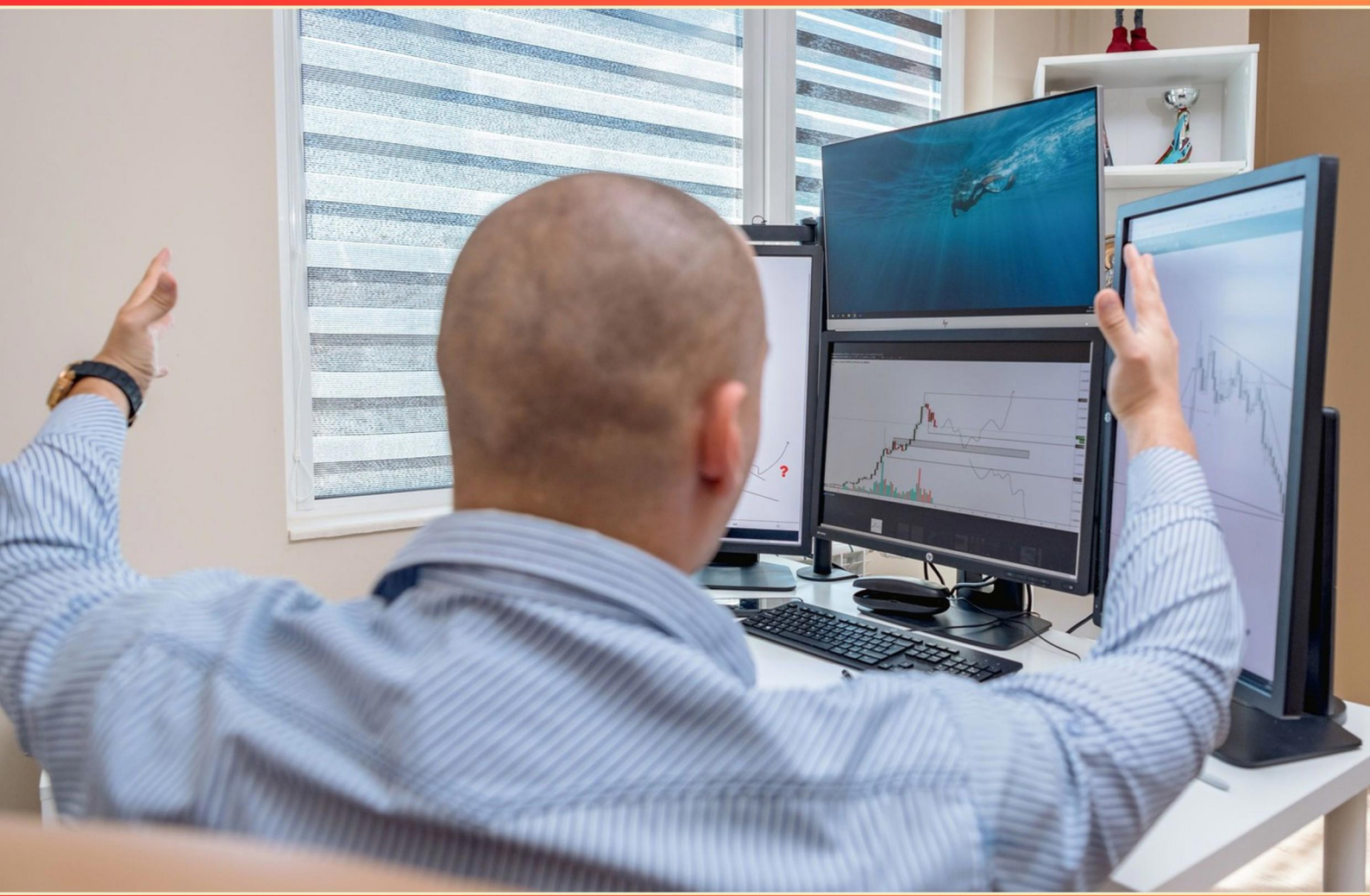
TESTOUT LABS PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://testoutlabs.examzify.com

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. What static IPv4 address and subnet were assigned to the DMZ interface?

A. 172.16.1.1/16

B. 192.168.0.1/24

C. 10.0.0.1/8

D. 172.30.0.1/16

2. Which BIOS action must be performed to enable BitLocker on the OS drive in this lab?

A. Turn on and activate TPM Security

B. Enable Secure Boot

C. Disable TPM in BIOS

D. Set BIOS to Legacy Boot

3. Explain the NTFS permissions model and the difference between DACL and SACL.

A. DACL controls access to files/folders; SACL controls auditing

B. DACL controls auditing; SACL controls access

C. DACL is discretionary; SACL is static

D. DACL encrypts data; SACL compresses

4. Which path allows restricting a user's logon to specific computers?

A. Account tab Logon Hours

B. Account tab Log On To

C. User tab Login Restrictions

D. Security tab Access Rights

5. 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

6. What is the configured Maximum Password Age in days in the Local Security Policy lab?

A. 60 days

B. 180 days

C. 90 days

D. 365 days

7. Which statement best describes IPAM's role in network management?

A. IPAM ensures IP address allocation with DNS/DHCP integration to avoid conflicts and track assets

B. IPAM manages physical server racks

C. IPAM is a replacement for DNS servers

D. IPAM encrypts IP packets for security

8. What is the primary function of a firewall?

A. Authenticate users

B. Route packets

C. Block all traffic by default

D. Filter traffic based on rules

9. Name two common wireless frequencies and discuss their typical use cases.

A. 2.4 GHz: longer range but more interference; 5 GHz: higher speed but shorter range.

B. 2.4 GHz: shorter range and less interference; 5 GHz: lower speed and more interference.

C. 900 MHz: common for Wi-Fi; 2.4 GHz and 5 GHz

D. 3 GHz and 4 GHz

10. What Tunnel Network was configured for the OpenVPN server?

A. 198.28.56.0/24

B. 198.28.20.0/16

C. 198.168.20.0/24

D. 198.28.20.0/24

Answers

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

Explanations

1. What static IPv4 address and subnet were assigned to the DMZ interface?

A. 172.16.1.1/16

B. 192.168.0.1/24

C. 10.0.0.1/8

D. 172.30.0.1/16

Isolating the DMZ relies on placing its devices on a dedicated private subnet and giving the interface a static address within that subnet. In this setup, the DMZ uses the 172.16.0.0/16 private range, so the DMZ interface should have an address that falls inside 172.16.0.0 to 172.16.255.255 with a 255.255.0.0 mask. The address 172.16.1.1 with a /16 (255.255.0.0) mask fits exactly into that DMZ subnet, making it a proper static address for the DMZ interface. The other options place the interface on different private subnets (for example, 192.168.0.0/24, 10.0.0.0/8, or 172.30.0.0/16), which do not correspond to the designated DMZ network in this configuration.

2. Which BIOS action must be performed to enable BitLocker on the OS drive in this lab?

A. Turn on and activate TPM Security

B. Enable Secure Boot

C. Disable TPM in BIOS

D. Set BIOS to Legacy Boot

BitLocker on the OS drive uses the TPM to securely store the encryption keys and to verify boot integrity. The TPM provides hardware-backed protection so the encryption key remains with the hardware, making it much harder for an attacker to access the data if the drive is moved to another system or tampered with during boot. Because of this, the BIOS/UEFI must have the TPM enabled and activated (and initialized) so Windows can take ownership of the TPM and use it to protect the BitLocker key. That's why turning on and activating TPM security is the required step. Enabling Secure Boot helps with boot integrity and overall security, but BitLocker can work without it, so it's not strictly required to enable BitLocker. Disabling the TPM would prevent TPM-backed protection, potentially forcing BitLocker into a less secure software-only mode. Setting the BIOS to Legacy Boot bypasses UEFI features that BitLocker often relies on, and is not necessary for enabling BitLocker on the OS drive.

3. Explain the NTFS permissions model and the difference between DACL and SACL.

A. DACL controls access to files/folders; SACL controls auditing

B. DACL controls auditing; SACL controls access

C. DACL is discretionary; SACL is static

D. DACL encrypts data; SACL compresses

NTFS permissions revolve around two control lists attached to every file or folder. The DACL, or Discretionary Access Control List, defines who is allowed or denied access and what they can do with the object. Each entry specifies a user or group and the rights granted or denied (such as read, write, modify, or full control). The system evaluates a user's identity and group memberships against this list, applying deny entries first and then allow entries, with the owner or an administrator able to modify the DACL at will. That flexibility is why it's called discretionary. The SACL, or System Access Control List, handles auditing. It lists which access attempts should be recorded in the security audit log and whether successes, failures, or both should be logged. Importantly, the SACL does not change whether access is granted or denied; it only determines what events are remembered for monitoring and forensic purposes. So the key difference is that the DACL controls access decisions—who can do what with the object—while the SACL controls auditing of those access attempts. The other statements mix up these roles or introduce unrelated concepts like encryption or static behavior, which do not describe what DACLs or SACLs do.

4. Which path allows restricting a user's logon to specific computers?

A. Account tab Logon Hours

B. Account tab Log On To

C. User tab Login Restrictions

D. Security tab Access Rights

Restricting where a user can log on is controlled by a per-user setting that specifies which machines they may log on from. This is configured on the Account tab of the user's properties, using the Log On To option to list the computers the user is allowed to log on to. This directly enforces login restrictions to designated devices. By comparison, Logon Hours controls when logon is allowed, not where; the Security tab focuses on permissions and access rights, not the computers a user can log on from; and a separate Login Restrictions path on the User tab isn't the mechanism used here. So to limit a user's logon to specific computers, use the Log On To setting on the Account tab.

5. 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.

6. What is the configured Maximum Password Age in days in the Local Security Policy lab?

A. 60 days

B. 180 days

C. 90 days

D. 365 days

Maximum Password Age is the number of days a password stays valid before it must be changed. In this lab it's set to 90 days, so passwords must be updated at least every 90 days. This helps limit the window of opportunity if a password is compromised. A shorter value (like 60 days) means more frequent changes, increasing security but adding user burden. A longer value (like 180 or 365 days) reduces how often changes are required, which can lower security if passwords are exposed. The 90-day setting is a common balance between maintaining security and keeping the login process practical for users. (Note: a value of zero would mean the password never expires.)

7. Which statement best describes IPAM's role in network management?

A. IPAM ensures IP address allocation with DNS/DHCP integration to avoid conflicts and track assets

B. IPAM manages physical server racks

C. IPAM is a replacement for DNS servers

D. IPAM encrypts IP packets for security

IPAM coordinates IP address allocation and tracking across a network and works closely with DNS and DHCP to keep mappings current and avoid conflicts. By centralizing the inventory of available and in-use addresses, IPAM helps ensure addresses aren't assigned twice and that subnet usage follows policy. When devices obtain addresses via DHCP, IPAM can record the lease and automate updates to DNS so hostnames resolve to the correct IPs, keeping asset records accurate and making audits easier. It's about managing the IP space and its related records, not about physically organizing servers or encrypting traffic. It doesn't replace DNS servers, and encryption of packets is a separate security function.

8. What is the primary function of a firewall?

A. Authenticate users

B. Route packets

C. Block all traffic by default

D. Filter traffic based on rules

The main job of a firewall is to control access between networks by filtering traffic according to security rules. It sits at the network edge and examines each data packet against criteria such as where the packet came from, where it's headed, the protocol, and the ports involved. Based on the configured rules, it permits or blocks traffic to enforce what is allowed and what is denied. Stateful firewalls also consider the context of active connections, making smarter decisions as conversations unfold. This rule-based, policy-driven filtering is what protects networks from unwanted access while still allowing legitimate communications. Authenticating users is handled by authentication systems, not the firewall's primary purpose. Routing packets is the job of a router. While some environments use a default-deny posture, blocking all traffic by default is a policy choice, not the core function of a firewall.

9. Name two common wireless frequencies and discuss their typical use cases.

A. 2.4 GHz: longer range but more interference; 5 GHz: higher speed but shorter range.

B. 2.4 GHz: shorter range and less interference; 5 GHz: lower speed and more interference.

C. 900 MHz: common for Wi-Fi; 2.4 GHz and 5 GHz

D. 3 GHz and 4 GHz

Lower wireless frequencies travel farther and penetrate obstacles more effectively, while higher frequencies carry more data but lose strength more quickly with distance and through walls. Two common Wi Fi bands reflect this: 2.4 GHz typically provides longer range and broader coverage, but it's crowded with many devices (Bluetooth, microwaves, cordless phones, etc.), so interference is more likely. On the other hand, 5 GHz supports higher data speeds and has more channels, with generally less interference, but its signal doesn't travel as far and is more easily attenuated by walls and distance. This combination is why many networks are dual-band, letting devices choose between the broader reach of 2.4 GHz and the faster performance of 5 GHz as needed. Other frequency options listed aren't standard Wi Fi bands and don't describe the typical trade-offs accurately.

10. What Tunnel Network was configured for the OpenVPN server?

A. 198.28.56.0/24

B. 198.28.20.0/16

C. 198.168.20.0/24

D. 198.28.20.0/24

The tunnel network is the virtual IP space OpenVPN uses to assign addresses to all connected clients and to route traffic through the VPN. It should be a dedicated, non-overlapping range chosen for the VPN so client addresses don't collide with real networks. In this setup, the tunnel network is 198.28.20.0/24. That means the VPN will treat 198.28.20.0 as the network address, 198.28.20.255 as the broadcast, and assign individual client IPs from 198.28.20.1 through 198.28.20.254. This /24 is a sensible, compact range commonly used for VPN tunnels and does not intrude on other networks. Why the other options aren't the best fit: a /24 starting at 198.28.56.0 would designate a different VPN network, which isn't the one configured here; a /16 would allocate a much larger space (over 65,000 addresses) and is unusual for a tunnel network, risking overlaps with other networks; 198.168.20.0/24 uses a different first octet, misaligning with the lab's addressing plan.

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://testoutlabs.examzify.com

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