

# CompTIA

## Exam Questions SK0-005

CompTIA Server+ Certification Exam



**NEW QUESTION 1**

A server administrator mounted a new hard disk on a Linux system with a mount point of /newdisk. It was later determined that users were unable to create directories or files on the new mount point. Which of the following commands would successfully mount the drive with the required parameters?

- A. echo /newdisk >> /etc/fstab
- B. net use /newdisk
- C. mount -o remount, rw /newdisk
- D. mount -a

**Answer: C**

**Explanation:**

The administrator should use the command mount -o remount,rw /newdisk to successfully mount the drive with the required parameters. The mount command is used to mount file systems on Linux systems. The -o option specifies options for mounting file systems. The remount option re-mounts an already mounted file system with different options. The rw option mounts a file system with read-write permissions. In this case, /newdisk is a mount point for a new hard disk that was mounted with read-only permissions by default. To allow users to create directories or files on /newdisk, the administrator needs to re-mount /

Reference:

<https://unix.stackexchange.com/QUESTION NO:s/149399/how-to-remount-as-read-write-a-specific-mount-of-device>

**NEW QUESTION 2**

A data center employee shows a driver's license to enter the facility Once the employee enters, the door immediately doses and locks, triggering a scale that then weighs the employee before granting access to another locked door. This is an example of.

- A. mantrap.
- B. a bollard
- C. geofencing
- D. RFID.

**Answer: A**

**Explanation:**

A mantrap is a security device that consists of a small space with two sets of interlocking doors, such that the first set of doors must close before the second one opens. A mantrap can be used to control access to a data center by verifying the identity and weight of the person entering. A bollard is a sturdy post that prevents vehicles from entering a restricted area. Geofencing is a technology that uses GPS or RFID to create a virtual boundary around a location and trigger an action when a device crosses it. RFID is a technology that uses radio waves to identify and track objects or people. References:

? <https://www.techopedia.com/definition/16293/mantrap>

? <https://www.techopedia.com/definition/1437/bollard>

? <https://www.techopedia.com/definition/23961/geofencing>

? <https://www.techopedia.com/definition/506/radio-frequency-identification-rfid>

**NEW QUESTION 3**

An administrator is rebooting servers manually after a group of updates were deployed through SCCM. The administrator notices several of the servers did not receive the deployed update. Which of the following should the administrator review first?

- A. Confirm the server has the current OS updates and security patches installed.
- B. Confirm the server OS has a valid Active Directory account.
- C. Confirm the server does not have the firewall running.
- D. Confirm the server is in the collection scheduled to receive the update.

**Answer: D**

**Explanation:**

The first thing the administrator should check is whether the server is in the collection that was scheduled to receive the update through SCCM. A collection is a group of resources, such as computers or users, that can be managed as a single entity by SCCM. If the server is not in the collection, it will not receive the update. The other options are less likely to be the cause of the problem, as they would affect other aspects of the server's functionality besides receiving updates. References: CompTIA Server+ Certification Exam Objectives, Domain 5.0: Security, Objective 5.4: Given a scenario, apply patches/updates and validate their installation.

**NEW QUESTION 4**

A server administrator is installing a new server that uses 40G0 network connectivity. The administrator needs to find the proper cables to connect the server to the switch. Which of the following connectors should the administrator use?

- A. SFP+
- B. GBIC
- C. SFP
- D. QSFP+

**Answer: D**

**Explanation:**

QSFP+ is a type of connector that should be used to connect a server to a switch that uses 40G network connectivity. QSFP+ (Quad Small Form-factor Pluggable Plus) is a compact, hot-pluggable transceiver module that supports data rates up to 40 Gbps. QSFP+ modules can be used for various network protocols and media types, such as Ethernet, Fibre Channel, InfiniBand, or optical fiber. QSFP+ modules have a 38-pin edge connector and can be inserted into a QSFP+ port on a switch or a server. SFP+ (Small Form-factor Pluggable Plus) is a type of connector that supports data rates up to 10 Gbps, but not 40 Gbps. SFP+ modules have a 20-pin edge connector and can be inserted into an SFP+ port on a switch or a server. GBIC (Gigabit Interface Converter) is an older type of connector that supports data rates up to 1 Gbps, but not 40 Gbps. GBIC modules have an SC duplex connector and can be inserted into a GBIC port on a switch or a server. SFP

(Small Form-factor Pluggable) is another older type of connector that supports data rates up to 1 Gbps or 4 Gbps, but not 40 Gbps. SFP modules have an LC duplex connector and can be inserted into an SFP port on a switch or a server. References: <https://www.howtogeek.com/190014/virtualization-basics-understanding-techniques-and-fundamentals/> <https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-it-matter/> <https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual-files/>

#### NEW QUESTION 5

Joe, a user in the IT department cannot save changes to a sensitive file on a Linux server. An ls -l shows the following listing:

```
-rw-r--r 1 Ann IT 6780 12 June 2019 filename
```

Which of the following commands would BEST enable the server technician to allow Joe to have access without granting excessive access to others?

- A. chmod 777 filename
- B. chown Joe filename
- C. Chmod g+w filename
- D. chgrp IT filename

**Answer: C**

#### Explanation:

The chmod command is used to change the permissions of files and directories. The g+w option means to grant write permission to the group owner of the file. Since Joe is a member of the IT group, which is also the group owner of the file, this command will allow him to save changes to the file without affecting the permissions of other users. Verified References: [Linux chmod command]

#### NEW QUESTION 6

A systems administrator recently upgraded the memory in a server, and now the server does not turn on, and nothing is displayed on the screen. Which of the following is the next step the administrator should take to diagnose the error without opening the machine?

- A. Perform a cold reboot.
- B. Listen for POST code beeps.
- C. Call technical support.
- D. Check the monitor connection.

**Answer: B**

#### Explanation:

A power-on self-test (POST) is a diagnostic process that runs when a server is turned on to check the basic functionality of the hardware components and report any errors or faults. A POST code is a series of beeps or flashes that indicate the status of the POST process and identify any problems that prevent the server from booting up. A POST code can be heard through a speaker or seen on a display attached to the server motherboard. A POST code is useful for diagnosing errors without opening the machine or using any software tools.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 5, Lesson 5.1, Objective 5.1

#### NEW QUESTION 7

A systems administrator is performing maintenance on 12 Windows servers that are in different racks at a large datacenter. Which of the following would allow the administrator to perform maintenance on all 12 servers without having to physically be at each server? (Choose two.)

- A. Remote desktop
- B. IP KVM
- C. A console connection
- D. A virtual administration console
- E. Remote drive access
- F. A crash cart

**Answer: AB**

#### Explanation:

The methods that would allow the administrator to perform maintenance on all 12 servers without having to physically be at each server are remote desktop and IP KVM. Remote desktop is a feature that allows a user to access and control another computer over a network using a graphical user interface (GUI). Remote desktop can enable remote administration, troubleshooting, and maintenance of servers without requiring physical presence at the server location. IP KVM (Internet Protocol Keyboard Video Mouse) is a device that allows a user to access and control multiple servers over a network using a single keyboard, monitor, and mouse. IP KVM can provide remote access to servers regardless of their operating system or power state, and can also support virtual media and serial console functions.

Reference:

<https://www.blackbox.be/en-be/page/27559/Resources/Technical-Resources/Black-Box-Explains/kvm/Benefits-of-using-KVM-over-IP>

#### NEW QUESTION 8

A server administrator is installing an OS on a new server. Company policy states no one is to log in directly to the server. Which of the following installation methods is BEST suited to meet the company policy?

- A. GUI
- B. Core
- C. Virtualized
- D. Clone

**Answer: B**

#### Explanation:

A core installation is a type of installation method that is best suited to meet the company policy that states no one is to log in directly to the server. A core

installation is a minimal installation option that is available when deploying some editions of Windows Server. A core installation includes most but not all server roles and features, but does not include a graphical user interface (GUI). A core installation can only be managed remotely using command-line tools such as PowerShell or Windows Admin Center, or using graphical tools such as Server Manager or Remote Desktop from another computer. This reduces the attack surface, resource consumption, and maintenance requirements of the server. A GUI installation is a type of installation method that includes a graphical user interface (GUI) and allows local or remote management using graphical tools or command-line tools. A virtualized installation is a type of installation method that involves creating and running one or more virtual machines on a physical host using a hypervisor such as Hyper-V or VMware. A clone installation is a type of installation method that involves creating an exact copy of an existing server's configuration and data on another server using tools such as Sysprep or Clonezilla. References: <https://www.howtogeek.com/67469/the-beginners-guide-to-shell-scripting-the-basics/> <https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual-files/>  
<https://www.howtogeek.com/199068/how-to-upgrade-your-existing-hard-drive-in-under-an-hour/>

**NEW QUESTION 9**

Which of the following script types would MOST likely be used on a modern Windows server OS?

- A. Batch
- B. VBS
- C. Bash
- D. PowerShell

**Answer: D**

**Explanation:**

PowerShell is a scripting language and a command-line shell that is designed for Windows server administration. It can perform various tasks such as configuration, automation, and management of servers and applications. Verified References: [PowerShell], [Scripting language]

**NEW QUESTION 10**

Alter rack mounting a server, a technician must install four network cables and two power cables for the server. Which of the following is the MOST appropriate way to complete this task?

- A. Wire the four network cables and the two power cables through the cable management arm using appropriate-length cables.
- B. Run the four network cables up the left side of the rack to the top of the rack switch
- C. Run the two power cables down the right side of the rack toward the UPS.
- D. Use the longest cables possible to allow for adjustment of the server rail within the rack.
- E. Install an Ethernet patch panel and a PDU to accommodate the network and power cables.

**Answer: B**

**Explanation:**

This is the most appropriate way to complete the task because it follows the best practices of cable management. Cable management is a process of organizing and securing cables in a rack or a server room to improve airflow, accessibility, safety, and aesthetics. Running the network cables up the left side and the power cables down the right side of the rack helps to avoid cable clutter, interference, and confusion. It also makes it easier to trace and troubleshoot cables if needed. Using appropriate-length cables also helps to reduce cable slack and excess. Wiring the cables through the cable management arm may cause stress and damage to the cables when moving the server in or out of the rack. Using the longest cables possible may create cable loops and tangles that can block airflow and increase fire hazards. Installing an Ethernet patch panel and a PDU (Power Distribution Unit) may be useful for accommodating more network and power cables, but not necessary for a single server. References: <https://www.howtogeek.com/303282/how-to-manage-your-pcs-fans-for-optimal-airflow-and-cooling/>  
<https://www.howtogeek.com/303290/how-to-properly-manage-your-cables/>

**NEW QUESTION 10**

A systems administrator is setting up a new server that will be used as a DHCP server. The administrator installs the OS but is then unable to log on using Active Directory credentials. The administrator logs on using the local administrator account and verifies the server has the correct IP address, subnet mask, and default gateway. The administrator then gets on another server and can ping the new server. Which of the following is causing the issue?

- A. Port 443 is not open on the firewall
- B. The server is experiencing a downstream failure
- C. The local hosts file is blank
- D. The server is not joined to the domain

**Answer: D**

**Explanation:**

The server is not joined to the domain is causing the issue. A domain is a logical grouping of computers that share a common directory database and security policy on a network. Active Directory is a Microsoft technology that provides domain services for Windows-based computers. To use Active Directory credentials to log on to a server, the server must be joined to the domain that hosts Active Directory. If the server is not joined to the domain, it will not be able to authenticate with Active Directory and will only accept local accounts for logon. To join a server to a domain, the administrator must have a valid domain account with sufficient privileges and must know the name of the domain controller that hosts Active Directory.

**NEW QUESTION 14**

A server administrator needs to configure a server on a network that will have no more than 30 available IP addresses. Which of the following subnet addresses will be the MOST efficient for this network?

- A. 255.255.255.0
- B. 255.255.255.128
- C. 255.255.255.224
- D. 255.255.255.252

**Answer: C**

**Explanation:**

The most efficient subnet address for a network that will have no more than 30 available IP addresses is 255.255.255.224. This subnet mask corresponds to a /27

prefix length, which means that 27 bits are used for the network portion and 5 bits are used for the host portion of an IP address. With 5 bits for hosts, there are  $2^5 - 2 = 30$  possible host addresses per subnet, which meets the requirement. The other options are either too large or too small for the network size.  
Reference: <https://www.ibm.com/cloud/learn/subnet-mask>

**NEW QUESTION 19**

A server administrator needs to harden a server by only allowing secure traffic and DNS inquiries. A port scan reports the following ports are open:

- A. 21
- B. 22
- C. 23
- D. 53
- E. 443
- F. 636

**Answer:** D

**Explanation:**

The administrator should only allow secure traffic and DNS inquiries on the server, which means that only ports 22, 53, and 443 should be open. Port 22 is used for SSH (Secure Shell), which is a protocol that allows secure remote login and command execution over a network connection using a command-line interface (CLI). Port 53 is used for DNS (Domain Name System), which is a service that translates domain names into IP addresses and vice versa. Port 443 is used for HTTPS (Hypertext Transfer Protocol Secure), which is a secure version of HTTP that encrypts the data exchanged between a web browser and a web server.

Reference: [https://tools.cisco.com/security/center/resources/dns\\_best\\_practices](https://tools.cisco.com/security/center/resources/dns_best_practices)

**NEW QUESTION 23**

Hackers recently targeted a company with an attack that resulted in a system breach, which compromised the organization's data. Because of the system breach, the administrator had to bypass normal change management procedures. Which of the following change management activities was necessary?

- A. Cancelled change request
- B. Change request postponement
- C. Emergency change request
- D. Privilege change request
- E. User permission change request

**Answer:** C

**Explanation:**

An emergency change request is a type of change management activity that is used to address urgent issues that pose a significant risk to the organization, such as a system breach. An emergency change request requires immediate action and approval, and it may bypass some of the normal change management procedures, such as testing, documentation, or stakeholder communication<sup>12</sup>.

References = 1: Change Management Plans: A Definitive Guide -Indeed(<https://www.indeed.com/career-advice/career-development/change-management-activities>) 2: The 10 Best Change Management Activities-Connecteam(<https://connecteam.com/top-10-change-management-activities/>)

**NEW QUESTION 28**

A technician noted the RAID hard drives were functional while troubleshooting a motherboard failure. The technician installed a spare motherboard with similar specifications and used the original components. Which of the following should the technician do to restore operations with minimal downtime?

- A. Reinstall the OS and programs.
- B. Configure old drives to RAID.
- C. Reconfigure the RAID.
- D. Install from backup.

**Answer:** C

**Explanation:**

RAID (Redundant Array of Independent Disks) is a technology that combines multiple hard drives into a logical unit that provides improved performance, reliability, or capacity. RAID can be implemented by hardware, software, or a combination of both. Hardware RAID uses a dedicated controller to manage the RAID array, while software RAID uses the operating system or a driver to do the same<sup>1</sup>.

In this scenario, the technician noted that the RAID hard drives were functional while troubleshooting a motherboard failure. This means that the data on the drives was not corrupted or lost. However, the technician installed a spare motherboard with similar specifications and used the original components. This means that the new motherboard may not have the same RAID configuration as the old one, or it may not recognize the existing RAID array at all. Therefore, the technician needs to reconfigure the RAID in order to restore operations with minimal downtime.

**NEW QUESTION 33**

A technician wants to limit disk usage on a server. Which of the following should the technician implement?

- A. Formatting
- B. Compression
- C. Disk quotas
- D. Partitioning

**Answer:** C

**Explanation:**

Disk quotas are a way to limit disk usage on a server by setting a maximum amount of space that each user or group can use. Disk quotas can help manage disk space allocation, prevent disk space exhaustion, and enforce fair usage policies. Disk quotas can be set at the volume level or at the folder level, depending on the file system and operating system used. Reference: <https://docs.microsoft.com/en-us/windows-server/storage/ntfs/ntfs-disk-quotas-overview>

**NEW QUESTION 37**



Which of the following are measures that should be taken when a data breach occurs? (Select TWO).

- A. Restore the data from backup.
- B. Disclose the incident.
- C. Disable unnecessary ports.
- D. Run an antivirus scan.
- E. Identify the exploited vulnerability.
- F. Move the data to a different location.

**Answer:** BE

**Explanation:**

These are two measures that should be taken when a data breach occurs. A data breach is an unauthorized or illegal access to confidential or sensitive data by an internal or external actor. A data breach can result in financial losses, reputational damage, legal liabilities, and regulatory penalties for the affected organization. Disclosing the incident is a measure that involves informing the relevant stakeholders, such as customers, employees, partners, regulators, and law enforcement, about the nature, scope, and impact of the data breach. Disclosing the incident can help to mitigate the negative consequences of the data breach, comply with legal obligations, and restore trust and confidence. Identifying the exploited vulnerability is a measure that involves investigating and analyzing the root cause and source of the data breach. Identifying the exploited vulnerability can help to prevent further data loss, remediate the security gaps, and improve the security posture of the organization. Restoring the data from backup is a measure that involves recovering the lost or corrupted data from a secondary storage device or location. However, this does not address the underlying issue of how the data breach occurred or prevent future breaches. Disabling unnecessary ports is a measure that involves closing or blocking network communication endpoints that are not required for legitimate purposes. However, this does not address how the data breach occurred or what vulnerability was exploited. Running an antivirus scan is a measure that involves detecting and removing malicious software from a system or network. However, this does not address how the data breach occurred or what vulnerability was exploited. Moving the data to a different location is a measure that involves transferring the data to another storage device or location that may be more secure or less accessible. However, this does not address how the data breach occurred or what vulnerability was exploited. References: <https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-it-matter/> <https://www.howtogeek.com/202794/what-is-the-difference-between-127.0.0.1-and-0.0.0.0/> <https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual-files/>

**NEW QUESTION 42**

A server technician is installing a new server OS on legacy server hardware. Which of the following should the technician do FIRST to ensure the OS will work as intended?

- A. Consult the HCL to ensure everything is supported.
- B. Migrate the physical server to a virtual server.
- C. Low-level format the hard drives to ensure there is no old data remaining.
- D. Make sure the case and the fans are free from dust to ensure proper cooling.

**Answer:** A

**Explanation:**

The first thing that the technician should do before installing a new server OS on legacy server hardware is to consult the HCL (Hardware Compatibility List) to ensure everything is supported. The HCL is a list of hardware devices and components that are tested and certified to work with a specific OS or software product. The HCL helps to avoid compatibility issues and performance problems that may arise from using unsupported or incompatible hardware. Migrating the physical server to a virtual server may be a good option to improve scalability and flexibility, but it requires additional hardware and software resources and may not be feasible for legacy server hardware. Low-level formatting the hard drives may be a good practice to erase any old data and prepare the drives for a new OS installation, but it does not guarantee that the hardware will work with the new OS. Making sure the case and the fans are free from dust may be a good practice to ensure proper cooling and prevent overheating, but it does not guarantee that the hardware will work with the new OS. References: <https://www.howtogeek.com/190014/virtualization-basics-understanding-techniques-and-fundamentals/> <https://www.howtogeek.com/173353/how-to-low-level-format-or-write-zeros-to-a-hard-drive/> <https://www.howtogeek.com/303282/how-to-manage-your-pcs-fans-for-optimal-airflow-and-cooling/>

**NEW QUESTION 44**

An administrator is configuring a server to communicate with a new storage array. To do so, the administrator enters the WWPN of the new array in the server's storage configuration. Which of the following technologies is the new connection using?

- A. iSCSI
- B. eSATA
- C. NFS
- D. FcoE

**Answer:** A

**Explanation:**

Reference: [https://docs.oracle.com/cd/E26996\\_01/E18549/html/BABHBFHA.html](https://docs.oracle.com/cd/E26996_01/E18549/html/BABHBFHA.html)

**NEW QUESTION 47**

An administrator is tasked with building an environment consisting of four servers that can each serve the same website. Which of the following concepts is described?

- A. Load balancing
- B. Direct access
- C. Overprovisioning
- D. Network teaming

**Answer:** A

**Explanation:**

Load balancing is a concept that distributes the workload across multiple servers or other resources to optimize performance, availability, and scalability. Load balancing can be implemented at different layers of the network, such as the application layer, the transport layer, or the network layer. Load balancing can use various algorithms or methods to determine how to distribute the traffic, such as round robin, least connections, or weighted distribution.

References: CompTIA Server+ Study Guide, Chapter 6: Networking, page 241.

**NEW QUESTION 52**

Which of the following commands would MOST likely be used to register a new service on a Windows OS?

- A. set-service
- B. net
- C. sc
- D. services.msc

**Answer: C**

**Explanation:**

The sc command is used to create, delete, start, stop, pause, or query services on a Windows OS. It can also be used to register a new service by using the create option. References: <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/sc-create>

**NEW QUESTION 55**

A server technician has received reports of database update errors. The technician checks the server logs and determines the database is experiencing synchronization errors. To attempt to correct the errors, the technician should FIRST ensure:

- A. the correct firewall zone is active
- B. the latest firmware was applied
- C. NTP is running on the database system
- D. the correct dependencies are installed

**Answer: C**

**Explanation:**

The first thing that the technician should ensure to correct the database synchronization errors is that NTP is running on the database system. NTP (Network Time Protocol) is a protocol that synchronizes the clocks of network devices with a reference time source, such as an atomic clock or a GPS receiver. NTP ensures that all devices on a network have accurate and consistent time settings, which can affect various functions and applications. Database synchronization is a process of maintaining data consistency and integrity across multiple database servers or instances. Database synchronization can depend on accurate time settings, as time stamps are often used to determine which data is newer or older, and which data should be updated or overwritten. If NTP is not running on the database system, it may cause time drift or discrepancy between different database servers or instances, which can result in synchronization errors or data conflicts.

**NEW QUESTION 59**

A technician is attempting to log in to a Linux server as root but cannot remember the administrator password. Which of the following is the LEAST destructive method of resetting the administrator password?

- A. Boot using a Linux live CD and mount the hard disk to /mn
- B. Change to the /mnt/etc directory
- C. Edit the passwd file found in that directory.
- D. Reinstall the OS in overlay mod
- E. Reset the root password from the install GUI screen.
- F. Adjust the GRUB boot parameters to boot into single-user mod
- G. Run passwd from the command prompt.
- H. Boot using a Linux live CD and mount the hard disk to /mn
- I. SCP the /etc directory from a known accessible server to /mnt/etc.

**Answer: C**

**Explanation:**

This is the least destructive method of resetting the administrator password because it does not require modifying any files or reinstalling the OS. It only requires changing the boot parameters temporarily and running a command to change the password. References: [https://wiki.archlinux.org/title/Reset\\_lost\\_root\\_password#Using\\_GRUB](https://wiki.archlinux.org/title/Reset_lost_root_password#Using_GRUB)

**NEW QUESTION 61**

A server administrator is completing an OS installation for a new server. The administrator patches the server with the latest vendor-suggested software, configures DHCP, and verifies all network cables are properly connected in the IDF, but there is no network connectivity. Which of the following is the MOST likely reason for the lack of connectivity?

- A. The VLAN is improperly configured.
- B. The DNS configuration is invalid.
- C. The OS version is not compatible with the network switch vendor.
- D. The HIDS is preventing the connection.

**Answer: A**

**Explanation:**

If the server administrator patches the server with the latest vendor-suggested software, configures DHCP, and verifies all network cables are properly connected in the IDF, but there is no network connectivity, then the most likely reason for the lack of connectivity is that the VLAN is improperly configured. A VLAN (Virtual Local Area Network) is a logical grouping of network devices that share the same broadcast domain and can communicate with each other without routing. If the server is assigned to a different VLAN than the DHCP server or the default gateway, it will not be able to obtain an IP address or reach other network devices. The DNS configuration is not relevant for network connectivity, as DNS only resolves names to IP addresses. The OS version is not likely to be incompatible with the network switch vendor, as most network switches use standard protocols and interfaces. The HIDS (Host-based Intrusion Detection System) is not likely to prevent the connection, as HIDS only monitors and alerts on suspicious activities on the host. References: <https://www.howtogeek.com/190014/virtualization-basics-understanding-techniques-and-fundamentals/> <https://www.howtogeek.com/164981/how-to-use-nslookup-to-check-domain-name-information-in-microsoft-windows/> <https://www.howtogeek.com/202794/what-is-an-intrusion-detection-system-ids-and-how-does-it-work/>

**NEW QUESTION 63**

An administrator has been asked to verify that all traffic egressing from a company is secured. The administrator confirms all the information that is sent over the network is encrypted. Which of the following describes the type of traffic being encrypted?

- A. Network encapsulation
- B. Off-site data
- C. Secure FTP
- D. Data in transit

**Answer:** D

**Explanation:**

Data in transit is data that is being transferred over a network, such as the internet. It can be encrypted to protect it from unauthorized access or tampering.  
Verified References: [Data in transit], [Encryption]

**NEW QUESTION 68**

An organization implements split encryption keys for sensitive files. Which of the following types of risks does this mitigate?

- A. Hardware failure
- B. Malware
- C. Data corruption
- D. Insider threat

**Answer:** D

**Explanation:**

An insider threat is a type of risk that can be mitigated by implementing split encryption keys for sensitive files. An insider threat is a malicious actor who has authorized access to an organization's system or data and uses it for unauthorized or harmful purposes. An insider threat can cause data breaches, sabotage, fraud, theft, espionage, or other damages to the organization. Split encryption keys are a method of encrypting data using multiple keys that are stored separately and require collaboration to decrypt. Split encryption keys can prevent an insider threat from accessing or compromising sensitive data without being detected by another authorized party who holds another key. Hardware failure is a type of risk that involves physical damage or malfunction of hardware components such as hard drives, memory modules, power supplies, or fans. Hardware failure can cause data loss, system downtime, performance issues, or other problems for the organization. Hardware failure cannot be mitigated by split encryption keys, but by backup, redundancy, monitoring, and maintenance measures.

**NEW QUESTION 69**

A security analyst suspects a remote server is running vulnerable network applications. The analyst does not have administrative credentials for the server. Which of the following would MOST likely help the analyst determine if the applications are running?

- A. User account control
- B. Anti-malware
- C. A sniffer
- D. A port scanner

**Answer:** D

**Explanation:**

A port scanner is the tool that would most likely help the analyst determine if the applications are running on a remote server. A port scanner is a software tool that scans a network device for open ports. Ports are logical endpoints for network communication that are associated with specific applications or services. By scanning the ports on a remote server, the analyst can identify what applications or services are running on that server and what protocols they are using. A port scanner can also help detect potential vulnerabilities or misconfigurations on a server.

**NEW QUESTION 73**

A server administrator must respond to tickets within a certain amount of time. The server administrator needs to adhere to the:

- A. BIA.
- B. RTO.
- C. MTTR.
- D. SLA.

**Answer:** D

**Explanation:**

The server administrator needs to adhere to the Service Level Agreement (SLA) when responding to tickets within a certain amount of time. An SLA is a contract between a service provider and a customer that defines the quality, availability, and responsibilities of the service. An SLA may specify the response time for tickets, as well as other metrics such as uptime, performance, security, and backup frequency. Reference: <https://www.ibm.com/cloud/learn/service-level-agreements>

**NEW QUESTION 74**

Which of the following licenses would MOST likely include vendor assistance?

- A. Open-source
- B. Version compatibility
- C. Subscription
- D. Maintenance and support

**Answer:** D

**Explanation:**

Maintenance and support is a type of license that would most likely include vendor assistance. Maintenance and support is a contract that defines the level and



scope of service and assistance that a vendor provides to a customer for using their software product. Maintenance and support may include technical support, bug fixes, patches, updates, upgrades, documentation, training, and other benefits. Maintenance and support licenses usually have an annual fee based on the number of users or devices covered by the contract. Open-source is a type of license that allows free access to the source code and modification and distribution of the software product, but does not guarantee vendor assistance. Version compatibility is not a type of license, but a feature that ensures software products can work with different versions of operating systems or other software products. Subscription is a type of license that allows access to software products for a limited period of time based on recurring payments, but does not necessarily include vendor assistance. References: <https://www.techopedia.com/definition/1440/software-licensing>  
<https://www.techopedia.com/definition/1032/business-impact-analysis-bia>

**NEW QUESTION 77**

A systems administrator is setting up a server farm for a new company. The company has a public range of IP addresses and uses the addresses internally. Which of the following IP addresses best fits this scenario?

- A. 10.3.7.27
- B. 127.0.0.1
- C. 192.168.7.1
- D. 216.176.128.10

**Answer:** D

**Explanation:**

The IP address that best fits this scenario is 216.176.128.10. This is a public IP address that belongs to a range of addresses that are assigned and registered by an Internet service provider (ISP) and can be accessed from anywhere on the Internet. The company has a public range of IP addresses and uses them internally, which means that they do not use private IP addresses or network address translation (NAT) to communicate within their network.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 2, Lesson 2.2, Objective 2.2

**NEW QUESTION 81**

Which of the following is the MOST appropriate scripting language to use for a logon script for a Linux box?

- A. VBS
- B. Shell
- C. Java
- D. PowerShell
- E. Batch

**Answer:** B

**Explanation:**

Shell is the most appropriate scripting language to use for a logon script for a Linux box. Shell is a generic term for a command-line interpreter that allows users to interact with the operating system by typing commands and executing scripts. Shell scripts are files that contain a series of commands and instructions that can be executed by a shell. Shell scripts are commonly used for automating tasks, such as logon scripts that run when a user logs on to a system. There are different types of shells available for Linux systems, such as Bash, Ksh, Zsh, etc., but they all share a similar syntax and functionality.

**NEW QUESTION 83**

A data center environment currently hosts more than 100 servers that include homegrown and commercial software. The management team has asked the server administrator to find a way to eliminate all company-owned data centers. Which of the following models will the administrator most likely choose to meet this need?

- A. SaaS
- B. Private
- C. Public
- D. Hybrid

**Answer:** C

**Explanation:**

A public cloud model will most likely meet the need of eliminating all company-owned data centers. A public cloud is a type of cloud computing service that is provided by a third-party vendor over the internet. A public cloud offers scalability, flexibility, and cost-effectiveness for hosting servers and applications, as the customers only pay for the resources they use and do not have to maintain their own infrastructure. A public cloud can also provide high availability, security, and performance for the servers and applications, as the vendor manages the underlying hardware and software. A public cloud can support various types of services, such as software as a service (SaaS), platform as a service (PaaS), or infrastructure as a service (IaaS). References: [CompTIA Server+ Certification Exam Objectives], Domain 1.0: Server Administration, Objective 1.2: Given a scenario, compare and contrast server roles and requirements for each.

**NEW QUESTION 84**

A company uses a hot-site, disaster-recovery model. Which of the following types of data replication is required?

- A. Asynchronous
- B. Incremental
- C. Application consistent
- D. Constant

**Answer:** D

**Explanation:**

The type of data replication that is required for a hot-site disaster recovery model is constant. A hot site is a type of disaster recovery site that has fully operational IT infrastructure and equipment that can take over the primary site's functions immediately in case of a disaster or disruption. A hot site requires constant data replication between the primary site and the hot site to ensure that the data is up-to-date and consistent. Constant data replication means that any changes made to the data at the primary site are immediately copied to the hot site without any delay or lag.

**NEW QUESTION 85**

A company's security team has noticed employees seem to be blocking the door in the main data center when they are working on equipment to avoid having to gain access each time. Which of the following should be implemented to force the employees to enter the data center properly?

- A. A security camera
- B. A mantrap
- C. A security guard
- D. A proximity card

**Answer: B**

**Explanation:**

A mantrap is a security device that consists of two interlocking doors that allow only one person to enter at a time. A mantrap would prevent employees from blocking the door in the main data center and force them to enter properly using their credentials. The other options would not enforce proper entry to the data center

**NEW QUESTION 89**

A server administrator implemented a new backup solution and needs to configure backup methods for remote sites. These remote sites have low bandwidth and backups must not interfere with the network during normal business hours. Which of the following methods can be used to meet these requirements? (Select two).

- A. Open file
- B. Archive
- C. Cloud
- D. Snapshot
- E. Differential
- F. Synthetic full

**Answer: BE**

**Explanation:**

Archive is a method of storing historical data that is not frequently accessed or modified. Archive can reduce the amount of data that needs to be backed up and save bandwidth and storage space. Differential is a method of backing up only the data that has changed since the last full backup. Differential can also save bandwidth and storage space, as well as speed up the backup process.

References:

CompTIA Server+ Certification Exam Objectives<sup>1</sup>, page 12

Server Management: Server Hardware Installation and Management<sup>2</sup>, Module 2, Lesson 5

**NEW QUESTION 92**

A server administrator needs to create a new folder on a file server that only specific users can access. Which of the following BEST describes how the server administrator can accomplish this task?

- A. Create a group that includes all users and assign it to an ACL.
- B. Assign individual permissions on the folder to each user.
- C. Create a group that includes all users and assign the proper permissions.
- D. Assign ownership on the folder for each user.

**Answer: C**

**Explanation:**

The top portion of the dialog box lists the users and/or groups that have access to the file or folder.

Reference: <https://www.uwec.edu/kb/article/drives-establishing-windows-file-and-folder-level-permissions/>

**NEW QUESTION 93**

An administrator has been asked to deploy a database server that provides the highest performance with fault tolerance. Which of the following RAID levels will fulfill this request?

- A. RAID 0
- B. RAID 1
- C. RAID 5
- D. RAID 6
- E. RAID 10

**Answer: E**

**Explanation:**

RAID 10 is the best option to deploy a database server that provides the highest performance with fault tolerance. RAID 10 is a type of RAID level that combines RAID 1 (mirroring) and RAID 0 (striping) to create an array of mirrored stripes. RAID 10 offers high performance by distributing data across multiple disks in parallel (striping), which improves read/write speed and I/O operations. RAID 10 also offers fault tolerance by duplicating data across two or more disks in each stripe (mirroring), which provides redundancy and data protection in case of disk failure. RAID 10 requires at least four disks to implement and has a high storage overhead, as half of the disk space is used for mirroring. References: [CompTIA Server+ Certification Exam Objectives]

**NEW QUESTION 96**

Which of the following BEST describes overprovisioning in a virtual server environment?

- A. Committing more virtual resources to virtual machines than there are physical resources present
- B. Installing more physical hardware than is necessary to run the virtual environment to allow for future expansion
- C. Allowing a virtual machine to utilize more resources than are allocated to it based on the server load
- D. Ensuring there are enough physical resources to sustain the complete virtual environment in the event of a host failure

**Answer: A**

**Explanation:**

This is the best definition of overprovisioning in a virtual server environment because it means allocating more CPU, memory, disk, or network resources to the virtual machines than what is actually available on the physical host. This can lead to performance issues and resource contention.

References:<https://www.hpe.com/us/en/insights/articles/10-virtualization-mistakes-everyone-makes-1808.html>

**NEW QUESTION 97**

A server administrator is creating a script that will move files only if they were created before a date input by the user. Which of the following constructs will allow the script to apply this test until all available files are assessed?

- A. Variable
- B. Loop
- C. Comparator
- D. Conditional

**Answer: B**

**Explanation:**

A loop is a script construct that allows the script to repeat a block of code until a certain condition is met or for a specified number of times. A loop can be used to apply a test to each file in a directory and move the files that meet the criteria. For example, in a bash script, a loop can be written as:

```
#!/bin/bash
# Ask the user for the date echo"Enter the date (YYYY-MM-DD):" readdate
# Loop through all the files in the current directory forfilein*
do
# Check if the file was created before the date if[[ $(date-r"$file"+%F) <$date]]
then
# Move the file to another location mv"$file"/path/to/destination
fi done Copy
```

A variable is a script construct that allows the script to store and manipulate data. A variable can be used to store the date input by the user, but it cannot apply a test to each file1

A comparator is a script construct that allows the script to compare two values and determine their relationship. A comparator can be used to check if a file was created before the date, but it cannot repeat the test for all files1

A conditional is a script construct that allows the script to execute different blocks of code based on certain conditions. A conditional can be used to decide whether to move a file or not, but it cannot iterate over all files1

1: CompTIA Server+ Certification Exam Objectives

**NEW QUESTION 101**

A remote physical server is unable to communicate to the network through the available NICs, which were misconfigured. However, the server administrator is still able to configure the server remotely. Which of the following connection types is the server administrator using to access the server?

- A. Out-of-band management
- B. Crash cart access
- C. Virtual administrator console
- D. Local KVM setup
- E. RDP connection

**Answer: A**

**Explanation:**

The connection type that the server administrator is using to access the server remotely is out-of-band management. Out-of-band management is a method of accessing and controlling a server through a dedicated network interface or port that is separate from the regular data network. Out-of-band management allows administrators to perform tasks such as rebooting, configuring, troubleshooting, or updating a server even if the server is offline or unresponsive through the regular network. Out-of-band management can use protocols such as IPMI, iLO, DRAC, or BMC. Reference:<https://www.ibm.com/cloud/learn/out-of-band-management>

**NEW QUESTION 104**

The Chief Information Officer (CIO) of a datacenter is concerned that transmissions from the building can be detected from the outside. Which of the following would resolve this concern? (Choose two.)

- A. RFID
- B. Proximity readers
- C. Signal blocking
- D. Camouflage
- E. Reflective glass
- F. Bollards

**Answer: CE**

**Explanation:**

The best solutions to resolve the concern of transmissions from the building being detected from outside are signal blocking and reflective glass. Signal blocking is a method of preventing or interfering with electromagnetic signals from escaping or entering a certain area. Signal blocking can be achieved by using various materials or devices that create physical barriers or generate noise or jamming signals. Signal blocking can protect data transmissions from being intercepted or eavesdropped by unauthorized parties. Reflective glass is a type of glass that has a coating or film that reflects light and heat. Reflective glass can reduce glare and solar radiation, as well as prevent visual observation from outside. Reflective glass can enhance privacy and security for datacenter operations.

**NEW QUESTION 106**

Two developers are working together on a project, and they have built out a set of snared servers that both developers can access over the internet. Which of the following cloud models is this an example of?

- A. Hybrid
- B. Public
- C. Private
- D. Community

**Answer:** B

**Explanation:**

A public cloud is a cloud model that provides shared resources and services over the internet to multiple users or organizations. The cloud provider owns and manages the infrastructure and charges users based on their usage or subscription. A public cloud can offer scalability, flexibility, and cost-efficiency for users who need access to various applications and data without investing in their own hardware or software. Verified References: [Public cloud], [Cloud model]

**NEW QUESTION 108**

A server administrator just installed a new physical server and needs to harden the OS. Which of the following best describes the OS hardening method?

- A. Apply security updates.
- B. Disable unneeded hardware.
- C. Set a BIOS password.
- D. Configure the boot order.

**Answer:** A

**Explanation:**

Applying security updates is one of the common operating system hardening methods that can help protect the OS from cyberattacks and vulnerabilities. Security updates are released by the OS developer to fix bugs, patch security holes, and improve performance. By installing the latest updates, the server administrator can ensure that the OS is up to date and secure<sup>12</sup>.

**NEW QUESTION 112**

A technician has moved a data drive from a new Windows server to an older Windows server. The hardware recognizes the drive, but the data is not visible to the OS. Which of the following is the most likely cause of the issue?

- A. The disk uses GPT.
- B. The partition is formatted with ext4.
- C. The partition is formatted with FAT32.
- D. The disk uses MBR.

**Answer:** A

**Explanation:**

The most likely cause of the issue is that the disk uses GPT. GPT stands for GUID Partition Table, which is a newer standard for disk partitioning that supports larger disks and more partitions than the older MBR (Master Boot Record) standard<sup>1</sup>. However, GPT is not compatible with some older operating systems, such as Windows XP or Windows Server 2003<sup>2</sup>. Therefore, if the data drive was formatted with GPT on a new Windows server and then moved to an older Windows server, the older server may not be able to recognize the GPT partitions and access the data on the drive.

The partition being formatted with ext4, FAT32, or MBR are not likely causes of the issue. Ext4 is a file system that is commonly used on Linux-based systems, but it can also be read by Windows with some third-party software<sup>3</sup>. FAT32 is a file system that is widely compatible with most operating systems and devices, but it has some limitations such as a maximum file size of 4 GB and a maximum partition size of 8 TB<sup>4</sup>. MBR is not a file system, but a partitioning scheme that can support various file systems such as NTFS, FAT32, or exFAT<sup>5</sup>. However, MBR has some disadvantages compared to GPT, such as a maximum disk size of 2 TB and a maximum number of primary partitions of four<sup>1</sup>.

**NEW QUESTION 117**

A technician set up a new multifunction printer. After adding the printer to the print server, the technician configured the printer on each user's machine. Several days later, users reported that they were no longer able to print, but scanning to email worked. Which of the following is most likely causing this issue?

- A. The gateway is no longer being reached.
- B. The network firewall was enabled.
- C. The printer's network interface failed.
- D. The printer had DHCP enabled.

**Answer:** D

**Explanation:**

The most likely cause of this issue is that the printer had DHCP enabled, which changed its IP address after adding it to the print server and configuring it on each user's machine. DHCP (Dynamic Host Configuration Protocol) is a network protocol that assigns IP addresses and other network configuration parameters to devices automatically, without manual intervention. DHCP can simplify network management and avoid IP conflicts, but it can also cause problems if the devices are not configured to use static or reserved IP addresses. If the printer had DHCP enabled, it might have received a different IP address from the DHCP server after rebooting or reconnecting to the network, which would make it unreachable by the print server and the users' machines that were configured with the previous IP address. Scanning to email would still work, as it does not depend on the print server or the users' machines, but on the printer's SMTP settings and internet connection. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Networking, Objective 4.1: Given a scenario, configure network settings for servers.

**NEW QUESTION 120**

Which of the following should an administrator use to transfer log files from a Linux server to a Windows workstation?

- A. Telnet
- B. Robocopy
- C. XCOPY
- D. SCP

**Answer:** D



**Explanation:**

The administrator should use SCP to transfer log files from a Linux server to a Windows workstation. SCP (Secure Copy Protocol) is a protocol that allows secure file transfer between two devices using SSH (Secure Shell) encryption. SCP can transfer files between different operating systems, such as Linux and Windows, as long as both devices have an SSH client installed. SCP can also preserve file attributes, such as permissions and timestamps, during the transfer.

**NEW QUESTION 124**

A security analyst completed a port scan of the corporate production-server network. Results of the scan were then provided to a systems administrator for immediate action. The following table represents the requested changes:

Server name	Block	Do not change
MailSrv	20, 21, 22, 23, 53	25, 3389
WebSrv	20, 21, 22, 23, 53	80, 443, 3389
SQLSrv	20, 21, 22, 23, 53	1443, 3389
DNSSrv	20, 21, 22, 23, 53	67, 68, 3389

The systems administrator created local firewall rules to block the ports indicated above. Immediately, the service desk began receiving calls about the internet being down. The systems administrator then reversed the changes, and the internet became available again. Which of the following ports on DNSSrv must remain open when the firewall rules are reapplied?

- A. 20
- B. 21
- C. 22
- D. 23
- E. 53

**Answer: E**

**Explanation:**

Port 53 is the standard port for DNS (Domain Name System) queries and responses. DNS is a service that translates domain names (such as www.example.com) into IP addresses (such as 192.0.2.1) and vice versa. DNS is essential for internet connectivity, as it allows users and applications to access websites and other online resources by using human-readable names instead of numerical addresses.

The DNSSrv server is a DNS server that provides name resolution for the corporate network. If port 53 is blocked on this server, it will not be able to communicate with other DNS servers or clients, and the name resolution will fail. This will prevent users from accessing any websites or online services that rely on domain names, such as web browsers, email clients, or cloud applications. Therefore, port 53 must remain open on DNSSrv to allow DNS traffic to flow.

**NEW QUESTION 129**

Several new components have been added to a mission-critical server, and corporate policy states all new components must meet server hardening requirements. Which of the following should be applied?

- A. Definition updates
- B. Driver updates
- C. OS security updates
- D. Application updates

**Answer: B**

**Explanation:**

Driver updates should be applied to the new components that have been added to a mission-critical server, as part of the server hardening requirements. Drivers are software programs that enable the communication and functionality of hardware devices, such as network cards, storage controllers, or graphics cards. Updating drivers can improve the performance, compatibility, and stability of the new components with the server operating system and applications. References: CompTIA Server+ Certification Exam Objectives, Domain 2.0: Hardware, Objective 2.2: Given a scenario, install, configure and maintain server components.

**NEW QUESTION 132**

A server administrator notices the /var/log/audit/audit.log file on a Linux server is rotating too frequently. The administrator would like to decrease the number of times the log rotates without losing any of the information in the logs. Which of the following should the administrator configure?

- A. increase the audit
- B. log file size in the appropriate configuration file.
- C. Decrease the duration of the log rotate cycle for the audit
- D. log file.
- E. Remove the log rotate directive from the audit .log file configuration.
- F. Move the audit
- G. log files to a remote syslog server.

**Answer: A**

**Explanation:**

The audit.log file is a file that records security-related events on a Linux server, such as user login, file access, and system commands. The logrotate utility is a tool that rotates, compresses, and deletes old log files based on certain criteria, such as size, time, or frequency. To decrease the number of times the log rotates without losing any information, the administrator should increase the audit.log file size in the appropriate configuration file, such as /etc/logrotate.conf or /etc/logrotate.d/auditd. Verified References: [audit.log], [logrotate]

**NEW QUESTION 135**

Which of the following should a technician verify FIRST before decommissioning and wiping a file server?

- A. The media destruction method
- B. The recycling process

- C. Asset management documentation
- D. Non-utilization

**Answer:** D

**Explanation:**

The first thing that a technician should verify before decommissioning and wiping a file server is non-utilization, which means that no one is using or accessing the server or its data. This can be done by checking logs, monitoring network traffic, or contacting users or stakeholders. Non-utilization ensures that decommissioning and wiping will not cause any data loss or disruption to business operations. Verified References: [Server Decommissioning Checklist]

**NEW QUESTION 138**

A company stores extremely sensitive data on an alt-gapped system. Which of the following can Be Implemented to increase security against a potential insider threat?

- A. Two-person Integrity
- B. SSO
- C. SIEM
- D. Faraday cage
- E. MFA

**Answer:** A

**Explanation:**

Two-person integrity is a security measure that can be implemented to increase security against a potential insider threat on an air-gapped system. An air-gapped system is a system that is isolated from any network connection and can only be accessed physically. An insider threat is a malicious actor who has authorized access to an organization's system or data and uses it for unauthorized or harmful purposes. Two- person integrity is a system of storage and handling that requires the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures, for accessing certain sensitive data or material. This way, no single person can compromise the security or integrity of the data or material without being noticed by another person. SSO (Single Sign-On) is a feature that allows users to access multiple applications or systems with one set of credentials, but it does not prevent insider threats. SIEM (Security Information and Event Management) is a tool that collects and analyzes log data from various sources to detect and respond to security incidents, but it does not work on air-gapped systems. A Faraday cage is a structure that blocks electromagnetic signals from entering or leaving, but it does not prevent physical access or insider threats. MFA (Multi-Factor Authentication) is a method that requires users to provide two or more pieces of evidence to verify their identity, such as something they know, something they have, or something they are, but it does not prevent insider threats. References: <https://www.howtogeek.com/169080/air-gap-how-to-isolate-a-computer-to-protect-it-from-hackers/> <https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-it-matter/> <https://www.howtogeek.com/202794/what-is-the-difference-between-127.0.0.1-and-0.0.0.0/> <https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual-files/>

**NEW QUESTION 142**

Which of the following commands should a systems administrator use to create a batch script to map multiple shares'?

- A. nbtstat
- B. netuse
- C. tracert
- D. netstst

**Answer:** B

**Explanation:**

The net use command is a Windows command that can be used to create a batch script to map multiple shares. The net use command can connect or disconnect a computer from a shared resource, such as a network drive or a printer, or display information about computer connections. The syntax of the net use command is:

```
net use [devicename | *] [\computername\sharename[\u0003volume] [password | *]] [/user:[domainname\]username] [/user:[dotted domain name\]username] [/user:[username@dotted domain name] [/savecred] [/smartcard] [{/delete | /persistent:{yes | no}}] where:
```

devicename = the drive letter or printer port to assign to the shared resource  
computername = the name of the computer that provides access to the shared resource  
sharename = the name of the shared resource  
password = the password needed to access the shared resource  
/user = specifies a different username to make the connection

/savecred = stores the provided credentials for future use  
/smartcard = uses a smart card for authentication  
/delete = cancels a network connection and removes the connection from the list of persistent connections  
/persistent = controls whether the connection is restored at logon

To create a batch script to map multiple shares, you can use the net use command with different drive letters and share names, for example:

```
net use W: \\computer1\share1 net use X: \\computer2\share2 net use Y: \\computer3\share3
```

You can also add other options, such as passwords, usernames, or persistence, as needed. To save the batch script, you can use Notepad or any text editor and save the file with a .bat extension<sup>12</sup>.

References: 1 <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/net-use> 2 <https://www.watchingthenet.com/create-a-batch-file-to-map-drives-folders.html>

**NEW QUESTION 145**

A company needs a media server set up that provides the highest availability with a minimum requirement of at least 10TB. The company purchased five HDDs, each with a 4TB capacity. Which of the options would provide the highest fault tolerance and meet the requirements?

- A. RAID 0
- B. RAID 5
- C. RAID 6
- D. RAID 10

**Answer:** C

**Explanation:**

RAID 6 is a RAID level that uses disk striping with two parity blocks distributed across all member disks. It can tolerate the failure of up to two disks without losing any data. RAID 6 can provide a minimum of 10TB of usable storage space with five 4TB disks, as the formula for calculating the RAID 6 capacity is  $(n-2) \times S_{min}$ , where  $n$  is the number of disks and  $S_{min}$  is the smallest disk size. In this case, the RAID 6 capacity is  $(5-2) \times 4TB = 12TB$ . References:

? CompTIA Server+ Certification Exam Objectives<sup>1</sup>, page 8

? RAID Levels and Types Explained: Advantages and Disadvantages<sup>2</sup>

? RAID Levels & Fault Tolerance<sup>3</sup>

#### NEW QUESTION 147

A server has experienced several component failures. To minimize downtime, the server administrator wants to replace the components while the server is running. Which of the following can MOST likely be swapped out while the server is still running? (Select TWO).

- A. The power supply
- B. The CPU
- C. The hard drive
- D. The GPU
- E. The cache
- F. The RAM

**Answer:** AC

#### Explanation:

The power supply and the hard drive are two components that can most likely be swapped out while the server is still running, if they support hot swapping or hot plugging. Hot swapping or hot plugging means that the device can be added or removed without shutting down the system. The operating system automatically recognizes the changes that have been made. This feature is useful for minimizing downtime and improving availability. The CPU, the GPU, the cache, and the RAM are not hot swappable and require the system to be powered off before replacing them. References: <https://www.geeksforgeeks.org/what-is-hot-swapping/><https://www.howtogeek.com/268249/what-is-hot-swapping-and-what-devices-support-it/>

#### NEW QUESTION 150

An administrate is helping to replicate a large amount of data between two Windows servers. The administrator is unsure how much data has already been transferred. Which of the following will BEST ensure all the data is copied consistently?

- A. rsync
- B. copy
- C. scp
- D. robocopy

**Answer:** D

#### Explanation:

Robocopy (Robust File Copy) is a command-line tool that can copy files and folders between Windows servers or computers. It has many features and options that can ensure all the data is copied consistently, such as retrying failed copies, resuming interrupted copies, copying permissions and attributes, mirroring source and destination directories, and logging the copy progress and results. Verified References: [Robocopy], [File copy]

#### NEW QUESTION 154

A technician is unable to access a server's package repository internally or externally. Which of the following are the MOST likely reasons? (Choose two.)

- A. The server has an architecture mismatch
- B. The system time is not synchronized
- C. The technician does not have sufficient privileges
- D. The external firewall is blocking access
- E. The default gateway is incorrect
- F. The local system log file is full

**Answer:** DE

#### Explanation:

The most likely reasons why the technician is unable to access a server's package repository internally or externally are that the external firewall is blocking access and that the default gateway is incorrect. A package repository is a source of software packages that can be installed or updated on a server using a package manager tool. A package repository can be accessed over a network using a URL or an IP address. However, if there are any network issues or misconfigurations, the access to the package repository can be blocked or failed. An external firewall is a device or software that controls the incoming and outgoing network traffic based on predefined rules or policies. An external firewall can block access to a package repository if it does not allow traffic on certain ports or protocols that are used by the package manager tool. A default gateway is a device or address that routes network traffic from one network to another network. A default gateway can be incorrect if it does not match the actual device or address that connects the server's network to other networks, such as the internet. An incorrect default gateway can prevent the server from reaching the package repository over other networks.

#### NEW QUESTION 158

A technician is setting up a small office that consists of five Windows 10 computers. The technician has been asked to use a simple IP configuration without manually adding any IP addresses. Which of the following will the technician MOST likely use for the IP address assignment?

- A. Static
- B. Router-assigned
- C. APIPA
- D. DHCP

**Answer:** D

#### Explanation:

DHCP stands for Dynamic Host Configuration Protocol and it is a network protocol that automatically assigns IP addresses and other network configuration parameters to devices on a network. DHCP can help simplify IP configuration without manually adding any IP addresses. DHCP works by using a DHCP server

that maintains a pool of available IP addresses and leases them to devices that request them. The devices can renew or release their IP addresses as needed. References: <https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives> (Objective 2.1)

**NEW QUESTION 159**

Due to a recent application migration, a company's current storage solution does not meet the necessary requirements for hosting data without impacting performance when the data is accessed in real time by multiple users. Which of the following is the BEST solution for this Issue?

- A. Install local external hard drives for affected users.
- B. Add extra memory to the server where data is stored.
- C. Compress the data to increase available space.
- D. Deploy a new Fibre Channel SAN solution.

**Answer:** D

**Explanation:**

A Fibre Channel SAN solution is a type of storage area network (SAN) that uses high-speed optical fiber cables to connect servers and storage devices. A SAN allows for hosting data without impacting performance when the data is accessed in real time by multiple users, as it provides fast data transfer rates, low latency, high availability, and scalability<sup>12</sup>. A local external hard drive (A) would not be suitable for multiple users, as it would limit the accessibility and security of the data. Adding extra memory to the server (B) would not solve the problem of data access performance, as it would not increase the bandwidth or reduce the congestion of the network. Compressing the data © would not improve the performance either, as it would add extra overhead and complexity to the data processing and retrieval. References: 1 <https://www.techradar.com/best/best-cloud-storage> 2 <https://solutionsreview.com/data-storage/the-best-enterprise-data-storage-solutions/>

**NEW QUESTION 161**

Which of the following would a systems administrator implement to ensure all web traffic is secure?

- A. SSH
- B. SSL
- C. SMTP
- D. PGP

**Answer:** B

**Explanation:**

Secure Sockets Layer (SSL): SSL and its successor Transport Layer Security (TLS) enable client and server computers to establish a secure connection session and manage encryption and decryption activities. Reference: <https://paginas.fe.up.pt/~als/mis10e/ch8/chpt8-4bullettext.htm>

**NEW QUESTION 166**

An administrator is only able to log on to a server with a local account. The server has been successfully joined to the domain and can ping other servers by IP address. Which of the following locally defined settings is MOST likely misconfigured?

- A. DHCP
- B. WINS
- C. DNS
- D. TCP

**Answer:** C

**Explanation:**

This is the most likely misconfigured setting because DNS is the service that resolves hostnames to IP addresses and vice versa. If the DNS server is incorrect or unreachable, the administrator will not be able to log on to the server with a domain account because the server will not be able to authenticate with the domain controller.

References: <https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/dns-troubleshooting>

**NEW QUESTION 170**

Which of the following types of asset management documentation is commonly used as a reference when processing the replacement of a faulty server component?

- A. Warranty
- B. Purchase order
- C. License
- D. Baseline document

**Answer:** A

**Explanation:**

A warranty is a type of asset management documentation that is commonly used as a reference when processing the replacement of a faulty server component. A warranty is a guarantee from the manufacturer or vendor that covers the repair or replacement of defective parts within a specified period of time. A purchase order, a license, or a baseline document are not directly related to the replacement of a faulty server component. References: [CompTIA Server+ Certification Exam Objectives], Domain 1.0: Server Architecture, Objective 1.4: Explain asset management and documentation processes.

**NEW QUESTION 175**

A server technician is installing a Windows server OS on a physical server. The specifications for the installation call for a 4TB data volume. To ensure the partition is available to the OS, the technician must verify the:

- A. hardware is UEFI compliant
- B. volume is formatted as GPT
- C. volume is formatted as MBR
- D. volume is spanned across multiple physical disk drives



**Answer:** B

**Explanation:**

To ensure the partition is available to the OS, the technician must verify that the volume is formatted as GPT. GPT (GUID Partition Table) is a partitioning scheme that defines how data is organized on a hard disk drive (HDD) or a solid state drive (SSD). GPT uses globally unique identifiers (GUIDs) to identify partitions and supports up to 128 primary partitions per disk. GPT also supports disks larger than 2 TB and has a backup copy of the partition table at the end of the disk for data recovery. GPT is required for installing Windows on UEFI-based PCs, which offer faster boot time and better security than legacy BIOS-based PCs.

**NEW QUESTION 179**

Which of the following attacks is the most difficult to mitigate with technology?

- A. Ransomware
- B. Backdoor
- C. SQL injection
- D. Phishing

**Answer:** D

**Explanation:**

Phishing is a type of attack that is the most difficult to mitigate with technology. Phishing is a technique of deceiving users into revealing their personal or confidential information, such as passwords, credit card numbers, or bank accounts, by sending them fraudulent emails or messages that appear to be from legitimate sources. Phishing relies on human factors, such as curiosity, greed, or fear, to trick users into clicking on malicious links or attachments, or entering their credentials on fake websites. Technology solutions, such as antivirus software, firewalls, or spam filters, can help detect and block some phishing attempts, but they cannot prevent users from falling victim to social engineering tactics. References: [CompTIA Server+ Certification Exam Objectives], Domain 5.0: Security, Objective 5.3: Given a scenario, explain methods and techniques to secure data.

**NEW QUESTION 181**

A server administrator is trying to determine the cause of a slowdown on a database server. Upon investigation, the administrator determines the issue is in the storage subsystem. Which of the following will most likely resolve this issue?

- A. Increasing IOPS by implementing flash storage
- B. Implementing deduplication on the storage
- C. Extending capacity by installing a 4TB SATA disk
- D. Reformatting the disk as FAT32

**Answer:** A

**Explanation:**

Increasing IOPS (input/output operations per second) by implementing flash storage is the most likely solution to resolve a slowdown issue in the storage subsystem of a database server. Flash storage uses solid-state drives (SSDs) that have faster read/write speeds and lower latency than traditional hard disk drives (HDDs). This can improve the performance of database queries and transactions. Implementing deduplication, extending capacity, or reformatting the disk as FAT32 are not likely to resolve the issue, as they do not affect the IOPS of the storage subsystem. References: [CompTIA Server+ Certification Exam Objectives], Domain 3.0: Storage, Objective 3.5: Summarize hardware and features of various storage technologies.

**NEW QUESTION 183**

A server administrator is configuring a new server that will hold large amounts of information. The server will need to be accessed by multiple users at the same time. Which of the following server roles will the administrator MOST likely need to install?

- A. Messaging
- B. Application
- C. Print
- D. Database

**Answer:** D

**Explanation:**

Few people are expected to use the database at the same time and users don't need to customize the design of the database.

Reference: <https://support.microsoft.com/en-us/office/ways-to-share-an-access-desktop-database-03822632-da43-4d8f-ba2a-68da245a0446>

The server role that the administrator will most likely need to install for a server that will hold large amounts of information and will need to be accessed by multiple users at the same time is database. A database is a collection of structured data that can be stored, queried, manipulated, and analyzed using various methods and tools. A database server is a server that hosts one or more databases and provides access to them over a network. A database server can handle large amounts of information and support concurrent requests from multiple users or applications.

**NEW QUESTION 186**

An administrator has been troubleshooting a server issue. The administrator carefully questioned the users and examined the available logs. Using this information, the administrator was able to rule out several possible causes and develop a theory as to what the issue might be. Through further testing, the administrator's theory proved to be correct. Which of the following should be the next step to troubleshoot the issue?

- A. Document the findings and actions.
- B. Escalate the issue to the management team.
- C. Implement the solution.
- D. Establish an action plan.

**Answer:** D

**Explanation:**

The next step to troubleshoot the issue after developing and testing a theory is to establish an action plan. This involves identifying the steps needed to implement

the solution, estimating the time and resources required, and evaluating the potential risks and impacts of the solution. Documenting the findings and actions, escalating the issue to the management team, or implementing the solution are steps that should be done after establishing an action plan. References: [CompTIA Server+ Certification Exam Objectives], Domain 6.0: Disaster Recovery, Objective 6.2: Explain troubleshooting theory and methodologies.

**NEW QUESTION 190**

Which of the following open ports should be closed to secure the server properly? (Choose two.)

- A. 21
- B. 22
- C. 23
- D. 53
- E. 443
- F. 636

**Answer:** AC

**Explanation:**

The administrator should close ports 21 and 23 to secure the server properly. Port 21 is used for FTP (File Transfer Protocol), which is an unsecure protocol that allows file transfer between a client and a server over a network connection. FTP does not encrypt the data or the credentials that are transmitted, making them vulnerable to interception or modification by attackers. Port 23 is used for Telnet, which is an unsecure protocol that allows remote login and command execution over a network connection using a CLI. Telnet does not encrypt the data or the credentials that are transmitted, making them vulnerable to interception or modification by attackers.

Reference:

<https://www.csoononline.com/article/3191531/securing-risky-network-ports.html>

**NEW QUESTION 193**

A large number of connections to port 80 is discovered while reviewing the log files on a server. The server is not functioning as a web server. Which of the following represent the BEST immediate actions to prevent unauthorized server access? (Choose two.)

- A. Audit all group privileges and permissions
- B. Run a checksum tool against all the files on the server
- C. Stop all unneeded services and block the ports on the firewall
- D. Initialize a port scan on the server to identify open ports
- E. Enable port forwarding on port 80
- F. Install a NIDS on the server to prevent network intrusions

**Answer:** CF

**Explanation:**

The best immediate actions to prevent unauthorized server access are to stop all unneeded services and block the ports on the firewall. Stopping unneeded services reduces the attack surface of the server by eliminating potential entry points for attackers. For example, if the server is not functioning as a web server, there is no need to run a web service on port 80. Blocking ports on the firewall prevents unauthorized network traffic from reaching the server. For example, if port 80 is not needed for any legitimate purpose, it can be blocked on the firewall to deny any connection attempts on that port.

**NEW QUESTION 195**

A server administrator is installing a new server on a manufacturing floor. Because the server is publicly accessible, security requires the server to undergo hardware hardening. Which of the following actions should the administrator take?

- A. Close unneeded ports.
- B. Disable unused services.
- C. Set a BIOS password.
- D. Apply driver updates.

**Answer:** C

**Explanation:**

An action that the administrator should take to harden the hardware of a new server is to set a BIOS password. BIOS (Basic Input/Output System) is a firmware that initializes the hardware components and settings of a system before loading the operating system. BIOS password is a security feature that requires a user to enter a password before accessing or modifying the BIOS settings or booting up the system. By setting a BIOS password, the administrator can prevent unauthorized or malicious users from changing the hardware configuration or boot order of the server.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 5, Lesson 5.1, Objective 5.1

**NEW QUESTION 196**

A server administrator needs to implement load balancing without purchasing any new hardware or implementing any new software. Which of the following will the administrator most likely implement?

- A. Round robin
- B. Link aggregation
- C. Most recently used
- D. Heartbeat

**Answer:** B

**Explanation:**

Link aggregation is a technique that allows multiple network interfaces to act as one logical interface, increasing the bandwidth and redundancy of the connection. This can improve the load balancing of network traffic without requiring any new hardware or software. Round robin, most recently used, and heartbeat are not load balancing methods, but rather scheduling algorithms or monitoring techniques. References: CompTIA Server+ Certification Exam Objectives, Domain 2.0: Networking, Objective 2.3: Given a scenario, configure NIC teaming.

#### NEW QUESTION 197

Due to a disaster incident on a primary site, corporate users are redirected to cloud services where they will be required to be authenticated just once in order to use all cloud services.

Which of the following types of authentications is described in this scenario?

- A. MFA
- B. NTLM
- C. Kerberos
- D. SSO

**Answer:** D

#### NEW QUESTION 199

An administrator is researching the upcoming licensing software requirements for an application that usually requires very little technical support. Which of the following licensing models would be the LOWEST cost solution?

- A. Open-source
- B. Per CPU socket
- C. Per CPU core
- D. Enterprise agreement

**Answer:** A

#### Explanation:

Open-source software is software that is freely available and can be modified and distributed by anyone. It usually requires very little technical support and has no licensing fees. Therefore, it would be the lowest cost solution for an application that does not need much support. References:

<https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives> (Objective 2.3)

#### NEW QUESTION 202

A technician recently upgraded several pieces of firmware on a server. Ever since the technician rebooted the server, it no longer communicates with the network. Which of the following should the technician do FIRST to return the server to service as soon as possible?

- A. Replace the NIC
- B. Make sure the NIC is on the HCL
- C. Reseat the NIC
- D. Downgrade the NIC firmware

**Answer:** D

#### Explanation:

The first thing that the technician should do to return the server to service as soon as possible is downgrade the NIC firmware. Firmware is a type of software that controls the basic functions of hardware devices, such as network interface cards (NICs). Firmware updates can provide bug fixes, performance improvements, or new features for hardware devices. However, firmware updates can also cause compatibility issues, configuration errors, or functionality failures if they are not installed properly or if they are not compatible with the device model or driver version. Downgrading the firmware means reverting to an older version of firmware that was previously working fine on the device. Downgrading the firmware can help resolve any problems caused by a faulty firmware update and restore normal operation of the device.

#### NEW QUESTION 207

A server administrator purchased a single license key to use for all the new servers that will be imaged this year. Which of the following MOST likely refers to the licensing type that will be used?

- A. Per socket
- B. Open-source
- C. Per concurrent user
- D. Volume

**Answer:** D

#### Explanation:

This is the most likely licensing type that will be used because volume licensing allows a single license key to be used for multiple installations of a software product. Volume licensing is typically used by organizations that need to deploy software to a large number of devices or users. References:

<https://www.microsoft.com/en-us/licensing/licensing-programs/volume-licensing-programs>

#### NEW QUESTION 210

Which of the following licensing models allows the greatest number of concurrent Windows VMS to run on a host for the lowest cost?

- A. per user
- B. per core
- C. Per instance
- D. Per concurrent user

**Answer:** A

#### Explanation:

The answer to this question may depend on several factors, such as the number and type of Windows VMs, the number and type of host machines, the number and type of users, and the specific licensing terms and conditions of each licensing model. However, based on the information available from the web search results, one possible answer is per user. Per user licensing model is a licensing model that allows a user to access Windows VMs from any device, regardless of the number of devices or VMs. Per user licensing model is available for Windows 10 Enterprise E3/E5, Windows VDA E3/E5, and Microsoft 365 F3/E3/E5. Per

user licensing model may offer the greatest number of concurrent Windows VMs to run on a host for the lowest cost if the following conditions are met:

- ? The user needs to access multiple Windows VMs from different devices, such as desktops, laptops, tablets, or smartphones.
- ? The user needs to access Windows VMs that run different versions or editions of Windows, such as Windows 10 Enterprise, Windows 10 Pro, or Windows 7 Enterprise.
- ? The user needs to access Windows VMs that run on different types of host machines, such as physical servers, virtual servers, or cloud servers.
- ? The user does not need to access Windows VMs that run on dedicated hardware or have specific performance or security requirements.

According to the web search results<sup>1</sup>, per user licensing model costs \$84 per user per year for Windows 10 Enterprise E3, \$168 per user per year for Windows 10 Enterprise E5,

\$100.80 per user per year for Windows VDA E3, and \$196.80 per user per year for Windows VDA E5. These prices are based on the Open License Program and may vary depending on the volume and agreement level<sup>2</sup>

Per core licensing model is a licensing model that requires a license for each core of the processor on the host machine that runs Windows VMs. Per core licensing model is available for Windows Server 2022 Datacenter and Standard editions. Per core licensing model may offer a lower cost than per user licensing model if the following conditions are met:

- ? The host machine has a low number of cores or a high core density.
- ? The host machine runs a high number of Windows VMs with low resource consumption.
- ? The host machine runs only Windows Server VMs with the same edition as the host machine.

According to the web search results<sup>2</sup>, per core licensing model costs \$6,155 for 16 core licenses for Windows Server 2022 Datacenter edition and \$1,069 for 16 core licenses for Windows Server 2022 Standard edition. These prices are suggested retail prices and may vary depending on the reseller<sup>2</sup>

Per instance licensing model is a licensing model that requires a license for each instance of Windows that runs on a host machine or a VM. Per instance licensing model is available for Windows Server 2022 Essentials edition and some older versions of Windows Server. Per instance licensing model may offer a lower cost than per user or per core licensing model if the following conditions are met:

- ? The host machine runs only one instance of Windows Server with low resource consumption.
- ? The host machine does not need to run any other VMs or applications.
- ? The host machine does not need any advanced features or functions that are available in Datacenter or Standard editions.

According to the web search results<sup>2</sup>, per instance licensing model costs \$501 for one server license for Windows Server 2022 Essentials edition. This price is suggested retail price and may vary depending on the reseller<sup>2</sup>

Per concurrent user licensing model is a licensing model that allows a certain number of users to access Windows VMs at the same time, regardless of the number of devices or VMs. Per concurrent user licensing model is not available for any current version of Windows or Windows Server. Per concurrent user licensing model was available for some older versions of Windows Server Terminal Services or Remote Desktop Services, but it was discontinued due to complexity and compliance issues. Therefore, per concurrent user licensing model cannot be used for running Windows VMs on a host.

#### NEW QUESTION 215

Following a recent power outage, a server in the data center has been constantly going offline and losing its configuration. Users have been experiencing access issues while using the application on the server. The server technician notices the date and time are incorrect when the server is online. All other servers are working. Which of the following would most likely cause this issue? (Select two).

- A. The server has a faulty power supply.
- B. The server has a CMOS battery failure.
- C. The server requires OS updates.
- D. The server has a malfunctioning LED panel.
- E. The servers have NTP configured.
- F. CPU frequency scaling is set too high.

**Answer:** BE

#### Explanation:

A CMOS battery failure can cause the server to lose its BIOS settings, including the date and time, which can affect the server's functionality and connectivity. The servers have NTP (Network Time Protocol) configured to synchronize their clocks with a reliable time source, which can prevent time drift and ensure consistent timestamps. If one server has a wrong date and time, it can cause conflicts and errors with the other servers that have NTP configured.

References:

- ? CompTIA Server+ Certification Exam Objectives<sup>1</sup>, page 9
- ? Signs or symptoms of a CMOS battery failure<sup>2</sup>
- ? NTP: Network Time Protocol

#### NEW QUESTION 216

A technician is troubleshooting a server issue. The technician has determined several possible causes of the issue and has identified various solutions. Which of the following should the technician do next?

- A. Consult internet forums to determine which is the most common cause and deploy only that solution.
- B. Test each solution individually to determine the root cause, rolling back the changes in between each test.
- C. Implement the shortest solution first to identify the issue and minimize downtime.
- D. Test each solution in succession and restore the server from the latest snapshot.

**Answer:** B

#### Explanation:

According to the CompTIA troubleshooting methodology, the fourth step is to establish a plan of action to resolve the problem and implement the solution<sup>1</sup>. The best practice is to test each solution individually to determine the root cause, rolling back the changes in between each test. This way, the technician can isolate the cause and avoid introducing new problems or making the situation worse. Testing each solution in succession and restoring the server from the latest snapshot (D) is not a good option because it may not identify the root cause and may overwrite important data. Implementing the shortest solution first to identify the issue and minimize downtime © is also not a good option because it may not solve the problem or may create new issues. Consulting internet forums to determine which is the most common cause and deploy only that solution (A) is not a good option because it may not apply to the specific situation or may be outdated or inaccurate

#### NEW QUESTION 219

Hackers recently targeted a company with an attack that resulted in a system breach, which compromised the organization's data. Because of the system breach, the administrator had to bypass normal change management procedures. Which of the following change management activities was necessary?

- A. Cancelled change request
- B. Change request postponement



- C. Emergency change request
- D. Privilege change request
- E. User permission change request

**Answer:** C

**Explanation:**

An emergency change request is a type of change request that is initiated in response to an urgent situation, such as a system breach, that requires immediate action to restore normal operations or prevent further damage. An emergency change request may bypass some of the normal change management procedures, such as approval, testing, or documentation, in order to expedite the implementation of the change. However, an emergency change request should still follow the basic steps of change management, such as identification, analysis, planning, execution, and evaluation, and should be reviewed and documented after the change is completed.

References: CompTIA Server+ Study Guide, Chapter 11: Change Management, page 443.

**NEW QUESTION 221**

A server administrator receives a report that Ann, a new user, is unable to save a file to her home directory on a server. The administrator checks Ann's home directory permissions and discovers the following:

`dr-xr-xr-- /home/Ann`

Which of the following commands should the administrator use to resolve the issue without granting unnecessary permissions?

- A. `chmod777/home/Ann`
- B. `chmod666/home/Ann`
- C. `chmod711/home/Ann`
- D. `chmod754/home/Ann`

**Answer:** D

**Explanation:**

The administrator should use the command `chmod 754 /home/Ann` to resolve the issue without granting unnecessary permissions. The `chmod` command is used to change the permissions of files and directories on a Linux server. The permissions are represented by three numbers, each ranging from 0 to 7, that correspond to the read (r), write (w), and execute (x) permissions for the owner, group, and others respectively. The numbers are calculated by adding up the values of each permission: r = 4, w = 2, x = 1. For example, 7 means rwx (4 + 2 + 1), 6 means rw- (4 + 2), 5 means r-x (4 + 1), etc. In this case, Ann's home directory has the permissions `dr-xr-xr--`, which means that only the owner (d) can read (r) and execute (x) the directory, and the group and others can only read (r) and execute (x) but not write (w) to it. This prevents Ann from saving files to her home directory. To fix this issue, the administrator should grant write permission to the owner by using `chmod 754 /home/Ann`, which means that the owner can read (r), write (w), and execute (x) the directory, the group can read (r) and execute (x) but not write (w) to it, and others can only read (r) but not write (w) or execute (x) it. This way, Ann can save files to her home directory without giving unnecessary permissions to others.

Reference:

<https://linuxize.com/post/what-does-chmod-777-mean/>

**NEW QUESTION 225**

A technician runs `top` on a dual-core server and notes the following conditions: `top -- 14:32:27, 364 days, 14 usersload average 60.5 12.4 13.6`

Which of the following actions should the administrator take?

- A. Schedule a mandatory reboot of the server
- B. Wait for the load average to come back down on its own
- C. Identify the runaway process or processes
- D. Request that users log off the server

**Answer:** C

**Explanation:**

The administrator should identify the runaway process or processes that are causing high load average on the server. Load average is a metric that indicates how many processes are either running on or waiting for the CPU at any given time. A high load average means that there are more processes than available CPU cores, resulting in poor performance and slow response time. A runaway process is a process that consumes excessive CPU resources without terminating or releasing them. A runaway process can be caused by various factors, such as programming errors, infinite loops, memory leaks, etc. To identify a runaway process, the administrator can use tools such as `top`, `ps`, or `htop` to monitor CPU usage and process status. To stop a runaway process, the administrator can use commands such as `kill`, `pkill`, or `killall` to send signals to terminate it.

**NEW QUESTION 230**

A server administrator is building a pair of new storage servers. The servers will replicate; therefore, no redundancy is required, but usable capacity must be maximized. Which of the following RAID levels should the server administrator implement?

- A. 1
- B. 5
- C. 6
- D. 10

**Answer:** A

**Explanation:**

The RAID level that should be implemented to maximize usable capacity without requiring redundancy is RAID 0. RAID (Redundant Array of Independent Disks) is a technology that combines multiple physical disks into a logical unit that provides improved performance, reliability, or both. RAID 0 is a RAID level that splits data evenly across two or more disks without parity or mirroring. RAID 0 does not provide any redundancy or fault tolerance, but it increases usable capacity and performance by allowing parallel read and write operations.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 1, Lesson 1.2, Objective 1.2

**NEW QUESTION 234**

A server administrator encounters some issues with the server OS after applying monthly patches. Which of the following troubleshooting steps should the

administrator perform?

- A. Implement rollback procedures.
- B. Upgrade the drivers.
- C. Reinstall the OS.
- D. Reboot the server.

**Answer:** A

**Explanation:**

This option would restore the server OS to a previous state before applying the monthly patches. This would help troubleshoot the issues caused by the patches and determine if they are compatible with the server OS. The other options would either not address the issues, cause data loss, or require more time and resources

**NEW QUESTION 236**

A new 40GB NIC has just been installed in a server but is not detected within the Windows server OS. Which of the following would most likely fix the issue?

- A. Update the firmware on the NIC.
- B. Update the server OS.
- C. Update the remote management console.
- D. Update the switch firmware.

**Answer:** A

**Explanation:**

Updating the firmware on the NIC is the most likely solution to fix the issue of a new 40GB NIC not being detected within the Windows server OS. Firmware is a software program that controls the functionality of a hardware device, such as a NIC (network interface card). A NIC is a device that enables network communication for a server by providing an interface between the server and the network cable or wireless connection. Updating the firmware on the NIC can improve its performance, compatibility, and stability with the server OS and network protocols. References: CompTIA Server+ Certification Exam Objectives, Domain 4.0: Networking, Objective 4.1: Given a scenario, configure network settings for servers.

**NEW QUESTION 239**

Which of the following should be placed at the top of a Bash script to ensure it can be executed?

- A. bash
- B. !execute
- C. #!
- D. @echo off

**Answer:** C

**Explanation:**

#! is the symbol that should be placed at the top of a Bash script to ensure it can be executed. #! is also known as shebang or hashbang. It is a special notation that tells the operating system which interpreter to use to run the script. The shebang is followed by the path to the interpreter, such as /bin/bash for Bash, /bin/python for Python, or /bin/perl for Perl. For example, a Bash script that prints "Hello World" would start with:

```
#!/bin/bash echo "Hello World"
```

The shebang must be the first line of the script and must not have any spaces between the

# and ! symbols. bash is not a valid shebang by itself, as it does not specify the path to the interpreter. !execute is not a valid shebang at all, as it does not start with #. @echo off is a command that disables the echoing of commands in a batch file on Windows, but it has nothing to do with Bash scripts on Linux.

References: <https://www.howtogeek.com/67469/the-beginners-guide-to-shell-scripting-the-basics/> <https://www.howtogeek.com/435903/what-is-a-shebang-line/>

**NEW QUESTION 244**

An administrator is able to ping the default gateway and internet sites by name from a file server. The file server is not able to ping the print server by name. The administrator is able to ping the file server from the print server by both IP address and computer name. When initiating an initiating from the file server for the print server, a different IP address is returned, which of the following is MOST Likely the cause?

- A. A firewall blocking the ICMP echo reply.
- B. The DHCP scope option is incorrect
- C. The DNS entries for the print server are incorrect.
- D. The hosts file misconfigured.

**Answer:** D

**Explanation:**

The hosts file is a file that maps hostnames to IP addresses on a server or a computer. It can be used to override or supplement the DNS (Domain Name System) resolution for certain hosts or domains. If the hosts file is misconfigured, it may return a different IP address for a hostname than the one registered in the DNS server, causing connectivity issues or errors. Verified References: [Hosts file], [DNS]

**NEW QUESTION 247**

A server administrator is swapping out the GPU card inside a server. Which of the following actions should the administrator take FIRST?

- A. Inspect the GPU that is being installed.
- B. Ensure the GPU meets HCL guidelines.
- C. Shut down the server.
- D. Disconnect the power from the rack.

**Answer:** C

**Explanation:**

The first action that the administrator should take before swapping out the GPU card inside a server is to shut down the server. This is to ensure that the server is not running any processes that might be using the GPU card, and to prevent any damage to the hardware or data loss due to sudden power loss. Shutting down the server also reduces the risk of electrostatic discharge (ESD) that might harm the components. Reference: <https://pcgearhead.com/installing-a-new-gpu/>

**NEW QUESTION 248**

A technician has been tasked to install a new CPU. Prior to the installation the server must be configured. Which of the following should the technician update?

- A. The RAID card
- B. The BIOS
- C. The backplane
- D. The HBA

**Answer:** B

**Explanation:**

The BIOS (Basic Input/Output System) is a firmware that controls the initialization and booting of a server. It also provides settings for the CPU, such as speed, voltage, and temperature. Updating the BIOS can improve the performance and compatibility of the CPU and other hardware components. Verified References: [BIOS], [CPU]

**NEW QUESTION 251**

Which of the following can be BEST described as the amount of time a company can afford to be down during recovery from an outage?

- A. SLA
- B. MTBF
- C. RTO
- D. MTTR

**Answer:** C

**Explanation:**

The term that best describes the amount of time a company can afford to be down during recovery from an outage is RTO. RTO (Recovery Time Objective) is a metric that defines the maximum acceptable downtime for an application, system, or process after a disaster or disruption. RTO helps determine the level of urgency and resources required for restoring normal business operations. RTO is usually measured in minutes, hours, or days, depending on the criticality and impact of the service.

Reference:

<https://whatis.techtarget.com/definition/recovery-time-objective-RTO>

**NEW QUESTION 252**

An application server's power cord was accidentally unplugged. After plugging the cord back in the server administrator notices some transactions were not written to the disk array. Which of the following is the MOST likely cause of the issue?

- A. Backplane failure
- B. CMOS failure
- C. Misconfigured RAID
- D. Cache battery failure

**Answer:** D

**Explanation:**

A cache battery is a battery that provides backup power to the cache memory of a disk array controller. The cache memory stores data that is waiting to be written to the disk array. If the cache battery fails, the data in the cache memory may be lost or corrupted when the power is interrupted. Verified References: [Cache battery], [Disk array controller]

**NEW QUESTION 257**

Which of the following asset management documents is used to identify the location of a server within a data center?

- A. Infrastructure diagram
- B. Workflow diagram
- C. Rack layout
- D. Service manual

**Answer:** C

**Explanation:**

A rack layout is a document that shows the physical location and arrangement of servers and other devices within a rack. It can include information such as server names, IP addresses, power consumption, and cable connections. A rack layout can help identify and locate servers easily and efficiently in a data center. Verified References: [Rack layout], [Data center]

**NEW QUESTION 260**

An administrator notices high traffic on a certain subnet and would like to identify the source of the traffic. Which of the following tools should the administrator utilize?

- A. Anti-malware
- B. Nbtstat
- C. Port scanner
- D. Sniffer

**Answer:**

D

**Explanation:**

Application consistent backup is a method of backing up data that ensures the integrity and consistency of the application state. It involves notifying the application to flush its data from memory to disk and quiescing any write operations before taking a snapshot of the data. If the databases were not backed up to be application consistent, they might contain incomplete or corrupted data that cannot be restored properly.

References:

CompTIA Server+ Certification Exam Objectives1, page 12 What is Application Consistent Backup and How to Achieve It2 Application-Consistent Backups3

**NEW QUESTION 261**

A server technician has been asked to upload a few files from the internal web server to the internal FTP server. The technician logs in to the web server using PuTTY, but the connection to the FTP server fails. However, the FTP connection from the technician's workstation is successful. To troubleshoot the issue, the technician executes the following command on both the web server and the workstation:

```
ping ftp.acme.local
```

The IP address in the command output is different on each machine. Which of the following is the MOST likely reason for the connection failure?

- A. A misconfigured firewall
- B. A misconfigured hosts.deny file
- C. A misconfigured hosts file
- D. A misconfigured hosts.allow file

**Answer:** D

**Explanation:**

A misconfigured hosts file can cause name resolution issues on a server. A hosts file is a text file that maps hostnames to IP addresses on a local system. It can be used to override DNS settings or provide custom name resolution for testing purposes. However, if the hosts file contains incorrect or outdated entries, it can prevent the system from resolving hostnames properly and cause connectivity problems. To fix this issue, the administrator should check and edit the hosts file accordingly.

**NEW QUESTION 264**

A server in a remote datacenter is no longer responsive. Which of the following is the BEST solution to investigate this failure?

- A. Remote desktop
- B. Access via a crash cart
- C. Out-of-band management
- D. A Secure Shell connection

**Answer:** C

**Explanation:**

The best solution to investigate the failure of a server in a remote datacenter is out-of-band management. Out-of-band management is a method of accessing and controlling a server or a device using a dedicated channel that is separate from its normal network connection. Out-of-band management can use various technologies, such as serial ports, modems, KVM switches, or dedicated management cards or interfaces. Out-of-band management can provide remote access to servers or devices even when they are powered off, unresponsive, or disconnected from the network. Out-of-band management can enable troubleshooting, configuration, maintenance, or recovery tasks without requiring physical presence at the server location.

Reference:

[https://www.lantronix.com/wp-content/uploads/pdf/Data\\_Center\\_Mgmt\\_WP.pdf](https://www.lantronix.com/wp-content/uploads/pdf/Data_Center_Mgmt_WP.pdf)

**NEW QUESTION 265**

Which of the following is the MOST secure method to access servers located in remote branch offices?

- A. Use an MFA out-of-band solution.
- B. Use a Telnet connection.
- C. Use a password complexity policy.
- D. Use a role-based access policy.

**Answer:** A

**Explanation:**

This is the most secure method to access servers located in remote branch offices because MFA stands for multi-factor authentication, which requires users to provide more than one piece of evidence to prove their identity. An out-of-band solution means that one of the factors is delivered through a separate channel, such as a phone call, a text message, or an email. This adds an extra layer of security and prevents unauthorized access even if a password is compromised. References: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks>

**NEW QUESTION 270**

A server is reporting a hard drive S.M.A.R.T. error. When a technician checks on the drive, however, it appears that all drives in the server are functioning normally. Which of the following is the reason for this issue?

- A. A S.M.A.R.
- B. error is a predictive failure notice
- C. The drive will fail in the near future and should be replaced at the next earliest time possible
- D. A S.M.A.R.
- E. error is a write operation error
- F. It has detected that the write sent to the drive was incorrectly formatted and has requested a retransmission of the write from the controller
- G. A S.M.A.R.
- H. error is simply a bad sector
- I. The drive has marked the sector as bad and will continue to function properly
- J. A S.M.A.R.



- K. error is an ECC erro
- L. Due to error checking and correcting, the drive has corrected the missing bit and completed the write operation correctly.

**Answer:** A

**Explanation:**

A S.M.A.R.T. error is a predictive failure notice. The drive will fail in the near future and should be replaced at the next earliest time possible. S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) is a feature that monitors the health and performance of hard drives and alerts the user of any potential problems or failures. S.M.A.R.T. can detect various indicators of drive degradation, such as bad sectors, read/write errors, temperature, or spin-up time. If a S.M.A.R.T. error is reported, it means that the drive has exceeded a predefined threshold of acceptable operation and is likely to fail soon. The drive may still function normally for a while, but it is recommended to back up the data and replace the drive as soon as possible to avoid data loss or system downtime.

**NEW QUESTION 272**

A technician is trying to determine the reason why a Linux server is not communicating on a network. The returned network configuration is as follows:

```
eth0: flags=4163<UP, BROADCAST,RUNNING,MULTICAST> mtu 1500
```

inet 127.0.0.1 network 255.255.0.0 broadcast 127.0.0.1 Which of the following BEST describes what is happening?

- A. The server is configured to use DHCP on a network that has multiple scope options
- B. The server is configured to use DHCP, but the DHCP server is sending an incorrect subnet mask
- C. The server is configured to use DHCP on a network that does not have a DHCP server
- D. The server is configured to use DHCP, but the DHCP server is sending an incorrect MTU setting

**Answer:** C

**Explanation:**

The reason why the Linux server is not communicating on a network is that it is configured to use DHCP on a network that does not have a DHCP server. DHCP (Dynamic Host Configuration Protocol) is a protocol that allows a client device to obtain an IP address and other network configuration parameters from a DHCP server automatically. However, if there is no DHCP server on the network, the client device will not be able to obtain a valid IP address and will assign itself a link-local address instead. A link-local address is an IP address that is only valid within a local network segment and cannot be used for communication outside of it. A link-local address has a prefix of 169.254/16 in IPv4 or fe80::/10 in IPv6. In this case, the Linux server has assigned itself a link-local address of 127.0.0.1, which is also known as the loopback address. The loopback address is used for testing and troubleshooting purposes and refers to the device itself. It cannot be used for communication with other devices on the network.

**NEW QUESTION 276**

Which of the following is the most effective way to mitigate risks associated with privacy- related data leaks when sharing with a third party?

- A. Third-party acceptable use policy
- B. Customer data encryption and masking
- C. Non-disclosure and indemnity agreements
- D. Service- and operational-level agreements

**Answer:** B

**Explanation:**

The most effective way to mitigate risks associated with privacy-related data leaks when sharing with a third party is customer data encryption and masking. Encryption is a process of transforming data into an unreadable format that can only be decrypted with a key or password. Masking is a process of hiding or replacing sensitive data with fake or meaningless data. By encrypting and masking customer data, the organization can protect the confidentiality and integrity of the data and prevent unauthorized access or disclosure by the third party.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.3, Objective 3.3

**NEW QUESTION 278**

Which of the following technologies would allow an administrator to build a software RAID on a Windows server?

- A. Logical volume management
- B. Dynamic disk
- C. GPT
- D. UEFI

**Answer:** B

**Explanation:**

Dynamic disk is a technology that allows an administrator to build a software RAID on a Windows server. Dynamic disk is a type of disk management that supports creating volumes that span multiple disks, stripe data across disks, mirror data between disks, or use parity for fault tolerance. Dynamic disk can be used to create RAID 0 (striping), RAID 1 (mirroring), RAID 5 (striping with parity), or spanned volumes on Windows servers. Logical volume management is a technology that allows creating and resizing logical volumes on Linux servers. GPT (GUID Partition Table) is a standard for defining the partition structure on a disk. UEFI (Unified Extensible Firmware Interface) is a specification for the interface between the operating system and the firmware. References: <https://www.howtogeek.com/school/using-windows-admin-tools-like-a-pro/lesson2/> <https://www.howtogeek.com/howto/40702/how-to-manage-and-use-lvm-logical-volume-management-in-ubuntu/> <https://www.howtogeek.com/193669/whats-the-difference-between-gpt-and-mbr-when-partitioning-a-drive/> <https://www.howtogeek.com/56958/htg-explains-how-uefi-will-replace-the-bios/>

**NEW QUESTION 281**

A backup application is copying only changed files each line it runs. During a restore, however, only a single file is used. Which of the following backup methods does this describe?

- A. Open file
- B. Synthetic full
- C. Full Incremental
- D. Full differential

**Answer:** B

**Explanation:**

A synthetic full backup is a backup method that describes copying only changed files each time it runs and using only a single file during a restore. A synthetic full backup is a backup approach that involves creating a new full backup by using the previous full backup and related incremental backups. This means that a backup solution does not have to transfer the full amount of data from the source machine and can synthesize the latest incremental backups with the last full backup to create a new full backup. This reduces the backup window and network bandwidth consumption. During a restore, only the latest synthetic full backup file is needed to recover the data. Open file backup is a backup method that allows backing up files that are in use or locked by applications. Full incremental backup is a backup method that involves performing a full backup first and then backing up only the changed files since the last backup. Full differential backup is a backup method that involves performing a full backup first and then backing up only the changed files since the last full backup. References: <https://www.nakivo.com/blog/what-is-synthetic-backup/> <https://www.howtogeek.com/192115/what-you-need-to-know-about-creating-system-image-backups/>

**NEW QUESTION 283**

The management team at a healthcare organization is concerned about being able to access the dairy vital records if there is an IT disaster that causes both servers and the network to be offline. Which of the following backup types can the organization use to mitigate this risk?

- A. Tape
- B. Cloud
- C. Disk
- D. Print

**Answer:** D

**Explanation:**

A print backup is a type of backup that can be used to mitigate the risk of being unable to access the daily vital records if there is an IT disaster that causes both servers and the network to be offline. A print backup is a backup that involves printing out the data on paper and storing it in a secure location. A print backup can provide offline access to the data without relying on any hardware or software components that may be affected by the disaster. However, a print backup has some drawbacks such as high cost, low efficiency, low security, and environmental impact. A tape backup is a type of backup that involves storing the data on magnetic tape cartridges that can be accessed using a tape drive or a tape library. A tape backup can provide offline access to the data with high capacity, low cost, and long durability, but it requires special equipment and software that may not be available during a disaster. A cloud backup is a type of backup that involves storing the data on remote servers or platforms that can be accessed over the internet using a web browser or an application. A cloud backup can provide online access to the data with high scalability, flexibility, and security, but it requires network connectivity and bandwidth that may not be available during a disaster. A disk backup is a type of backup that involves storing the data on hard disk drives or solid state drives that can be accessed using a computer or a device. A disk backup can provide online or offline access to the data with high performance, reliability, and portability, but it requires compatible hardware and software that may not be available during a disaster. References: <https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-it-matter/> <https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual-files/> <https://www.howtogeek.com/199068/how-to-upgrade-your-existing-hard-drive-in-under-an-hour/> <https://www.howtogeek.com/202794/what-is-the-difference-between-127>

**NEW QUESTION 288**

A technician needs to install a Type 1 hypervisor on a server. The server has SD card slots, a SAS controller, and a SATA controller, and it is attached to a NAS. On which of the following drive types should the technician install the hypervisor?

- A. SD card
- B. NAS drive
- C. SATA drive
- D. SAS drive

**Answer:** D

**Explanation:**

The technician should install the Type 1 hypervisor on a SAS drive. A Type 1 hypervisor is a layer of software that runs directly on top of the physical hardware and creates virtual machines that share the hardware resources. A Type 1 hypervisor requires fast and reliable storage for optimal performance and stability. A SAS drive is a type of hard disk drive that uses Serial Attached SCSI (SAS) as its interface protocol. SAS drives offer high speed, low latency, and high reliability compared to other types of drives, such as SD cards, NAS drives, or SATA drives. SD cards are flash memory cards that offer low cost and portability but have low speed, low capacity, and low durability. NAS drives are network-attached storage devices that offer high capacity and easy access but have high latency and low reliability due to network dependency. SATA drives are hard disk drives that use Serial ATA (SATA) as their interface protocol. SATA drives offer moderate speed, moderate cost, and moderate reliability but have lower performance and durability than SAS drives.

**NEW QUESTION 291**

A server technician is placing a newly configured server into a corporate environment. The server will be used by members of the accounting department, who are currently assigned by the VLAN identified below:

VLAN name	VLAN ID	IP address	Default gateway	Exclusion range
Accounting	25	172.16.25.1–172.16.25.254/24	172.16.25.254	172.16.25.50–172.16.25.100

Which of the following IP address configurations should the technician assign to the new server so the members of the accounting group can access the server?

- A. IP address: 172.16.25.90/24 Default gateway: 172.16.25.254
- B. IP address: 172.16.25.101/16 Default gateway: 172.16.25.254
- C. IP address: 172.16.25.254/24 Default gateway: 172.16.25.1
- D. IP address: 172.16.26.101/24 Default gateway: 172.16.25.254

**Answer:** A

**Explanation:**

The IP address configuration that the technician should assign to the new server so the members of the accounting group can access the server is

172.16.25.90/24 for the IP address and 172.16.25.254 for the default gateway. This configuration matches the VLAN identified in the image, which has a network address of 172.16.25.0/24 and a subnet mask of 255.255.255.0. The IP address of the server must be within the same network range as the VLAN, which is from 172.16.25.1 to 172.16.25.254, excluding the network and broadcast addresses (172.16.25.0 and 172.16.25.255). The default gateway of the server must be the same as the VLAN, which is 172.16.25.254, to allow communication with other networks or devices outside the VLAN. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Networking, Objective 4.1: Given a scenario, configure network settings for servers.

#### NEW QUESTION 293

Ann, an administrator, is configuring a two-node cluster that will be deployed. To check the cluster's functionality, she shuts down the active node. Cluster behavior is as expected, and the passive node is now active. Ann powers on the server again and wants to return to the original configuration. Which of the following cluster features will allow Ann to complete this task?

- A. Heartbeat
- B. Failback
- C. Redundancy
- D. Load balancing

**Answer:** B

#### Explanation:

The cluster feature that will allow Ann to complete her task is failback. A cluster is a group of servers that work together to provide high availability, scalability, and load balancing for applications or services. A cluster can have different nodes or members that have different roles or states. An active node is a node that is currently running an application or service and serving requests from clients. A passive node is a node that is on standby and ready to take over if the active node fails. A failover is a process of switching from a failed or unavailable node to another node in a cluster. A failback is a process of switching back from a failover node to the original node after it becomes available again. Failback can be automatic or manual depending on the cluster configuration.

#### NEW QUESTION 297

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### SK0-005 Practice Exam Features:

- \* SK0-005 Questions and Answers Updated Frequently
- \* SK0-005 Practice Questions Verified by Expert Senior Certified Staff
- \* SK0-005 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SK0-005 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SK0-005 Practice Test Here](#)**