CompTIA

Exam Questions SK0-005

CompTIA Server+ Certification Exam

NEW QUESTION 1
A snapshot is a feature that can be used in hypervisors to:

A. roll back firmware updates.
B. restore to a previous version.
C. roll back application drivers.
D. perform a backup restore.

Answer: B

Explanation:
A snapshot is a feature that can be used in hypervisors to restore to a previous version. A snapshot is a point-in-time copy of a virtual machine (VM) that captures the state and data of the VM at a specific moment. A snapshot can be created instantly and with minimal overhead, as it only stores the changes made to the VM after the snapshot was taken. A snapshot can be used to restore the VM to its previous state in case of data loss or corruption.

NEW QUESTION 2
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 3
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 4
A company is implementing a check-in desk to heighten physical security. Which of the following access controls would be the most appropriate to facilitate this implementation?

A. Security guards
B. Security cameras
C. Bollards
D. An access control vestibule

Answer: D

Explanation:
An access control vestibule, or mantrap, is a type of physical access control that provides a space between two sets of interlocking doors. It is designed to prevent unauthorized individuals from following authorized individuals into facilities with controlled access, such as a check-in desk. The vestibule can be configured to limitthe number of individuals who enter the controlled area and to verify their authorization for physical access1. The other options are incorrect because they are not as effective as an access control vestibule in
facilitating the implementation of a check-in desk. Security guards, security cameras, and bollards are useful for monitoring, deterring, or preventing unauthorized access, but they do not provide the same level of control and verification as an access control vestibule

NEW QUESTION 5
An organization purchased six new 4TB drives for a server. An administrator is tasked with creating an efficient RAID given the minimum disk space requirement of 19TBs. Which of the following should the administrator choose to get the most efficient use of space?

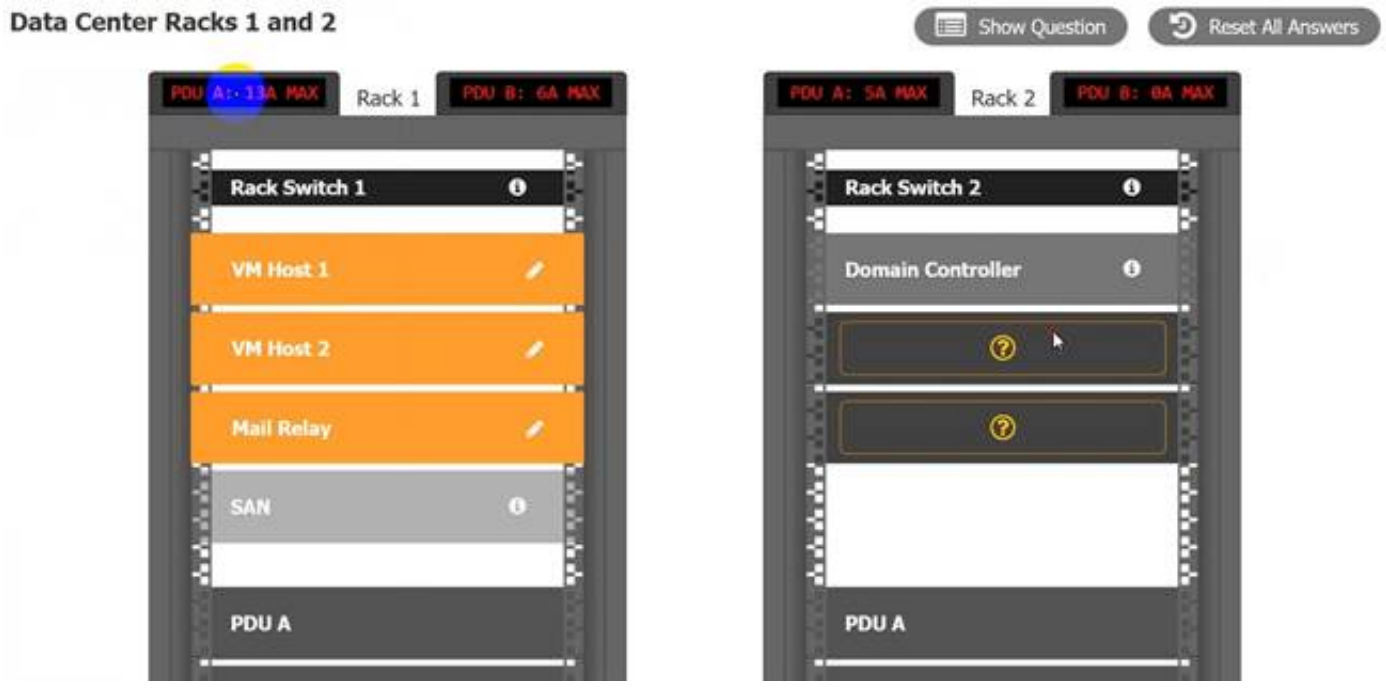
A. RAID 1
B. RAID 5
C. RAID 6

D. RAID 10

Answer: B

Explanation:
RAID 5 is a RAID level that uses disk striping with parity. It requires a minimum of three disks and can handle one disk failure. RAID 5 distributes the parity information across all the disks in the array, which improves the read performance and reduces the write penalty. The capacity of a RAID 5 array is (N-1) times the size of the smallest disk, where N is the number of disks in the array. Therefore, for six 4TB disks, the capacity of a RAID 5 array would be (6-1) x 4TB = 20TB, which meets the minimum disk space requirement of 19TB. RAID 5 also has the leastamount of disk space lost to RAID overhead among the options, as it only uses onedisk's worth of space for parity

NEW QUESTION 6
DRAG DROP
A recent power Outage caused email services to go down. A sever administrator also received alerts from the datacenter's UPS.
After some investigation, the server administrator learned that each POU was rated at a maximum Of 12A.
INSTRUCTIONS
Ensure power redundancy is implemented throughout each rack and UPS alarms are resolved. Ensure the maximum potential PDU consumption does not exceed 80% or 9.6A).
* a. PDU selections must be changed using the pencil icon.
* b. VM Hosts 1 and 2 and Mail Relay can be moved between racks.
* c. Certain devices contain additional details



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 7
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 8
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 tour network cables up the left side of the rack to the top of the rack switc
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 cablespossible 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 9
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 10
A user cannot save large files to a directory on a Linux server that was accepting smaller files a few minutes ago. Which of the following commands should a technician use to identify the issue?

A. pvdisplay
B. mount
C. df -h
D. fdisk -l

Answer: C

Explanation:
The df -h command should be used to identify the issue of not being able to save large files to a directory on a Linux server. The df -h command displays disk space usage in human-readable format for all mounted file systems on the server. It shows the total size, used space, available space, percentage of use, and mount point of each file system. By using this command, a technician can check if there is enough free space on the file system where the directory is located or if it has reached its capacity limit.

NEW QUESTION 10
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 15
A server administrator is currently working on an incident. Which of the following steps should the administrator perform before resolving the issue?

A. Inform the impacted users.
B. Make the changes to the system.
C. Determine the probable causes.
D. Identify changes to the server.

Answer: C

Explanation:
The step that the server administrator should perform before resolving the issue is to determine the probable causes. This step is part of the troubleshooting process that follows a logical and systematic approach to identify and solve problems with servers and applications. The troubleshooting process consists of several steps, such as:
? Identify the problem: Gather information from various sources, such as users, logs, or alerts, to understand the symptoms and scope of the problem.
? Establish a theory of probable cause: Analyze the information and formulate one or more possible causes of the problem based on evidence or experience.
? Test the theory to determine cause: Perform tests or experiments to verify or eliminate each possible cause until the root cause is found.
? Establish a plan of action to resolve the problem and implement the solution: Design and execute a plan to fix the problem using appropriate tools and techniques.
? Verify full system functionality and implement preventive measures: Confirm that the problem is resolved and that no other issues arise as a result of the solution. Implement preventive measures to avoid recurrence of the problem or improve performance.
? Document findings, actions, and outcomes: Record the details of the problem, its cause, its solution, and its outcome for future reference or knowledge sharing. References: [CompTIA Server+ Certification Exam Objectives], Domain 6.0: Troubleshooting, Objective 6.1: Given a scenario involving server hardware issues (e.g., power supply failure), troubleshoot using appropriate tools.

NEW QUESTION 18
A server room with many racks of servers is managed remotely with occasional on-site support. Which of the following would be the MOST cost-effective option to administer and troubleshoot network problems locally on the servers?

A. Management port
B. Crash cart
C. IP KVM
D. KVM

Answer: C

Explanation:
An IP KVM (keyboard, video, mouse) is a device that allows remote access and control of multiple servers over a network using a web browser or a clientsoftware. An IP KVM is a cost-effective option to administer and troubleshoot network problems locally on the servers, as it eliminates the need for physical presence or dedicated hardware for each server. A management port (A) is a network interface that is used for out-of-band management of network devices, such as routers or switches. A management port does not provide local access to servers. A crash cart (B) is a mobile unit that contains a monitor, keyboard, mouse, and other tools for troubleshooting servers in a data center. A crash cart requires physical access to each server and may not be cost-effective for many racks of servers. A KVM (D) is a device that allows switching between multiple servers using a single keyboard, video, and mouse. A KVM does not provide remote access over a network and requires physical connection to each server. References: https://www.enterprisestorageforum.com/management/best-data-storage-solutions-and- software-2021/https://www.microsoft.com/en-us/microsoft-365/business-insights- ideas/resources/cloud-storage-vs-on-premises-servers

NEW QUESTION 22
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 same1.
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 24
A Linux server was recently updated. Now, the server stops during the boot process with a blank screen and an£s> prompt. When of the following is the MOST likely cause of this issue?

A. The system is booting to a USB flash drive
B. The UEFI boot was interrupted by a missing Linux boot file
C. The BIOS could not find a bootable hard disk
D. The BIOS firmware needs to be upgraded

Answer: B

Explanation:
The most likely cause of this issue is that the UEFI boot was interrupted by a missing Linux
boot file, such as grub.cfg or vmlinuz, which are essential for loading the Linux kernel and booting the system. The £s> prompt indicates that the system entered

into UEFI Shell mode, which is a command-line interface for troubleshooting UEFI boot issues. The administrator can use UEFI Shell commands to locate and restore the missing boot file or change the boot order. Verified References: [UEFI Shell Guide]

NEW QUESTION 29
A technician is installing a variety of servers in a rack. Which of the following is the BEST course of action for the technician to take while loading the rack?

A. Alternate the direction of the airflow
B. Install the heaviest server at the bottom of the rack
C. Place a UPS at the top of the rack
D. Leave 1U of space between each server

Answer: B

Explanation:
The technician should install the heaviest server at the bottom of the rack to load the rack properly. Installing the heaviest server at the bottom of the rack helps to balance the weight distribution and prevent the rack from tipping over or collapsing. Installing the heaviest server at the bottom of the rack also makes it easier to access and service the server without lifting or moving it. Installing the heaviest server at any other position in the rack could create instability and safety hazards.

NEW QUESTION 34
A technician is checking a server rack. Upon entering the room, the technician notices the tans on a particular server in the rack are running at high speeds. This is the only server in the rack that is experiencing this behavior. The ambient temperature in the room appears to be normal. Which of the following is the MOST likely reason why the fans in that server are operating at full speed?

A. The server is In the process of shutting down, so fan speed operations have been defaulted to high.
B. An incorrect fan size was inserted into the server, and the server has had to Increase the fan speed to compensate.
C. A fan failure has occurred, and the other fans have increased speed to compensate.
D. The server is utilizing more memory than the other servers, so it has increased the fans to compensate.

Answer: C

Explanation:
This is the most likely reason why the fans in that server are operating at full speed while the ambient temperature in the room is normal and the other servers in the rack are not experiencing this behavior. A fan failure is a situation where one or more fans in a server stop working or malfunction due to wear and tear, dust, or other factors. This can cause overheating and performance issues on the server. To prevent this, most servers have a fan redundancy feature that allows the other fans to increase their speed and airflow to compensate for the failed fan and maintain a safe temperature level. The server is not likely to be in the process of shutting down, as this would not cause the fans to run at high speeds. An incorrect fan size is not likely to be inserted into the server, as most fans are standardized and compatible with the server chassis and motherboard. The server is not likely to be utilizing more memory than the other servers, as this would not cause a significant increase in temperature or fan speed. References: https://www.howtogeek.com/303282/how-to-manage-your-pcs-fans-for-optimal-airflow-and-cooling/https://www.howtogeek.com/174288/how-to-tell-if-your-computer-is-overheating-and-what-to-do-about-it/

NEW QUESTION 39
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 thatinvolves 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 41
A server is only able to connect to a gigabit switch at 100Mb. Other devices are able to access the network port at full gigabit speeds, and when the server is brought to another location, it is able to connect at full gigabit speed. Which of the following should an administrator check first?

A. The switch management
B. The VLAN configuration
C. The network cable
D. The network drivers

Answer: C

Explanation:
The first thing that the administrator should check is the network cable. The network cable is a physical medium that connects a server to a switch or other network device. The network cable can affect the speed and quality of the network connection, depending on its type, length, and condition. If the network cable is damaged, faulty, or incompatible, it can cause the server to connect at a lower speed than expected. Therefore, the administrator should check the network cable for any signs of wear, tear, or mismatch, and replace it if necessary.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 2, Lesson 2.1, Objective 2.1

NEW QUESTION 42
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

NEW QUESTION 46
After configuring IP networking on a newly commissioned server, a server administrator installs a straight- through network cable from the patch panel to the switch. The administrator then returns to the server to test network connectivity using the ping command. The partial output of the ping and ipconfig commands are displayed below:

```
ipconfig/all

IPv4 address: 192.168.1.5
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: Request timed out
Reply from 192.168.1.2: Request timed out
Reply from 192.168.1.2: Request timed out
Reply from 192.168.1.2: Request timed out
```

The administrator returns to the switch and notices an amber link light on the port where the server is connected. Which of the following is the MOST likely reason for the lack of network connectivity?

A. Network port security
B. An improper VLAN configuration
C. A misconfigured DHCP server
D. A misconfigured NIC on the server

Answer: D

Explanation:
A misconfigured NIC on the server is the most likely reason for the lack of network connectivity. The output of the ping command shows that the server is unable to reach its default gateway (10.0.0.1) or any other IP address on the network. The output of the ipconfig command shows that the server has a valid IP address (10.0.0.10) and subnet mask (255.255.255.0) but no default gateway configured. This indicates that there is a problem with the NIC settings on the server, such as an incorrect IP address, subnet mask, default gateway, DNS server, etc. A misconfigured NIC can also cause an amber link light on the switch port, which indicates a speed or duplex mismatch between the NIC and the switch.

NEW QUESTION 47
Users in an office lost access to a file server following a short power outage. The server administrator noticed the server was powered off. Which of the following should the administrator do to prevent this situation in the future?

A. Connect the server to a KVM
B. Use cable management
C. Connect the server to a redundant network
D. Connect the server to a UPS

Answer: D

Explanation:
The administrator should connect the server to a UPS to prevent this situation in the future. A UPS (Uninterruptible Power Supply) is a device that provides backup power to a server or other device in case of a power outage or surge. A UPS typically consists of one or more batteries and an inverter that converts the battery power into AC power that the server can use. A UPS can also protect the server from power fluctuations that can damage its components or cause data corruption. By connecting the server to a UPS, the administrator can ensure that the server will continue to run or shut down gracefully during a power failure.

NEW QUESTION 49
A server administrator added a new drive to a server. However, the drive is not showing up as available. Which of the following does the administrator need to do to make the drive available?

A. Partition the drive.
B. Create a new disk quota.
C. Configure the drive as dynamic.
D. Set the compression.

Answer: A

Explanation:
To make a new drive available on a server, the administrator needs to partition the drive first. Partitioning is a process that divides the drive into one or more logical sections that can be formatted and assigned drive letters or mount points. Partitioning can be done using tools such as Disk Management on Windows or fdisk on Linux. Creating a new disk quota would not help, as disk quotas are used to limit the amount of disk space that users or groups can use on a partition. Configuring the drive as dynamic would not help either, as dynamic disks are used to create volumes that span multiple disks or use RAID features. Setting the compression would not help, as compression is used to reduce the size of files on a partition. References: https://www.howtogeek.com/school/using-windows-admin-tools-like-a-pro/lesson2/https://www.howtogeek.com/howto/17001/how-to-format-a-usb-drive-in- ubuntu-using-gparted/

NEW QUESTION 51
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 53
Users at a company work with highly sensitive data. The security department implemented an administrative and technical control to enforce least-privilege access assigned to files. However, the security department has discovered unauthorized data exfiltration. Which of the following is the BEST way to protect the data from leaking?

A. Utilize privacy screens.
B. Implement disk quotas.
C. Install a DLP solution.
D. Enforce the lock-screen feature.

Answer: C

Explanation:
Components of a Data Loss Solution Reference:https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/
The best way to protect the data from leaking is to install a DLP solution. A DLP (Data Loss Prevention) solution is a software that helps businesses prevent confidential data from being leaked or stolen by unauthorized parties. A DLP solution can identify, monitor, and protect data as it moves across networks and devices, such as endpoints, email, web, cloud applications, or removable media. A DLP solution can also enforce security policies based on content and context for data in use, in motion, and at rest. A DLP solution can detect and prevent data breaches by using various techniques, such as content inspection, contextual analysis, encryption, blocking, alerting, warning, quarantining, or other remediation actions.

NEW QUESTION 54
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, itwill 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 59

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 64
Which of the following license types most commonly describes a product that incurs a yearly cost regardless of how much it is used?

A. Physical
B. Subscription
C. Open-source
D. Per instance
E. Per concurrent user

Answer: B

Explanation:
A subscription license is a type of license that grants the user the right to use a product or service for a fixed period of time, usually a year. The user pays a recurring fee, regardless of how much they use the product or service. Subscription licenses are common for cloud- based software and services, such as Microsoft 3651 or DocuSign2.
References = 1: Compare All Microsoft 365 Plans (Formerly Office 365) - Microsoft Store(https://www.microsoft.com/en-us/microsoft-365/buy/compare-all-microsoft-365- products) 2: DocuSign Pricing | eSignature Plans for Personal & Business(https://ecom.docusign.com/plans-and-pricing/esignature)

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. Marware
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 requirecollaboration 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 73
A datacenter technician is attempting to troubleshoot a server that keeps crashing. The server runs normally for approximately five minutes, but then it crashes. After restoring the server to operation, the same cycle repeats. The technician confirms none of the configurations have changed, and the load on the server is steady from power-on until the crash. Which of the following will MOST likely resolve the issue?

A. Reseating any expansion cards in the server
B. Replacing the failing hard drive
C. Reinstalling the heat sink with new thermal paste
D. Restoring the server from the latest full backup

Answer: C

Explanation:
The most likely solution to resolve the issue of the server crashing after running normally for approximately five minutes is to reinstall the heat sink with new thermal paste. A heat sink is a device that dissipates heat from a component, such as a processor or a graphics card, by transferring it to a cooling medium, such as air or liquid. A heat sink is usually attached to the component using thermal paste, which is a substance that fills the gaps between the heat sink and the component and improves thermal conductivity. Thermal paste can degrade over time and lose its effectiveness, resulting in overheating and performance issues. If a server crashes after running for a short period of time, it may indicate that the processor is overheating due to insufficient cooling. To resolve this issue, the technician should remove the heat sink, clean the old thermal paste, apply new thermal paste, and reinstall the heat sink.

NEW QUESTION 74
An administrator gave Ann modify permissions to a shared folder called DATA, which is located on the company server. Other users need read access to the files in this folder. The current configuration is as follows:

Folder name	Share permissions	File permissions
DATA	Authenticated users: read Ann: read	Ann: modify

The administrator has determined Ann cannot write anything to the DATA folder using the network. Which of the following would be the best practice to set up Ann's permissions correctly, exposing only the minimum rights required?

A.

Folder name	Share permissions	File permissions
DATA	Authenticated users: read	Ann: full control

B.

Folder name	Share permissions	File permissions
DATA	Ann: full control	Ann: full control

C.

Folder name	Share permissions	File permissions
DATA	Authenticated users: full control	Ann: modify

D.

Folder name	Share permissions	File permissions
DATA	Authenticated users: read Ann: read	Ann: full control

A. Option A
B. Option B
C. Option C
D. Option D

Answer: D

Explanation:
Option D is the best practice to set up Ann's permissions correctly, exposing only the minimum rights required. Option D shows that the share permissions on the DATA folder grant Ann Change access, which allows her to read, write, and delete files in the shared folder. The file permissions grant Ann Modify access, which allows her to read, write, execute, and delete files in the folder. This combination of permissions givesAnn the ability to write anything to the DATA folder using the network, as well as to modify and delete existing files. This meets the requirement of giving Ann modify permissions to the shared folder.

NEW QUESTION 76
A technician has been asked to check on a SAN. Upon arrival, the technician notices the red LED indicator shows a disk has failed. Which of the following should the technician do NEXT, given the disk is hot swappable?

A. Stop sharing the volume
B. Replace the disk
C. Shut down the SAN
D. Stop all connections to the volume

Answer: B

Explanation:
The next thing that the technician should do, given the disk is hot swappable, is to replace the disk. A hot swappable disk is a disk that can be removed and replaced without shutting down the system or affecting its operation. A hot swappable disk is typically used in a storage array that has RAID (Redundant Array of Independent Disks) configuration that provides fault tolerance and redundancy. If a disk fails in a RAID array, it can be replaced by a new disk without interrupting the service or losing any data. The new disk will automatically rebuild itself using the data from the other disks in the array.

NEW QUESTION 78
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 83
A server administrator wants to ensure a storage array can survive the failure of two drives without the loss of data. Which of the following RAID levels should the administrator choose?

A. 1
B. 5
C. 6

Answer: D

Explanation:
RAID 6 is a level of RAID that can survive the failure of two drives without the loss of data. RAID 6 uses block-level striping with two parity blocks distributed across all member disks. RAID 6 can tolerate two simultaneous drive failures and still provide data access and redundancy. RAID 0 is a level of RAID that uses striping without parity or mirroring, and offers no fault tolerance. RAID 0 cannot survive any drive failure without data loss. RAID 1 is a level of RAIDthat uses mirroring without parity or striping, and offers fault tolerance by duplicating data on two or more disks. RAID 1 can survive one drive failure without data loss, but not two. RAID 5 is a level of RAID that uses block-level striping with one parity block distributed across all member disks. RAID 5 can tolerate one drive failure without data loss, but not two. References:
? https://en.wikipedia.org/wiki/Standard_RAID_levels

NEW QUESTION 86
A technician installed a kernel upgrade to a Linux server. The server now crashes regularly. Which of the following is the most likely cause?

A. Necessary dependencies were installed for multiple architectures.
B. There is not enough hard drive space.
C. The server is infected with a virus.
D. Some modules are not compatible.

Answer: D

Explanation:
A kernel upgrade is a process of updating the core component of a Linux operating system that manages the hardware, memory, processes, and drivers. A kernel upgrade can improve the performance, security, and compatibility of the system, but it can also introduce errors if some modules are not compatible with the new kernel version. Modules are pieces of code that can be loaded and unloaded into the kernel to provide additional functionality or support for specific devices. If a module is not compatible with the kernel, it can cause crashes or instability.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 4, Lesson 4.2, Objective 4.2

NEW QUESTION 87
An application needs 10GB of RAID 1 for log files, 20GB of RAID 5 for data files, and 20GB of RAID 5 for the operating system. All disks will be 10GB in capacity. Which of the following is the MINIMUM number of disks needed for this application?

A. 6
B. 7
C. 8
D. 9

Answer: C

Explanation:
To calculate the minimum number of disks needed for this application, we need to consider the RAID levels and their disk requirements. RAID 1 requires a minimum of two disks and provides mirroring, which means that data is duplicated on both disks. RAID 5 requires a minimum of three disks and provides striping with parity, which means that data is distributed across all disks with one disk storing parity information for error correction. RAID 5 can tolerate one disk failure without losing data. To create a 10GB RAID 1 array for log files, we need two 10GB disks. To create a 20GB RAID 5 array for data files, we need four 10GB disks (three for data and one for parity). To create a 20GB RAID 5 array for the operating system, we need another four 10GB disks (three for data and one for parity). Therefore, the total number of disks needed is 2 + 4 + 4 = 10. However, since we can use different RAID levels for different partitions on the same disk, we can optimize the disk usage by using only eight disks as follows: Disk 1: 10GB RAID 1 (log files) + 10GB RAID 5 (data files) Disk 2: 10GB RAID 1 (log files) + 10GB RAID 5 (data files) Disk 3: 10GB RAID 5 (data files) + 10GB RAID 5 (OS) Disk 4: 10GB RAID 5 (data files) + 10GB RAID 5 (OS) Disk 5: 10GB RAID 5 (parity for data files) + 10GB RAID 5 (OS) Disk 6: 10GB RAID 5 (OS) + unused space Disk 7: 10GB RAID 5 (parity for OS) + unused space Disk 8: unused space
References:https://en.wikipedia.org/wiki/Standard_RAID_levels

NEW QUESTION 92
An analyst is planning a new point-to-point Ethernet connection between a university campus and a newly acquired space downtown that is about 5mi (8km) away. The analyst would like the fastest possible connection speed. Which of the following would best meet the analyst's needs?

A. 1000BASE-LX 1Gb single-mode plenum fiber connection
B. 10GBASE-T 10Gb copper plenum Ethernet connection
C. 1000BASE-T 1Gb copper non-plenum Ethernet connection
D. 10GBASE-SR 10Gb multimode plenum fiber connection

Answer: A

Explanation:
A 1000BASE-LX 1Gb single-mode plenum fiber connection would best meet the analyst’s needs for a new point-to-point Ethernet connection between a university campus and a newly acquired space downtown that is about 5mi (8km) away. A 1000BASE-LX is a type of Ethernet standard that supports data transmission at 1 gigabit per second over single- mode fiber cables using long wavelength lasers. A single-mode fiber cable is a type of optical fiber cable that has a small core diameter and allows only one mode of light to propagate through it. A single-mode fiber cable can transmit data over long distances at high speeds, but it requires more expensive transceivers and connectors than multimode fiber cables. A plenum fiber cable is a type of optical fiber cable that has a special coating that prevents the spread of fire or toxic fumes in case of burning. A plenum fiber cable is suitable for installation in plenum spaces, which are areas used for air circulation in buildings, such as above ceilings or below floors. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Networking, Objective 4.2: Given a scenario involving server networking issues (e.g., network interface card failure), troubleshoot using appropriate tools.

NEW QUESTION 93
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.
C. 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 97
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 99
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 theolder MBR (Master Boot Record) standard1.However, GPT is not compatible with some older operating systems, such as Windows XP or Windows Server 20032. 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 software3.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 TB4.MBR is not a file system, but a partitioning scheme that can support various file systems such as NTFS, FAT32, or exFAT5.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 four1.

NEW QUESTION 101
A company needs to increase the security controls on its servers. Anadministrator is implementing MFA on all servers using cost effective techniques. Which of the following should the administrator use to satisfy the MFA requirement?

A. Biometrics
B. Push notifications
C. Smart carts
D. Physical tokens

Answer: B

Explanation:
Push notifications are messages that are sent from an application or a service to a user's device without requiring the user to open or request them. They can be used as a cost- effective technique for implementing MFA (Multi-Factor Authentication) on servers by sending verification codes or approval requests to the user's smartphone or tablet when they try to log in to the server. Verified References: [Push notifications], [MFA]

NEW QUESTION 102
An administrator notices nigh traffic on a certain subnetand wouldlike 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:
A sniffer is a tool that captures and analyzes network traffic on a subnet or a network interface. It can help identify the source, destination, protocol, and content of the traffic and detect any anomalies or issues on the network. Verified References: [Sniffer], [Network traffic]

NEW QUESTION 106
Which of the following symbols is used to write a text description per line within a PowerShell script?

A. %
B. @
C. &
D. #

Answer: D

Explanation:
The # symbol is used to write a text description per line within a PowerShell script. A text description is also known as a comment, which is a line of code that is ignored by the PowerShell interpreter and serves as documentation or explanation for human readers. The # symbol indicates that everything following it on the same line is a comment and not part of the script commands or expressions. For example:
This is a comment in PowerShellWrite-Host “Hello World” # This command prints Hello World to the console
References: CompTIA Server+ Certification Exam Objectives, Domain 6.0: Troubleshooting, Objective 6.3: Given a scenario, troubleshoot scripting errors using PowerShell commands.

NEW QUESTION 110
An administrator is alerted to a hardware failure in a mission-critical server. The alert states that two drives have failed. The administrator notes the drives are in different RAID 1 arrays, and both are hot-swappable. Which of the following steps will be the MOST efficient?

A. Replace one drive, wait for a rebuild, and replace the next drive.
B. Shut down the server and replace the drives.
C. Replace both failed drives at the same time.
D. Replace all the drives in both degraded arrays.

Answer: C

Explanation:
Since both drives are in different RAID 1 arrays and both are hot-swappable, the most efficient step is to replace both failed drives at the same time. This can minimize the downtime and avoid unnecessary reboots. RAID 1 provides mirroring, which means that data is duplicated on both drives in the array. Therefore, replacing one drive will not affect the data on the other drive or the functionality of the array.References:https://en.wikipedia.org/wiki/Standard_RAID_levels#RAID_1

NEW QUESTION 111
A server administrator wants to run a performance monitor for optimal system utilization. Which of the following metrics can the administrator use for monitoring? (Choose two.)

A. Memory
B. Page file
C. Services
D. Application
E. CPU
F. Heartbeat

Answer: AE

Explanation:
Memory and CPU are two metrics that can be used for monitoring system utilization. Memory refers to the amount of RAM that is available and used by the system and its processes. CPU refers to the percentage of processor time that is consumed by the system and its processes. Both memory and CPU can affect the performance and responsiveness of the system and its applications. Monitoring memory and CPU can help identify bottlenecks, resource contention, memory leaks, high load, etc.

NEW QUESTION 113
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 ofnumerical addresses1.
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 117
Which of the following backup types copies changed data from a server and then combines the backups on the backup target?

A. Differential
B. Incremental
C. Synthetic full
D. Snapshot

Answer: C

Explanation:
A synthetic full backup is a type of backup that copies changed data from a server and then combines the backups on the backup target. This way, the backup target always has a full backup of the server, without requiring a full backup to be performed over the network. A synthetic full backup reduces the network bandwidth and time required for backups, while also simplifying the restoration process1

NEW QUESTION 122
A site is considered a warm site when it:
? has basic technical facilities connected to it.
? has faulty air conditioning that is awaiting service.
? is almost ready to take over all operations from the primary site.

A. is fully operational and continuously providing services.

Answer: A

Explanation:
A warm site is a backup site that has some of the necessary hardware, software, and network resources to resume operations, but not all of them. A warm site requires some time and effort to become fully operational. A warm site is different from a cold site, which has minimal or no resources, and a hot site, which has all the resources and is ready to take over immediately.
References: CompTIA Server+ Study Guide, Chapter 10: Disaster Recovery, page 403.

NEW QUESTION 125
Which of the following cloud models is BEST described as running workloads on resources that are owned by the company and hosted in a company-owned data center, as well as on rented servers in another company's data center?

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

Answer: B

Explanation:
This is the best description of a hybrid cloud model because it combines both private and public cloud resources. A private cloud is a cloud environment that is owned and operated by a single organization and hosted in its own data center. A public cloud is a cloud environment that is owned and operated by a third-party provider and hosted in its data center. A hybrid cloud allows an organization to leverage both types of cloud resources depending on its needs and preferences.References:https://azure.microsoft.com/en-us/overview/what-is-hybrid-cloud- computing/

NEW QUESTION 129
Which of the following backup types should be chosen for database servers?

A. Differential
B. Incremental
C. Synthetic full
D. Open file

Answer: C

Explanation:
A synthetic full backup is a type of backup that combines a full backup with one or more incremental backups to create a new full backup without accessing the source data. This type of backup is suitable for database servers, as it reduces the backup window, minimizes the impact on the server performance, and provides faster recovery time. Verified References: [Synthetic Full Backup]

NEW QUESTION 133
A company wants to deploy software to all users, Out very few of men will be using the software at any one point in time. Which of the following licensing models would be BEST lot the company?

A. Per site
B. Per concurrent user
C. Per core
D. Per instance

Answer: B

Explanation:
Per concurrent user licensing is a model that allows a fixed number of users to access the software at any one point in time. This model is best for the company that wants to deploy software to all users, but very few of them will be using the software at any one point in time. This way, the company can save money by paying only for the number of simultaneous users, rather than for every user who has access to the software. Per site licensing is a model that allows unlimited users within a specific location to use the software. Per core licensing is a model that charges based on the number of processor cores on the server where the software is installed. Per instance licensing is a model that charges based on the number of copies of the software running on different servers or virtual machines.References: https://www.pcmag.com/encyclopedia/term/concurrent-use-licensehttps://www.techopedia.com/definition/1440/software-licensing

NEW QUESTION 136
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 138
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) x Smin, where n is the number of disks and Smin is the smallest disk size. In this case, the RAID 6 capacity is (5-2) x 4TB = 12TB. References:
? CompTIA Server+ Certification Exam Objectives1, page 8
? RAID Levels and Types Explained: Advantages and Disadvantages2
? RAID Levels & Fault Tolerance3

NEW QUESTION 142
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 146
A technician is deploying a single server to monitor and record me security cameras at a remote site, which of the following architecture types should be used to minimize cost?

A. Virtual
B. Blade
C. Tower
D. Rack mount

Answer: C

Explanation:
A tower server is a type of server architecture that is best suited to minimize cost when deploying a single server to monitor and record the security cameras at a remote site. A tower server is a standalone server that has a similar form factor and design as a desktop computer. It does not require any special mounting equipment or rack space and can be placed on or under a desk or table. A tower server is suitable for small businesses or remote offices that need only one or few servers for basic tasks such as file sharing, print serving, or security monitoring. A tower server is usually cheaper and easier to maintain than other types of servers, but it may have lower performance, scalability, and redundancy features. A virtual server is a type of server architecture that involves creating and running one or more virtual machines on a physical host using a hypervisor such as Hyper-V or VMware. A virtual server can reduce hardware costs and improve flexibility and efficiency, but it requires additional software licenses and management tools. A blade server is a type of server architecture that involves inserting multiple thin servers called blades into a chassis that provides power, cooling, network, and management features. A blade server can improve performance, density, and scalability, but it requires more initial investment and specialized equipment. A rack mount server is a type of server architecture that involves mounting one or more servers into standardized frames called racks that provide power, cooling, network, and security features

NEW QUESTION 151
Which of the following encryption methodologies would MOST likely be used to ensure encrypted data cannot be retrieved if a device is stolen?

A. End-to-end encryption
B. Encryption in transit
C. Encryption at rest
D. Public key encryption

Answer: C

Explanation:
Encryption at rest is a type of encryption methodology that would most likely be used to ensure encrypted data cannot be retrieved if a device is stolen. Encryption at rest is a process of encrypting stored data on a device such as a hard drive, SSD, USB flash drive, or mobile device. This way, if the device is lost or stolen, the data cannot be accessed without the encryption key or password. Encryption at rest can be implemented using software tools such as BitLocker on Windows or FileVault on Mac OS, or hardware features such as self-encrypting drives or Trusted Platform Module chips. End-to-end encryption is a type of encryption methodology that ensures encrypted data cannot be intercepted or modified by third parties during transmission over a network. Encryption in transit is a type of encryption methodology that protects encrypted data while it is moving from one location to another over a network. Public key encryption is a type of encryption algorithm that uses a pair of keys: a public key that can be shared with anyone and a private key that is kept secret by the owner. References: https://www.howtogeek.com/196541/bitlocker-101-what-it-is-how-it-works-and-how-to-use- it/ https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual-files/ https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-it-matter/https://www.howtogeek.com/195877/what-is-encryption- and-how-does-it-work/

NEW QUESTION 152
Which of the following security risks provides unauthorized access to an application?

A. Backdoor
B. Data corruption
C. Insider threat
D. Social engineering

Answer: A

Explanation:
A backdoor is a security risk that provides unauthorized access to an application. A backdoor is a hidden or undocumented way of bypassing the normal authentication or encryption mechanisms of an application, allowing an attacker to gain remote access, execute commands, or steal data. A backdoor can be created intentionally by the developer, maliciously by an attacker, or unintentionally by a programming
error. References: CompTIA Server+ Certification Exam Objectives, Domain 5.0: Security, Objective 5.2: Given a scenario, apply logical access control methods.

NEW QUESTION 154
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 158
Which of the following often-overlooked parts of the asset life cycle can cause the greatest number of issues in relation to Pll exposure?

A. Usage
B. End-of-life
C. Procurement
D. Disposal

Answer: D

Explanation:
Disposal is the part of the asset life cycle that can cause the greatest number of issues in relation to PII exposure. PII stands for personally identifiable information, which is any data that can be used to identify a specific individual, such as name, address, phone number, email, social security number, etc. PII exposure is the unauthorized access or disclosure of PII, which can result in identity theft, fraud, or other harms to the individuals whose data is compromised. Disposal is the process of getting rid of an asset that is no longer needed or useful, such as a server, a hard drive, or a mobile device. If the disposal is not done properly, the PII stored on the asset may still be accessible or recoverable by unauthorized parties, such as hackers, thieves, or competitors. Therefore, it is important to follow best practices for secure disposal of assets that contain PII, such as wiping, encrypting, shredding, or physically destroying the data storage media

NEW QUESTION 161
A server administrator has received tickets from users who report the system runs very slowly and various unrelated messages pop up when they try to access an internet-facing web application using default ports. The administrator performs a scan to check for open ports and reviews the following report:
Starting Nmap 7.70 https://nmap.org) at 2019-09-19 14:30 UTC Nmap scan report for www.abc.com (172.45.6.85)
Host is up (0.0021s latency)
Other addresses for www.abc.com (not scanned) : 4503 : F7b0 : 4293: 703: : 3209 RDNS record for 172.45.6.85: 1ga45s12-in-f1.2d100.net
Port State Service 21/tcp filtered ftp 22/tcp filtered ssh 23/tcp filtered telnet
69/tcp open @username.com 80/tcp open http
110/tcp filtered pop 143/tcp filtered imap 443/tcp open https
1010/tcp open www.popup.com 3389/tcp filtered ms-abc-server
Which of the following actions should the server administrator perform on the server?

A. Close ports 69 and 1010 and rerun the scan.
B. Close ports 80 and 443 and rerun the scan.
C. Close port 3389 and rerun the scan.
D. Close all ports and rerun the scan.

Answer: A

Explanation:
Port 69 is used for TFTP (Trivial File Transfer Protocol), which is an insecure and unencrypted protocol for file transfer. Port 1010 is used for a malicious website that generates pop-up ads. Both of these ports are likely to be exploited by hackers or malware to compromise the server or the web application. The server administrator should close these ports and rerun the scan to verify that they are no longer open12.
References = 1: Why Are Some Network Ports Risky, And How Do You Secure Them? - How-To Geek(https://www.howtogeek.com/devops/why-are-some-ports-risky-and-how-do- you-secure-them/) 2: Switchport Port Security Explained With Examples - ComputerNetworkingNotes(https://www.computernetworkingnotes.com/ccna-study-guide/switchport-port-security-explained-with-examples.html)

NEW QUESTION 162
Due to a recent application migration, a company's current storage solution does not meet the necessary requirements tor 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 scalability12. 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 extraoverhead 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 167
A company deploys antivirus, anti-malware, and firewalls that can be assumed to be functioning properly. Which of the following is the MOST likely system vulnerability?

A. Insider threat
B. Worms
C. Ransomware
D. Open ports
E. Two-person integrity

Answer: A

Explanation:
Insider threat is the most likely system vulnerability in a company that deploys antivirus, anti-malware, and firewalls that can be assumed to be functioning properly. An insider threat is a malicious or negligent act by an authorized user of a system or network that compromises the security or integrity of the system or

network. An insider threat can include data theft, sabotage, espionage, fraud, or other types of attacks. Antivirus, anti-malware, and firewalls are security tools that can protect a system or network from external threats, such as viruses, worms, ransomware, or open ports. However, these tools cannot prevent an insider threat from exploiting their access privileges or credentials to harm the system or network.

NEW QUESTION 170
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 174
After installing a new file server, a technician notices the read times for accessing the same file are slower than the read times for other file servers.
Which of the following is the first step the technician should take?

A. Add more memory.
B. Check if the cache is turned on.
C. Install faster hard drives.
D. Enable link aggregation.

Answer: B

Explanation:
The cache is a temporary storage area that holds frequently accessed data or instructions for faster retrieval. The cache can improve the read times for accessing files by reducing the need to access the hard drive, which is slower than the cache memory1. Therefore, the first step the technician should take is to check if the cache is turned on for the new file server. If the cache is turned off, the technician should enable it and see if the read times improve. The other options are incorrect because they are not the first steps to take. Adding more memory, installing faster hard drives, or enabling link aggregation are possible ways to improve the performance of the file server, but they are more costly and time-consuming than checking the cache. Moreover, they may not address the root cause of the problem if the cache is turned off.

NEW QUESTION 179
A server administrator has received calls regarding latency and performance issues with a file server. After reviewing all logs and server features the administrator discovers the server came with four Ethernet ports, out only one port is currently in use. Which of the following features will enable the use of all available ports using a single IP address?

A. Network address translation
B. in-band management
C. Round robin
D. NIC teaming

Answer: D

Explanation:
NIC teaming is a feature that allows the use of multiple network interface cards (NICs) as a single logical interface with a single IP address. It can improve the network performance, bandwidth, and redundancy of a server. Verified References: [NIC teaming], [Network interface card]

NEW QUESTION 180
The HIDS logs on a server indicate a significant number of unauthorized access attempts via USB devices at startup. Which of the following steps should a server administrator take to BEST secure the server without limiting functionality?

A. Set a BIOS/UEFI password on the server.
B. Change the boot order on the server and restrict console acces
C. Configure the host OS to deny login attempts via USB.
D. Disable all the USB ports on the server.

Answer: B

Explanation:
Changing the boot order on the server and restricting console access would prevent unauthorized access attempts via USB devices at startup, as the server would not boot from any external media and only authorized users could access the console. Setting a BIOS/UEFI password on the server would also help, but it could be bypassed by resetting the CMOS battery or using a backdoor password. Configuring the host OS to deny login attempts via USB would not prevent booting from a malicious USB device that could compromise the system before the OS loads. Disabling all the USB ports on the server would limit functionality, as some peripherals or devices may need to use them. References:
? https://www.pcmag.com/how-to/dont-plug-it-in-how-to-prevent-a-usb-attack
? https://www.techopedia.com/definition/10362/boot-order
? https://www.techopedia.com/definition/10361/console-access
? https://www.techopedia.com/definition/102/bios-password
? https://www.techopedia.com/definition/10363/cmos-battery

NEW QUESTION 183
A systems administrator has noticed performance degradation on a company file server, and one of the disks on it has a solid amber light. The administrator logs

on to the disk utility and sees the array is rebuild ing. Which of the following should the administrator do NEXT once the rebuild is finished?

A. Restore the server from a snapshot.
B. Restore the server from backup.
C. Swap the drive and initialize the disk.
D. Swap the drive and initialize the array.

Answer: C

Explanation:
The next action that the administrator should take once the rebuild is finished is to swap the drive and initialize the disk. This is to replace the faulty disk that has a solid amber light, which indicates a predictive failure or a SMART error. Initializing the disk will prepare it for use by the RAID controller and add it to the array. The administrator should also monitor the array status and performance after swapping the drive.Reference:https://www.salvagedata.com/how-to-rebuild-a-failed-raid/

NEW QUESTION 184
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 189
An administrator needs to disable root login over SSH. Which of the following tiles should be edited to complete this task?

A. /root.ssh/sshd/config
B. /etc.ssh/sshd_config
C. /root/.ssh/ssh_config
D. /etc.sshs_shd_config

Answer: B

Explanation:
To disable root login over SSH, the server administrator needs to edit the SSH configuration file located at /etc/ssh/sshd_config. This file contains various settings for the SSH daemon that runs on the server and accepts incoming SSH connections. The administrator needs to find the line that says PermitRootLogin and change it to no or comment it out with a # symbol. Then, the administrator needs to restart the SSH service for the changes to take effect.
References:https://www.howtogeek.com/828538/how-and- why-to-disable-root-login-over-ssh-on-linux/

NEW QUESTION 194
Which of the following is typical of software licensing in the cloud?

A. Per socket
B. Perpetual
C. Subscription-based
D. Site-based

Answer: C

Explanation:
Cloud software licensing refers to the process of managing and storing software licenses in the cloud. The benefits of cloud software licensing models are vast. The main and most attractive benefit has to do with the ease of use for software vendors and the ability to provide customizable cloud software license management based on customer needs and desires1. Cloud-based licensing gives software developers and vendors the opportunity to deliver software easily and quickly and gives customers full control over their licenses, their analytics, and more1. Cloud based licensing gives software sellers the ability to add subscription models to their roster of services1. Subscription models are one of the most popular forms of licensing today1. Users sign up for a subscription (often based on various options and levels of use, features, etc.) and receive theirlicenses instantly1. References: 1 Everything You Need to Know about Cloud Licensing | Thales

NEW QUESTION 197
A company is reviewing options for its current disaster recovery plan and potential changes to it. The security team will not allow customer data to egress to non-company equipment, and the company has requested recovery in the shortest possible time. Which of the following will BEST meet these goals?

A. A warm site
B. A hot site
C. Cloud recovery
D. A cold site

Answer: B

Explanation:

A hot site is a type of disaster recovery site that has all the equipment and data ready to resume operations as soon as possible after a disaster. A hot site is usually located in a different geographic area than the primary site and has redundant power, cooling, network, and security systems. A hot site is best for the company that wants to recover in the shortest possible time and does not want customer data to egress to non- company equipment. A warm site is a type of disaster recovery site that has some equipment and data ready, but requires some configuration and restoration before resuming operations. A cold site is a type of disaster recovery site that has only basic infrastructure and space available, but requires significant setup and installation before resuming operations. Cloud recovery is a type of disaster recovery service that uses cloud- based resources and platforms to store backups and restore data and applications after a disaster. References: https://www.techopedia.com/definition/11172/hot-site https://www.techopedia.com/definition/11173/warm-site https://www.techopedia.com/definition/11174/cold- sitehttps://www.techopedia.com/definition/29836/cloud-recovery

NEW QUESTION 200
A user has been unable to authenticate to the company's external, web-based database after clicking a link in an email that required the user to change the account password. Which of the following steps should the company take next?

A. Disable the user's account and inform the security team.
B. Create a new log-in to the external database.
C. Ask the user to use the link again to reset the password.
D. Reset the user's password and ask the user to log in again.

Answer: A

Explanation:
The user has likely fallen victim to a phishing scam, which is a fraudulent attempt to obtain sensitive information, such as passwords, by disguising as a legitimate entity. The link in the email that required the user to change the account password was probably a fake website that mimicked the company’s external database, and captured the user’s credentials when they entered them. This could compromise the security and integrity of the company’s data, as well as the user’s identity and privacy12.
The company should take immediate action to prevent further damage and investigate the incident. The first step is to disable the user’s account and inform the security team. Disabling the user’s account can prevent unauthorized access to the external database by the attackers, who may use the stolen credentials to log in and manipulate or steal data. Informing the security team can alert them of the breach and allow them to take appropriate measures, such as scanning for malware, changingpasswords, notifying other users, and reporting the incident34.

NEW QUESTION 203
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 205
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 209
A technician is decommissioning a server from a production environment. The technician removes the server from the rack but then decides to repurpose the system as a lab server instead of decommissioning it. Which of the following is the most appropriate NEXT step to recycle and reuse the system drives?

A. Reinstall the OS.
B. Wipe the drives.
C. Degauss the drives.
D. Update the IP schema.

Answer: B

Explanation:
Wiping the drives is the most appropriate step to recycle and reuse the system drives. Wiping the drives means erasing all the data on the drives and overwriting them with random or meaningless data. This can help prevent data leakage, comply with regulations, and prepare the drives for a new installation or configuration.

Wiping the drives is different from deleting or formatting the drives, which only remove the references to the data but not the data itself.References: https://www.comptia.org/training/resources/exam- objectives/comptia-server-sk0-005-exam-objectives (Objective 1.3)

NEW QUESTION 214
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 218
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 220
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 222
A server technician installs a new NIC on a server and configures the NIC for IP connectivity. The technician then tests the connection using thepingcommand. Given the following partial output of thepingandipconfigcommands:

```
ipconfig /all

IPv4 address: 192.168.1.5
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.1

pinging 192.168.1.1 with 32 bytes of data:

Request timed out
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Request timed out
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
```

Which of the following caused the issue?

A. Duplicate IP address
B. Incorrect default gateway
C. DHCP misconfiguration
D. Incorrect routing table

Answer: A

Explanation:
? The ping command output shows that the NIC has an IP address of 192.168.1.100 and a default gateway of 192.168.1.1. However, when the technician tries to ping the default gateway, the reply comes from another IP address: 192.168.1.101. This means that there is another device on the network that has the same IP address as the default gateway, and it is responding to the ping request instead of the intended destination.
? A duplicate IP address can cause network connectivity problems, such as packet loss, routing errors, or unreachable hosts. To resolve this issue, the technician should either change the IP address of the default gateway or the device that is conflicting with it, or use DHCP to assign IP addresses automatically and avoid conflicts.
? The other options are not correct because they do not explain the ping output. An incorrect default gateway would cause no reply or a destination unreachable message, not a reply from a different IP address. A DHCP misconfiguration would cause an invalid or no IP address on the NIC, not a duplicate IP address on the network. An incorrect routing table would cause routing errors or unreachable destinations, not a reply from a different IP address.
References:
? https://askleo.com/what_is_ping_and_what_does_its_output_tell_me/
? https://learn.microsoft.com/en-us/windows-server/administration/windows- commands/ping

NEW QUESTION 224
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 229
A change in policy requires a complete backup of the accounting server every seven days and a backup of modified data every day. Which of the following would be BEST to restore a full backup as quickly as possible in the event of a complete loss of server data?

A. A full, weekly backup with daily open-file backups
B. A full,weekly backup with daily archive backups
C. A full, weekly backup with daily incremental backups
D. A full, weekly backup with daily differential backups

Answer: D

Explanation:
A differential backup is a type of backup that copies all the files that have changed since the last full backup. A differential backup requires more storage space than an incremental backup, which only copies the files that have changed since the last backup of any type, but it also requires less time to restore in case of data loss. By combining a full, weekly backup with daily differential backups, the administrator can ensure that only two backup sets are needed to restore a full backup as quickly as possible. Verified References: [Incremental vs Differential Backup]

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 233
Which of me following should be placed at the top of a Bash script to ensure it can be executed?

A. bash
B. !execute
C. #!
D. @eacho 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 234
A server administrator is configuring the IP address on a newly provisioned server in the testing environment. The network VLANs are configured as follows:

VLAN name	VLAN ID	Gateway IP address	Active switchports
Testing	10	192.168.10.1/24	2, 4, 6, 8, 10, 12, 14, 18
Production	20	192.168.20.1/24	3, 5, 7, 9, 11, 13, 15, 17
Administration	30	192.168.30.1/24	1, 24

The administrator configures the IP address for the new server as follows: IP address: 192.168.1.1/24
Default gateway: 192.168.10.1
A ping sent to the default gateway is not successful. Which of the following IP address/default gateway combinations should the administrator have used for the new server?

A. IP address: 192.168.10.2/24Default gateway: 192.168.10.1
B. IP address: 192.168.1.2/24 Default gateway: 192.168.10.1
C. IP address: 192.168.10.3/24Default gateway: 192.168.20.1
D. IP address: 192.168.10.24/24Default gateway: 192.168.30.1

Answer: A

Explanation:
The IP address/default gateway combination that the administrator should have used for the new server is IP address: 192.168.10.2/24 and Default gateway: 192.168.10.1. The IP address and the default gateway of a device must be in the same subnet to communicate with each other. A subnet is a logical division of a network that allows devices to share a common prefix of their IP addresses. The subnet mask determines how many bits of the IP address are used for the network prefix and how many bits are used for the host identifier. A /24 subnet mask means that the first 24 bits of the IP address are used for the network prefix and the last 8 bits are used for the host identifier. Therefore, any IP address that has the same first 24 bits as the default gateway belongs to the same subnet. In this case, the default gateway has an IP address of 192.168.10.1/24, which means that any IP address that starts with 192.168.10.x/24 belongs to the same subnet. The new server has an IP address of 192.168.1.1/24, which does not match the first 24 bits of the default gateway, so it belongs to a different subnet and cannot communicate with the default gateway. To fix this issue, the administrator should change the IP address of the new server to an unused IP address that starts with 192.168.10.x/24, such as 192.168.10.2/24.

NEW QUESTION 238
Which of the following server types would benefit MOST from the use of a load balancer?

A. DNS server
B. File server
C. DHCP server
D. Web server

Answer: D

Explanation:
The server type that would benefit most from the use of a load balancer is web server. A web server is a server that hosts web applications or websites and responds to requests from web browsers or clients. A load balancer is a device or software that distributes network traffic across multiple servers based on various criteria, such as availability, capacity, or performance. A load balancer can improve the scalability, reliability, and performance of web servers by balancing the workload and preventing any single server from being overloaded or unavailable.
Reference:
https://www.dnsstuff.com/what-is-server-load-balancing

NEW QUESTION 243
A technician is creating a network snare that will be used across both Unix and Windows clients at the same time. Users need read and write access to the files. Which of the following would be BEST for the technician to deploy?

A. iSCSI
B. CIFS
C. HTTPS
D. DAS

Answer: B

Explanation:
CIFS (Common Internet File System) is a protocol that allows file sharing across different operating systems, such as Unix and Windows. It supports read and write access to files and folders on a network share. It is also known as SMB (Server Message Block). Verified References: [CIFS], [File sharing]

NEW QUESTION 248
An administrator is configuring the storage for a new database server, which will host databases that are mainly used for archival lookups. Which of the following storage types
will yield the fastest database read performance?

A. NAS
B. SSD
C. 10K rpm SATA
D. 15K rpm SCSI

Answer: B

Explanation:
The storage type that will yield the fastest database read performance is SSD. SSD (Solid State Drive) is a type of storage device that uses flash memory to store data. SSDs have no moving parts and can access data faster than traditional hard disk drives (HDDs) that use spinning platters and magnetic heads. SSDs are especially suitable for databases that are mainly used for archival lookups, as they can provide faster response times and lower latency for read operations. References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 1, Lesson 1.2, Objective 1.2

NEW QUESTION 250
Which of the following techniques can be configured on a server for network redundancy?

A. Clustering
B. Vitalizing
C. Cloning
D. Teaming

Answer: D

Explanation:
Teaming is a technique that can be configured on a server for network redundancy. Teaming involves combining two or more network adapters into a single logical unit that acts as one network interface. This way, if one network adapter fails, another one can take over without disrupting network connectivity. Teaming can also improve network performance by load balancing traffic across multiple network adapters. Clustering is a technique that involves grouping two or more servers together to act as one system for high availability and fault tolerance. Virtualizing is a technique that involves creating multiple virtual machines on a single physical server to optimize resource utilization and flexibility. Cloning is a technique that involves creating an exact copy of a server's configuration and data for backup or migration purposes. References: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming/nic- teaming https://www.techopedia.com/definition/19588/clustering https://www.techopedia.com/definition/4790/virtualizationhttps://www.techopedia.com/definition/4776/cloning

NEW QUESTION 251
A technician is configuring a server that requires secure remote access. Which of the following ports should the technician use?

A. 21
B. 22
C. 23
D. 443

Answer: B

Explanation:
The technician should use port 22 to configure a server that requires secure remote access. Port 22 is the default port for Secure Shell (SSH), which is a protocol that
allows secure remote login and command execution over a network connection using a command-line interface (CLI). SSH encrypts both the authentication and data transmission between the client and the server, preventing eavesdropping, tampering, or spoofing. SSH can be used to perform various tasks on a server remotely, such as configuration, administration, maintenance, troubleshooting, etc.

NEW QUESTION 255
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 sucessful. 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 260
Which of the following allows for a connection of devices to both sides inside of a blade enclosure?

A. Midplane
B. Active backplane
C. Passive backplane
D. Management module

Answer: A

Explanation:
The component that allows for a connection of devices to both sides inside of a blade enclosure is midplane. A midplane is a board or panel that connects two sets of connectors or devices in parallel with each other. A midplane is typically used in blade enclosures or chassis to provide power and data connections between blade servers on one side and power supplies, cooling fans, switches, or management modules on the other side. A midplane can also act as a backplane by providing bus signals or communication channels between devices.

NEW QUESTION 261
A technician has several possible solutions to a reported server issue. Which of the following BEST represents how the technician should proceed with troubleshooting?

A. Determine whether there is a common element in the symptoms causing multiple problems.
B. Perform a root cause analysis.
C. Make one change at a time and test.
D. Document the findings, actions, and outcomes throughout the process.

Answer: C

Explanation:
This is the best way to proceed with troubleshooting when the technician has several possible solutions to a reported server issue. Making one change at a time and testing allows the technician to isolate the cause and effect of each solution and determine which one works best. It also helps to avoid introducing new problems or complicating existing ones by making multiple changes at once. Determining whether there is a common element in the symptoms causing multiple problems is a good step to perform before identifying possible solutions, but not after. Performing a root cause analysis is a good step to perform after resolving the issue, but not during. Documenting the findings, actions, and outcomes throughout the process is a good practice to follow at every step of troubleshooting, but not a specific way to proceed with testing possible solutions. References: https://www.howtogeek.com/174288/how-to-tell-if-your-computer-is-overheating-and-what-to-do-about-it/https://www.howtogeek.com/428483/what-is-end-to- end-encryption-and-why-does-it-matter/

NEW QUESTION 265
The Chief Information Officer of a data center is concerned that transmissions from the building can be detected from the outside. Which of the following would resolve this concern? (Select TWO).

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

Answer: CD

Explanation:
Signal blocking is a technique that prevents or reduces the transmission of electromagnetic signals from a building to the outside. Signal blocking can be achieved by using materials that absorb, reflect, or scatter the signals, such as metal, concrete, or mesh. Signal blocking can protect the data center from eavesdropping, interference, or jamming by unauthorized parties1.
Camouflage is a technique that disguises or conceals the appearance of a building to make
it less noticeable or identifiable from the outside. Camouflage can be achieved by using colors, patterns, shapes, or vegetation that blend in with the surrounding environment. Camouflage can protect the data center from detection, reconnaissance, or targeting by hostile parties

NEW QUESTION 266
The management team has mandated the encryption of all server administration traffic. Which of the following should MOST likely be implemented?

A. SSH
B. VPN
C. SELinux
D. FTPS

Answer: A

Explanation:
SSH stands for Secure Shell and it is a network protocol that provides encrypted and authenticated communication between two hosts. SSH can be used to remotely access and administer a server using a command-line interface or a graphical user interface. SSH can ensure the encryption of all server administration traffic, which can prevent eavesdropping, tampering, or spoofing by unauthorized parties.References: https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam- objectives (Objective 2.4)

NEW QUESTION 268
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 270
A technician re working on a Linux server and re trying to access another server over the network. The technician gets server notfoundmessage when trying to execute ping servername but no error messages when usingpingservername. Domain.com. Which ofthe following should the technician do to resolve the error?

A. Configure the domain search variable
B. Change the permissions on resol
C. conf
D. Configure the DNS address
E. Modify nsswitc
F. Conf.

Answer: A

Explanation:
The domain search variable is used to specify a list of domains that are appended to a hostname when resolving it. If the servername is not fully qualified, the resolver will try each domain in the list until it finds a match or fails. By configuring the domain search variable, the technician can avoid typing the full domain name every time they want to ping a server. Verified References: [How to configure DNS suffixes on Linux systems]

NEW QUESTION 272
An administrator is installing a new file server that has four drive bays available. Which of the following RAID types would provide the MOST storage as well as disk redundancy?

A. RAIDO
B. RAID 1
C. RAID 5
D. RAID 10

Answer: C

Explanation:
RAID 5 is a RAID level that provides striping with parity, which means that data is distributed across all disks with one disk storing parity information for error correction. RAID 5 can tolerate one disk failure without losing data. RAID 5 provides the most storage as well as disk redundancy out of the four RAID levels given, since it only uses one disk for parity and the rest for data. For example, if four 200GB drives are used in a RAID 5 array, the total storage capacity would be 600GB (200GB x 3), while in RAID 0 it would be 800GB (200GB x 4), in RAID 1 it would be 200GB (200GB x 1), and in RAID 10 it would be 400GB (200GB x 2).References:https://en.wikipedia.org/wiki/Standard_RAID_levels#RAID_5

NEW QUESTION 274
Which of the following DR testing scenarios is described as verbally walking through each step of the DR plan in the context of a meeting?

A. Live failover
B. Simulated failover
C. Asynchronous
D. Tabletop

Answer: D

Explanation:
The DR testing scenario that is described as verbally walking through each step of the DR plan in the context of a meeting is tabletop. A tabletop test is a type of disaster recovery (DR) test that involves discussing and reviewing the DR plan with key stakeholders and participants in a simulated scenario. A tabletop test does not involve any actual execution of the DR plan or any disruption of the normal operations. A tabletop test can help identify gaps, issues, or inconsistencies in the DR plan and improve communication and coordination among the DR team members.

NEW QUESTION 278
Which of the following is used for fail over, providing access to all the services currently in use by an organization without having to physically move any servers or employees?

A. The cloud
B. A cold site
C. A warm site
D. An emergency operations center

Answer: A

Explanation:
The solution that is used for failover, providing access to all the services currently in use by an organization without having to physically move any servers or employees, is the cloud. The cloud is a term that refers to a network of remote servers that are hosted on the Internet and provide various services, such as storage, computing, networking, andapplications. The cloud can be used for failover, which is a backup operation that automatically switches to a standby system or service in case of a failure or disruption of the primary system or service. By using the cloud for failover, an organization can ensure continuous availability and accessibility of its services without requiring any physical relocation or intervention.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 6, Lesson 6.4, Objective 6.4

NEW QUESTION 282
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 284
While running a local network security scan an administrator discovers communication between clients and one of the web servers is happening in cleartext. Company policy requires all communication lo be encrypted. Which of the following ports should be closed to stop the deartext communication?

A. 21
B. 22
C. 443
D. 3389

Answer: A

Explanation:
Port 21 is used for FTP (File Transfer Protocol), which is a protocol that transfers files between servers and clients in cleartext, meaning that anyone can intercept and read the data. To stop this communication, port 21 should be closed on the web server and replaced with a secure protocol, such as SFTP (Secure File Transfer Protocol) or FTPS (File Transfer Protocol Secure), which use encryption to protect the data. Verified References: [FTP vs SFTP vs FTPS]

NEW QUESTION 287
A technician learns users are unable to tog in to a Linux server with known-working LDAP credentials. The technician logs in to the server with a local account and confirms the system is functional can communicate over the network, and is configured correctly However, the server log has entries regarding Kerberos errors. Which of the following is the MOST likely source of the issue?

A. A local firewall is blocking authentication requests.
B. The users have expired passwords
C. The system clock is off by more than five minutes
D. The server has no access to the LDAP host

Answer: C

Explanation:
Kerberos is a network authentication protocol that uses tickets to allow clients and servers to prove their identity to each other. Kerberos relies on accurate time synchronization between the parties involved, as the tickets have expiration dates and timestamps. If the system clock of a Linux server is off by more than five minutes from the LDAP server or the domain controller, the Kerberos authentication will fail and generate errors. A local firewall is unlikely to block authentication requests if the server can communicate over the network and is configured correctly. The users' passwords are not relevant if they are known-working LDAP credentials. The server has access to the LDAP host if it can communicate over the network and is configured correctly. References:
? https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/identity_management_guide/kerberos_errors
? https://www.ibm.com/docs/en/aix/7.2?topic=authentication-kerberos-time- synchronization

NEW QUESTION 292
An administrator is troubleshooting a server that is rebooting and crashing. The administrator notices that the server is making sounds that are louder than usual. Upon closer inspection, the administrator
discovers that the noises are coming from the front of the chassis. Which of the following is the most likely reason for this behavior?

A. One of the fans has failed.
B. The power supply has failed.
C. The RAM is malfunctioning.
D. The CPU is overheating.

Answer: A

Explanation:
A server has multiple fans inside the chassis to cool down the components and prevent overheating. If one of the fans fails, it can cause the server to reboot and crash due to thermal issues. A failed fan can also make loud noises due to friction or vibration. The administrator should check the fans and clean them from dust and debris, or replace them if they are damaged12.
References = 1: It's Too Loud! 3 Solutions to Remedy Server Noise - Computerware Blog | DC Metro | Computerware Blog(https://www.cwit.com/blog/it-s-too-

loud-3-solutions-to-
remedy-server-noise) 2: What factors affect the noise level of a server? - Server Fault(https://serverfault.com/questions/430550/what-factors-affect-the-noise-level-of-a-server)

NEW QUESTION 297
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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