

# TestOut Labs Practice Test (Sample)

## Study Guide



**Everything you need from our exam experts!**

**Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.**

**ALL RIGHTS RESERVED.**

**No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.**

**Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.**

**SAMPLE**

# Table of Contents

<b>Copyright</b> .....	<b>1</b>
<b>Table of Contents</b> .....	<b>2</b>
<b>Introduction</b> .....	<b>3</b>
<b>How to Use This Guide</b> .....	<b>4</b>
<b>Questions</b> .....	<b>5</b>
<b>Answers</b> .....	<b>8</b>
<b>Explanations</b> .....	<b>10</b>
<b>Next Steps</b> .....	<b>15</b>

SAMPLE

# 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

SAMPLE

- 1. Which command shows all supplementary groups for a user?**
  - A. whoami**
  - B. groups cflynn**
  - C. id cflynn**
  - D. ls -l /home/cflynn**
  
- 2. In the Kerberos policy, what is the maximum lifetime for a user ticket?**
  - A. 3 hours**
  - B. 180 minutes**
  - C. 1 minute**
  - D. 3 days**
  
- 3. Which OUs should the Workstation Settings GPO be linked to?**
  - A. Marketing; Sales; Support**
  - B. CorpNet.local only**
  - C. Marketing > TempMarketing; Sales > TempSales; Support**
  - D. Sales > TempSales only**
  
- 4. What is the update interval configured for Snort rules?**
  - A. 1 Day**
  - B. 12 Hours**
  - C. 1 Hour**
  - D. 7 Days**
  
- 5. What is the purpose of the Windows Registry and what is a safe practice when editing it?**
  - A. The Registry stores configuration; back up before editing and avoid making changes unless documented**
  - B. The Registry is the device driver store; always edit without backup**
  - C. The Registry is used for scheduling tasks; back up after editing**
  - D. The Registry is a temporary storage for user files; edit freely**

- 6. What port/protocol combination is used for the DNS block/allow rules in pfBlockerNG?**
- A. TCP 53**
  - B. UDP 80**
  - C. UDP 443**
  - D. UDP 53**
- 7. How long can you defer a feature update in Windows Update Advanced options?**
- A. 30 days**
  - B. 90 days**
  - C. 0 days**
  - D. 60 days**
- 8. Which statement best describes the role of apt-get, yum, and dnf?**
- A. They are virtualization tools.**
  - B. They are package managers for Linux distributions.**
  - C. They are text editors.**
  - D. They are firewall configuration utilities.**
- 9. How do you add a process exclusion for welcome.scr in Windows Defender?**
- A. Exclusions > Add an exclusion; then select Process. In the Enter process name field, type welcome.scr; then select Add.**
  - B. Quarantine > Add exception**
  - C. Virus & threat protection settings > Manage exclusions > Add process**
  - D. Threat protection updates > Add new exclusion**
- 10. In the email filtering lab, which setting ensures only emails from the safe senders list are allowed?**
- A. Exclusive**
  - B. Normal**
  - C. Moderate**
  - D. Strict**

## Answers

SAMPLE

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

SAMPLE

## **Explanations**

SAMPLE

1. Which command shows all supplementary groups for a user?

- A. whoami
- B. groups cflynn**
- C. id cflynn
- D. ls -l /home/cflynn

To see what groups a user belongs to, use the groups command followed by the username. This prints the names of all groups that user is a member of, which includes the primary group and any supplementary groups they've been added to. So, running groups with the username shows all the groups for that user, directly answering the question about their supplementary memberships. For comparison, whoami only prints the current user's name, id shows UID, GID, and all group memberships (giving more detail than just the list), and listing a directory has no relevance to group memberships.

2. In the Kerberos policy, what is the maximum lifetime for a user ticket?

- A. 3 hours**
- B. 180 minutes
- C. 1 minute
- D. 3 days

In Kerberos, tickets are time-bound to limit how long a stolen credential could be misused. A user ticket (the TGT) has a maximum lifetime set by policy, which defines the longest period that ticket can remain valid before a new authentication is required. Setting this to three hours provides a balance: it allows users to stay logged in for a reasonable period without re-authenticating, while keeping the exposure window short enough to reduce risk if the ticket is compromised. After those three hours (or if renewal isn't permitted or is exhausted), the user must re-authenticate to obtain a fresh TGT. Service tickets, issued for specific services, generally have shorter lifetimes and can be renewed within policy, but the overall maximum for the user ticket remains the limiting factor.

3. Which OUs should the Workstation Settings GPO be linked to?

- A. Marketing; Sales; Support
- B. CorpNet.local only
- C. Marketing > TempMarketing; Sales > TempSales; Support**
- D. Sales > TempSales only

In Active Directory, the scope of a GPO is determined by where it's linked and the OU structure beneath it. To apply workstation settings only to the intended machines, link the Workstation Settings GPO to the temporary sub-OUs that actually contain those computers—TempMarketing under Marketing, TempSales under Sales, and TempSupport under Support. This confines the policy to the specific temporary workstations you want to configure, while leaving the permanent department machines untouched. Linking to the broader Marketing, Sales, or Support OUs would apply the settings to all devices in those departments, which is usually not desired. Linking to the domain root or a top-level domain would apply the policy even more broadly, often unwanted. By targeting the Temp sub-OUs, you achieve precise, manageable scope for the workstation settings.

**4. What is the update interval configured for Snort rules?**

- A. 1 Day**
- B. 12 Hours**
- C. 1 Hour**
- D. 7 Days**

Rule updates for Snort are about how often the system pulls in new rule signatures. The update interval sets the schedule for refreshing the rule set from your rule source. A daily interval fetches the latest rules once every 24 hours, which is a solid balance: you stay reasonably current with new threats while keeping network traffic and processing overhead manageable. More frequent pulls (every 12 hours or every hour) increase overhead and may yield diminishing returns for many environments. Less frequent updates (every 7 days) leave you vulnerable to newer signatures for longer. So the configured update interval is daily.

**5. What is the purpose of the Windows Registry and what is a safe practice when editing it?**

- A. The Registry stores configuration; back up before editing and avoid making changes unless documented**
- B. The Registry is the device driver store; always edit without backup**
- C. The Registry is used for scheduling tasks; back up after editing**
- D. The Registry is a temporary storage for user files; edit freely**

The Registry is a centralized database Windows uses to store configuration settings for the OS, hardware, and installed software. It contains the rules and options that Windows and programs read to determine behavior, preferences, and how components should operate. Because these settings directly affect how the system runs, making changes can have wide and sometimes harmful effects if done carelessly. A safe practice when editing is to back up before making any changes and to only modify values that are documented or clearly understood. This can be done by exporting the specific registry key you plan to edit or by creating a System Restore point. If you're unsure about a change, it's best not to edit. The other descriptions refer to different parts of Windows, such as a driver store, task scheduling, or temporary file storage, which is why they don't accurately describe the Registry's purpose.

**6. What port/protocol combination is used for the DNS block/allow rules in pfBlockerNG?**

- A. TCP 53
- B. UDP 80
- C. UDP 443
- D. UDP 53**

DNS queries primarily use port 53 and most of them travel over UDP because the requests and responses are small and fast. pfBlockerNG's DNS block/allow rules are built around this standard path, filtering traffic destined to or from UDP port 53 to control which domain lookups are permitted or blocked. While DNS can use TCP on occasions (for large responses or zone transfers), the typical and most relevant traffic for filtering is UDP 53, so that's the correct combination. Ports 80 and 443 are for web traffic, not DNS, so they aren't used for DNS filtering.

**7. How long can you defer a feature update in Windows Update Advanced options?**

- A. 30 days
- B. 90 days
- C. 0 days
- D. 60 days**

Deferring a feature update is a way to delay a major OS upgrade so you can test compatibility and prepare drivers and apps before the new version lands on devices. In Windows Update Advanced options, the available deferral window for feature updates is capped, and in this context the maximum you can set is sixty days. That's why sixty days is the best answer: it represents the longest postponement allowed in this setting, while shorter options (like thirty days) or zero days would either limit the deferral or remove it altogether. A deferral of ninety days would exceed the allowed limit in this scenario.

**8. Which statement best describes the role of apt-get, yum, and dnf?**

- A. They are virtualization tools.
- B. They are package managers for Linux distributions.**
- C. They are text editors.
- D. They are firewall configuration utilities.

These tools are package managers for Linux distributions. They automate finding, installing, updating, and removing software, and they manage software repositories and dependencies so programs get the components they need without you having to track them manually. apt-get is used on Debian- and Ubuntu-based systems, yum was the traditional manager for Red Hat-based systems, and dnf is the modern successor used on Fedora and newer Red Hat-based releases. They let you install software with simple commands like installing a package, updating the whole system, or removing software, while automatically resolving dependencies and ensuring you're pulling from trusted sources. They aren't virtualization tools, text editors, or firewall configuration utilities. Instead, they focus on managing software in the system catalog, keeping applications and their required libraries in sync with what's available in the configured repositories.

**9. How do you add a process exclusion for welcome.scr in Windows Defender?**

**A. Exclusions > Add an exclusion; then select Process. In the Enter process name field, type welcome.scr; then select Add.**

**B. Quarantine > Add exception**

**C. Virus & threat protection settings > Manage exclusions > Add process**

**D. Threat protection updates > Add new exclusion**

Excluding a specific process from Windows Defender means telling Defender not to scan or block that process while it runs. To do this, go to Windows Security, Virus & threat protection, Exclusions, then Add an exclusion, choose Process, enter the process name (for example, welcome.scr), and click Add. This path directly targets a running process and uses the correct UI to specify what to exclude. Quarantine and Add exception aren't the right paths for creating a per-process exclusion, and the option about threat protection updates isn't related to exclusions. Remember to only exclude a trusted process to avoid reducing protection.

**10. In the email filtering lab, which setting ensures only emails from the safe senders list are allowed?**

**A. Exclusive**

**B. Normal**

**C. Moderate**

**D. Strict**

This tests how strict the allowlist (safe senders list) policy is in email filtering. The safe senders list is an allowlist of trusted addresses. The Exclusive setting enforces a deny-all-else approach, meaning only emails from addresses on that safe senders list are allowed and anything not on the list is blocked. The other levels are less strict, letting non-listed senders through under some conditions, so they don't guarantee that only safe-sender messages pass. So the setting that achieves an only-allowlisted pass is Exclusive.

## 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](mailto:hello@examzify.com).**

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

**<https://testoutlabs.examzify.com>**

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

SAMPLE