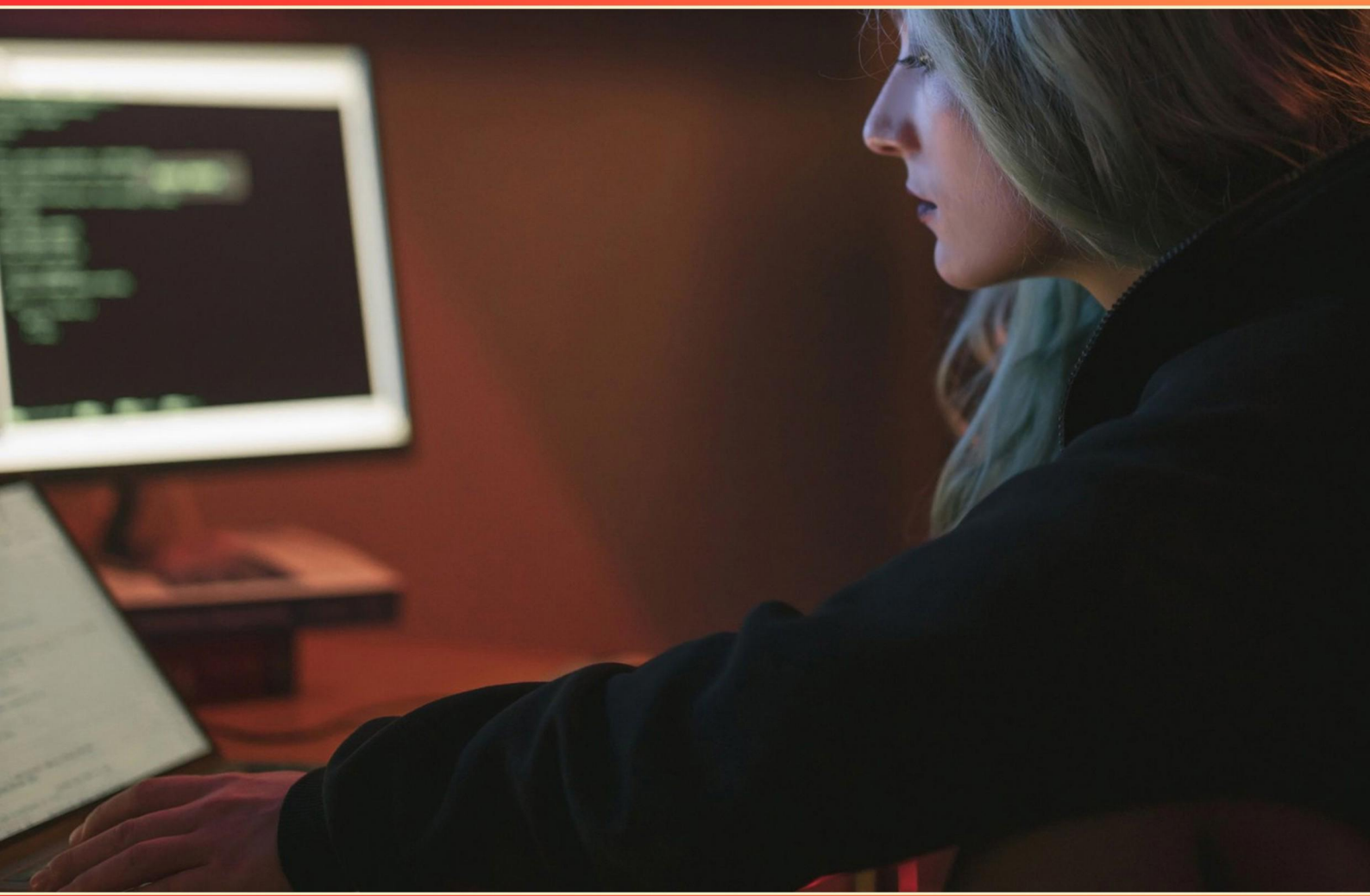
SOPHOS CERTIFIED TECHNICIAN PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://sophoscerttech.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. **How do you implement Sophos updates on endpoints?**

   A. Through a manual process on each device

   B. By using Sophos Central or a local update manager

   C. Through third-party software

   D. By disabling existing software

2. **You have configured and run AD Sync. You notice a user that is present in AD is missing from Central. What is the first step in troubleshooting this issue?**

   A. Check the user permissions in Central

   B. Re-run the AD Sync utility to re-create the missing user

   C. Verify the AD configuration settings

   D. Restart the Central server

3. **In case of a failed software update, what is one potential cause to investigate?**

   A. Power supply issues

   B. Outdated software version

   C. Lack of internet connection

   D. Insufficient user permissions

4. **What encryption standard does Sophos Full Disk Encryption use?**

   A. Triple DES

   B. AES (Advanced Encryption Standard)

   C. RSA Encryption

   D. Blowfish Encryption

5. **What can a server policy for Threat Protection in Sophos Central be assigned to?**

   A. Users and roles

   B. Devices and device groups

   C. Networks and locations

   D. Applications and permissions

SAMPLE

6. The Central Admin Dashboard shows that none of your endpoints are using one of your update caches. What command do you use to investigate this?

A. tracert

B. nslookup

C. ping

D. telnet

7. How can the Competitor Removal Tool be modified to remove software that has not been detected?

A. Modify the executable file

B. Edit ProductCatalog.xml

C. Update the configuration settings

D. Use the built-in repair option

8. In which three ways can you allow a quarantined file to be restored?

A. By using the file name

B. By the certificate

C. Through SHA-256

D. Using the file paths

9. What is a notable benefit of Sophos' Sandbox technology?

A. It reduces the overall size of data storage

B. It performs automatic backups

C. It safely analyzes suspicious files in an isolated environment before allowing execution

D. It eliminates the need for antivirus software

10. In terms of reporting, what does Sophos focus on to ensure operational compliance?

A. Application development timelines

B. Employee training programs

C. Audit logs and compliance status reports

D. Network hardware performance

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. How do you implement Sophos updates on endpoints?

A. Through a manual process on each device

B. By using Sophos Central or a local update manager

C. Through third-party software

D. By disabling existing software

Implementing Sophos updates on endpoints through Sophos Central or a local update manager is the most effective approach because it centralizes management and automation of updates, ensuring that all endpoints are kept current with the latest security definitions and software enhancements. Sophos Central provides a cloud-based platform that allows administrators to manage security configurations, monitor security events, and deploy updates remotely across all endpoints without the need for manual intervention on each device. This streamlines the process and reduces the likelihood of human error, ensuring that all systems have the latest protection against threats. Using a local update manager achieves a similar goal for environments where cloud management is not feasible due to network constraints or specific organizational policies. It allows for the dissemination of updates in a controlled manner, ensuring endpoints receive timely updates while maintaining network security. In contrast, manual updates on each device can lead to inconsistencies and delays, leaving systems vulnerable. Third-party software may not integrate seamlessly with Sophos, compromising the effectiveness of updates. Disabling existing security software introduces risk by exposing endpoints to potential threats, making it counterproductive to maintaining security posture.

2. You have configured and run AD Sync. You notice a user that is present in AD is missing from Central. What is the first step in troubleshooting this issue?

A. Check the user permissions in Central

B. Re-run the AD Sync utility to re-create the missing user

C. Verify the AD configuration settings

D. Restart the Central server

In troubleshooting the issue of a missing user from Central after configuring and running AD Sync, the first step should be to re-run the AD Sync utility. This utility is specifically designed to synchronize users from Active Directory (AD) to Central. If a user exists in AD but is not reflected in Central, there may have been an issue during the initial sync process that prevented the user from being imported. Re-running the AD Sync can help to determine if the issue was a temporary glitch or a one-time error in data transfer. The sync process will attempt to fetch any updates, including any users that may have been newly created or missed during the previous synchronization attempt. This serves as a practical initial measure in resolving the discrepancy. Verifying the AD configuration settings or checking user permissions could be relevant steps later if re-running the sync does not resolve the issue. However, addressing the sync itself first is the most direct method to resolve a missing user from the environment. Restarting the Central server generally pertains to service reliability rather than directly addressing issues of user synchronization.

SAMPLE

3. In case of a failed software update, what is one potential cause to investigate?

A. Power supply issues

B. Outdated software version

C. Lack of internet connection

D. Insufficient user permissions

Investigating a lack of internet connection is crucial in the event of a failed software update, as many updates rely on access to online repositories or servers for downloading the necessary files. A stable and reliable internet connection ensures that the required update packages can be retrieved during the installation process. If the device is offline or there are connectivity issues, the software update will be unable to complete, leading to a failure. While other factors like power supply issues, outdated software versions, and insufficient user permissions can also contribute to problems, the absence of an internet connection directly prevents the update from being downloaded and installed, making it an essential point of investigation when troubleshooting failed updates. A thorough examination of network connectivity should be prioritized, as resolving that often leads to a timely fix for the update issue.

4. What encryption standard does Sophos Full Disk Encryption use?

A. Triple DES

B. AES (Advanced Encryption Standard)

C. RSA Encryption

D. Blowfish Encryption

Sophos Full Disk Encryption utilizes the Advanced Encryption Standard (AES) for securing data on the disk. AES is a widely recognized and trusted encryption standard known for its high level of security and efficiency. It works by encrypting data in fixed block sizes and supports key lengths of 128, 192, and 256 bits, providing flexibility based on the required security level. The robustness of AES stems from its design, which makes it resistant to various types of cryptographic attacks, ensuring that even if an unauthorized party accesses the encrypted data, without the decryption key, it remains unintelligible. This makes it particularly suitable for full disk encryption scenarios, where protecting all data on a device against unauthorized access is crucial. Employing AES aligns with best practices in cybersecurity, and its widespread adoption by governments and organizations worldwide underlines its reliability as a secure encryption method. This choice enhances the overall security posture of devices that use Sophos Full Disk Encryption, helping to safeguard sensitive information effectively.

SAMPLE

5. What can a server policy for Threat Protection in Sophos Central be assigned to?

A. Users and roles

B. Devices and device groups

C. Networks and locations

D. Applications and permissions

A server policy for Threat Protection in Sophos Central is specifically designed to be assigned to devices and device groups. This is because server policies are tailored to manage and secure the server environment effectively, focusing on physical or virtual servers within an organization's network. Devices include individual machines that are being protected, whether they are on-premises servers, cloud servers, or other types of server infrastructure. Device groups allow the administrator to easily manage policies across multiple servers that share common characteristics or roles within the organization. By assigning the policy at the device or group level, it enables streamlined management and consistent enforcement of security measures, including threat detection and response. The other options do not align with how server policies are configured in Sophos Central. Users and roles relate to identity management but are not directly tied to server protection management. Networks and locations are broader concepts that involve configurations related to network security and traffic management rather than device-specific policies. Applications and permissions deal with user access and software controls rather than the application of threat protection policies to server devices.

6. The Central Admin Dashboard shows that none of your endpoints are using one of your update caches. What command do you use to investigate this?

A. tracert

B. nslookup

C. ping

D. telnet

Using the nslookup command is the appropriate choice for investigating why none of your endpoints are using one of your update caches. nslookup is a network utility that allows you to query Domain Name System (DNS) records to obtain information about hostnames and IP addresses. In the context of update caches, it can help you verify that the endpoints are properly resolving the DNS name of the update cache server. If there are issues with DNS resolution, it may lead to endpoints failing to contact the update cache, which is critical for ensuring that software updates are applied correctly. This command provides insight into potential misconfigurations in DNS settings or issues with the connectivity to the update cache by confirming whether the endpoint can resolve the network location of the cache. Effective troubleshooting often starts with ensuring that network addresses can be correctly resolved, making nslookup a fundamental tool in this scenario.

SAMPLE

7. How can the Competitor Removal Tool be modified to remove software that has not been detected?

A. Modify the executable file

B. Edit ProductCatalog.xml

C. Update the configuration settings

D. Use the built-in repair option

The correct approach to modify the Competitor Removal Tool for removing software that has not been detected is to edit the ProductCatalog.xml file. This file contains the definitions and parameters that the tool uses to identify and remove various software products. By updating the ProductCatalog.xml, you can include new software entries or modify existing ones. This allows the tool to recognize and remove software that it would not typically detect based on its initial configuration. The XML file serves as a catalog where you can list the applications to be targeted, including their installation paths or other identifiers. The other options do not effectively address the requirement for modifying the detection capabilities of the Competitor Removal Tool. Simply modifying the executable file or using configuration settings may not specifically enhance detection for undocumented software. The built-in repair option is intended for fixing issues with existing software rather than including new items for removal.

8. In which three ways can you allow a quarantined file to be restored?

A. By using the file name

B. By the certificate

C. Through SHA-256

D. Using the file paths

The ability to restore a quarantined file typically involves utilizing certain metadata associated with the file to ensure that the restoration process is secure and valid. One of the key methods for restoring a quarantined file is by the certificate, which is relevant in identifying the legitimacy and authenticity of the file. When a file is quarantined, it often includes signature information or certificates that can confirm it was originally from a trusted source. Therefore, allowing the restoration of a file based on its certificate helps to verify that the file can be safely reinstated without risking security. Using the file name, SHA-256, or file paths could potentially lead to the restoration of unverified or harmful files. File names can be easily altered, and while SHA-256 hash values provide a unique identifier for a file, they do not inherently confirm the file's origin as securely as a certificate. Similarly, file paths may not effectively guarantee that the file has not been tampered with or that it remains safe to restore. Hence, focusing on the certificate ensures a higher level of trust and security in the restoration process.

SAMPLE

9. What is a notable benefit of Sophos' Sandbox technology?

A. It reduces the overall size of data storage

B. It performs automatic backups

C. It safely analyzes suspicious files in an isolated environment before allowing execution

D. It eliminates the need for antivirus software

The notable benefit of Sophos' Sandbox technology is its ability to safely analyze suspicious files in an isolated environment before allowing execution. By using a sandbox, Sophos can execute files in a controlled setting that does not affect the rest of the system. This allows for the detection of potentially harmful behavior, enabling the system to identify malware without risking the integrity of the actual environment. Sandbox technology is essential in modern cybersecurity as it helps organizations determine the safety of files before they can cause harm. By isolating the executable within a virtual environment, Sophos can monitor its actions and identify any malicious attributes, thus preventing possible breaches or attacks. This proactive approach to threat detection is critical in maintaining strong security measures and protecting sensitive data. The other options do not accurately represent the capabilities or purposes of Sandbox technology in the context of cybersecurity. Reducing data storage size and performing automatic backups are unrelated functionalities, while the claim about eliminating the need for antivirus software overlooks the fact that Sandbox technology is often used in conjunction with antivirus solutions to enhance overall security posture.

10. In terms of reporting, what does Sophos focus on to ensure operational compliance?

A. Application development timelines

B. Employee training programs

C. Audit logs and compliance status reports

D. Network hardware performance

Sophos emphasizes audit logs and compliance status reports in its reporting processes to ensure operational compliance. This focus is crucial because audit logs provide a detailed record of activities, changes, and access within the system, allowing organizations to track adherence to established security policies and regulatory requirements. Compliance status reports compile this information, offering insights into the organization's compliance level, potential vulnerabilities, and areas that may require attention. By analyzing this data, organizations can verify whether they are meeting necessary compliance standards and implement necessary changes or enhancements to their security posture. This practice not only provides transparency but also helps in preparing for external audits and demonstrating accountability to stakeholders. On the other hand, application development timelines, employee training programs, and network hardware performance, while important in their respective areas, do not directly focus on the essential elements needed to monitor and report compliance effectively.

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://sophoscerttech.examzify.com

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

SAMPLE