CompTIA Server+ (SK0-004) Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **Which methodology would be used to present a SAN hosted LUN to only a single host?**

   A. LUN masking

   B. LUN ID assignment

   C. Port mapping

   D. Port zoning

2. **Which networking tool should a system administrator use to verify network connectivity?**

   A. arp

   B. netstat

   C. ipconfig

   D. ping

3. **What is the MOST secure way to dispose of 150 computers with SATA HDDs?**

   A. Use a degaussing tool on the hard drives

   B. Use disk-wiping software

   C. Use a shredder to physically destroy the platters

   D. Use zero-fill utility on the hard drive

4. **What is the best method to ensure high availability for a mission-critical application on a single server?**

   A. Configure failover clustering using Server A and a new server.

   B. Add multiple disks and configure RAID 5.

   C. Add an additional NIC and configure it as standby.

   D. Move the application to another server with more resources.

5. **In troubleshooting an email issue, which ordered steps should the administrator take first?**

   A. Reboot the email server, document findings, collect information

   B. Collect information, determine the scope, document findings

   C. Document findings, reboot the server, collect information

   D. Determine scope, collect information, reboot and document

6. What is the most likely reason a systems administrator cannot back up user files?

A. The files are currently open

B. The files have been copied

C. The files have been modified

D. The files are compressed

7. How can a server administrator increase the availability of a web server without clustering?

A. Configure round robin DNS entries

B. Configure an active/active service

C. Configure an active/passive service

D. Configure two servers with the same IP address

8. Which of the following protocols can be used to query for host, user, and group information for clients?

A. LDAP

B. DNS

C. DHCP

D. SNMP

9. To ensure safety against toxic fumes, which cable type is recommended?

A. CAT6 cables

B. Plenum cables

C. Fiber cables

D. Coaxial cables

10. Which tool is most effective for a security administrator to analyze network traffic on a single VLAN used by vendors?

A. Port scanner

B. Cipher

C. Sniffer

D. Checksum

Answers

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

Explanations

1. Which methodology would be used to present a SAN hosted LUN to only a single host?

A. LUN masking

B. LUN ID assignment

C. Port mapping

D. Port zoning

LUN masking is a crucial methodology used in storage area networks (SAN) to control which hosts are able to access specific Logical Unit Numbers (LUNs). By implementing LUN masking, administrators can effectively present a LUN to only a designated single host, ensuring that access is limited and secure. This is particularly pertinent in environments where multiple hosts may be connected to the same SAN, as it prevents unauthorized access to data and helps maintain data integrity. LUN ID assignment, while related to the identification of LUNs, does not control which hosts can access them but rather designates the unique identifiers for the LUNs themselves. Port mapping, on the other hand, refers to the configuration that determines how a host communicates with specific storage resources, which does not restrict access to LUNs by particular hosts. Port zoning is a security technique used to control access at the port level within the fabric of the SAN, but it does not directly address the issue of presenting a LUN to just one host. Therefore, LUN masking is the most effective method for ensuring that a LUN is presented solely to a single host, protecting the data and maintaining appropriate access controls.

2. Which networking tool should a system administrator use to verify network connectivity?

A. arp

B. netstat

C. ipconfig

D. ping

The most appropriate tool for a system administrator to verify network connectivity is the ping command. This utility sends Internet Control Message Protocol (ICMP) Echo Request messages to a specified IP address or hostname and waits for an Echo Reply. By using ping, an administrator can check whether a device is reachable over the network and determine the round-trip time for messages sent from the source to the destination and back. If the ping command receives replies, it indicates that the network connection to the target device is functioning properly. In contrast, the other options have different primary functions. The arp command is used for displaying and modifying the Address Resolution Protocol (ARP) cache, which maps IP addresses to MAC addresses, and is not specifically designed to test connectivity. The netstat command provides network statistics and details about open connections but does not verify connectivity directly. Lastly, the ipconfig command (or ifconfig in Linux environments) displays the current network configuration of a device, including IP addresses, subnet masks, and gateways, but it does not check the reachability of other devices; it is more about configuration than connectivity verification.

3. What is the MOST secure way to dispose of 150 computers with SATA HDDs?

A. Use a degaussing tool on the hard drives

B. Use disk-wiping software

C. Use a shredder to physically destroy the platters

D. Use zero-fill utility on the hard drive

The most secure method for disposing of computers with SATA HDDs is to physically destroy the platters using a shredder. This approach ensures that the data on the drives cannot be recovered by any means. When platters are shredded, they are broken into small, unrecognizable pieces, physically preventing any access to the data stored on them. This method is particularly effective for organizations that must meet strict data security requirements or regulatory compliance, as it provides absolute assurance that sensitive information cannot be retrieved. While other methods, such as degaussing, wiping software, or zero-fill utilities, can effectively eliminate or obscure data, they do not guarantee the complete physical destruction of the storage media. For instance, while degaussing can render a hard drive unusable, sophisticated methods can sometimes recover data from damaged disks. Similarly, wiping software may be effective under normal circumstances, but there are instances where residual data may be recoverable, especially if the software is not properly used or if the drives are malfunctioning. Hence, shredding the platters offers the highest level of data protection and security.

4. What is the best method to ensure high availability for a mission-critical application on a single server?

A. Configure failover clustering using Server A and a new server.

B. Add multiple disks and configure RAID 5.

C. Add an additional NIC and configure it as standby.

D. Move the application to another server with more resources.

To ensure high availability for a mission-critical application on a single server, configuring failover clustering is the most effective method. Failover clustering allows multiple servers to work together as a single system to provide continuous availability. If one server (also known as a node) fails, the application can automatically switch over to another server in the cluster, which minimizes downtime and risk of disruption to users. This method is especially powerful for mission-critical applications, as it enables seamless failover without significant interruption. By using additional hardware resources, such as a second server, organizations can create redundancy and maintain service continuity even in the event of hardware or software failures. The other options, while beneficial in their own contexts, do not provide the same level of high availability. Adding multiple disks and configuring RAID 5 improves data reliability and redundancy but does not protect against server failures. Similarly, adding an additional NIC configured as standby enhances network reliability but does not address the overall availability of the server itself. Moving the application to another server may provide more resources, but it does not inherently offer a solution for high availability on the original server. Thus, failover clustering is the optimal choice for achieving high availability in this scenario.

5. In troubleshooting an email issue, which ordered steps should the administrator take first?

A. Reboot the email server, document findings, collect information

B. Collect information, determine the scope, document findings

C. Document findings, reboot the server, collect information

D. Determine scope, collect information, reboot and document

The appropriate sequence of steps when troubleshooting an email issue begins with collecting information, determining the scope of the problem, and then documenting findings. This structured approach is crucial because it allows the administrator to gather all relevant data about the issue at hand, which is necessary to understand its impact fully. First, collecting information should involve investigating error messages, user reports, and server logs to identify any anomalies. Next, determining the scope helps assess how widespread the issue is—whether it's affecting a single user, a specific group, or an entire system. This clarity is essential for prioritizing the response and informing any subsequent actions. Following these initial steps, documenting findings becomes critical for maintaining a record of what has transpired, which will be useful for future reference and in evaluating the effectiveness of the solutions applied. Rebooting the server is often a last resort or part of a solution rather than a starting action. Immediate reboots could overlook critical data that's necessary for diagnosing the problem. Thus, the best strategy involves first gathering comprehensive information and assessing the situation before taking any corrective measures.

6. What is the most likely reason a systems administrator cannot back up user files?

A. The files are currently open

B. The files have been copied

C. The files have been modified

D. The files are compressed

The most likely reason a systems administrator cannot back up user files is that the files are currently open. When files are open, especially in applications that maintain a lock on the file (such as databases or documents being edited), the operating system may prevent any processes, including backup operations, from accessing those files to ensure data integrity. Backing up open files can lead to inconsistent or corrupt backup copies, as the files may change during the backup process. In contrast, files that have been copied, modified, or compressed generally do not prevent a backup from occurring. A copied file is simply a duplicate and can be backed up like any other file. Similarly, modified files can still be backed up, and the backup may capture the most recent version of the file. Compressed files, while handled differently by backup software, are also not typically a barrier to performing a backup. Thus, the state of a file being open presents a unique situation that can hinder the backup process.

7. How can a server administrator increase the availability of a web server without clustering?

A. Configure round robin DNS entries

B. Configure an active/active service

C. Configure an active/passive service

D. Configure two servers with the same IP address

The correct strategy to increase the availability of a web server without using clustering is to configure round robin DNS entries. This method allows multiple IP addresses to be associated with a single domain name. When a client makes a request to the server, the DNS server responds with one of the available IP addresses in a rotating manner, which distributes the incoming traffic across several servers. This not only balances the load but also provides redundancy; if one server goes down, requests can still be served by the remaining servers. Configuring an active/active service involves having multiple servers actively processing requests simultaneously, which can be complex and often requires clustering to manage the load efficiently. An active/passive service setup typically involves one server actively handling requests while another is on standby, which may not improve availability since the passive server only becomes active when the primary fails. Configuring two servers with the same IP address would lead to networking conflicts, causing connectivity issues rather than enhancing availability.

8. Which of the following protocols can be used to query for host, user, and group information for clients?

A. LDAP

B. DNS

C. DHCP

D. SNMP

The correct answer is LDAP, which stands for Lightweight Directory Access Protocol. LDAP is specifically designed to enable applications to query and modify directory services running over TCP/IP. It is commonly used for accessing and maintaining distributed directory information services, which store details about users, groups, and resources on a network. Using LDAP, organizations can efficiently manage information such as user authentication, authorization, and roles within a centralized directory service. For example, when a client system needs to find information about a user or a group, it can send a query to the LDAP server, which will return the relevant details. This makes LDAP an essential protocol in environments where user and group management is crucial, such as in enterprise settings that utilize directory services for identity management. Other protocols listed do serve various roles in networking, but they do not specifically provide the functionality of querying host, user, and group information in the same way that LDAP does. For instance, DNS (Domain Name System) is used primarily for resolving domain names to IP addresses, while DHCP (Dynamic Host Configuration Protocol) is responsible for dynamically assigning IP addresses to devices on a network. SNMP (Simple Network Management Protocol) is utilized for monitoring and managing network devices but does not handle directory services or user/group information. Therefore

9. To ensure safety against toxic fumes, which cable type is recommended?

A. CAT6 cables

B. Plenum cables

C. Fiber cables

D. Coaxial cables

Plenum cables are specifically designed for use in areas where they could be exposed to air circulation, such as in the spaces above ceilings or below floors where HVAC systems are present. These cables have a special fire-retardant jacket that helps prevent the spread of flames and reduces the amount of toxic fumes that would be emitted if the cable were to catch fire. In environments where safety against toxic fumes is a concern, such as commercial buildings or data centers, it is essential to use cabling that meets safety standards for flame resistance and low emissions of harmful gases. Plenum-rated cables are able to do this, making them the recommended choice for such applications. Other types of cables, like CAT6, fiber, and coaxial cables, do not necessarily have the same level of fire safety specifications tailored for use in plenum spaces, thus making them less suitable for ensuring safety in those environments.

10. Which tool is most effective for a security administrator to analyze network traffic on a single VLAN used by vendors?

A. Port scanner

B. Cipher

C. Sniffer

D. Checksum

A sniffer is a tool designed specifically to capture and analyze network traffic. In the context of monitoring traffic on a VLAN used by vendors, a sniffer can intercept packets that traverse the network, providing insights into the data flowing to and from devices within that VLAN. This enables a security administrator to examine the contents of packets, identify potential security issues, track usage patterns, monitor for unauthorized access, and troubleshoot network problems. Using a sniffer, the administrator can determine if any suspicious activity is occurring, such as unauthorized access attempts or the presence of potentially malicious traffic. This capability is essential in maintaining the security and integrity of the network, especially in environments where external vendors may have access to sensitive information. Other tools mentioned, such as a port scanner, are useful for discovering open ports and services on devices but do not provide the detailed traffic analysis needed for in-depth monitoring or troubleshooting of network communications. Similarly, a cipher is related to the encryption and decryption of data, while a checksum is used to verify data integrity rather than analyze traffic. Therefore, a sniffer is the most effective tool for the specific task of analyzing network traffic within a VLAN.