RED HAT CERTIFIED SYSTEMS ADMIN (RHCSA) EX200 PRACTICE EXAM (SAMPLE)

STUDY GUIDE

Prepare with structure. Pass with confidence

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. Which command lists all currently loaded service units?

A. systemctl list-unit-files --type=service

B. systemctl status --type=service

C. systemctl show --type=service

D. systemctl list-units --type=service

2. Which command would set a user's password to expire in 90 days and warn 7 days before expiration?

A. chage -M 90 -W 7 username

B. passwd -w 7 -t 90 username

C. chage -e 90 -W 7 username

D. chage -m 90 -W 7 username

3. Which command removes all ACL entries from a file named file1?

A. setfacl --clear file1

B. setfacl -x all file1

C. setfacl --remove-all file1

D. setfacl --remove-default file1

4. In an Access Control List (ACL) enabled file, which component defines the maximum effective permissions that can be granted to all entries?

A. The file owner

B. The ACL mask

C. The default ACL

D. The owner permissions

5. Which command lists processes owned by a given user with their PIDs and names?

A. pgrep -u <username> -l

B. ps -u <username> -o pid,etimes

C. top -u <username>

D. pkill -u <username>

6. Which form redirects both standard output and standard error to the same file in a Bash shell?

A. command > File 2>&1

B. command 2> File

C. command > File

D. command &> File

7. What do scp and sftp refer to?

A. Secure Copy Protocol and SSH File Transfer Protocol

B. Secure Copy and SSH File Transfer Protocol

C. Secure Copy and Secure File Transfer Protocol

D. Secure Copy Protocol and Secure File Transfer Protocol

8. Which command lists all yum repositories, including both enabled and disabled?

A. yum repolist all

B. yum repolist enabled

C. yum repos

D. yum list repos

9. Which command identifies which package provides a given file, with example /bin/ls?

A. dnf list /bin/ls

B. dnf provides /bin/ls

C. dnf search /bin/ls

D. dnf info /bin/ls

10. Which approach configures log rotation to run daily and keep 14 rotated logs?

A. Create a /etc/logrotate.d/<name> with daily and rotate 14; then run logrotate -f /etc/logrotate.conf to test or apply

B. Edit /etc/logrotate.conf to set daily and rotate 14 and run logrotate

C. Use logrotate -d to simulate daily rotation

D. Use crontab to run logrotate daily

Answers

1. D
2. A
3. C
4. B
5. A
6. D
7. C
8. A
9. B
10. A

Explanations

1. Which command lists all currently loaded service units?

A. systemctl list-unit-files --type=service

B. systemctl status --type=service

C. systemctl show --type=service

D. systemctl list-units --type=service

You're being tested on how to see which systemd units are currently loaded into memory, specifically the service units. The command that lists those loaded units is systemctl list-units with a type filter for services. This command shows you the units that systemd has actively loaded, along with their current state (load, active, and sub state) and a short description. Filtering by type=service ensures you only see service units, not other unit types like sockets or timers. The other options don't fit this purpose. Listing unit files shows definitions on disk, not what's currently loaded in memory. Asking for status or show targets a particular unit (or a set of units) to display details about it, not a comprehensive list of all loaded services. So the command that correctly lists all currently loaded service units is the one that queries the in-memory set of units and restricts the output to services.

2. Which command would set a user's password to expire in 90 days and warn 7 days before expiration?

A. chage -M 90 -W 7 username

B. passwd -w 7 -t 90 username

C. chage -e 90 -W 7 username

D. chage -m 90 -W 7 username

Managing when a password must be changed is done with the chage command. The two key options are -M, which sets the maximum number of days the password is valid, and -W, which specifies how many days before that expiry to warn the user. Setting -M to 90 means the password will expire after 90 days, and setting -W to 7 makes the system start warning the user 7 days before the expiry. Using both for the target user with chage -M 90 -W 7 username gives the desired behavior: a 90-day password life with a 7-day warning window. Other choices don't fit: a passwd option set is not appropriate for this aging configuration; -e would define an absolute account expiration date, not a password expiry; -m would set a minimum interval between changes, not the expiration itself.

3. Which command removes all ACL entries from a file named file1?

A. setfacl --clear file1

B. setfacl -x all file1

C. setfacl --remove-all file1

D. setfacl --remove-default file1

The concept being tested is how to remove every additional access rule attached to a file, i.e., clearing all ACL entries so the file is governed only by its standard permission bits (owner, group, others). The best command is the one that instructs the tool to remove all ACL entries in one go. This option tells setfacl to delete every ACL entry associated with the file, leaving no extra per-file permissions behind. After this, only the normal file permissions remain in effect. Why the other forms aren't suitable: removing a single entry with -x requires specifying exactly which ACL entry to delete, so it cannot wipe out everything in one go. Removing only the default ACL would affect only default entries (often used for directories), not the entire ACL set on the file. The explicit remove-all option targets the complete clearing of all ACL entries, which is precisely what you want when you need to reset the file to standard permissions.

4. In an Access Control List (ACL) enabled file, which component defines the maximum effective permissions that can be granted to all entries?

A. The file owner

B. The ACL mask

C. The default ACL

D. The owner permissions

In POSIX ACLs, the component that sets the upper limit on what any named user or named group can receive is the mask entry. It acts as a cap for all user and group entries, so the effective permissions for those entries are the intersection of what the entry requests and what the mask allows. The owner's permissions and the world/other permissions are governed by the traditional owner, group, and other bits (and the world entry in the ACL), and are not constrained by the mask in the same way. If a named entry asks for more rights than the mask permits, the mask wins and the entry's actual rights are limited accordingly. This is why the mask defines the maximum effective permissions that can be granted to all entries.

5. Which command lists processes owned by a given user with their PIDs and names?

A. pgrep -u <username> -l

B. ps -u <username> -o pid,etimes

C. top -u <username>

D. pkill -u <username>

Listing processes owned by a specific user with their PIDs and names is best done with a tool that filters the process table by owner and can show the PID alongside the process name. The command pgrep -u <username> -l does exactly that: -u restricts the results to processes owned by the given user, and -l prints the process name (the command name) together with the PID. This yields a straightforward list where each line contains the PID and the corresponding process name, which matches the requested output. Other commands aren't as direct for this exact need. ps can show PIDs and names if you tailor the output (for example, ps -u <user> -o pid,comm), but pgrep with -u and -l provides the concise, on-demand listing in a single command. Top is interactive and focused on real-time monitoring by default, and pkill is for signaling processes rather than listing them.

6. Which form redirects both standard output and standard error to the same file in a Bash shell?

A. command > File 2>&1

B. command 2> File

C. command > File

D. command &> File

Redirecting both standard output and standard error to the same file in Bash uses a single, concise redirection that covers both streams at once. The &> operator tells Bash to duplicate both file descriptors (1 for stdout and 2 for stderr) into the target file, so all output lands in that file regardless of which stream produced it. This approach is straightforward and less error-prone than mixing separate redirections or needing a specific order. Other forms can achieve the same result but require more care. For example, redirecting stdout to a file and then redirecting stderr to the same destination (command > File 2>&1) does work, but it depends on the order of redirections being exactly right; a small mistake can send one stream elsewhere. Redirecting only one stream (command > File or command 2> File) does not send both streams to the file, only stdout or only stderr respectively.

7. What do scp and sftp refer to?

A. Secure Copy Protocol and SSH File Transfer Protocol

B. Secure Copy and SSH File Transfer Protocol

C. Secure Copy and Secure File Transfer Protocol

D. Secure Copy Protocol and Secure File Transfer Protocol

Scp and sftp are two secure ways to move files over a network using SSH. SCP stands for Secure Copy Protocol, and it provides a straightforward way to copy files between hosts over an SSH connection. It's simple and fast for single transfers but isn't designed for interactive file management or advanced operations. Sftp stands for SSH File Transfer Protocol, a separate protocol that runs over SSH and offers a full file-transfer interface, either interactively or via batch commands. You can list directories, transfer multiple files, create and remove directories, and manage files with more control. While some sources loosely call it a "Secure File Transfer Protocol," the standard and precise name is SSH File Transfer Protocol, which is why that form is the most accurate for sftp.

8. Which command lists all yum repositories, including both enabled and disabled?

A. yum repolist all

B. yum repolist enabled

C. yum repos

D. yum list repos

This tests how to view every yum repository defined on the system, including those that aren't currently enabled. The command that does this is yum repolist all, which lists every repository found in the yum configuration and marks which ones are enabled and which are disabled. If you instead use yum repolist enabled, you'll only see the repositories that are active right now, not the disabled ones. Other commands like yum repos or yum list repos aren't valid for listing repositories and won't provide the full set.

9. Which command identifies which package provides a given file, with example /bin/ls?

A. dnf list /bin/ls

B. dnf provides /bin/ls

C. dnf search /bin/ls

D. dnf info /bin/ls

To find which package owns a specific file, use a provides query. Running the command that provides /bin/ls asks the package manager to search its metadata for the package that supplies that exact file. It will typically respond with the package (such as coreutils) that includes the /bin/ls binary. This is the direct and reliable way to map a filesystem file to its owning package. Other commands don't target file ownership. Listing packages with dnf list /bin/ls shows packages by name or status, not which one contains that file. Searching with dnf search /bin/ls looks through package names and descriptions, not the actual file-provides data. Asking for info on /bin/ls (dnf info /bin/ls) treats the argument as a package name, which won't resolve the file-to-package relationship. If you know the package name, you can use dnf info on that package, or you can use rpm -qf /bin/ls as an alternative way to find the owning package.

10. Which approach configures log rotation to run daily and keep 14 rotated logs?

A. Create a /etc/logrotate.d/<name> with daily and rotate 14; then run logrotate -f /etc/logrotate.conf to test or apply

B. Edit /etc/logrotate.conf to set daily and rotate 14 and run logrotate

C. Use logrotate -d to simulate daily rotation

D. Use crontab to run logrotate daily

Log rotation is driven by a main configuration that includes per-log rules. The preferred approach is to put a dedicated rule for the specific log under /etc/logrotate.d, where you set daily to rotate each day and rotate 14 to keep the latest 14 rotated backups. Since /etc/logrotate.conf includes the files in /etc/logrotate.d, adding your own file automatically becomes part of the overall rotation policy. Running logrotate with the main configuration, for example logrotate -f /etc/logrotate.conf, applies the rules immediately (the -f flag forces rotation, which is useful for testing or applying right away). This modular method is better than editing the central file because it keeps policies isolated and easier to manage. Using -d would only simulate rotation, not perform it, and relying on a separate crontab entry to run logrotate daily bypasses the built-in, centralized scheduling and configuration mechanism.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://rhcsaex200.examzify.com

We wish you the very best on your exam journey. You've got this!