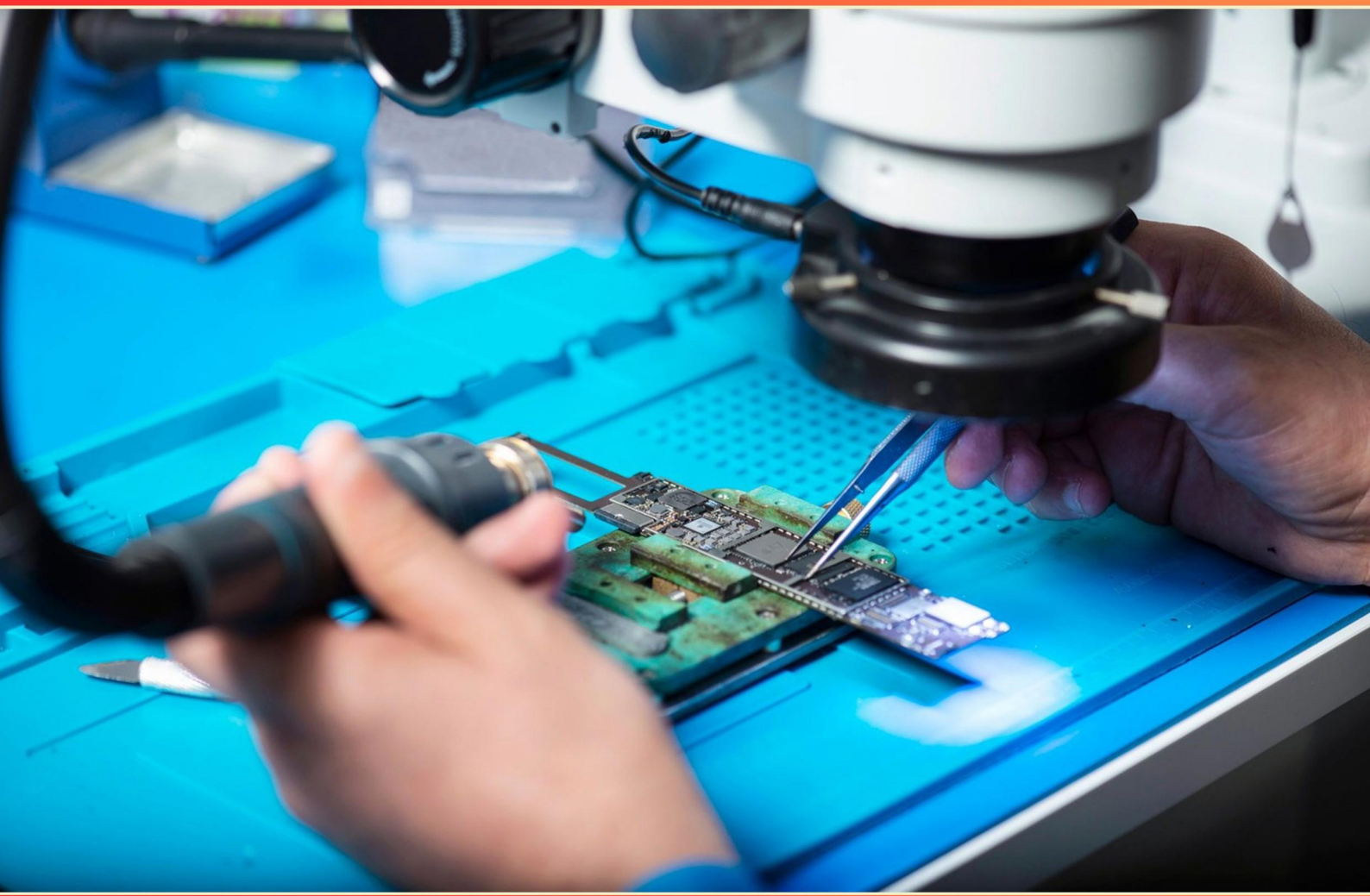
COMPTIA A+ CORE 2 (220-1002) CERTIFICATION PRACTICE EXAM (SAMPLE)

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. What protocol is primarily used for secure email transmission?

A. IMAPS

B. SMTPS

C. HTTP

D. POP3

2. What is often a consequence of high latency in a network?

A. Delayed data transmission and response times

B. Increased data storage capacity

C. Enhanced data encryption

D. Improved network security

3. What technology allows users to access applications and files remotely over the internet?

A. Cloud computing

B. Local Area Network (LAN)

C. Virtual Private Network (VPN)

D. File Transfer Protocol (FTP)

4. Which methods can be used to avoid electrostatic discharge (ESD)?

A. Use an antistatic wrist strap

B. Use a vacuum cleaner

C. Touch the chassis of the computer

D. Use an antistatic mat

5. If you find someone unconscious with a live electrical wire nearby, what should you do first?

A. Run out and call 911

B. Grab the person and drag him out

C. Grab a piece of wood and use it to move the wire

D. Grab the wire and fling it off

6. What is the primary purpose of an antivirus program?

A. To detect, prevent, and remove malicious software

B. To optimize system performance

C. To create backups of files

D. To manage software updates

7. Which of the following are administrative share names? (Select two best answers)

A. C$

B. C:\\Windows

C. ADMIN$

D. System32

8. What is the typical use of a firewall?

A. Storing files securely

B. Creating virtual machines

C. Monitoring network usage

D. Controlling incoming and outgoing network traffic

9. Which issue is a technician most likely troubleshooting when using certmgr.msc?

A. Trusted root CA

B. Hijacked e-mail

C. Spam

D. Browser redirection

10. What is the most effective mode for scanning a computer for viruses?

A. Safe Mode

B. Reset the PC

C. Command Prompt only

D. Boot into Windows normally

Answers

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

Explanations

1. What protocol is primarily used for secure email transmission?

A. IMAPS

B. SMTPS

C. HTTP

D. POP3

The protocol primarily used for secure email transmission is SMTPS. SMTPS stands for Simple Mail Transfer Protocol Secure, and it is an extension of the standard SMTP protocol that incorporates security through Transport Layer Security (TLS) or Secure Sockets Layer (SSL). This adds an encryption layer, which ensures that the email content, as well as the transmission itself, are protected from interception and eavesdropping while being sent from the sender to the recipient. The importance of SMTPS lies in its ability to enhance the security of email communications, which typically transmit sensitive information. By using SMTPS, organizations can ensure that emails are delivered securely over the internet, safeguarding them against potential cybersecurity threats. In contrast, protocols such as IMAPS, HTTP, and POP3 serve different functions. IMAPS is used for retrieving emails securely, whereas POP3 is also a mail retrieval protocol but primarily lacks the encryption feature that SMTPS provides. HTTP is a protocol for transferring hypertext and is unrelated to email transmission. Thus, SMTPS is the right choice for secure email transmission due to its focus on secure delivery and encryption during transport.

2. What is often a consequence of high latency in a network?

A. Delayed data transmission and response times

B. Increased data storage capacity

C. Enhanced data encryption

D. Improved network security

High latency in a network primarily leads to delayed data transmission and response times. Latency refers to the time taken for data to travel from the source to the destination, and when this time is prolonged, it can create significant delays in how quickly information is sent or received. This is particularly noticeable in applications that require real-time interaction, such as video conferencing, online gaming, or financial trading. Users may experience lag, causing frustration and impairing the overall effectiveness of the communication or transaction. The other options relate to different network attributes that do not directly result from high latency. For instance, increased data storage capacity pertains to the ability of a storage system to hold more data, which is independent of latency characteristics. Similarly, enhanced data encryption and improved network security are associated with measures taken to protect data and the network infrastructure itself, rather than issues resulting from high latency. Hence, the correct answer illustrates a direct consequence that users would observe in the performance of a network exhibiting high latency.

3. What technology allows users to access applications and files remotely over the internet?

A. Cloud computing

B. Local Area Network (LAN)

C. Virtual Private Network (VPN)

D. File Transfer Protocol (FTP)

Cloud computing refers to the delivery of various services over the internet, including applications, storage, and processing power. It enables users to access data and applications remotely, eliminating the need for local storage and computing resources. This technology supports a wide range of applications, from software as a service (SaaS) to infrastructure as a service (IaaS), allowing users to work from different locations and devices seamlessly. Local Area Network (LAN) does not facilitate remote access over the internet; it is designed for networking within a limited area, such as a home or office. A Virtual Private Network (VPN) provides a secure connection over the internet to allow users to access a network remotely but does not offer applications or files independently of another service. File Transfer Protocol (FTP) is specifically used for transferring files between computers over a network but does not encompass the broader capabilities of accessing applications or storing data remotely like cloud computing does.

4. Which methods can be used to avoid electrostatic discharge (ESD)?

A. Use an antistatic wrist strap

B. Use a vacuum cleaner

C. Touch the chassis of the computer

D. Use an antistatic mat

Using an antistatic wrist strap is a highly effective method for preventing electrostatic discharge (ESD). The wrist strap is designed to safely ground the user, ensuring that any static electricity is dissipated before it can cause damage to sensitive electronic components. When the strap is worn properly, the electrical charges on the body are neutralized, effectively minimizing the risk of ESD while working on or near computer equipment. An antistatic mat, which is also an effective measure against ESD, provides a similar grounding function. It creates a controlled environment that reduces static buildup during the handling of electronic devices. While options like touching the chassis of the computer may offer some immediate grounding, they are not as reliable as using a wrist strap or mat, especially in more sensitive environments. Vacuum cleaners, particularly those not designed for static control, can generate static electricity during use and are not advisable for ESD prevention. Instead, specialized ESD-safe vacuum cleaners are needed to mitigate risks in environments where ESD is a concern. Overall, wearing an antistatic wrist strap is a fundamental practice in the field of electronics repair and assembly, ensuring optimal safety against ESD damage.

5. If you find someone unconscious with a live electrical wire nearby, what should you do first?

A. Run out and call 911

B. Grab the person and drag him out

C. Grab a piece of wood and use it to move the wire

D. Grab the wire and fling it off

The first step in this scenario is to ensure personal safety before attempting to assist the unconscious individual. By using a piece of wood to move the wire, you are employing a non-conductive material to create a safe distance between yourself and the live electrical hazard. This method minimizes the risk of electrocution, allowing you to address the situation without putting yourself in danger. It's crucial to avoid directly touching the electrical wire, as that could result in serious injury or death from electrical shock. Simply running out to call for help without considering the potential dangers may not resolve the immediate threat. Dragging the person to safety could also expose you to the risk of electrical shock, especially if the unconscious person is still in contact with the live wire. The last option, grabbing the wire directly, is highly dangerous and can lead to severe injury or fatality. By taking proactive measures to ensure safety with a non-conductive item, you are prioritizing both your own safety and that of the unconscious individual, as you prepare to assist them effectively once the immediate danger has been neutralized.

6. What is the primary purpose of an antivirus program?

A. To detect, prevent, and remove malicious software

B. To optimize system performance

C. To create backups of files

D. To manage software updates

The primary purpose of an antivirus program is to detect, prevent, and remove malicious software. Antivirus programs are specifically designed to identify various types of malware, including viruses, worms, trojans, ransomware, and spyware. They use a combination of signature-based detection (recognizing known malware patterns) and heuristic analysis (detecting new, previously unknown viruses or changes to existing ones) to provide protection. By continually scanning files and monitoring system behavior, antivirus software helps ensure that a device remains secure against malware threats. Other options, while important in a comprehensive IT and cybersecurity strategy, relate to different functions. Optimization of system performance focuses on improving the efficiency and speed of the device rather than protecting it from threats. Creating backups is critical for data recovery but does not involve direct malware protection. Managing software updates ensures that programs and their security features are up to date but is a separate process from the core function of detecting and eliminating malware.

7. Which of the following are administrative share names? (Select two best answers)

A. C$

B. C:\\Windows

C. ADMIN$

D. System32

The administrative shares are special types of network shares in Windows operating systems that allow for managing disk access remotely. Among the options provided, the appropriate administrative share names are C$ and ADMIN$. C$ is the default share for the root of the C: drive, and it is used to remotely access the contents of the main drive on a machine. This share is hidden from standard network browsing and is primarily used by system administrators to perform administrative tasks remotely. ADMIN$ is another administrative share that points to the Windows directory (typically C:\Windows). This share is also created for administrative purposes, allowing system administrators to access the operating system's installation files for management and troubleshooting. The other options, C:\\Windows and System32, do not represent administrative shares. C:\\Windows is simply a path to a directory on the file system and does not function as a network share. System32, likewise, is a directory within C:\\Windows that contains critical operating system files, but it is not designated as an administrative share by itself and is also a local path rather than a network share.

8. What is the typical use of a firewall?

A. Storing files securely

B. Creating virtual machines

C. Monitoring network usage

D. Controlling incoming and outgoing network traffic

A firewall is primarily designed to control incoming and outgoing network traffic based on predetermined security rules. This is essential for protecting private networks from unauthorized access and attacks while allowing legitimate communication to flow. By doing so, it establishes a barrier between a trusted internal network and untrusted external networks, such as the internet. Firewalls can be hardware-based, software-based, or a combination of both, and their configurations can be tailored to meet specific security requirements. The other options, while related to different aspects of IT and network management, do not align with the core functionality of a firewall. Storing files securely relates more to file storage solutions and security protocols rather than traffic management. Creating virtual machines pertains to virtualization technologies rather than network traffic control. Monitoring network usage involves analyzing traffic patterns and performance but does not inherently control or regulate that traffic, which is the primary role of a firewall.

9. Which issue is a technician most likely troubleshooting when using certmgr.msc?

A. Trusted root CA

B. Hijacked e-mail

C. Spam

D. Browser redirection

When using certmgr.msc, the technician is primarily working with certificate management on Windows systems. Certmgr.msc is a Microsoft Management Console (MMC) snap-in that allows users to manage certificates for the current user account and the local computer. Certificates are essential for establishing trust in secure communications, particularly in scenarios involving SSL/TLS connections. The "Trusted root CA" option refers to the list of trusted Root Certificate Authorities (CAs) that the system recognizes as valid, which can be crucial for establishing secure connections. If a problem arises with a certificate, such as a missing or untrusted root CA certificate, it can lead to issues with secure websites not loading or generating security warnings. In contrast, other issues listed, such as hijacked email, spam, and browser redirection, are not directly related to the management of certificates using certmgr.msc. These issues involve different aspects of cybersecurity and may require tools and methods outside of certificate management. Therefore, the focus on trusted root certificate authorities makes this the most relevant issue in the context of using certmgr.msc.

10. What is the most effective mode for scanning a computer for viruses?

A. Safe Mode

B. Reset the PC

C. Command Prompt only

D. Boot into Windows normally

Using Safe Mode is indeed the most effective mode for scanning a computer for viruses. Safe Mode operates with a minimal set of drivers and services, which means that only essential system programs and services are loaded. This reduced environment allows antivirus software to run more effectively, as it is less likely that malicious software will be able to interfere with the scanning process or evade detection while the system is in this state. In Safe Mode, many of the programs and processes that could potentially hinder the antivirus operations are disabled. This can help ensure that all portions of the file system are scanned completely and that malware, which may be running in the background when the computer is booted normally, cannot hide or terminate the scanning process. Resetting the PC is not a scanning method but rather a troubleshooting step that reinstalls the operating system, which may resolve issues but does not specifically target the scanning of viruses. Using Command Prompt only could help in some advanced scanning tasks or recovery operations, but it does not offer the comprehensive virus detection and removal capabilities that a full antivirus scan provides. Booting into Windows normally can expose the system to active threats, as malicious software can load during the startup process, making it harder for an antivirus scan to detect and remove them. Therefore, Safe

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://comptiaapluscore22201002.examzify.com

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