COMPTIA CASP+ PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://compltia-caspplus.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 is the primary role of a security administrator when handling an e-discovery request?**

   A. Limit data access to specific users

   B. Provide accurate data in accordance with policies

   C. Reassess data retention protocols

   D. File a report on company's data handling

2. **To achieve an availability target of 99.9999%, which strategy is critical?**

   A. Implement regular backups

   B. Ensure redundancy in systems and components

   C. Limit access to essential personnel only

   D. Conduct training for all employees

3. **In the context of network security, what best describes the function of network access control (NAC)?**

   A. Preventing data leakage

   B. Identifying and restricting unauthorized devices

   C. Monitoring user activity for compliance

   D. Encrypting data in transit

4. **What is a recommended security measure to address risks of disclosing intellectual property when outsourcing email services?**

   A. Encrypt all outbound emails

   B. Enable data loss protection to minimize emailing PII

   C. Limit access to company email accounts

   D. Conduct background checks on the service provider

5. **What does an SRTM provide according to the engineers' network design?**

   A. A compliance checklist for regulatory standards.

   B. A set of requirements for network performance and functionalities.

   C. A validation method for connection protocols.

   D. A framework for incident response practices.

SAMPLE

6. What is a common tool a penetration tester is likely to use for black box testing of a web application?

A. Static analysis tools

B. Network performance analyzers

C. Fuzz testing software

D. Vulnerability scanning tools

7. What valid roles can SAML entities operate in?

A. Data processor and service provider.

B. User and database administrator.

C. Identity provider and service provider.

D. Client and server.

8. What is the most likely cause of malfunctioning after deploying a new PHP module on separate zones in a Solaris server?

A. The PHP module was installed incorrectly in the backend zone.

B. The PHP module was not compatible with the Solaris 10 environment.

C. The PHP module was placed in the management zone and is trying to interact directly with the customer zone.

D. The PHP module lacks sufficient permissions to access the backend zone.

9. Which configuration might be used to address performance issues after analyzing router stats?

A. Increase the bandwidth of the internal network.

B. Replace old hardware components.

C. Reconfigure routing protocols.

D. Minimize network traffic during peak hours.

10. What solution should be implemented for cost-effective multi-factor authentication in a company utilizing PKI?

A. Install hardware tokens for all users

B. Implement biometric authentication

C. Issue individual private/public key pairs to each user

D. Establish a single sign-on solution

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the primary role of a security administrator when handling an e-discovery request?

A. Limit data access to specific users

B. Provide accurate data in accordance with policies

C. Reassess data retention protocols

D. File a report on company's data handling

The primary role of a security administrator when handling an e-discovery request is to provide accurate data in accordance with policies. This involves ensuring that data retrieved during the e-discovery process meets legal and regulatory standards as well as internal policies regarding data integrity, confidentiality, and security. The administrator must understand what data is relevant to the request, and work to extract this data while maintaining its accuracy and authenticity. This accuracy is critical because the information provided may be used in legal proceedings, and any discrepancies or failures to comply could lead to severe legal implications for the organization. Therefore, the security administrator plays a vital role in ensuring that the data is not only accessible but is also provided in a way that adheres to compliance and regulatory requirements. Other responsibilities, such as limiting data access to specific users, reassessing data retention protocols, and filing reports on data handling, may be relevant in the broader context of data governance and security, but they are secondary to the immediate necessity of providing accurate and policy-compliant data during the e-discovery process.

2. To achieve an availability target of 99.9999%, which strategy is critical?

A. Implement regular backups

B. Ensure redundancy in systems and components

C. Limit access to essential personnel only

D. Conduct training for all employees

Achieving an availability target of 99.9999%, also known as "six nines" availability, requires a robust strategy for minimizing downtime and ensuring that critical systems remain operational at all times. Ensuring redundancy in systems and components is essential because it involves having backup systems or components that can take over immediately in the event of a failure. This redundancy can exist at multiple levels, including hardware (such as servers, power supplies, and network components) and software (like load balancing and failover protocols). The implementation of redundancy helps to mitigate the risks associated with single points of failure. For instance, if one component fails, the redundant component can sustain operations without causing service disruption. This level of preparedness is crucial in environments where uptime is critical, as even a brief outage can have significant ramifications for business operations. While regular backups, limiting access, and training employees are important strategies for maintaining overall security and operational integrity, they do not directly address the immediate need for system availability in the event of a failure. Backups are more focused on data preservation and recovery, rather than real-time availability. Limiting access is primarily concerned with security, and while it is important, it does not enhance system uptime. Training employees, though valuable for ensuring staff

SAMPLE

3. In the context of network security, what best describes the function of network access control (NAC)?

A. Preventing data leakage

B. Identifying and restricting unauthorized devices

C. Monitoring user activity for compliance

D. Encrypting data in transit

Network Access Control (NAC) primarily focuses on identifying and restricting unauthorized devices from accessing a network. This function is crucial for maintaining the security and integrity of the network environment. By enforcing policies that determine which devices are allowed to connect based on their compliance with predefined security standards, NAC helps organizations minimize the risk of unauthorized access and potential attacks. The ability of NAC to assess the security posture of devices before granting access—ensuring that they meet criteria such as security updates, antivirus status, and other configurations—enhances the overall security framework. This proactive approach in managing access ensures that only trusted endpoints, which are compliant with security policies, can interact with sensitive network resources. While preventing data leakage, monitoring user activity for compliance, and encrypting data are all important security functions, they do not specifically capture the core function of NAC, which is centered on controlling access to the network itself.

4. What is a recommended security measure to address risks of disclosing intellectual property when outsourcing email services?

A. Encrypt all outbound emails

B. Enable data loss protection to minimize emailing PII

C. Limit access to company email accounts

D. Conduct background checks on the service provider

Enabling data loss protection (DLP) is a recommended security measure to address the risks of disclosing intellectual property when outsourcing email services. DLP solutions help monitor, detect, and respond to data breaches or unauthorized data transfer. When dealing with sensitive information, such as intellectual property, DLP can effectively prevent users from sending sensitive content outside the organizational boundaries through email. DLP policies can be customized to regulate what data can be sent or received, particularly when it pertains to personally identifiable information (PII) or confidential business information. By implementing these measures, organizations can mitigate the risk of accidental or intentional disclosure of their intellectual property during email exchanges. While encrypting outbound emails enhances the security of the content being sent, it does not specifically prevent the occurrence of sending sensitive information that shouldn't be shared. Limiting access to company email accounts could help protect intellectual property, but it does not directly address the risks associated with outsourcing. Conducting background checks on the service provider is important for establishing trust, but it does not provide a technical solution to prevent data loss. In contrast, DLP is expressly designed to safeguard against information leakage, making it the most effective choice in this context.

SAMPLE

5. What does an SRTM provide according to the engineers' network design?

A. A compliance checklist for regulatory standards.

B. A set of requirements for network performance and functionalities.

C. A validation method for connection protocols.

D. A framework for incident response practices.

An SRTM, or Service Requirements Traceability Matrix, is a tool used in network engineering that outlines a clear set of requirements corresponding to network performance and functionalities. This document is crucial during the design and implementation phases, as it helps engineers trace service requirements back to the specific functionalities they support. It ensures that all necessary features and performance metrics are met throughout the project lifecycle. By establishing these requirements, the SRTM aids in verifying that the designed network aligns with the strategic goals and user needs. This clarity supports effective decision-making, minimizes design flaws, and facilitates communication among stakeholders, ensuring that the final network solution meets its intended purpose and operates efficiently under expected load conditions. In contrast to the other options, compliance checklists relate to regulatory standards and do not focus specifically on performance requirements. A validation method for connection protocols is more focused on ensuring protocols function correctly rather than defining the performance criteria for the network as a whole. Incident response practices address how to handle security events rather than defining network functionalities. Thus, the emphasis on performance and functionalities makes option B the most applicable choice regarding the role of an SRTM.

6. What is a common tool a penetration tester is likely to use for black box testing of a web application?

A. Static analysis tools

B. Network performance analyzers

C. Fuzz testing software

D. Vulnerability scanning tools

Fuzz testing software is a common tool used by penetration testers during black box testing of web applications because it involves sending a wide range of invalid, unexpected, or random data inputs to the application to uncover vulnerabilities. The goal is to see how the application handles unexpected inputs, which can reveal issues such as buffer overflows, input validation flaws, and other security weaknesses. In black box testing, the tester does not have prior knowledge of the internal workings of the application, which aligns perfectly with the functionality of fuzz testing. It enables the tester to discover how the application reacts solely based on its external behavior. This approach mimics real-world attack scenarios where an attacker has no insider knowledge of the system's architecture or source code. Static analysis tools analyze code without executing it, which is more pertinent during a white box testing phase where insight into the application's code is available. Network performance analyzers focus on the performance rather than security aspects, making them less suitable for uncovering vulnerabilities in web applications. Vulnerability scanning tools typically assess known vulnerabilities based on databases and are less effective in simulating unpredictable attack patterns as fuzz testing does. Thus, fuzz testing uniquely fits the needs of black box penetration testing.

SAMPLE

7. What valid roles can SAML entities operate in?

A. Data processor and service provider.

B. User and database administrator.

C. Identity provider and service provider.

D. Client and server.

SAML (Security Assertion Markup Language) entities operate in two primary roles: the identity provider (IdP) and the service provider (SP). The identity provider is responsible for authenticating users and providing the necessary authentication assertions (such as SAML tokens) to other services. This means that the IdP verifies the user's identity and delivers that verification to the service provider, which relies on this information to grant access to its resources. The service provider, on the other hand, is the entity that provides services or resources to users, relying on assertions from the identity provider to authenticate those users. The service provider trusts the identity provider to manage user identities and security, thus enabling single sign-on (SSO) capabilities across different services. These roles are fundamental in federated identity management, where users can access multiple services without needing separate credentials for each service. This streamlines the user experience and enhances security by centralizing user authentication. The other roles mentioned—data processor and user, database administrator, client and server—are not relevant to the specific functioning of SAML entities within the context of identity management and security protocols.

8. What is the most likely cause of malfunctioning after deploying a new PHP module on separate zones in a Solaris server?

A. The PHP module was installed incorrectly in the backend zone.

B. The PHP module was not compatible with the Solaris 10 environment.

C. The PHP module was placed in the management zone and is trying to interact directly with the customer zone.

D. The PHP module lacks sufficient permissions to access the backend zone.

The most likely cause of malfunctioning after deploying a new PHP module on separate zones in a Solaris server is that the PHP module was placed in the management zone and is trying to interact directly with the customer zone. In Solaris, zones are isolated environments where applications run independently. The management zone is primarily intended for administrative tasks, while the customer zones are designated for application deployment. When a module is incorrectly installed in the management zone, it may not have the necessary context or environment to function correctly within customer zones. The management zone is not designed to host applications directly; thus, an attempt to execute or access resources from this zone can lead to errors or malfunctions. Proper installation of the PHP module should occur in the specific customer zone where it is intended to operate, ensuring that all dependencies and configurations are appropriately set for the environment in which the module is meant to function. Though the other options address potential issues—like installation errors, compatibility concerns, or permission limitations—the specific scenario of inappropriate placement within the zones best accounts for the observed malfunction due to the inherent isolation and design of Solaris zones.

SAMPLE

9. Which configuration might be used to address performance issues after analyzing router stats?

A. Increase the bandwidth of the internal network.

B. Replace old hardware components.

C. Reconfigure routing protocols.

D. Minimize network traffic during peak hours.

Reconfiguring routing protocols can effectively address performance issues identified through router statistics. Routing protocols determine how data is directed through a network. If the current configuration is leading to inefficiencies, such as too many hops or not utilizing the best paths, it can slow down overall performance. By reconfiguring these protocols, you can implement changes such as adjusting the load balancing, modifying metrics, or prioritizing certain types of traffic. This can lead to more efficient data routing and ultimately enhance network performance. The analysis of router statistics likely revealed specific inefficiencies that could be remedied through this approach, making it a suitable solution to improve performance. The other options may address performance concerns but are not directly related to the analysis of router stats. Increasing bandwidth might help if the network is saturated, replacing hardware could resolve issues with failing components, and minimizing traffic during peak times could lessen congestion issues, but these do not specifically utilize the insights gained from router statistics as directly as reconfiguring routing protocols does.

10. What solution should be implemented for cost-effective multi-factor authentication in a company utilizing PKI?

A. Install hardware tokens for all users

B. Implement biometric authentication

C. Issue individual private/public key pairs to each user

D. Establish a single sign-on solution

Implementing individual private/public key pairs for each user is a strong cost-effective solution for multi-factor authentication, especially in a company utilizing Public Key Infrastructure (PKI). This method leverages the existing PKI framework to provide secure identity verification through cryptographic means. In a PKI system, users possess a unique private key that is securely stored on their devices, while the corresponding public key is available on the central server. This two-key system enables strong authentication, as the private key is required to sign transactions or authenticate to services, while the public key validates the identity of the signer. Using these key pairs enhances security by ensuring that even if one key is compromised, the other remains protected, adding a layer of assurance in the authentication process. This approach is also cost-effective because it eliminates the need for physical tokens or biometric systems, which can involve higher costs for deployment, maintenance, and user training. Instead, by utilizing existing infrastructure and focusing on software-based mechanisms, the company can ensure robust authentication while minimizing additional costs. The other options do not align as closely with the existing PKI framework or have higher implementation costs and complexity. For instance, hardware tokens require significant upfront investment and ongoing management, while biometric authentication necessitates specialized technology and

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://compltia-caspplus.examzify.com

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

SAMPLE