

Glossary

\$PATH A variable that contains a list of directories that are searched for executable files when a user enters a command.

- The current directory. Its value can be requested using the **pwd** command.

A

absolute filename A filename that is complete and starts with the name of the root directory, including all directories up to the current file or directory.

access control list (ACL) In Linux permissions, a system that makes it possible to grant permissions to more than one user and more than one group. Access control lists also allow administrators to set default permissions for specific directories.

Alma Linux Free open source alternative for Red Hat Enterprise Linux, which consists of the RHEL source code with all licensing removed.

anacron A service that ensures that vital cron jobs can be executed when the server is down at the moment that the job normally should be executed. Can be considered an extension to cron.

AND A logical construction that can be used in scripts. In an AND construction, the second command is executed only after successful execution of the first command.

application profile A collection of packages that may be used to install a specific version of software, according to a specific installation profile.

application stream A specific version of a dnf module that can be installed as such.

archiving A system that ensures that data can be properly backed up.

at A service that can be used to schedule future jobs for one-time execution.

attribute A property that can be set to a file or directory and that will be enforced no matter which user with access permission accesses the file. For instance, a file that has the immutable (**i**) attribute set cannot be deleted, not

even by the root user. However, the root user does have the capability to change the attribute, which would allow the root user to delete the file anyway.

audit log The main log file in `/var/log/audit/audit.log`, which by default contains all messages that are logged by the auditd service.

auditd A service that runs by default on Red Hat Enterprise Linux and can be configured to log very detailed information about what is happening on RHEL. Auditing is complementary to system logging and can be used for compliancy reasons. On RHEL, the auditing system takes care of logging SELinux-related messages, which makes it a relatively important system.

autofs A service that takes care of automatically mounting file systems at the moment that a specific directory is accessed. This service is very useful to ensure the automatic mounting of home directories for users in a centralized user management system, as can be implemented by the LDAP service.

automount The process that is started by the autofs service. *See* autofs for more details.

B

background process A process that is running on a system without actively occupying a console. Processes can be started in the background by adding a `&` after the command that starts the process. *See also* foreground process.

backup A copy of important data, which can be restored if at any point in time the original data gets lost.

Bash The default shell that is used on Red Hat Enterprise Linux.

Basic Input/Output System (BIOS) The first software that is started when a computer starts on older IBM-compatible computers. Settings in the BIOS can be changed by using the BIOS setup program. *See also* Unified Extensible Firmware Interface (UEFI).

binary A numbering scheme that is based on bit values that can be on or off. Binary numbers are 0 and 1. Because binary numbers are difficult to use, decimal, hexadecimal, or octal numbers often are used.

BIOS *See* Basic Input/Output System.

boot loader Program that is started as the very first thing while starting a computer and that takes care of loading the operating system kernel and `initramfs`.

Btrfs A general-purpose Linux file system that is expected to become the default file system on Red Hat Enterprise Linux in a future release.

bzip2 A compression utility that can be used as an alternative to `gzip`.

C

cache In memory management, the area of memory where recently used files are stored. Cache is an important mechanism to speed up reads on servers.

capability A specific task that can be performed on Linux. User root has access to all capabilities; normal users have access to limited sets of capabilities only.

CentOS A Linux distribution that uses all Red Hat packages but has removed the Red Hat logo from all these packages to make it possible to distribute the software for free. CentOS is the best option for practicing for the RHCSA exam if you do not have access to RHEL.

certificate In PKI cryptography, contains the public key of the issuer of the certificate. This public key is signed with the certificate of a certificate authority, which guarantees its reliability.

certificate authority (CA) A commonly known organization that can be used to guarantee the reliability of PKI certificates. The certificate authority provides a certificate that can be used to sign public key certificates. Instead of using commonly known organizations, self-signed certificates can be used for internal purposes as well.

chrony The service that offers time synchronization services in Red Hat Enterprise Linux.

chroot An environment where a part of the file system is presented as if it were the root of the file system. Chroot is used as a security feature that hides part of the operating system that is not required by specific services.

CIFS *See* Common Internet File System.

cloud A computing platform that allows for flexible usage of hosted computing resources.

Common Internet File System (CIFS) The standardized version of the Microsoft Server Message Block (SMB) protocol, which is used to provide access to shared printers, files, and directories in a way that is compatible with Windows servers and clients. CIFS has become the de facto standard for file sharing in IT.

compression A technology that is used to reduce the size of files by analyzing redundant patterns and storing them more efficiently.

conditional loop In shell scripting, a set of commands that is executed only if a specific condition has been met.

connection (in network card configuration) A set of network configuration parameters that is associated to a network interface.

connection (in network communication) A session between two parties that has been initialized and will exist until the moment that the connection is tiered down.

console In Linux, the primary terminal where a user works. It is also a specific device with the name `/dev/console`.

container A ready-to-run application that is started from an image and includes all application dependencies.

container engine The code that allows containers to run on top of an operating system.

context In SELinux, a label that is used to define the security attributes of users, processes, ports, and directories. These contexts are used in the SELinux policy to define security rules.

context switch When the CPU switches from executing one task to executing another task.

context type In SELinux, a label that identifies the SELinux properties of users, ports, and processes.

Coordinated Universal Time (UTC) A time standard that is globally the same, no matter which specific time zone a user is in. UTC roughly corresponds to Greenwich Mean Time (GMT).

credentials file A file that can be used to mount CIFS file systems automatically from the `/etc/fstab` file. The credentials file is stored in a secure place, like the home directory of user root, and contains the username and password that are used to mount the remote file system.

CRI-o The default container engine on RHEL 9. Pronounced *CRY-o*.

cron A service that takes care of starting services repeatedly at specific times.

cryptography A technique used to protect data, often by converting information to an unreadable state, where keys are used to decipher the scrambled data. Cryptography is used not only to protect files while in transit but also to secure the authentication procedure.

D

deduplication A storage technology that analyzes data to be stored on disk and takes out duplicate patterns to allow for more efficient storage.

default route The route that is used by default to forward IP packets that have a destination on an external network.

dependency Generally, a situation where one item needs another item. Dependencies occur on multiple levels in Linux. In RPM package management, a dependency is a software package that needs to be present for another package to be installed. In Systemd, a dependency is a Systemd unit that must be loaded before another unit can be loaded.

dependency hell Situation where for package installation, other packages are needed, which by themselves could require dependencies as well. The problem of dependency hell has been fixed by the introduction of repository-based systems.

destination In rsyslog, the place where log messages should be sent by the logging system. Destinations are often files, but can also be input modules, output modules, users, or hosts.

device A peripheral that is attached to a computer to perform a specific task.

device file A file that is created in the /dev directory and that is used to represent and interact with a device.

device mapper A service that is used by the Linux kernel to communicate with storage devices. Device mapper is used by LVM, multipath, and other devices, but not by regular hard disks. Device files that are created by device mapper can be found in the /dev/mapper directory.

directory A folder in the file system that can be used to store files in an organized manner.

disabled mode The SELinux mode in which SELinux is completely deactivated.

distribution A Linux version that comes with its own installation program or which is ready for usage. Because Linux is a collection of different tools and other components, the Linux distribution gathers these tools and other components, may or may not enhance them, and distributes them so that users do not have to gather all the different components for themselves.

dmesg Utility that can be used to read the kernel ring buffer, which contains log messages that were generated by the Linux kernel.

dnf The new software manager that replaces the **yum** utility in RHEL 9.

Docker A common solution to run containers. Docker was the default container solution in RHEL 8 but is no longer supported and was replaced with CRI-o/podman in RHEL 9.

Domain Name System (DNS) The global system used to match logical server names to IP addresses.

dracut A utility used to generate the initramfs, an essential part of the Linux operating system that contains drivers and other vital files required to start a Linux system.

Dynamic Host Configuration Protocol (DHCP) A protocol used to ensure that hosts can obtain an IP address and related information automatically.

dynamic route A network route that is managed by an automatic routing protocol.

E

enforcing mode The SELinux mode where SELinux is fully operational and applies all restrictions that have been configured for a specific system.

environment The collection of settings that users or processes are using to do their work.

epoch time In Linux, the number of seconds that have passed since epoch (corresponds to midnight on January 1, 1970). Some utilities write epoch time instead of real clock time.

escaping In a shell environment, using special syntax to ensure that specific characters are not interpreted by the shell. Escaping may be necessary to show specific characters onscreen or to ensure that regular expression metacharacters are not interpreted by the bash shell first.

exec A system call that replaces the current process with another one. *See also* fork.

export In NFS, a directory that is shared on an NFS server to allow access to other servers.

Ext2, Ext3, and Ext4 Three different versions of the Ext file system. Up to RHEL 6, Ext4 was the default file system. It is now considered inadequate for modern storage needs, which is why Ext4 in RHEL 7 was replaced by XFS as the default file system.

extended partition A solution to create more than four partitions on an MBR disk. On MBR disks, a maximum of four partitions can be stored in the partition table. To make it possible to go beyond that number, one of the four partitions can be created as an extended partition. Within an extended partition, logical partitions can be created, which will perform just like regular partitions, allowing system administrators to create more partitions.

external command A command that exists as a file on disk.

F

facility In rsyslogd, the source where log information comes from. A strictly limited number of facilities have been defined in rsyslogd.

Fedora The free and open source Linux distribution that is sponsored by Red Hat. In Fedora, new features are provided and tested. Some of these features will be included in later releases of Red Hat Enterprise Linux.

FHS *See* Filesystem Hierarchy Standard.

file descriptor A pointer that is used by a Linux process to refer to files that are in use by the process.

file system A logical structure that is created on a storage device. In a Linux file system, inodes are used for file system administration, and the actual data is written to blocks. *See also* inode.

Filesystem Hierarchy Standard (FHS) A standard that defines which Linux directories should be used for which purpose. Read **man 7 file-hierarchy** for a specification of the FHS.

firewall A solution that can be used to filter packets on a network. Firewalls are used to ensure that only authorized traffic can reach a system. A firewall can be offered through the Linux kernel netfilter functionality but often is also offered as an appliance on the network.

firewalld The modern service (replacing iptables) that is used since RHEL 7 to implement firewalling based on the Linux kernel firewalling framework.

folder Also referred to as a directory, a structure in the file system used to organize files that belong together.

foreground process A process that is running on a system and occupies the console it is running on. Linux processes that are started by users can be started in the foreground or in the background. If a process has been started as a foreground process, no other processes can be started in the same terminal until it finishes or is moved to the background. *See also* background process.

fork A system call that starts a new process as a child of the current process. This is the default way commands are executed. *See also* exec.

fstab A configuration file that is used on Linux to mount file systems automatically when the system starts.

fully qualified domain name (FQDN) A complete DNS hostname that contains the name of the host (like myserver), as well as the DNS domain it is used in (like example.com).

G

GECOS A field in the `/etc/passwd` file that can be used to store personal data about a user on the Linux operating system. GECOS originally stood for General Electric Comprehensive Operating Supervisor.

globally unique ID (GUID) An identification number that consists of parts that ensure that it is globally unique.

GPT *See* GUID Partition Table.

group A collection of items. In user management, a group is used to assign permissions to multiple users simultaneously. In Linux, every user is a member of at least one group.

group owner The group that has been set as the owner of a file or a directory. On Linux, every file and directory has a user owner and a group owner. Group ownership is set when files are created, and unless configured otherwise, it is set to the primary group of the user who creates the file.

GRUB 2 The boot loader that is installed on most systems that need to start Linux. GRUB 2 provides a boot prompt from which different kernel boot options can be entered, which is useful if you need to troubleshoot the boot procedure.

GUID *See* globally unique ID.

GUID Partition Table (GPT) A modern solution to store partitions on a hard disk, as opposed to the older MBR partition table. In GUID partitions, a total of 128 partitions can be created, and no difference exists between primary, extended, and logical partitions anymore.

gzip One of the most common utilities that is used for compression and decompression of files on Linux.

H

hard link A name associated with an inode. Inodes are used to store Linux files. An inode contains the complete administration of the file, including the blocks in which the file is stored. A file that does not have at least one hard link is considered a deleted file. To increase file accessibility, more than one hard link can be created for an inode.

hardware time The time that is provided by computer hardware, typically the BIOS clock. When a Linux system boots, it sets the software time based on the hardware time. Because hardware time often is inaccurate, most Linux systems use the Network Time Protocol (NTP) to synchronize the system time with a reliable time source.

hexadecimal A 16-based numbering system that is based on groups of 4 bytes. Hexadecimal numbers start with the range 0 through 9, followed by A through F. Because hexadecimal is much more efficient in computer technology, hexadecimal numbers are often used. In IPv6, IP addresses are written as hexadecimal numbers.

hypervisor A piece of computer software, firmware, or hardware that creates and runs virtual machines. In Linux, KVM is used as the common hypervisor software.

I

image The read-only instance from which a container is started.

inheritance In permission management, the situation where new files that are created in a directory inherit the permission settings from the parent directory.

init The first process that is started once the Linux kernel and initramfs have been loaded. From the init process, all other processes are started. As of RHEL 7, the init process has been replaced by Systemd.

initramfs The initial RAM file system. Contains drivers and other files that are needed in the first stages of booting a Linux system. On Red Hat Enterprise Linux, the initramfs is generated during installation and can be manually re-created using the **dracut** utility.

inode A structure that contains the complete administration of a file. Every Linux file has an inode, and the inode contains all properties of the file but not the filename.

input module In rsyslog, a module that allows rsyslog to receive log messages from specific sources.

interface In Linux networking, the set of configuration parameters that can be activated for a specific device. Several interface configurations can exist for a device, but only one interface can be active at a time for a device.

internal command A command that is a part of the shell and does not exist as a file on disk.

Internet Protocol (IP) The primary communications protocol that is used by computers for communication. The Internet Protocol exists in two versions (IPv4 and IPv6). Apart from node addressing, it defines routing, which enables nodes to contact one another.

IP See Internet Protocol.

iptables An older solution to create firewall rules on the Linux operating system. It interfaces with the netfilter Linux kernel firewalling functionality and was the default solution to create software firewalls on earlier versions of RHEL. As of RHEL 7, iptables has been replaced by firewalld.

IPv4 Version 4 of the Internet protocol. It was developed in the 1970s and introduced in 1981. It allows a theoretical maximum of about 4 billion nodes to be addressed by using a 32-bit address space. It is still the most important IP version in use.

IPv6 Version 6 of the Internet protocol. It was developed in the 1990s to address the shortage in IPv4 addresses. It uses a 128-bit address space that allows for addressing $3,4e38$ nodes and thus is considered a virtually unlimited address space.

iteration In shell scripting, one time of many that a conditional loop has been processed until the desired result has been reached.

J

job In a Linux shell, a task running in the current terminal. Jobs can be started in the foreground and in the background. Every job is also visible as a process.

journalctl The command used to manage `systemd-journald`.

journald *See* `systemd-journald`.

K

kernel The central component of the operating system. It manages I/O requests from software and translates them into data processing instructions for the hardware in the computer.

kernel ring buffer A part of memory where messages that are generated by the kernel are stored. The **dmesg** command enables you to read the contents of the kernel ring buffer.

kernel space The part of memory that is reserved for running privileged instructions. Kernel space is typically accessible by the operating system kernel, kernel extensions, and most device drivers. Applications normally run in user space, which ensures that a faulty application cannot crash the computer system.

Kernel-based Virtual Machine (KVM) The Linux kernel module that acts as a hypervisor and makes it possible to run virtual machines directly on top of the Linux kernel.

key-based login In SSH, login that uses public/private keys to prove the identity of the user who wants to log in. Key-based login is generally considered more secure than password-based login.

kill A command that can be used to send a signal to a Linux process. Many signals are defined (see **man 7 signal**), but only a few are commonly used, including `SIGTERM` and `SIGKILL`, both of which are used to stop processes.

Kubernetes The standard in container orchestration and also the foundation of Red Hat OpenShift.

KVM *See* Kernel-based Virtual Machine.

L

label A name that can be assigned to a file system. Using labels can be a good idea, because once a label is assigned, it will never be changed, which guarantees that the file system can still be mounted, even if other parameters such as the device name have changed. However, UUIDs are considered safer than labels because the chance of having a duplicate label by accident is much higher than the chance of having a duplicate UUID. *See also* universally unique ID (UUID).

line anchor In regular expressions, a character that refers to a specific position in a line.

linger The Systemd feature that is needed to start Systemd user units at system boot and not at user login.

Linux A UNIX-like operating system that consists of a kernel that was originally developed by Linus Torvalds (hence the name Linux). A current Linux operating system consists of a kernel and lots of open source tools that provide a complete operating system. Linux is packaged in the form of a distribution. Currently, Red Hat Enterprise Linux is among the most widely used Linux distributions.

log rotation A service that ensures that log files cannot grow too big. Log files are monitored according to specific parameters, such as a maximum age or size. Once this parameter is reached, the log file will be closed and a new log file will be opened. Old log files are kept for a limited period and will be removed, often after only a couple of weeks.

logical extent The building block that is used in LVM to create logical volumes. It normally has a size of a few megabytes that corresponds to the size of the physical extents that are used.

logical partition A partition that is created in an extended partition. *See also* extended partition.

logical volume In LVM, the entity on which a file system is created. Logical volumes are often used on RHEL because they offer important advantages, such as the option to dynamically resize the logical volume and the file system that it hosts.

Logical Volume Manager (LVM) The software that makes it possible to work with logical volumes.

login shell The shell that is opened directly after a user has logged in.

LVM *See* Logical Volume Manager.

M

masquerading A solution that enables a private IP address range that is not directly accessible from outside networks to be accessed by using one public IP address that is exposed on a router. This is also referred to as Network Address Translation (NAT).

Master Boot Record (MBR) On a BIOS system, the first 512 bytes on the primary hard disk. It contains a boot loader and a partition table that give access to the different partitions on the hard disk of that computer.

MBR *See* Master Boot Record.

module A piece of snap-in code. Modules are used by several systems on Linux, such as the kernel, GRUB 2, rsyslog, and more. Via modules, Linux components can be extended easily, and adding functionality does not require a total rewrite of the software.

module (in dnf) A collection of software packages that can be managed as one entity and can contain different versions of a software solution.

mount A connection that is made between a device and a directory. To access files on specific storage devices, the storage device needs to be mounted on a directory. This sets up the specified directory as the access point to files on the storage device. Mounts are typically organized by the system administrator and are not visible to end users.

multiplier In regular expressions, a character that indicates that multiples of the previous character are referred to.

N

namespace An isolated environment that is created by the Linux kernel and allows for running containers in complete isolation. Namespaces exist for multiple aspects of the operating system, including mounts, processes, users, and more.

netfilter The part of the Linux kernel that implements firewalling.

netmask *See* subnet mask.

Network Address Translation (NAT) *See* masquerading.

Network File System (NFS) A common UNIX solution to export physical file systems to other hosts on the network. The other hosts can mount the exported NFS directory in their local file system.

network time Time that is provided on the network.

Network Time Protocol (NTP) A standard that is used to provide reliable time to servers in a network. NTP on RHEL 9 is implemented by the `chronyd` service.

NFS *See* Network File System.

nftables The service that manages kernel firewalling. It is a replacement of the older `iptables` service.

nice A method to change the priority of Linux processes. A negative `nice` value will make the process more aggressive, giving it a higher priority (which is expressed by a lower priority number); a positive `nice` value will make a process less eager so that it gives priority to other processes.

NTP *See* Network Time Protocol.

O

octal A numbering scheme that uses the numbers 0 through 7 only. Used when working with Linux permissions using the `umask` setting or the `chmod` command.

OpenShift The Red Hat platform, based on Kubernetes, that is used for container orchestration.

OR A logical operation where the second command is executed only if the first command is not able to execute.

orchestration The technique that ensures containers can be offered in a scalable and redundant way in corporate environments.

output module In `rsyslog`, a module that is used to send log messages to a specific destination. Output modules make `rsyslogd` flexible and allow for the usage of log destinations that are not native to `rsyslog`.

ownership In file system permissions, the basis of the effective permissions that a user has. Every file has a user owner and a group owner assigned to it.

P

package A bundle that is used to distribute software. A package typically contains a compressed archive of files and metadata that includes instructions on how to install those files.

package group A group of packages that can be installed as such using the `dnf groups install` command.

package group (in dnf) A group of software packages that can be installed with a single command.

pager A program that can be used to browse page by page through a text file. The **less** utility provides one of the most common Linux pagers.

parent shell The environment from which a shell script or program is started. Processes or child scripts will inherit settings from the parent shell.

partition A subdivision of a hard disk on which a file system can be created to mount it into the directory structure.

passphrase Basically a password, but is supposed to be longer and more secure than a password.

password A token that is used in authentication. The password is a secret word that can be set by individual users and will be stored in an encrypted way.

path The complete reference to the location of a file.

permissions Attributes that can be set on files or directories to allow users or groups access to these files or directories.

permissive mode The SELinux mode where nothing is blocked but everything is logged in the audit log. This mode is typically used for troubleshooting SELinux issues.

physical extent The physical building block that is used when creating LVM physical volumes. Typically, the size is multiple megabytes.

physical volume The foundation building block of an LVM configuration. The physical volume typically corresponds to a partition or a complete disk device.

PID *See* process identification number.

pipe A structure that can be used to forward the output of one command to be used as input for another command.

policy *See* SELinux policy.

port A number that is used by a process to offer access to the process through a network connection.

port forwarding A firewalling technique where traffic that is coming in on a specific port is forwarded to another port that may be on the same host or on a different host.

Portable Operating System Interface (POSIX) A standard that was created to maintain compatibility between operating systems. The standard mainly applies to UNIX and guarantees that different flavors of Linux and UNIX are compatible with one another.

portmapper A Remote Procedure Call service that needs to run on systems that provide RPC services. Portmapper uses dynamic ports that do not correspond to

specific TCP or UDP ports; the service will pick a UDP or TCP port that will be used as long as the process is active. When the process is restarted, chances are that different ports are used. They need to be mapped to fixed UDP and TCP ports in order to make it possible to open the firewall for these ports. Portmapper is still used by components of the NFS service.

POSIX *See* Portable Operating System Interface.

primary group The group that is listed in the group membership field for a user in `/etc/passwd`. Every Linux user is a member of a primary group. Apart from that, users can be made a member of secondary groups as well.

primary partition In MBR, one of a maximum of four partitions that can be created in the Master Boot Record. *See also* extended partition.

priority (in process handling) Specifies the importance of a process. Process priority is expressed with a number (which can be modified using **nice**). Processes with a lower priority number are serviced before processes with a higher priority number.

priority (in rsyslog) Used to specify the severity of a logged event. Based on the severity, specific actions can be taken.

private key In public/private key encryption, the key that is used to generate encrypted data.

privileged user *See* root.

proc A kernel interface that provides access to kernel information and kernel tunables. This interface is available through the `/proc` file system.

process A task that is running on a Linux machine. Roughly, a process corresponds to a program, although one program can start multiple processes.

process identification number (PID) A unique number that is used to identify a process running on a Linux system.

profile In **tuned**, a collection of performance settings that can easily be applied.

protocol A set of rules that is used in computing, such as in computer networking, to establish communications between two computers.

public key In cryptography, the key that is typically sent by a server to a client so that the client can send back encrypted data.

PV *See* physical volume.

Q

queue In process management, where processes wait before they can be executed.

R

real-time clock (RTC) The hardware clock that is installed on the computer motherboard.

reboot The procedure of stopping the computer and starting it again.

Red Hat Customer Portal The platform that Red Hat offers to provide patches for customers that have an active subscription. To provide these patches and updates, Red Hat Network provides the repositories that are needed for this purpose.

Red Hat Enterprise Linux (RHEL) The name of the software that Red Hat sells subscriptions for. It is available in a server edition and a desktop edition.

Red Hat Package Manager (RPM) The name for the package format that is used on RHEL for software packages and for the Package Management software. RPM has become the standard for package management on many other Linux distributions as well.

reference clock A clock that is used as a time source in an NTP time configuration. Typically, a reference clock is a highly reliable clock on the Internet, but it can be an internal clock on the computer's motherboard as well.

registry A location where container images are started from.

regular expression A search pattern that allows users to search text patterns in a flexible way. Not to be confused with shell metacharacters.

relative filename A filename that is relative to a directory that is not the root directory.

Remote Procedure Calls (RPC) A method for interprocess communication that allows a program to execute code in another address space. Remote Procedure Calls is an old protocol and as such is still used in the Network File System.

repository An installation source that contains installable packages and an index that contains information about the installable packages so that the installation program **dnf** can compare the version of packages currently installed with the version of packages available in the repository.

resident memory Memory pages that are in use by a program.

resolver The DNS client part that contains a list of DNS servers to contact to resolve DNS queries.

RHEL *See* Red Hat Enterprise Linux.

rich rules Rules in **firewalld** that allow the usage of a more complicated syntax so that more complex rules can be defined.

Rocky Linux Free open source alternative for Red Hat Enterprise Linux, which consists of the RHEL source code with all licensing removed.

root The privileged user account that is used for system administration tasks. User root has access to all capabilities, which means that permissions do not apply to user root and the root user account is virtually unlimited.

root directory The starting point of the file system hierarchy, noted as /.

RPC *See* Remote Procedure Calls.

RPM *See* Red Hat Package Manager.

rsyslogd The generic daemon that logs messages.

RTC *See* real-time clock.

S

Samba The name for the Linux service that implements the SMB protocol.

SAN *See* storage-area network.

scheduler The part of the Linux kernel that monitors the queue of runnable processes and allocates CPU time to these processes.

secondary group A group that a user is a member of but which membership is not defined in the /etc/passwd file. When new files are created, the secondary group will not automatically become the owner of those files.

Secure Shell (SSH) A solution that allows users to open a shell on a remote server where security is implemented by using public/private key cryptography.

Secure Sockets Layer (SSL) *See* Transport Layer Security (TLS).

SELinux A Linux kernel security module that provides a mechanism for supporting access control security policies.

SELinux Policy The collection of rules that is used to define SELinux security.

Server Message Block (SMB) An application-level protocol that is used to provide shared access to files, printers, and serial ports, which on Linux is implemented in the Samba server.

service (in firewalld) A configuration of firewall settings that is used to allow access to specific processes.

services (in Systemd) Processes that need to be started to provide specific functionality.

share A directory to which remote access is configured using a remote file system protocol such as NFS or CIFS.

shebang The characters used in a script to indicate which shell should be used for executing the code in the shell script. If no shebang is used, the script code will be interpreted by the parent shell, which may lead to errors in some cases. A shebang starts with a #, which is followed by a ! and the complete pathname of the shell, such as `#!/bin/bash`.

shell The environment from which commands can be executed. Bash is the default shell on Linux, but other shells exist as well.

shell metacharacters Characters such as *, ?, and [a-z] that allow users to refer to characters in filenames in a flexible way.

signal An instruction that can be sent to a process. Common signals exist, such as SIGTERM and SIGKILL, but the Linux kernel allows a total of 32 different signals to be used. To send a signal to a process, use the **kill** command.

SMB *See* Server Message Block.

snapshot A “photo” of the actual state of a file system.

software time *See* system time.

source context In SELinux, the context of the processes or users that initiate an action. A context in SELinux is a label that identifies allowed operations. Everything in an SELinux environment has a context.

SSH *See* Secure Shell.

standard error (STDERR) The default location where a program sends error messages.

standard input (STDIN) The default location where a program gets its input.

standard output (STDOUT) The default location where a program sends its regular output.

star A legacy extended version of **tar**, which offers support for extended attributes. Currently no longer required, as all of its functionality has been integrated in **tar**.

static route A route that is defined manually by a network administrator.

STDERR *See* standard error.

STDIN *See* standard input.

STDOUT *See* standard output.

storage-area network (SAN) A solution where disk devices are shared at a block level over the network. As such, they can be used in the same way as local disk devices on a Linux system. iSCSI and Fibre Channel are the common SAN protocols.

Stratis The new volume managing file system that was introduced in RHEL 8.

stratum In time synchronization, used to indicate the distance between a server and an authoritative Internet time source.

subnet mask A logical subdivision of an IP network.

subshell A shell that is started from another shell. Typically, a subshell is started by running a shell script.

symbolic link A special type of file that contains a reference to another file or directory in the form of an absolute or relative path.

sysfs The kernel interface that is mounted on the /sys directory and which is used to provide access to parameters that can be used for managing hardware settings.

system call A low-level operating system instruction.

system time The time that is maintained by the operating system. When a Linux system boots, system time is set to the current hardware time, and while the operating system is running, it is often synchronized using the Network Time Protocol (NTP).

Systemd The service manager on RHEL 9. Systemd is the very first process that starts after the kernel has loaded, and it takes care of starting all other processes and services on a Linux system.

systemd-journald The part of Systemd that takes care of logging information about events that have been happening. The introduction of journald ensures that information about all services can be logged, regardless of how the service itself is configured to deal with information that is to be logged.

T

tainted kernel A kernel in which unsupported kernel modules have been loaded.

tar The Tape Archiver; the default Linux utility that is used to create and extract backups.

target In Systemd, a collection of unit files that can be managed together.

target context The SELinux context that is set to a target object, such as a port, file, or directory.

terminal Originally, the screen that was used by a user to type commands on. On modern Linux systems, pseudo terminals can be used as a replacement. A pseudo terminal offers a shell window from which users enter the commands that need to be executed.

thin allocation In storage, an approach that enables the system to present more storage to the storage user than what is really available by using smart technologies to store data, like deduplication.

thread A thread is a subdivision of a process. Many processes are single threaded, which means that process is basically one entity that needs to be serviced. On a multicore or multi-CPU computer system, working with multithreaded processes makes sense. That way, the different cores can be used to handle the different threads, which allows a process to benefit from multicore or multithreaded environments.

time synchronization A system that ensures that multiple servers are using the exact same time. To accomplish time synchronization, it is common to use an external time server, as defined in the Network Time Protocol (NTP).

timer A Systemd unit type that can be used as an alternative to cron jobs and run units at a specific time.

timestamp An identifier that can be used on files, database records, and other types of data to identify when the last modification has been applied. Many services rely on timestamps. To ensure that timestamp-based systems work properly, time synchronization needs to be configured.

TLS *See* Transport Layer Security.

Transport Layer Security (TLS) A cryptographic protocol that is created to ensure secured communications over a computer network. In TLS, public and private keys are used, and certificates authenticate the counterparty. TLS was formerly known as SSL.

TTY A program that provides a virtual terminal on Linux. Every terminal still has a TTY name, which is either `tty1-6` for virtual TTYs or `/dev/pts/0-nn` for pseudo terminals.

tuned A service on RHEL that enables administrators to easily apply performance settings by using profiles.

U

udev A service that works with the Linux kernel to initialize hardware.

UEFI *See* Unified Extensible Firmware Interface.

umask An octal value that defines the default permissions as a shell property.

umount The command that is used to decouple a file system from the directory on which it is mounted.

Unified Extensible Firmware Interface (UEFI) A replacement of the Basic Input/Output System used on older IBM-compatible computers as the first program that runs when the computer is started. UEFI is the layer between the operating system and the computer firmware.

unit An item that is managed by Systemd. Different types of units exist, including service, path, mount, and target units.

universally unique ID (UUID) An identification number consisting of a long random hexadecimal number that is globally unique.

unprivileged user A regular non-root user account to which access restrictions apply, as applied by permissions.

user An entity that is used on Linux to provide access to specific system resources. Users can be used to represent people, but many services also have a dedicated user account, which allows the service to run with the specific permissions that are needed for that service.

user space The area of memory that is accessible by application software that has been started with non-root privileges.

UTC *See* Coordinated Universal Time.

UUID *See* universally unique ID.

V

value The data that is assigned to a specific property, variable, or record.

variable A label that contains a specific value that can be changed dynamically. In scripting, variables are frequently used to allow the script to be flexible.

VFAT The Linux kernel driver that is used to access FAT-based file systems. FAT is a commonly used file system in Windows environments. The Linux VFAT driver allows usage of this file system.

VG *See* volume group.

virtual host In the Apache web server, a collection of configuration settings that is used to address a web server. What makes it a virtual host is that one installation of the Apache web server can be configured with multiple virtual hosts, which allows administrators to run multiple websites on one Apache server.

virtual memory The total amount of addressable memory. Virtual memory is called *virtual* memory because it does not refer to memory that really exists. Its only purpose is to make sure that Linux programs can set an address pointer that is unique and not in use by other programs.

volume group (VG) The abstraction layer that in Logical Volume Manager is used to represent all available storage presented by physical volumes from which logical volumes can be created.

W

want An indication for a Systemd unit file that it is supposed to be started from a specific Systemd target.

wildcard The * character, which in a shell environment refers to an unlimited number of any characters.

X

XFS A high-performance 64-bit file system that was created in 1993 by SGI and which in RHEL 9 is used as the default file system.

Xz A compression utility that can be used as an alternative to gzip or bzip2.

Y

Yellowdog Update, Modified The full name for Yum, the meta package handler that on older versions of RHEL was used to install packages from yum repositories. Now replaced with **dnf**.

Yum See Yellowdog Update, Modified.

Z

zombie A process that has lost contact with its parent and for that reason cannot be managed using regular tools.

zone In firewalld, a collection of one or more network interfaces that specific firewalld rules are associated with.