CompTIA Server+ (SK0-005) Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

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. **In the event of a server hardware failure, what ensures that application data can continue to be accessed?**

   A. Local backups

   B. Data replication

   C. RAID configurations

   D. Cloud storage

2. **What should a technician attempt FIRST to resolve missing files in a home directory on a Linux server?**

   A. mount /home

   B. Check file permissions

   C. Restart the NFS service

   D. Run a file recovery tool

3. **A technician found a Linux server cannot mount an NFS share. What should be performed FIRST?**

   A. Check network connectivity

   B. Verify NFS server status

   C. Create the mount point

   D. Review NFS export settings

4. **What tool should a server administrator use to check for unnecessary running services across multiple servers?**

   A. A port scanner

   B. Remote Desktop

   C. Network monitor

   D. Task manager

5. **What is the BEST action to take before applying patches in a high availability cluster?**

   A. Backup the entire system

   B. Fallback cluster services

   C. Update user permissions

   D. Reboot all servers

6. What tool can be used to monitor and maintain server uptime?

A. Server management software

B. Power monitoring tools

C. MTTR calculation tools

D. Log analysis tools

7. An administrator encounters error messages when using YUM to update applications on a server. What should be checked FIRST?

A. YUM dependencies

B. Server hardware

C. Network connectivity

D. System logs

8. Which file is essential for configuring SSH settings on a Linux server?

A. /etc/ssh/ssh_config

B. /etc/ssh/sshd_config

C. /etc/passwd

D. /etc/group

9. Which method can be used to monitor compliance with a code of conduct among employees?

A. Regular audits

B. Anonymous reporting tools

C. Frequent training sessions

D. All of the above

10. What type of backup records only the changes made to data blocks on a virtual machine?

A. Full backup

B. Differential backup

C. Incremental backup

D. Mirror backup

Answers

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

Explanations

1. In the event of a server hardware failure, what ensures that application data can continue to be accessed?

A. Local backups

B. Data replication

C. RAID configurations

D. Cloud storage

RAID (Redundant Array of Independent Disks) configurations are specifically designed to enhance data availability and reliability in the event of a hardware failure. By utilizing multiple disks to store data, RAID can provide redundancy, which means that if one disk fails, the data can still be accessed from the remaining disks within the array. Various RAID levels offer different balances of redundancy, performance, and storage capacity; for example, RAID 1 mirrors data between two disks, while RAID 5 distributes data and parity across three or more disks. This redundancy ensures that applications can continue to function with minimal disruption even if a hardware component, such as a hard drive, experiences failure. In contrast, local backups involve creating copies of data that are stored separately from the primary data source. While helpful for disaster recovery, local backups do not provide immediate access to application data if the server fails. Data replication, which involves duplicating data across different locations or systems, can be effective but may require additional configuration and slightly longer recovery times than what RAID systems provide. Cloud storage offers off-site data accessibility, but again, it usually involves a re-establishment of connectivity to access the data, which may not serve the immediate need for continuous application operation upon hardware failure. Thus, RAID configurations

2. What should a technician attempt FIRST to resolve missing files in a home directory on a Linux server?

A. mount /home

B. Check file permissions

C. Restart the NFS service

D. Run a file recovery tool

Mounting the /home directory should be the first step to resolve missing files on a Linux server because the home directory is typically a separate filesystem that needs to be mounted for access. If the /home directory is not mounted, users will not see any of their files or subdirectories, which can lead to the misunderstanding that files are missing. By mounting the /home directory, the technician can verify whether the relevant filesystem containing the user home directories has been properly attached and is accessible. Other options such as checking file permissions or restarting the NFS service could be necessary steps after ensuring that the filesystem itself is mounted. If the home directory is not mounted, checking permissions or trying to recover files would not yield any results, as the system wouldn't have access to the actual directory structure or files. Similarly, running a file recovery tool would only be warranted if it was confirmed that the files were indeed missing from an accessible filesystem, which is not the case if the mounting issue is at play.

3. A technician found a Linux server cannot mount an NFS share. What should be performed FIRST?

A. Check network connectivity

B. Verify NFS server status

C. Create the mount point

D. Review NFS export settings

To address the issue of a Linux server being unable to mount an NFS share, the first step should be to ensure that the mount point exists. The mount point is the directory on the local system where the NFS share will be accessed. If this directory does not exist, the system will be unable to successfully complete the mount operation, leading to errors. Creating the mount point is critical before proceeding to further diagnostics or checks. While it is indeed important to verify network connectivity, the status of the NFS server, and the export settings later in the troubleshooting process, having a valid mount point is a prerequisite for any successful mounting operation. If the mount point is absent, no further troubleshooting will be effective until that fundamental issue is addressed. Therefore, establishing the mount point is the first logical step in resolving the inability to mount the NFS share.

4. What tool should a server administrator use to check for unnecessary running services across multiple servers?

A. A port scanner

B. Remote Desktop

C. Network monitor

D. Task manager

A port scanner is an effective tool for a server administrator to check for unnecessary running services across multiple servers because it allows for the examination of the services and their associated ports being utilized on those servers. By scanning the network, the administrator can quickly identify which services are actively running, determine their status, and ascertain whether any of them are unnecessary or potentially vulnerable. This approach is especially beneficial in a larger server environment, where manually checking each server may be impractical. A port scanner provides a systematic way to assess service configurations across multiple endpoints efficiently. In contrast, while remote desktop can provide access to a server to view running services, it requires logging into each system individually, which is time-consuming for multiple servers. A network monitor is useful for analyzing traffic and performance metrics but does not directly identify specific services running on the servers. Task manager allows viewing running services on an individual server but does not cater to managing multiple servers simultaneously.

5. What is the BEST action to take before applying patches in a high availability cluster?

A. Backup the entire system

B. Fallback cluster services

C. Update user permissions

D. Reboot all servers

The best action to take before applying patches in a high availability cluster is to fallback cluster services. In a high availability (HA) environment, services across multiple nodes work in tandem to ensure that applications remain operational even if one node fails. By gracefully falling back cluster services, you can ensure that the remaining nodes maintain the workload and that users experience minimal disruption during the patching process. Falling back services allows for a controlled transition, reducing the risk of downtime and maintaining service availability. It facilitates the patching of one node at a time, so that if a problem arises after applying the patch, the impact can be quickly mitigated by returning the service to another active node. This approach is vital in maintaining the cluster's integrity and provides a safety net for the maintenance operations being performed. In contrast, backing up the entire system and updating user permissions are best practices that should be part of regular maintenance and preparation, but they do not specifically address the immediate need to maintain service availability during the patching process. Rebooting all servers may lead to downtime or service interruptions, which contradicts the purpose of having an HA cluster.

6. What tool can be used to monitor and maintain server uptime?

A. Server management software

B. Power monitoring tools

C. MTTR calculation tools

D. Log analysis tools

Server management software is designed specifically to monitor, manage, and maintain the performance and uptime of servers. This type of software provides a range of functionalities, including real-time monitoring of system health, performance metrics, and alerts for any issues that could affect server availability. It helps administrators ensure servers are functioning optimally and can quickly identify and address problems that arise, thereby reducing downtime. In contrast, power monitoring tools primarily focus on the power consumption and electrical performance of server hardware. They do not directly monitor server uptime but can play a role in preventing downtime caused by power issues. MTTR (Mean Time to Repair) calculation tools measure the average time required to repair a system after failure. While understanding MTTR can assist administrators in assessing service response and repair efficiency, it does not provide real-time monitoring or maintenance capabilities. Log analysis tools are useful for reviewing and analyzing logs generated by the server, which can help in troubleshooting and identifying trends over time. However, they do not actively monitor the server's operational status in real-time. Thus, server management software stands out as the most comprehensive solution for ensuring server uptime through proactive monitoring and management.

7. An administrator encounters error messages when using YUM to update applications on a server. What should be checked FIRST?

A. YUM dependencies

B. Server hardware

C. Network connectivity

D. System logs

When encountering error messages while using YUM (Yellowdog Updater Modified) to update applications, the first step is to check YUM dependencies. This is crucial because YUM manages package installations based on dependencies required by the software being updated. If there are unmet or broken dependencies, it can prevent successful updates and result in errors appearing during the process. Understanding that these errors often stem from packages that rely on specific versions of libraries and other packages highlights the significance of checking dependencies first. If, for example, a required package is missing or is the wrong version, YUM will not be able to complete the update, and such issues need to be resolved before addressing other potential problems. Network connectivity can also be important since YUM may need to access online repositories to fetch the updates, but without first verifying that the dependencies are properly configured, you may not be able to ascertain if network issues are the root cause of the problem. Similarly, checking server hardware or system logs may be useful later on, but they are less directly related to the immediate issues being encountered with the package updates. Thus, focusing first on YUM dependencies is the most logical approach to troubleshoot the problem effectively.

8. Which file is essential for configuring SSH settings on a Linux server?

A. /etc/ssh/ssh_config

B. /etc/ssh/sshd_config

C. /etc/passwd

D. /etc/group

The file that is essential for configuring SSH settings on a Linux server is /etc/ssh/sshd_config. This configuration file is specifically used by the SSH daemon (sshd), which handles incoming SSH connections. Within this file, system administrators can set various parameters that control the behavior of the SSH server, including options for authentication methods, allowed users, and port settings. This makes it crucial for establishing secure connections, managing user access, and implementing security policies for remote logins. It essentially governs how the SSH server operates and defines settings that directly affect the security and functionality of SSH on the server. In contrast, while /etc/ssh/ssh_config is also related to SSH, it is primarily used for client-side configuration. The other options, /etc/passwd and /etc/group, are important for managing user accounts and groups on the system but do not pertain to SSH configuration specifically.

9. Which method can be used to monitor compliance with a code of conduct among employees?

A. Regular audits

B. Anonymous reporting tools

C. Frequent training sessions

D. All of the above

To effectively monitor compliance with a code of conduct among employees, multiple strategies can be implemented, each serving a unique purpose. Regular audits are essential as they provide a systematic review of an organization's adherence to its established policies. Audits can reveal discrepancies and ensure that employees are following the expected behaviors and practices outlined in the code of conduct. Anonymous reporting tools play a critical role by allowing employees to report any violations or concerns without fear of retaliation. This method encourages open communication and can help management identify areas that require immediate attention or improvement. Frequent training sessions are also vital, as they not only educate employees about the code of conduct but also reinforce its importance through continual reminders. Training ensures that all employees are aware of the standards expected of them and understand the implications of not adhering to these guidelines. Utilizing all these methods together creates a comprehensive approach to monitoring compliance. Each method supports and enhances the effectiveness of the others, ensuring a culture of accountability and ethical behavior within the organization. This multifaceted approach is essential for fostering an environment where employees feel empowered to uphold the code of conduct.

10. What type of backup records only the changes made to data blocks on a virtual machine?

A. Full backup

B. Differential backup

C. Incremental backup

D. Mirror backup

The correct answer is incremental backup. Incremental backups are designed to capture only the changes that have occurred since the last backup, which can be either a full backup or the previous incremental backup. This approach optimizes storage use and reduces the backup time because it only focuses on new or modified data blocks on the virtual machine, rather than backing up all the data again. In a full backup, the entire set of data is backed up, creating a complete copy regardless of what has changed. Differential backups, on the other hand, save changes made since the last full backup, which can lead to larger backup sizes as time goes on because they accumulate changes. Mirror backups create an exact copy of the data at the moment of the backup but do not maintain a history of changes, which is not the focus of the question regarding only capturing changes. The incremental backup method is especially efficient for virtual machines, where storage space can be limited, and minimizing backup time is crucial.

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!