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

Study Guide

Everything you need from our exam experts!

Questions

1. **What are the BEST backup methods to use when a quick restore is desired while minimizing backup media usage?**

   A. Full backups and Incremental backups

   B. Differential and Synthetic full backups

   C. Mirroring and Cloud backups

   D. Snapshot backups and Local backups

2. **What is the first troubleshooting step to take when servers become unresponsive after an update?**

   A. Check physical connections

   B. Reinstall the operating system

   C. Monitor performance metrics

   D. Review patch notes for known issues

3. **What are the BEST immediate actions to prevent unauthorized server access when a large number of connections to port 80 are discovered on a non-web server?**

   A. Initialize a virus scan and disable all ports

   B. Audit all group privileges and permissions

   C. Reboot the server and update antivirus software

   D. Install a web application firewall

4. **To optimize application data performance, which RAID level should the administrator implement?**

   A. RAID 0

   B. RAID 1

   C. RAID 5

   D. RAID 6

5. **Which connector should a server administrator use when connecting a server that requires 40Gb network connectivity?**

   A. RJ-45

   B. LC

   C. QSFP+

   D. SC

6. What issue could be discovered if a server technician receives a failure message after pinging the server?

A. Firewall settings

B. Incorrect subnet mask

C. Duplicate IP address

D. Faulty network cable

7. What is a common result of having outdated firmware on a server?

A. Improved performance

B. Increased security vulnerabilities

C. Compatibility with newer applications

D. Reduced system downtime

8. What strategy would BEST help protect an organization against social engineering?

A. An updated code of conduct to enforce social media

B. Regular phishing tests

C. Employee training on security

D. Increased monitoring of network traffic

9. Which access control methodology is best described as granting a user the minimum required access based on their job needs?

A. Discretionary Access Control

B. Mandatory Access Control

C. Role-Based Access Control

D. Rule-Based Access Control

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

A. 80

B. 22

C. 443

D. 3389

Answers

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

Explanations

1. What are the BEST backup methods to use when a quick restore is desired while minimizing backup media usage?

A. Full backups and Incremental backups

B. Differential and Synthetic full backups

C. Mirroring and Cloud backups

D. Snapshot backups and Local backups

The most effective backup methods for achieving a quick restore while minimizing backup media usage are differential and synthetic full backups. Differential backups capture all changes made since the last full backup, which allows for a faster restore process compared to incremental backups, as only the last full and the most recent differential backup need to be restored. This significantly reduces the number of backup sets required for a complete recovery, as opposed to using full and incremental backups, which require restoring each incremental backup in the correct order. Synthetic full backups enhance this process by creating a full backup from previous backups without needing to revert to the original data source. They combine data from existing full and incremental backups to create a new full backup, minimizing the time required to restore data, while also conserving storage space. This combination effectively meets the dual requirements of quick restoration and reduced media usage, making it an optimal choice for backup strategy.

2. What is the first troubleshooting step to take when servers become unresponsive after an update?

A. Check physical connections

B. Reinstall the operating system

C. Monitor performance metrics

D. Review patch notes for known issues

When servers become unresponsive after an update, the first step should be to review patch notes for known issues. This approach helps identify any documented problems that might result from the recent update, including compatibility issues, bugs introduced by the update, or specific conditions under which problems may arise. By understanding the potential ramifications of the update, administrators can quickly determine if the unresponsiveness is related to the changes made. This initial step prioritizes informed decision-making and may provide guidance on how to proceed—whether it involves rolling back the update, applying additional fixes, or implementing workarounds. Recognizing these issues early can save time and prevent unnecessary troubleshooting efforts on unrelated factors. In contrast, checking physical connections, reinstalling the operating system, or monitoring performance metrics are also important troubleshooting steps, but they are typically not the most effective first measures. These actions may address symptoms but may not directly relate to the root cause stemming from the recent update.

3. What are the BEST immediate actions to prevent unauthorized server access when a large number of connections to port 80 are discovered on a non-web server?

A. Initialize a virus scan and disable all ports

B. Audit all group privileges and permissions

C. Reboot the server and update antivirus software

D. Install a web application firewall

The best immediate action to prevent unauthorized server access in the scenario described is to audit all group privileges and permissions. This approach is essential because it enables the identification of any misconfigurations or unauthorized changes that may have allowed increased connections to port 80, which is typically associated with web traffic. By auditing group privileges and permissions, you can ensure that only authorized users have access to sensitive areas of the server and can take appropriate actions to revoke any excessive rights that could facilitate unauthorized access. This not only helps in addressing the immediate concern of unauthorized connections but also establishes a security baseline for ongoing server management. In contrast, while initializing a virus scan and disabling all ports might seem like a drastic measure to halt unauthorized access immediately, it would significantly disrupt server operations, especially if legitimate services rely on those connections. Rebooting the server and updating antivirus software may improve overall security and performance but would not directly address the unauthorized access issue at hand. Similarly, installing a web application firewall is a valuable long-term solution for web traffic monitoring and securing web applications, but it doesn't provide the immediate assessment needed to identify and rectify current access issues. Thus, auditing group privileges and permissions stands out as the most effective immediate action to understand and manage access to your server effectively.

4. To optimize application data performance, which RAID level should the administrator implement?

A. RAID 0

B. RAID 1

C. RAID 5

D. RAID 6

When considering which RAID level to implement for optimizing application data performance, RAID 5 is often favored due to its balance of data redundancy and performance. RAID 5 utilizes striping with parity, meaning that data is split into blocks and distributed across multiple disks, which enhances read performance. This configuration allows simultaneous access to multiple drives, speeding up data retrieval processes, which is particularly beneficial for applications requiring quick access to data. The parity data, which is distributed across the drives, also provides fault tolerance, allowing for the recovery of data in the event of a single drive failure without significant downtime. This balance of enhanced performance and redundancy makes RAID 5 a common choice for improving application data performance while also protecting against data loss. In contrast, other RAID levels, such as RAID 0, focus solely on performance through striping but offer no redundancy. RAID 1 provides mirroring, which improves read speeds but can slow down write operations since data must be duplicated across drives. RAID 6 offers additional data protection through the use of double parity but typically incurs a performance cost compared to RAID 5 because it requires more processing to manage the additional parity information. This understanding of RAID levels highlights how RAID 5 delivers both improved performance and data security, making

5. Which connector should a server administrator use when connecting a server that requires 40Gb network connectivity?

A. RJ-45

B. LC

C. QSFP+

D. SC

The QSFP+ connector is specifically designed for high-speed data transmission, supporting 40Gb Ethernet and InfiniBand connections. It utilizes four channels, each capable of transmitting data at 10Gbps, allowing for a total of 40Gbps throughput. This higher bandwidth makes it ideal for data centers and environments where large amounts of data need to be transferred quickly. In contrast, RJ-45 is commonly used for standard Ethernet connections, typically supporting up to 1Gb Ethernet, with some newer standards reaching up to 10Gbps but still falling short for 40Gb connections. The LC and SC connectors are primarily used for fiber optic cables; while they are excellent for various data rates, they do not inherently support the 40Gbps connections associated with QSFP+. Thus, for scenarios where high-speed connectivity is essential, QSFP+ is the preferred choice.

6. What issue could be discovered if a server technician receives a failure message after pinging the server?

A. Firewall settings

B. Incorrect subnet mask

C. Duplicate IP address

D. Faulty network cable

When a server technician receives a failure message after pinging the server, one potential issue that could be identified is a duplicate IP address. If multiple devices on the network are configured with the same IP address, a conflict occurs. In such a scenario, one device may respond to the ping request while the other does not, leading to an indication of failure. This conflict can result in intermittent connectivity issues, making troubleshooting necessary to ensure each device has a unique IP configuration. Understanding how IP addressing works within a network is crucial, as unique addresses are required for proper communication. Recognizing the symptoms of duplicate IP addresses and addressing this issue is a foundational aspect of server management and network troubleshooting. This knowledge helps maintain network stability and reliability.

7. What is a common result of having outdated firmware on a server?

A. Improved performance

B. Increased security vulnerabilities

C. Compatibility with newer applications

D. Reduced system downtime

Having outdated firmware on a server commonly results in increased security vulnerabilities. Firmware is essential for the operation of hardware components, and manufacturers often release updates to patch known security issues, enhance functionality, and improve system stability. If the firmware is not updated, these vulnerabilities remain unaddressed, potentially exposing the server to attacks or exploitation by malicious actors. By keeping firmware up to date, system administrators can ensure that the server is protected against newly discovered threats and that any security patches implemented by the manufacturer are applied. This step is crucial for maintaining the integrity and security of the server and the data it processes.

8. What strategy would BEST help protect an organization against social engineering?

A. An updated code of conduct to enforce social media

B. Regular phishing tests

C. Employee training on security

D. Increased monitoring of network traffic

The best strategy to protect an organization against social engineering is employee training on security. Effective training equips employees with the knowledge and awareness to recognize social engineering tactics, such as impersonation or manipulation, that malicious actors might use. It encourages a culture of skepticism regarding unsolicited communications and teaches staff how to respond appropriately, such as verifying identities or reporting suspicious activity. Through regular security training sessions, employees learn about the common techniques used in social engineering, including phishing, pretexting, and baiting. This proactive approach empowers them to identify and avoid potential threats, thereby directly reducing the organization's vulnerability to these tactics. While an updated code of conduct and policies might outline acceptable behaviors, they are not as effective alone in changing employee behavior and awareness. Regular phishing tests are beneficial for assessing employee readiness, but they do not replace the foundational knowledge that comprehensive training provides. Increased monitoring of network traffic is more of a response measure rather than a preventative strategy against social engineering. Therefore, educating employees through targeted security training is critical for building a resilient defense against social engineering attacks.

9. Which access control methodology is best described as granting a user the minimum required access based on their job needs?

A. Discretionary Access Control

B. Mandatory Access Control

C. Role-Based Access Control

D. Rule-Based Access Control

The best access control methodology that involves granting a user the minimum required access based on their job needs is Role-Based Access Control (RBAC). This approach assigns permissions to users based on their specific roles within an organization. In RBAC, roles are defined according to job functions, and users are assigned to these roles. This ensures that individuals have access only to the information and resources necessary to perform their job duties, thereby following the principle of least privilege. This method not only enhances security by limiting access to sensitive information but also simplifies the management of permissions in environments with numerous users and varying access needs. By structuring access around roles, organizations can efficiently manage user privileges and ensure that users are not over-privileged, reducing the risk of data breaches and misuse. The other methodologies mentioned—Discretionary Access Control, Mandatory Access Control, and Rule-Based Access Control—have different focuses and mechanisms. Discretionary Access Control allows users to control access to resources they own, which can lead to broader access than necessary. Mandatory Access Control enforces strict rules determined by the system administrator, not tailored to individual job needs. Rule-Based Access Control relies on predefined rules to control access rather than roles, making it less aligned with the principle of granting access based solely

10. 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.