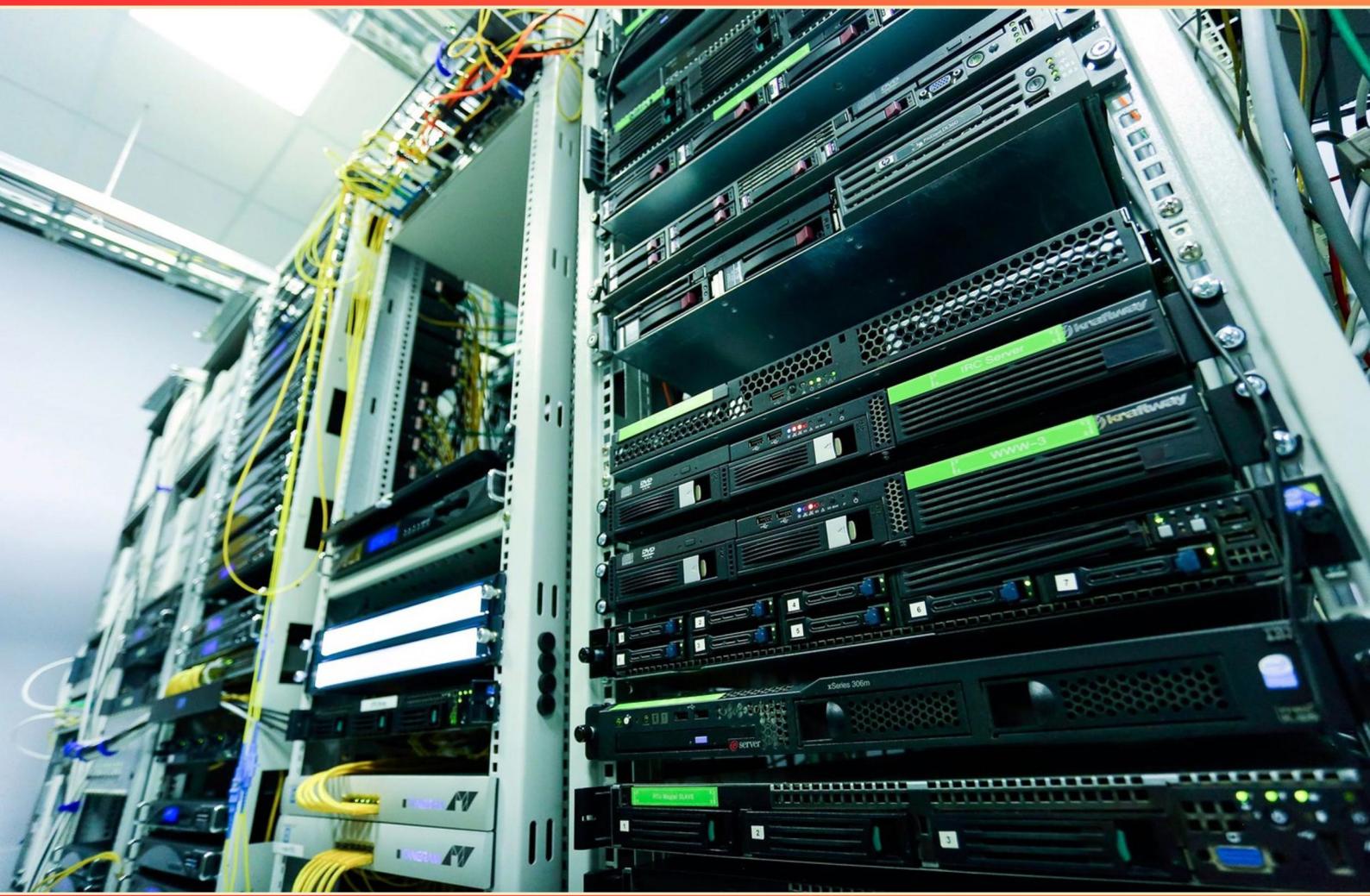
COMPTIA A+ CORE 2 (220-1102) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://comptiaapluscore22201102.examzify.com

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

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. What does the term "patch management" refer to?

A. The process of managing updates for software applications

B. The creation of new software features

C. The removal of outdated software

D. The process of backing up data

2. What is the difference between 32-bit and 64-bit operating systems?

A. 64-bit systems can run 32-bit applications only

B. 32-bit systems are more secure than 64-bit systems

C. 64-bit systems can manage more memory and run more advanced applications

D. 32-bit systems are faster than 64-bit systems

3. What is the most important action a technician can take to protect a server from possible infection when remote access is requested?

A. Create a policy to remove Internet access from the server during off hours

B. Set the local antivirus software on the server to update and scan daily

C. Ensure the server is patched with the latest security updates

D. Educate the manager on safe Internet browsing practices

4. What is the function of a proxy server?

A. To store data for offline access

B. To act as an intermediary for requests from clients

C. To provide local network access

D. To encrypt user data

5. What type of authentication method is being used when a user is prompted for a username and password?

A. Single-factor

B. Multifactor

C. RADIUS

D. TACACS

SAMPLE

6. What best practice could have prevented a corporate network from being infected by a malicious application on a flash drive?

A. Implementing strong passwords

B. Changing default credentials

C. Disabling AutoRun

D. Removing Guest account

7. What device should a technician recommend to ensure power during extreme weather conditions while preventing file corruption?

A. Uninterruptible power supply

B. Surge protector

C. Power strip

D. Power distribution unit

8. What does Active Directory primarily manage?

A. Physical resources in a network

B. Permissions and access to networked resources

C. Web hosting services

D. User data backups

9. What is the maximum RAM limit of a Windows 32-bit version?

A. No limit

B. 4GB

C. 8GB

D. 32GB

10. What network troubleshooting tool can be used to trace the route data takes to reach a destination?

A. Ping

B. Traceroute (Tracert)

C. Netstat

D. Ipconfig

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What does the term "patch management" refer to?

A. The process of managing updates for software applications

B. The creation of new software features

C. The removal of outdated software

D. The process of backing up data

Patch management refers to the process of managing updates for software applications. This includes identifying, acquiring, installing, and verifying patches or updates for software programs and systems. The primary goal of patch management is to enhance system security, improve functionality, and ensure that applications are up-to-date with the latest features and bug fixes. Effective patch management is critical for maintaining the integrity and security of systems, as many updates address vulnerabilities that could be exploited by attackers. By consistently applying patches, organizations can protect their systems against malware and other threats that exploit outdated software. In contrast, creating new software features, removing outdated software, or backing up data, while important aspects of software management and system administration, do not capture the entirety of patch management, which focuses specifically on updates and patches to existing software.

2. What is the difference between 32-bit and 64-bit operating systems?

A. 64-bit systems can run 32-bit applications only

B. 32-bit systems are more secure than 64-bit systems

C. 64-bit systems can manage more memory and run more advanced applications

D. 32-bit systems are faster than 64-bit systems

The distinction between 32-bit and 64-bit operating systems primarily revolves around their ability to manage memory and the type of applications they can run. A 64-bit operating system can utilize a significantly larger addressable memory space compared to a 32-bit system. Specifically, while a 32-bit system can typically handle up to 4 GB of RAM, a 64-bit system can theoretically address up to 16 exabytes, though practical limits are lower due to hardware and system design factors. This increased memory capacity allows 64-bit systems to run more complex and advanced applications that require greater amounts of RAM, such as graphic design software, video editing tools, and large databases. Furthermore, 64-bit systems can execute more threads and processes simultaneously, enhancing multitasking capabilities and overall performance in environments that demand significant computational power. The other choices involve inaccuracies regarding application compatibility, security, and performance which do not reflect the general characteristics of these systems. For example, while 64-bit systems can indeed run many 32-bit applications through compatibility layers, they are not limited to running only those.

SAMPLE

3. What is the most important action a technician can take to protect a server from possible infection when remote access is requested?

A. Create a policy to remove Internet access from the server during off hours

B. Set the local antivirus software on the server to update and scan daily

C. Ensure the server is patched with the latest security updates

D. Educate the manager on safe Internet browsing practices

The most important action a technician can take to protect a server from potential infection when remote access is requested is to ensure the server is patched with the latest security updates. Applying security patches is crucial because these updates often contain fixes for vulnerabilities that could be exploited by attackers. Servers, as critical components of IT infrastructure, are common targets for malware and other cyber threats. Regularly updating these systems minimizes the risk of exploitation through known vulnerabilities, providing a foundational layer of security against infections. While other actions such as updating antivirus software, creating internet access policies, and educating managers about safe browsing practices contribute to the overall security posture, they are typically secondary measures compared to the impact of patch management. Patching directly addresses vulnerabilities that could be targeted during remote access sessions, making it a priority for any technician tasked with protecting server environments.

4. What is the function of a proxy server?

A. To store data for offline access

B. To act as an intermediary for requests from clients

C. To provide local network access

D. To encrypt user data

A proxy server functions as an intermediary between a client and another server, handling requests made by clients and relaying those requests to the appropriate destination server. When a client, such as a computer or application, makes a request for a resource on the internet, the proxy server processes this request, potentially modifying it based on various rules, and forwards it to the target server. Once the target server responds, the proxy server receives the data and sends it back to the client. This functionality provides several benefits, including improved performance through caching, enhanced security features by hiding the client's IP address, and the ability to enforce access control over the network by filtering requests. The role of a proxy server is crucial in network management and is widely used in both personal and organizational settings. The other options refer to different technologies or concepts that serve other purposes—storing data for offline access pertains to local storage solutions, providing local network access relates to networking devices like routers or switches, and encrypting user data is typically the role of security protocols rather than a proxy server.

SAMPLE

5. What type of authentication method is being used when a user is prompted for a username and password?

A. Single-factor

B. Multifactor

C. RADIUS

D. TACACS

The authentication method in which a user is prompted for a username and password is classified as single-factor authentication. This approach relies on a single piece of evidence to verify the user's identity, which, in this case, is the combination of the username and password. Single-factor authentication is commonly used because it is straightforward and easy to implement; users are required only to provide something they know (the username and password) to gain access to a system or application. In contrast, multifactor authentication would require additional layers of security beyond just the username and password, such as a physical token or a biometric identifier, enhancing security by requiring two or more different authentication factors. RADIUS and TACACS are protocols used for network authentication but do not themselves define the type of factor being utilized (single or multifactor). Their function is to facilitate the process of authentication across a network by providing centralized management, rather than describing the method itself. Thus, when only a username and password are required, it distinctly falls under the domain of single-factor authentication.

6. What best practice could have prevented a corporate network from being infected by a malicious application on a flash drive?

A. Implementing strong passwords

B. Changing default credentials

C. Disabling AutoRun

D. Removing Guest account

Disabling AutoRun is a key best practice for preventing a corporate network from being infected by malicious applications on a flash drive. When AutoRun is enabled, any media such as a USB flash drive can automatically execute executables stored on it as soon as it is plugged into a computer. This feature can quickly lead to the unintentional propagation of malware without any user interaction, making it easier for malicious software to infect systems. By disabling AutoRun, an organization can ensure that plugged-in flash drives do not automatically launch programs, thereby providing an additional layer of security. This requires users to manually access the contents of the flash drive, giving them an opportunity to inspect files before executing any software, and reducing the risk of malware spreading across the network. Other practices, such as implementing strong passwords, changing default credentials, or removing guest accounts, focus on securing access controls and user accounts, but they do not specifically address the threat posed by malicious files on external drives. While important for overall security, they do not directly mitigate the risk of malware execution from a USB flash drive, making disabling AutoRun the most effective preventive measure in this context.

SAMPLE

7. What device should a technician recommend to ensure power during extreme weather conditions while preventing file corruption?

A. Uninterruptible power supply

B. Surge protector

C. Power strip

D. Power distribution unit

An uninterruptible power supply (UPS) is the optimal choice for ensuring power during extreme weather conditions while also preventing file corruption. A UPS provides battery backup power, which is crucial in scenarios where power outages may occur due to severe weather. It allows devices to continue operating uninterrupted for a period of time, thus preventing abrupt shutdowns that can cause data loss or file corruption. When devices are suddenly cut off from power, any ongoing processes or unsaved data risks being lost or corrupted. The UPS not only preserves power but also gives users the opportunity to save their work and safely shut down their systems if necessary, minimizing the risk of data issues. In contrast, a surge protector is primarily designed to defend against voltage spikes, not to provide backup power during outages. A power strip simply allows more devices to connect to a wall outlet without providing any protection against power interruptions. Similarly, a power distribution unit (PDU) is used to distribute power from a single power source to multiple devices but does not include battery backup capabilities. Hence, the UPS is the most suitable device for ensuring continuous operation during power failures and protecting against potential file corruption.

8. What does Active Directory primarily manage?

A. Physical resources in a network

B. Permissions and access to networked resources

C. Web hosting services

D. User data backups

Active Directory primarily manages permissions and access to networked resources, playing a crucial role in network security and administration. It serves as a centralized system that allows administrators to define user accounts, manage access rights, and enforce security policies across the entire network. By using Active Directory, IT professionals can effectively control who has access to specific resources, such as files, folders, applications, and other network services. This level of management is particularly essential in environments where multiple users and devices interact with a variety of resources, as it ensures that only authorized users can access sensitive information and perform critical tasks. Active Directory's organizational units and group policies help streamline the administration and provide granular control over permissions, making it easier to manage user access in large and complex network structures. While physical resources, web hosting services, and user data backups are important aspects of network management, they are not the primary focus of Active Directory. Instead, Active Directory's chief function focuses on user identities, authentication, and access control, which are critical for maintaining security within a networked environment.

SAMPLE

9. What is the maximum RAM limit of a Windows 32-bit version?

A. No limit

B. 4GB

C. 8GB

D. 32GB

The maximum RAM limit for a Windows 32-bit version is 4GB. This limitation is rooted in the architecture of 32-bit systems, which can only address a maximum of 2^32 memory addresses. This theoretical maximum results in 4GB (4,294,967,296 bytes) of addressable memory space. In practice, even less than 4GB of RAM may be usable due to system reserves and hardware requirements, which can reduce the amount available to the operating system and applications. As a result, while a 32-bit Windows operating system can recognize up to 4GB, the actual usable amount often falls slightly below this threshold. To elaborate, options like "no limit" or higher capacities such as 8GB and 32GB exceed the maximum addressing capability of 32-bit architecture, confirming that the 4GB ceiling is a fundamental characteristic of 32-bit systems. Hence, 4GB is the correct and recognized limit for RAM in a Windows 32-bit version.

10. What network troubleshooting tool can be used to trace the route data takes to reach a destination?

A. Ping

B. Traceroute (Tracert)

C. Netstat

D. Ipconfig

The correct answer is Traceroute (Tracert) because it is specifically designed to determine the path that data packets take from one network host to another. When a user issues a Traceroute command, the tool works by sending out a series of packets with incrementally increasing Time to Live (TTL) values. Each router that handles the packet decreases the TTL value by one; when the TTL reaches zero, the router sends back an ICMP Time Exceeded message. Through this process, Traceroute records the IP addresses of each intermediate router along the data's journey to the destination, allowing users to see the entire route and measure the time taken at each hop. This tool is particularly valuable for diagnosing network issues, as it provides insight into where delays or failures might be occurring along the path to a specific destination. On the other hand, Ping is used to test the reachability of a host on a network, measuring round-trip time but does not provide route detail. Netstat displays active connections, routing tables, and network interface statistics, but it does not trace routes. Ipconfig is used for displaying and managing IP address configurations for network interfaces on a machine, also not serving to trace routes.

SAMPLE

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://comptiaapluscore22201102.examzify.com

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

SAMPLE