decimal Conversion Overview

Binary Value	Decimal Value
	0
	32
	64
	96
	128
	160
	192
	224

Chapter 9

Table 9-2 Key Options in .repo Files

Option	Explanation
	Contains the label used as an identifier in the repository file.
	Specifies the name of the repository.
	Refers to a URL where information about mirror servers for this server can be obtained. Typically used for big online repositories only.
	Refers to the base URL where the RPM packages are found.
	Set to 1 if a GNU Privacy Guard (GPG) integrity check needs to be performed on the packages. If set to 1, a GPG key is required.
	Specifies the location of the GPG key that is used to check package integrity.

Table 9-3 Common **yum** Tasks

Task	Explanation
	Search for the exact name of a package.
	Perform a deep search in the package to look for specific files within the package.
	Provide more information about the package.
	Install the package.
	Remove the package.
	List all or installed packages.
	List package groups.
	Install all packages from a group.
	Update packages specified.
	Remove all stored metadata.

Table 9-4 Yum Module Terminology

Item	Explanation
	The default package format. Contains files, as well as metadata that describes how to install the files. Optionally may contain pre- and post-installation scripts as well.
	A delivery mechanism to install RPM packages. In a module different versions and profiles can be provided.
	A specific version of the module.
	A collection of packages that are installed together for a particular use case.

Table 9-5 Common RPM Query Commands

Command	Use
	Uses a filename as its argument to find the specific RPM package a file belongs to.
	Uses the RPM database to provide a list of files in the RPM package.
	Uses the RPM database to provide package information (equivalent to **yum info**).
	Uses the RPM database to show all documentation that is available in the package.
	Uses the RPM database to show all configuration files that are available in the package.
	Uses the RPM database to show scripts that are used in the package. This is particularly useful if combined with the **-p** option.
	The **-p** option is used with all the previously listed options to query individual RPM package files instead of the RPM package database. Using this option before installation helps you find out what is actually in the package before it is installed.
	Shows dependencies for a specific package.
	Shows which parts of a specific package have been changed since installation.
	Verifies all installed packages and shows which parts of the package have been changed since installation. This is an easy and convenient way to do a package integrity check.
	Lists all packages that are installed on this server.

Chapter 10

Table 10-2 Job Management Overview

Command	Use
	Starts the command immediately in the background.
	Stops the job temporarily so that it can be managed. For instance, it can be moved to the background.
	Sends the End Of File (EOF) character to the current job to indicate that it should stop waiting for further input.
	Can be used to cancel the current interactive job.
	Continues the job that has just been frozen using Ctrl-Z in the background.
	Brings back to the foreground the last job that was moved to background execution.
	Shows which jobs are currently running from this shell. Displays job numbers that can be used as an argument to the commands **bg** and **fg**.

Table 10-3 Linux Process States Overview

State	Meaning
	The process is currently active and using CPU time, or in the queue of runnable processes waiting to get services.
	The process is waiting for an event to complete.
	The process is in a sleep state that cannot be stopped. This usually happens while a process is waiting for I/O.
	The process has been stopped, which typically has happened to an interactive shell process, using the Ctrl-Z key sequence.
	The process has been stopped but could not be removed by its parent, which has put it in an unmanageable state.

Table 10-4 Tuned Profile Overview

Profile	Use
	The best compromise between power usage and performance
	Based on the balanced profile, but tuned for better response to interactive applications
	Tuned for maximum throughput
	Based on latency-performance, but with additional options to reduce network latency
	Based on throughput-performance, optimizes older CPUs for streaming content
	Tunes for maximum power saving
	Tunes for maximum throughput
	Optimizes Linux for running as a virtual machine
	Optimizes Linux for use as a KVM host

Chapter 11

Table 11-2 Systemd Status Overview

Status	Description
	The unit file has been processed and the unit is active.
	The unit is running with one or more active processes.
	The unit has successfully completed a one-time run.
	The unit is running and waiting for an event.
	The unit is not running.

Status	Description
	The unit will be started at boot time.
	The unit will not be started at boot time.
	The unit cannot be enabled but may be started by another unit automatically.

Table 11-3 **systemctl** Unit Overview Commands

Command	Description
	Shows only service units
	Shows all active service units (same result as the previous command)
	Shows inactive service units as well as active service units
	Shows all services that have failed
	Shows detailed status information about services

Chapter 13

Table 13-2 System Log Files Overview

Log File	Explanation
	Contains the most commonly used log file; it is the generic log file where most messages are written to.
	Contains kernel log messages.
	Contains authentication-related messages. Look here to see which authentication errors have occurred on a server.
	Contains messages that are related to system startup.
	Contains audit messages. SELinux writes to this file.
	Contains mail-related messages.
	Provides log files for the Samba service. Notice that Samba by default is not managed through rsyslog, but writes directly to the /var/log directory.
	Contains messages that have been written by the sssd service, which plays an important role in the authentication process.
	Contains log messages that were generated by the print service CUPS.
	Contains log files that are written by the Apache web server. Notice that Apache writes messages to these files directly and not through rsyslog.

Table 13-3 rsyslogd Facilities

Facility	Used by
	Messages related to authentication.
	Messages generated by the **crond** service.
	Generic facility that can be used for nonspecified daemons.
	Kernel messages.
	Messages generated through the legacy lpd print system.
	Email-related messages.
	Special facility that can be used to write a marker periodically.
	Messages generated by the NNTP news system.
	Same as auth/authpriv. Should not be used anymore.
	Messages generated by the syslog system.
	Messages generated in user space.
	Messages generated by the legacy UUCP system.
	Messages generated by services that are configured by any of the local0 through local7 facilities.

Table 13-4 rsyslogd Priorities

Priority	Description
	Debug messages that will give as much information as possible about service operation.
	Informational messages about normal service operation.
	Informational messages about items that might become an issue later.
	Something is suboptimal, but there is no real error yet.
	A noncritical error has occurred.
	A critical error has occurred.
	Message used when the availability of the service is about to be discontinued.
	Message generated when the availability of the service is discontinued.

Chapter 14

Table 14-3 Common Disk Device Types

Device Name	Description
/dev/sda	A hard disk that uses the SCSI driver. Used for SCSI and SATA disk devices. Common on physical servers but also in VMware virtual machines.
	The first hard disk on an NVM Express (NVMe) interface. NVMe is a server-grade method to address advanced SSD devices. Note at the end of the device name that the first disk in this case is referred to as *n1* instead of *a* (as is common with the other types).
	The (legacy) IDE disk device type. You will seldom see this device type on modern computers.
	A disk in a KVM virtual machine that uses the virtio disk driver. This is the common disk device type for KVM virtual machines.
	A disk in a Xen virtual machine that uses the Xen virtual disk driver. You see this when installing RHEL as a virtual machine in Xen virtualization. RHEL 8 cannot be used as a Xen hypervisor, but you might see RHEL 8 virtual machines on top of the Xen hypervisor using these disk types.

Table 14-4 File System Overview

File System	Description
	The default file system in RHEL 8.
	The default file system in previous versions of RHEL; still available and supported in RHEL 8.
	The previous version of Ext4. On RHEL 8, there is no need to use Ext3 anymore.
	A very basic file system that was developed in the early 1990s. There is no need to use this file system on RHEL 8 anymore.
	A relatively new file system that is not supported in RHEL 8.
	A Windows-compatible file system that is not supported on RHEL 8.
	A file system that offers compatibility with Windows and Mac and is the functional equivalent of the FAT32 file system. Useful on USB thumb drives that exchange data with other computers but not on a server's hard disks.

Table 14-5 /etc/fstab Fields

Field	Description
	The device that must be mounted. A device name, UUID, or label can be used.
	The directory or kernel interface where the device needs to be mounted.
	The file system type.
	Mount options.
	Use 1 to enable support to back up using the **dump** utility. This may be necessary for some backup solutions.
	This field specifies whether the file system should be checked automatically when booting. Use 0 to disable automated check, 1 if this is the root file system and it has to be checked automatically, and 2 for all other file systems that need automatic checking while booting. Network file systems should have this option set to 0.

Table 14-6 Common Mount Options

Option	Use
	Mounts [does not mount] the file system automatically.
	Adds support for file system access control lists (see Chapter 7, "Permissions Management").
	Adds support for user-extended attributes (see Chapter 7).
	Mounts the file system in read-only mode.
	Disables or enables access time modifications.
	Denies or allows execution of program files from the file system.
	Mounts a network file system. This option tells fstab to wait until the network is available before mounting this file system.

Chapter 15

Table 15-2 LVM Management Essential Commands

Command	Explanation
	Creates physical volumes
	Shows a summary of available physical volumes
	Shows a list of physical volumes and their properties

Command	Explanation
	Removes the physical volume signature from a block device
	Creates volume groups
	Shows a summary of available volume groups
	Shows a detailed list of volume groups and their properties
	Removes a volume group
	Creates logical volumes
	Shows a summary of all available logical volumes
	Shows a detailed list of available logical volumes and their properties
	Removes a logical volume

Chapter 16

Table 16-2 Linux Kernel Module Management Overview

Command	Use
	Lists currently loaded kernel modules
	Displays information about kernel modules
	Loads kernel modules, including all of their dependencies
	Unloads kernel modules, considering kernel module dependencies

Chapter 18

Table 18-2 Boot Phase Configuration and Troubleshooting Overview

Boot Phase	Configuring It	Fixing It
	Hardware configuration (F2, Esc, F10, or another key).	Replace hardware.
	BIOS/UEFI configuration or hardware boot menu.	Replace hardware or use rescue system.
	grub2-install and edits to /etc/defaults/grub.	Use the GRUB boot prompt and edits to /etc/defaults/grub, followed by **grub2-mkconfig**.
	Edits to the GRUB configuration and /etc/dracut.conf.	Use the GRUB boot prompt and edits to /etc/defaults/grub, followed by **grub2-mkconfig**.

Boot Phase	Configuring It	Fixing It
	Compiled into initramfs.	Use the **init= kernel** boot argument, **rd.break** kernel boot argument.
	Compiled into initramfs.	Use the **dracut** command. (You won't often have to troubleshoot this.)
	Edits to the /etc/fstab file.	Apply edits to the /etc/fstab file.
	Using **systemctl set-default** to create the /etc/systemd/system/ default.target symbolic link	Start the rescue.target as a kernel boot argument.

Chapter 20

Table 20-2 Most Useful sshd Configuration Options

Option	Use
	Defines the TCP listening port.
	Indicates whether to allow or disallow root login.
	Specifies the maximum number of authentication tries. After reaching half of this number, failures are logged to syslog.
	Indicates the maximum number of sessions that can be open from one IP address.
	Specifies a space-separated list of users who are allowed to connect to the server.
	Specifies whether to allow password authentication. This option is on by default.
	Indicates whether authentication through the GSSAPI needs to be enabled. Used for Kerberos-based authentication.
	Specifies whether or not to clean up inactive TCP connections.
	Specifies the interval, in seconds, that packets are sent to the client to figure out if the client is still alive.
	Specifies the number of client alive packets that need to be sent.
	If on, uses DNS name lookup to match incoming IP addresses to names.
	Specifies the interval, in seconds, that a client sends a packet to a server to keep connections alive.
	Specifies the maximum number of packets a client sends to a server to keep connections alive.

Chapter 22

Table 22-2 SELinux Core Elements

Element	Use
	A collection of rules that define which source has access to which target.
	The object that is trying to access a target. Typically a user or a process.
	The thing that a source domain is trying to access. Typically a file or a port.
	A security label that is used to categorize objects in SELinux.
	A specific part of the policy that determines which source domain has which access permissions to which target domain.
	Same as a context label, defined to determine which source domain has access to which target domain.

Chapter 23

Table 23-2 Firewalld Default Zones

Zone Name	Default Settings
	Incoming network connections are rejected with an “icmp-host-prohibited” message. Only network connections that were initiated on this system are allowed.
	For use on computers in the demilitarized zone. Only selected incoming connections are accepted, and limited access to the internal network is allowed.
	Any incoming packets are dropped and there is no reply.
	For use on external networks with masquerading (Network Address Translation [NAT]) enabled, used especially on routers. Only selected incoming connections are accepted.
	For use with home networks. Most computers on the same network are trusted, and only selected incoming connections are accepted.
	For use in internal networks. Most computers on the same network are trusted, and only selected incoming connections are accepted.
	For use in public areas. Other computers in the same network are not trusted, and limited connections are accepted. This is the default zone for all newly created network interfaces.
	All network connections are accepted.
	For use in work areas. Most computers on the same network are trusted, and only selected incoming connections are accepted.

Table 23-3 Common **firewall-cmd** Options

firewall-cmd Options	Explanation
	Lists all available zones
	Shows the zone currently set as the default zone
	Changes the default zone
	Shows all available services
	Shows services currently in use
	Adds a service to the current default zone or the zone that is specified
	Removes a service from the configuration
	Shows configuration for all zones
	Adds a port and protocol
	Removes a port from the configuration
	Adds an interface to the default zone or a specific zone that is specified
	Removes an interface from a specific zone
	Adds a specific IP address
	Removes an IP address from the configuration
	Writes configuration to disk and not to runtime
	Reloads the on-disk configuration

Chapter 25

Table 25-2 Understanding Linux Time

Concept	Explanation
	The hardware clock that resides on the main card of a computer system
	Same as the hardware clock
	The time that is maintained by the operating system
	Similar to system time

Concept	Explanation
	A worldwide standard time
	Calculation that is made to change time automatically when DST changes occur
	The time that corresponds to the time in the current time zone

Table 25-3 Commands Related to RHEL 8 Time Management

Command	Short Description
	Manages local time
	Manages hardware time
	Developed to manage all aspects of time on RHEL 8

Table 25-4 **timedatectl** Command Overview

Command	Explanation
	Shows current time settings
	Sets the current time
	Sets the current time zone
	Shows a list of all time zones
	Controls whether the RTC (the real-time clock, normally referred to as the hardware clock) is in local time
	Controls whether NTP is enabled