COMPTIA SERVER+ (SK0-005) PRACTICE EXAM (SAMPLE)

STUDY GUIDE

Prepare with structure. Pass with confidence

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

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. **A server administrator has configured a web server. Which of the following is needed to make the website trusted?**

   A. Firewall Configuration

   B. Anti-virus Software

   C. PKI

   D. Security Certificate

2. **What type of environment typically requires high data availability with minimal downtime?**

   A. Development

   B. Production

   C. Testing

   D. Backup

3. **What must a server administrator do to ensure that data on the SAN is not compromised if leaked?**

   A. Backup to a secure location

   B. Encrypt the data at rest

   C. Limit physical access

   D. Monitor access logs

4. **In a situation where user access on a file server is increasing, what might be a practical way to control storage usage?**

   A. Create user accounts with limited access

   B. Implement disk quotas

   C. Improve hardware resources

   D. Archive old data regularly

5. **What is the main purpose of setting up a RAID 5 array?**

   A. Data redundancy and fault tolerance

   B. Increase read/write speed

   C. Partitioning storage space

   D. Easy data recovery

6. **Which of the following tools can be used for network performance monitoring on a server?**

A. Wireshark

B. Task Manager

C. Disk Management

D. Process Explorer

7. **Which type of interface is BEST for setting up a RAID 5 array on a physical server storing sensitive data?**

A. SAS

B. SATA

C. IDE

D. USB

8. **Which port should a technician use for secure remote access to a server?**

A. 80

B. 22

C. 443

D. 3389

9. **What is the implication of a physical server hosting an application that is crashing on reboot due to an unauthorized software installation?**

A. The system is compromised

B. The application is incompatible with the new update

C. The server needs more RAM

D. The network configuration is incorrect

10. **An administrator is troubleshooting a failure in the datacenter in which a server shut down/powered off when utility power was lost. The server had redundant power supplies. Which of the following is the most likely cause of this failure?**

A. Both power supplies were faulty

B. One power supply was connected to a UPS

C. Both power supplies were connected to the same power feed

D. Server reached thermal shutdown

Answers

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

Explanations

1. A server administrator has configured a web server. Which of the following is needed to make the website trusted?

A. Firewall Configuration

B. Anti-virus Software

C. PKI

D. Security Certificate

To establish trust for a website, implementing a public key infrastructure (PKI) is crucial because it provides the framework necessary for managing digital certificates and encryption keys. In the context of a web server, a security certificate—often referred to as an SSL/TLS certificate—works in conjunction with PKI to ensure that data transmitted between the server and clients is encrypted and secure from interception. When a website has a valid security certificate, it signifies to users that their data is being handled securely and is trustworthy to interact with. While PKI is essential for managing the lifecycle of security certificates, it does not directly make the website trusted on its own. However, it underpins the security certificate's validity and the trustworthiness of the entities behind the website. This is why while a security certificate is necessary to indicate trustworthiness to users explicitly, PKI provides the necessary support structure for creating and verifying those certificates, ensuring they are issued by a trusted authority. In the landscape of web security, having a security certificate directly influences users' perceptions of trust, especially during the browsing experience when they see indicators like HTTPS in the URL. Thus, while the correct answer identifies PKI as an important component, it's essential to recognize that without a valid security certificate actively

2. What type of environment typically requires high data availability with minimal downtime?

A. Development

B. Production

C. Testing

D. Backup

A production environment typically requires high data availability with minimal downtime because it is the setting where live applications and services operate and are used by end users. In production, any interruptions can lead to financial losses, decreased customer satisfaction, or damage to an organization's reputation. The focus in this environment is on maintaining continuous operations, ensuring that systems are reliably available when needed. In contrast, while development and testing environments are also important, they often do not have the same level of criticality in terms of uptime and availability. These environments can tolerate downtime as they are primarily used for creating and evaluating new features or software, and can be restored or reset if issues arise. Backup environments are essential for data recovery but again are not in regular operational use; they play a supporting role rather than being constantly active in delivering services.

3. What must a server administrator do to ensure that data on the SAN is not compromised if leaked?

A. Backup to a secure location

B. Encrypt the data at rest

C. Limit physical access

D. Monitor access logs

To ensure that data on a Storage Area Network (SAN) is not compromised if leaked, encrypting the data at rest is a critical measure. Data at rest refers to data that is stored on a physical medium (like disks or tapes) and is crucial to protect it from unauthorized access. When data is encrypted, even if someone gains access to the storage medium, they will not be able to read or use the data without the appropriate decryption key. This adds a strong layer of security, ensuring that sensitive information remains confidential. While other options may contribute to the overall security strategy, they do not provide the same level of protection specifically related to the risk of data being leaked or accessed without authorization. Backing up data, limiting physical access, and monitoring access logs are important practices but do not inherently protect the confidentiality of the data itself if it is accessed unlawfully. Through encryption, you safeguard the data itself, meaning that even if it is leaked, it remains unreadable to unauthorized users. This makes it a fundamental tool for managing sensitive data in a SAN environment.

4. In a situation where user access on a file server is increasing, what might be a practical way to control storage usage?

A. Create user accounts with limited access

B. Implement disk quotas

C. Improve hardware resources

D. Archive old data regularly

Implementing disk quotas is a practical way to manage and control storage usage on a file server as it allows administrators to limit the amount of disk space that each user or group can consume. This method is especially effective in environments where user access is increasing because it helps prevent any single user from monopolizing storage resources. By setting these limits, organizations can encourage users to manage their files more responsibly and ensure that storage remains available for everyone. With disk quotas in place, administrators can monitor usage and enforce limits based on policy requirements. For example, if a quota is set for a user, they will receive alerts when they approach their limit, allowing them to take action before they exceed the allocated space. This proactive approach can enhance overall server performance and maintain a healthy balance of usage across the network. While creating user accounts with limited access can control who can access certain files, it does not directly address the issue of how much storage each user consumes. Improving hardware resources may help accommodate increased access but doesn't directly manage usage, and archiving old data regularly is a good practice but does not provide immediate control over current usage as effectively as implementing disk quotas does. Thus, using disk quotas directly addresses the concern by implementing a straightforward method to manage and limit storage consumption.

5. What is the main purpose of setting up a RAID 5 array?

A. Data redundancy and fault tolerance

B. Increase read/write speed

C. Partitioning storage space

D. Easy data recovery

Setting up a RAID 5 array primarily aims to provide data redundancy and fault tolerance. RAID 5 accomplishes this through a method known as striping with parity. In this configuration, data is divided into blocks and spread across three or more drives. Parity information is also distributed among the drives, which enables the array to reconstruct data if one of the drives fails. This means that, in the event of a single drive failure, the system can still function without data loss, as the missing data can be regenerated using the parity information stored on the remaining drives. This combination of redundancy and fault tolerance makes RAID 5 a popular choice for organizations that require both high availability and protection against data loss. While RAID 5 does offer some improvements in read performance due to data being spread across multiple drives, the primary focus is on protecting the integrity of data. The other mentioned options like partitioning storage space and easy data recovery are not the main purposes of a RAID 5 array; instead, they may represent features or benefits in different contexts within overall data management strategies.

6. Which of the following tools can be used for network performance monitoring on a server?

A. Wireshark

B. Task Manager

C. Disk Management

D. Process Explorer

Wireshark is a powerful tool used for network performance monitoring and packet analysis. It captures network packets in real-time, allowing you to inspect the data being transmitted over the network. This capability makes Wireshark an essential tool for diagnosing network issues, analyzing traffic patterns, and evaluating network performance. It provides detailed insights into the network's performance metrics, such as latency, bandwidth usage, and protocol analysis, which can help identify bottlenecks or other issues affecting the server's network connectivity. In contrast, the other options serve different purposes. Task Manager is primarily focused on monitoring system performance, such as CPU, memory, and running processes, but it does not provide detailed network analysis. Disk Management is a tool used for managing disk drives and partitions on a server, unrelated to network performance. Process Explorer is an advanced task manager that gives more detailed insights into running processes, including CPU and memory usage, but it does not have capabilities for network monitoring. Thus, Wireshark stands out as the only choice specifically designed for monitoring and analyzing network performance.

7. Which type of interface is BEST for setting up a RAID 5 array on a physical server storing sensitive data?

A. SAS

B. SATA

C. IDE

D. USB

The best interface for setting up a RAID 5 array on a physical server that stores sensitive data is SAS (Serial Attached SCSI). SAS is designed for enterprise environments and provides several advantages that make it ideal for managing a RAID configuration, particularly when dealing with sensitive information. SAS supports higher data transfer rates compared to the other interfaces, resulting in better performance, which is critical for RAID 5 arrays that require both read and write operations to be fast and efficient. Moreover, SAS allows for more drives to be connected per host adapter and offers better reliability and availability features. It also provides dual-port capabilities, which enhance fault tolerance by allowing two hosts to access the same drive simultaneously, increasing data availability. In addition to performance and scalability, SAS drives typically have a lower fail rate and are built for 24/7 access, making them more suitable for environments where data integrity and uptime are crucial. These qualities make SAS the most appropriate choice for setups that demand a higher level of reliability, such as servers handling sensitive data. While SATA, IDE, and USB interfaces are more common in consumer-grade systems and can be adequate for less demanding applications, they do not offer the same level of performance, reliability, and fault tolerance as SAS. This is particularly

8. Which port should a technician use for secure remote access to a server?

A. 80

B. 22

C. 443

D. 3389

For secure remote access to a server, the appropriate port to use is 22. This port is standard for SSH (Secure Shell), which is a protocol designed for secure remote login and other secure network services over an insecure network. When a technician uses SSH, they can connect securely to a server to execute commands, transfer files, and manage the system without exposing sensitive data to potential eavesdropping or attacks. Port 443 is primarily used for HTTPS (HTTP Secure), which encrypts web traffic and is not specifically designed for remote access. Port 80 is used for unencrypted HTTP traffic, which does not provide any security for remote access. Port 3389 is associated with RDP (Remote Desktop Protocol), which is used for accessing Windows desktop interfaces remotely, but it does not inherently provide the same level of security as SSH unless additional measures are taken for encryption. Therefore, when considering secure remote access to a server, port 22 is the appropriate choice.

9. What is the implication of a physical server hosting an application that is crashing on reboot due to an unauthorized software installation?

A. The system is compromised

B. The application is incompatible with the new update

C. The server needs more RAM

D. The network configuration is incorrect

The implication of a physical server hosting an application that crashes on reboot due to an unauthorized software installation is that the system is compromised. This suggests that the application is not operating as intended because the unauthorized software could introduce vulnerabilities or conflicts that disrupt normal operations. In the context of server management, unauthorized installations often bring risks, such as security threats or instability, which can lead to crashes or other failures. When unauthorized software is installed, it bypasses standard security controls and could be malicious or simply not properly configured for the server environment. Furthermore, the presence of such software can burden system resources or conflict with existing applications, potentially causing broader system issues. Therefore, recognizing that the server is compromised requires immediate corrective actions, such as assessing and possibly removing the unauthorized software, before further deterioration of system functionality occurs.

10. An administrator is troubleshooting a failure in the datacenter in which a server shut down/powered off when utility power was lost. The server had redundant power supplies. Which of the following is the most likely cause of this failure?

A. Both power supplies were faulty

B. One power supply was connected to a UPS

C. Both power supplies were connected to the same power feed

D. Server reached thermal shutdown

The most likely cause of the server's shutdown during a utility power loss is that both power supplies were connected to the same power feed. In a redundant power supply configuration, having the power supplies connected to separate power feeds ensures that if one feed fails (like in the case of a utility power outage), the other feed can continue to supply power to the server. When both power supplies are on the same power feed, they are both subject to the same electrical conditions. Therefore, if that feed loses power, neither supply will function, leading to the complete shutdown of the server. This design flaw undermines the redundancy that power supplies are meant to provide, ultimately resulting in the failure experienced. The other scenarios, such as both power supplies being faulty, one supply being connected to a UPS, or the server reaching thermal shutdown, do not explain the complete power loss that occurred when utility power was lost. If one supply were connected to a UPS, it should have maintained power during the outage. The thermal shutdown situation would typically indicate overheating, not a direct result of power loss.

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://comptiaserverplussk0005.examzify.com

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