# CompTIA

## Exam Questions SK0-005

CompTIA Server+ Certification Exam

**NEW QUESTION 1**
An administrator restores several database files without error while participating in a mock disaster recovery exercise. Later, the administrator reports that the restored databases are
corrupt and cannot be used. Which of the following would best describe what caused this issue?

A. The databases were not backed up to be application consistent.
B. The databases were asynchronously replicated
C. The databases were mirrored
D. The database files were locked during the restoration process.

**Answer:** A

**Explanation:**
Application consistent backup is a method of backing up data that ensures the integrity and consistency of the application state. It involves notifying the application to flush its data from memory to disk and quiescing any write operations before taking a snapshot of the data. If the databases were not backed up to be application consistent, they might contain incomplete or corrupted data that cannot be restored properly. References:
CompTIA Server+ Certification Exam Objectives1, page 12 What is Application Consistent Backup and How to Achieve It2 Application-Consistent Backups3

**NEW QUESTION 2**
An administrator needs to increase the size of an existing RAID 6 array that is running out of available space. Which of the following is the best way the administrator can perform this task?

A. Replace all the array drives at once and then expand the array.
B. Expand the array by changing the RAID level to 6.
C. Expand the array by changing the RAID level to 10.
D. Replace the array drives one at a time and then expand the array.

**Answer:** D

**Explanation:**
RAID 6 is a type of RAID that uses block-level striping with two parity blocks distributed across all member disks. It allows for two disk failures within the RAID set before any data is lost1. A minimum of four disks is requiredto create RAID 61. To increase the size of an existing RAID 6 array, the administrator can replace the array drives one at a time with larger drives and then expand the array. This way, the data and parity are rebuilt on each new drive and the array remains operational during the process2.

**NEW QUESTION 3**
A data center employee shows a driver's license to enter the facility Once the employee enters, the door immediately doses and locks, triggering a scale that then weighs the employee before granting access to another locked door. This is an example of.

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

**Answer:** A

**Explanation:**
A mantrap is a security device that consists of a small space with two sets of interlocking doors, such that the first set of doors must close before the second one opens. A mantrap can be used to control access to a data center by verifying the identity and weight of the person entering. A bollard is a sturdy post that prevents vehicles from entering a restricted area. Geofencing is a technology that uses GPS or RFID to create a virtual boundary around a location and trigger an action when a device crosses it. RFID is a technology that uses radio waves to identify and track objects or people. References:
? https://www.techopedia.com/definition/16293/mantrap
? https://www.techopedia.com/definition/1437/bollard
? https://www.techopedia.com/definition/23961/geofencing
? https://www.techopedia.com/definition/506/radio-frequency-identification-rfid

**NEW QUESTION 4**
Joe. a user m the IT department cannot save changes to a sensitive file on a Linux server. An 1s -1& snows the following listing;

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

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

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

**Answer:** C

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

**NEW QUESTION 5**

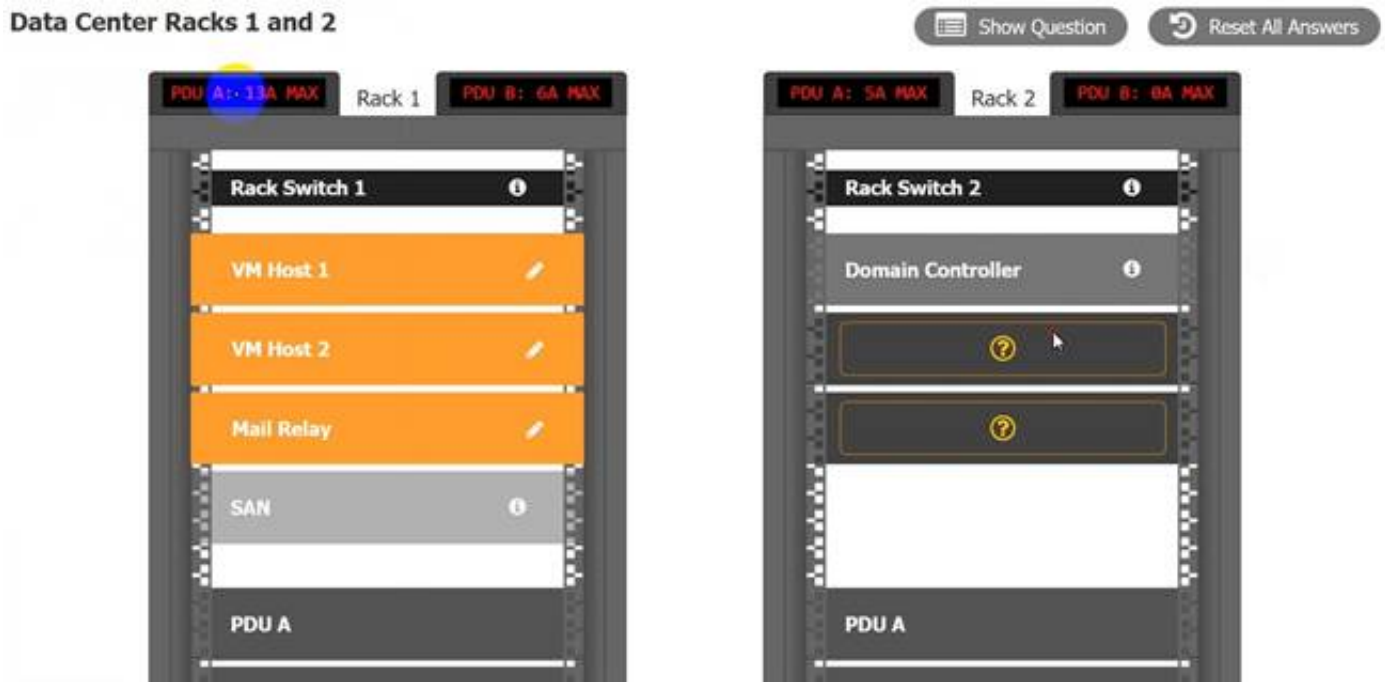
A systems administrator is performing maintenance on 12 Windows servers that are in different racks at a large datacenter. Which of the following would allow the administrator to perform maintenance on all 12 servers without having to physically be at each server? (Choose two.)

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

**Answer:** AB

**Explanation:**
The methods that would allow the administrator to perform maintenance on all 12 servers without having to physically be at each server are remote desktop and IP KVM. Remote desktop is a feature that allows a user to access and control another computer over a network using a graphical user interface (GUI). Remote desktop can enable remote administration, troubleshooting, and maintenance of servers without requiring physical presence at the server location. IP KVM (Internet Protocol Keyboard Video Mouse) is a device that allows a user to access and control multiple servers over a network using a single keyboard, monitor, and mouse. IP KVM can provide remote access to servers regardless of their operating system or power state, and can also support virtual media and serial console functions.
Reference:
https://www.blackbox.be/en-be/page/27559/Resources/Technical-Resources/Black-Box- Explains/kvm/ Benefits-of-using-KVM-over-IP

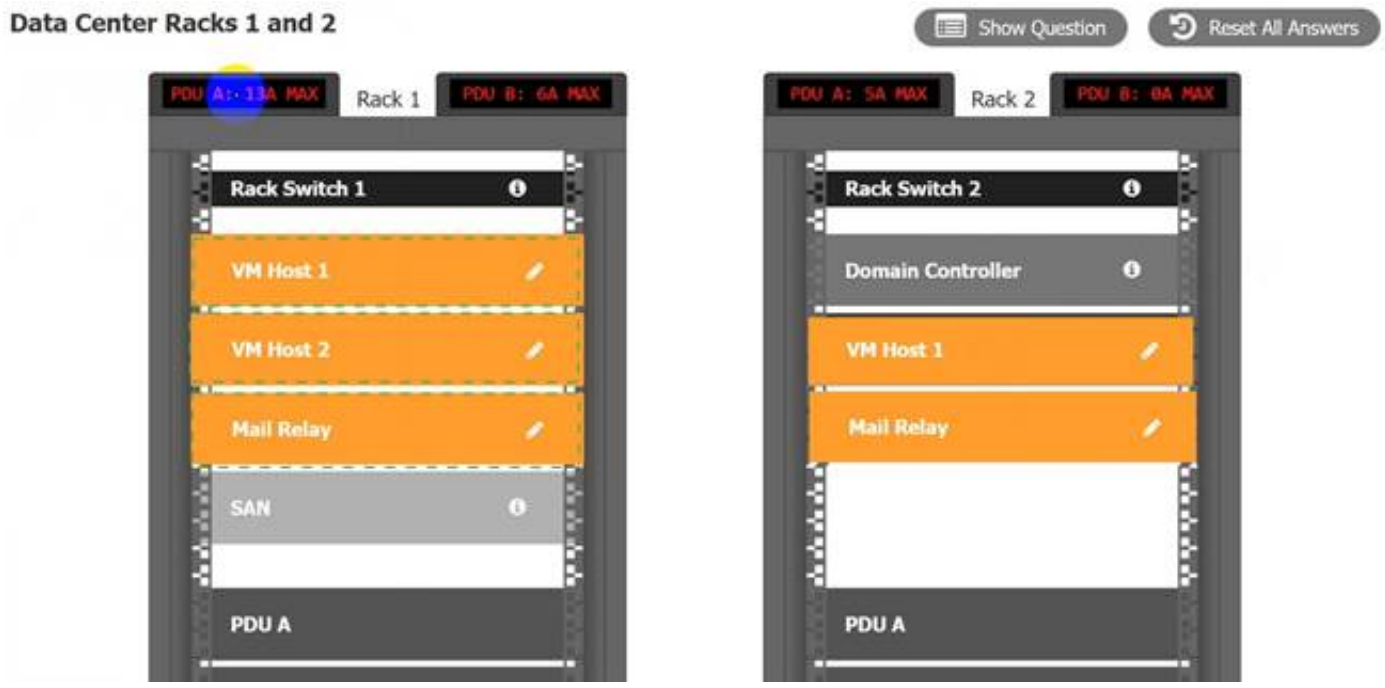
**NEW QUESTION 6**
DRAG DROP
A recent power Outage caused email services to go down. A sever administrator also received alerts from the datacenter's UPS.
After some investigation, the server administrator learned that each POU was rated at a maximum Of 12A.
INSTRUCTIONS
Ensure power redundancy is implemented 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**
Following a recent power outage, a server in the datacenter has been constantly going offline and losing its configuration. Users have been experiencing access issues while using the application on the server. The server technician notices the data and time are incorrect when the server is online. All other servers are working. Which of the following would MOST likely cause this issue? (Choose two.)

A. The server has a faulty power supply
B. The server has a CMOS battery failure
C. The server requires OS updates
D. The server has a malfunctioning LED panel
E. The servers do not have NTP configured
F. The time synchronization service is disabled on the servers

**Answer:** BF

**Explanation:**
The server has a CMOS battery failure and the time synchronization service is disabled on the servers. The CMOS battery is a small battery on the motherboard that powers the BIOS settings and keeps track of the date and time when the server is powered off. If the CMOS battery fails, the server will lose its configuration and display an incorrect date and time when it is powered on. This can cause access issues for users and applications that rely on accurate time stamps. The time synchronization service is a service that synchronizes the system clock with a reliable external time source, such as a network time protocol (NTP) server. If the time synchronization service is disabled on the servers, they will not be able to update their clocks automatically and may drift out of sync with each other and with the network. This can also cause access issues for users and applications that require consistent and accurate time across the network.

**NEW QUESTION 8**
A systems administrator notices a newly added server cannot see any of the LUNs on the SAN. The SAN switch and the local HBA do not display any link lights. Which of the following is most likely the issue?

A. A single-mode fiber cable is used in place of multimode.
B. The switchport is on the wrong virtual SAN.
C. The HBA driver needs to be installed on the server.
D. The zoning on the fiber switch is wrong.

**Answer:** A

**Explanation:**
The most likely issue that prevents the newly added server from seeing any of the LUNs on the SAN is that a single-mode fiber cable is used in place of multimode. 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 cablecan transmit data over long distances at high speeds, but it requires more expensive transceivers and connectors than multimode fiber cables. A multimode fiber cable is a type of optical fiber cable that has a larger core diameter and allows multiple modes of light to propagate through it. A multimode fiber cable can transmit data over short distances at lower speeds than single- mode fiber cables, but it is more compatible and cost-effective than single-mode fiber cables. If a single-mode fiber cable is used in place of multimode, it can cause signal loss, attenuation, or mismatch between the devices. References: [CompTIA Server+ Certification Exam Objectives], Domain 3.0: Storage, Objective 3.2: Given a scenario, compare and contrast various storage technologies.

**NEW QUESTION 9**
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 10**
A server administrator is installing a new server with multiple NICs on it. The Chief Information Officer has asked the administrator to ensure the new server will have the least amount of network downtime but a good amount of network speed. Which of the following best describes what the administrator should implement on the new server?

A. VLAN
B. vNIC
C. Link aggregation
D. Failover

**Answer:** C

**Explanation:**
Link aggregation is the best option to implement on the new server to ensure the least amount of network downtime but a good amount of network speed. Link aggregation is a technique of combining multiple physical network interfaces into one logical interface to increase bandwidth, redundancy, and load balancing. Link aggregation can improve the performance and availability of the server by allowing it to use more than one network path for data transmission and failover in case

of link failure. Link aggregation can be implemented using various protocols, such as IEEE 802.3ad (LACP), Cisco EtherChannel, or Linux bonding. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Networking, Objective 4.1: Given a scenario, configure network settings for servers.

**NEW QUESTION 10**
A technician needs to deploy an operating system that would optimize server resources. Which of the following server installation methods would BEST meet this requirement?

A. Full
B. Bare metal
C. Core
D. GUI

**Answer:** C

**Explanation:**
The server installation method that would optimize server resources is core. Core is a minimal installation option that is available for some operating systems, such as Windows Server and Linux. Core installs only the essential components and features of the operating system, without any graphical user interface (GUI) or other unnecessary services or applications. Core reduces the disk footprint, memory usage, CPU consumption, and attack surface of the server, making it more efficient and secure. Core can be managed remotely using command-line tools, PowerShell, or GUI tools.
Reference:
https://docs.microsoft.com/en-us/windows-server/administration/performance- tuning/hardware/

**NEW QUESTION 12**
An administrator is tasked with building an environment consisting of four servers that can each serve the same website. Which of the following concepts is described?

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

**Answer:** A

**Explanation:**
Load balancing is a concept that distributes the workload across multiple servers or other resources to optimize performance, availability, and scalability. Load balancing can be implemented at different layers of the network, such as the application layer, the transport layer, or the network layer. Load balancing can use various algorithms or methods to determine how to distribute the traffic, such as round robin, least connections, or weighted distribution.
References: CompTIA Server+ Study Guide, Chapter 6: Networking, page 241.

**NEW QUESTION 15**
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 19**
A security technician generated a public/private key pair on a server. The technician needs to copy the key pair to another server on a different subnet. Which of the following is the most secure method to copy the keys?
? HTTP

A. FTP
B. SCP
C. USB

**Answer:** C

**Explanation:**
SCP (Secure Copy Protocol) is a protocol that allows users to securely transfer files between servers using SSH (Secure Shell) encryption. SCP encrypts both the data and the authentication information, preventing unauthorized access, interception, ormodification of the files1. SCP also preserves the file attributes, such as permissions, timestamps, and ownership2.

**NEW QUESTION 20**
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 22**
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 25**
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 28**
A technician recently replaced a NIC that was not functioning. Since then, no device driver is found when starting the server, and the network card is not functioning. Which of the following should the technician check first?

A. The boot log
B. The BIOS
C. The HCL
D. The event log

**Answer:** C

**Explanation:**
The technician should check the hardware compatibility list (HCL) first to see if the new NIC is supported by the server’s operating system. The HCL is a list of hardware devices that have been tested and verified to work with a specific operating system. If the NIC is not on the HCL, it means that there is no device driver available or compatible for it, and the NIC will not function properly.
References: CompTIAServer+ SK0-005 Certification Study Guide, Chapter 5, Lesson 5.2, Objective 5.2

**NEW QUESTION 29**
A server administrator must respond to tickets within a certain amount of time. The server administrator needs to adhere to the:

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 33**
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 37**
A server administrator implemented a new backup solution and needs to configure backup methods for remote sites. These remote sites have low bandwidth and backups must not
interfere with the network during normal business hours. Which of the following methods can be used to meet these requirements? (Select two).

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

**Answer:** BE

**Explanation:**
Archive is a method of storing historical data that is not frequently accessed or modified. Archive can reduce the amount of data that needs to be backed up and save bandwidth and storage space. Differential is a method of backing up only the data that has changed since the last full backup. Differential can also save bandwidth and storage space, as well as speed up the backup process.
References:
CompTIA Server+ Certification Exam Objectives1, page 12
Server Management: Server Hardware Installation and Management2, Module 2, Lesson 5

**NEW QUESTION 40**
Which of the following physical security concepts would most likely be used to limit personnel access to a restricted area within a data center?

A. An access control vestibule
B. Video surveillance
C. Bollards
D. Data center camouflage

**Answer:** A

**Explanation:**
An access control vestibule is a physical security concept that limits personnel access to a restricted area within a data center. It is a small room or hallway that has two doors: one that leads to the outside and one that leads to the restricted area. The doors are controlled by an electronic lock that requires authentication, such as a card reader, biometric scanner, or keypad. Only authorized personnel can enter the vestibule and access the restricted area. References: CompTIA Server+ Certification Exam Objectives, Domain 5.0: Security, Objective 5.1: Given a scenario, apply physical security methods to a server.

**NEW QUESTION 42**
An administrator has been asked to deploy a database server that provides the highest performance with fault tolerance. Which of the following RAID levels will fulfill this request?

A. RAIDO
B. RAID1
C. RAID 5
D. RAID 6
E. RAID 10

**Answer:** E

**Explanation:**

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

**NEW QUESTION 45**
A systems administrator is trying to determine why users in the human resources department cannot access an application server. The systems administrator reviews the application logs but does not see any attempts by the users to access the application. Which of the following is preventing the users from accessing the application server?

A. NAT
B. ICMP
C. VLAN
D. NIDS

**Answer:** C

**Explanation:**
This is the most likely cause of preventing the users from accessing the application server because a VLAN is a logical segmentation of a network that isolates traffic based on certain criteria. If the human resources department and the application server are on different VLANs, they will not be able to communicate with each other unless there is a router or a switch that can route between VLANs.References:https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html

**NEW QUESTION 47**
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 49**
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 53**
A technician is connecting a Linux server to a share on a NAS. Which of the following is the MOST appropriate native protocol to use for this task?

A. CIFS
B. FTP
C. SFTP
D. NFS

**Answer:** D

**Explanation:**
The most appropriate native protocol to use for connecting a Linux server to a share on a NAS is NFS. NFS (Network File System) is a protocol that allows file sharing and remote access over a network. NFS is designed for Unix-like operating systems, suchas Linux, and supports features such as symbolic links, hard

links, file locking, and file permissions. NFS uses mount points to attach remote file systems to local file systems, making them appear as if they are part of the local file system. NFS can provide fast and reliable access to files stored on a NAS (Network Attached Storage), which is a device that provides centralized storage for network devices.

**NEW QUESTION 54**
A technician has received multiple reports of issues with a server. The server occasionally has a BSOD, powers off unexpectedly, and has fans that run continuously. Which of the following BEST represents what the technician should investigate during troubleshooting?

A. Firmware incompatibility
B. CPU overheating
C. LED indicators
D. ESD issues

**Answer:** B

**Explanation:**
Unexpected shutdowns. If the system is randomly shutting down or rebooting, the most likely cause is a heat problem.
Reference:https://www.microsoftpressstore.com/articles/article.aspx?p=2224043&seqNum
=3

**NEW QUESTION 55**
Which of the following BEST measures now much downtime an organization can tolerate Curing an unplanned outage?

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

**Answer:** C

**Explanation:**
RTO (Recovery Time Objective) is a measure of how much downtime an organization can tolerate during an unplanned outage. It is the maximum time allowed for restoring normal operations after a disaster. RTO is one of the key metrics for disaster recovery planning and testing. SLA (Service Level Agreement) is a contract that defines the expected level of service and performance between a provider and a customer. BIA (Business Impact Analysis) is a process that identifies and evaluates the potential effects of a disaster on critical business functions and processes. MTTR (Mean Time To Repair) is a measure of how long it takes to fix a failed component or system. References: https://parachute.cloud/rto-vs-rpo/ https://www.techopedia.com/definition/13622/service- level-agreement-sla https://www.techopedia.com/definition/1032/business-impact-analysis- biahttps://www.techopedia.com/definition/8239/mean-time-to-repair-mttr

**NEW QUESTION 57**
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 61**
Which of the following should an administrator use to transfer log files from a Linux server to a Windows workstation?

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

**Answer:** D

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

**NEW QUESTION 63**
A server administrator needs to keep a copy of an important fileshare that can be used to restore the share as quickly as possible. Which of the following is the BEST solution?

A. Copy the fileshare to an LTO-4 tape drive
B. Configure a new incremental backup job for the fileshare
C. Create an additional partition and move a copy of the fileshare

D. Create a snapshot of the fileshare

**Answer:** D

**Explanation:**
The best solution to keep a copy of an important fileshare that can be used to restore the share as quickly as possible is to create a snapshot of the fileshare. A snapshot is a point-in-time copy of a file system or a volume that captures the state and data of the fileshare at a specific moment. A snapshot can be created instantly and with minimal overhead, as it only stores the changes made to the fileshare after the snapshot was taken. A snapshot can be used to restore the fileshare to its previous state in case of data loss or corruption.

**NEW QUESTION 64**
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 69**
A server administrator noticesthe/var/log/audit/audit.logfileon a Linux server is rotating loo frequently. The administrator would like to decrease the number of times the leg rotates without losing any of the information in the logs. Which of the following should the administrator configure?

A. increase theaudi
B. log file size in the appropriate confutation file.
C. Decrease the duration of the log rotate cycle tor theaudi
D. log file.
E. Remove the tog rotate directive from the audit .log We configuration.
F. Move the audi
G. leg files to a remote syslog server.

**Answer:** A

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

**NEW QUESTION 70**
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 74**
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 75**
Which ofthefollowingshouldatechnician verify FIRST before decommissioning and wipinga file server?

A. Themedia destructionmethod
B. Therecycling poke?
C. Asset management documentation
D. Non-utilization

**Answer:** D

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

**NEW QUESTION 79**
A senior administrator instructs a technician to run the following script on a Linux server: for i in {1..65536); do echo Si; telnet localhost $i; done
The script mostly returns the following message: Connection refused. However, there are several entries in the console display that look like this:
80
Connected to localhost 443
Connected to localhost
Which of the following actions should the technician perform NEXT?

A. Look for an unauthorized HTTP service on this server
B. Look for a virus infection on this server
C. Look for an unauthorized Telnet service on this server
D. Look for an unauthorized port scanning service on this server.

**Answer:** A

**Explanation:**
The script that the technician is running is trying to connect to every port on the localhost (the same machine) using telnet, a network protocol that allows remote access to a command-line interface. The script mostly fails because most ports are closed or not listening for connections. However, the script succeeds on ports 80 and 443, which are the default ports for HTTP and HTTPS protocols, respectively. These protocols are used for web services and web browsers. Therefore, the technician should look for an unauthorized HTTP service on this server, as it may indicate a security breach or a misconfiguration. Looking for a virus infection on this server is also possible, but not the most likely source of the issue. Looking for an unauthorized Telnet service on this server is not relevant, as the script is using telnet as a client, not a server. Looking for an unauthorized port scanning service on this server is not relevant, as the script is scanning ports on the localhost, not on other machines. References:
? https://phoenixnap.com/kb/telnet-windows
? https://www.techopedia.com/definition/23337/http-port-80
? https://www.techopedia.com/definition/23336/https-port-443

**NEW QUESTION 84**
A server administrator is experiencing difficulty configuring MySQL on a Linux server. The administrator issues the getenforce command and receives the following output:
># Enforcing
Which of the following commands should the administrator issue to configure MySQL successfully?

A. setenforce 0
B. setenforce permissive
C. setenforce 1
D. setenforce disabled

**Answer:** A

**Explanation:**
The command that the administrator should issue to configure MySQL successfully is setenforce 0. This command sets the SELinux (Security-Enhanced Linux) mode to permissive, which means that SELinux will not enforce its security policies and will only log any violations. SELinux is a feature that provides mandatory access control (MAC) for Linux systems, which can enhance the security and prevent unauthorized access or modification of files and processes. However, SELinux can also interfere with some applications or services that require specific permissions or ports that are not allowed by SELinux by default. In this case, MySQL may not be able to run properly due to SELinux restrictions. To resolve this issue, the administrator can either disable SELinux temporarily by using setenforce 0, or permanently by editing the /etc/selinux/config file and setting SELINUX=disabled. Alternatively, the administrator can configure SELinux to allow MySQL
to run by using commands such as semanage or setsebool.
Reference:
https://blogs.oracle.com/mysql/selinux-and-mysql-v2

**NEW QUESTION 88**
A user can successfully connect to a database server from a home office but is unable to access it from a hotel room. Which of the following authentication methods is most likely
configured?

A. Delegation
B. Role-based
C. Rule-based
D. Scope-based

**Answer:** D

**Explanation:**

Scope-based authentication is a method of restricting access to resources based on the location, network, or device of the user. It can be used to prevent unauthorized access from outside the organization's network or from untrusted devices. In this case, the user can connect to the database server from the home office, which is likely within the scope of the authentication policy, but not from the hotel room, which is outside the scope.
References:
CompTIA Server+ Certification Exam Objectives1, page 15 CompTIA Server+: Authentication & Authorization2

**NEW QUESTION 93**
A junior administrator needs to configure a single RAID 5 volume out of four 200GB drives attached to the server using the maximum possible capacity. Upon completion, the server reports that all drives were used, and the approximate volume size is 400GB. Which of the following BEST describes the result of this configuration?

A. RAID 0 was configured by mistake.
B. RAID 5 was configured properly.
C. JBOD was configured by mistake.
D. RAID 10 was configured by mistake.

**Answer:** B

**Explanation:**
The output of the configuration shows that RAID 5 was configured properly using four 200GB drives. The approximate volume size of 400GB is correct, since RAID 5 uses one disk for parity and the rest for data. Therefore, the usable storage capacity is three-fourths of the total capacity, which is 600GB out of 800GB. The other RAID levels given would result in different volume sizes: RAID 0 would result in 800GB, RAID 1 would result in 200GB, and JBOD would result in an error since it does not support multiple drives in a single volume.References:https://en.wikipedia.org/wiki/Standard_RAID_levels#RAID_5

**NEW QUESTION 94**
An administrate is helping to replicate a large amount of data between two Windows servers. The administrator is unsure how much data has already been transferred. Which of the following will BEST ensure all the data is copied consistently?

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

**Answer:** D

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

**NEW QUESTION 99**
A technician is unable to access a server's package repository internally or externally. Which of the following are the MOST likely reasons? (Choose two.)

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

**Answer:** DE

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

**NEW QUESTION 100**
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 104**
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 107**
A data center has 4U rack servers that needto be replaced using VMsbutwithout losingany data. Whichofthefollowingmethodswill MOST likelybe used to replace these servers?

A. Unattended scripted OS installation
B. P2V
C. VM cloning

**Answer:** C

**Explanation:**
P2V (Physical to Virtual) is a method of converting a physical server into a virtual machine that can run on a hypervisor. This method can be used to replace 4U rack servers with VMs without losing any data, as it preserves the configuration and state of the original server. P2V can also reduce hardware costs, power consumption, and space requirements. Verified References: [What is P2V?]

**NEW QUESTION 112**
A Linux server was recently updated. Now, the server stops during the boot process with a blank screen and an f prompt. Which 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. UEFI (Unified Extensible Firmware Interface) is a standard that defines the interface and functionality of the firmware that initializes the hardware and software components of a system before loading the operating system. UEFI boot is a process that uses UEFI firmware to load and execute a boot loader, which is a program that loads the operating system kernel and other essential files. A Linux boot file is a file that contains information and instructions for the boot loader, such as the location of the kernel, the root file system, and the boot parameters. If a Linux boot file is missing or corrupted, the boot loader cannot find or load the kernel, and the system stops during the boot process with a blank screen and an f prompt.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 4, Lesson 4.1, Objective 4.1

**NEW QUESTION 116**
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 121**
An administrator is installing a new server and OS. After installing the OS, the administrator logs in and wants to quickly check the network configuration. Which of the following is the best command to use to
accomplish this task?

A. tracert
B. telnet
C. ipconfig

D. ping

**Answer:** C

**NEW QUESTION 123**
A technicianretailed a new4TBharddrive inaWindows server. Which of the following should the technician perform FIRST to provision the newdrive?

A. Configure the drive as a base disk.
B. Configure the drive as a dynamic disk.
C. Partition the drive using MBR.
D. Partition the drive using OPT.

**Answer:** D

**Explanation:**
GPT (GUID Partition Table) is a partitioning scheme that allows creating partitions on large hard drives (more than 2 TB). It supports up to 128 partitions per drive and uses 64-bit addresses to locate them. MBR (Master Boot Record) is an older partitioning scheme that has limitations on the size and number of partitions (up to 4 primary partitions or 3 primary and 1 extended partition per drive). To provision a new 4 TB drive, the technician should partition it using GPT. Verified References: [GPT], [MBR]

**NEW QUESTION 125**
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 130**
Which of the following types of asset management documentation is commonly used as a reference when processing the replacement of a faulty server component?

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

**Answer:** A

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

**NEW QUESTION 134**
Which of the following attacks is the most difficult to mitigate with technology?

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

**Answer:** D

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

**NEW QUESTION 136**
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 138**
A server administrator is trying to determine the cause of a slowdown on a database server. Upon investigation, the administrator determines the issue is in the storage subsystem. Which of the following will most likely resolve this issue?

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

**Answer:** A

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

**NEW QUESTION 141**
Due to a disaster incident on a primary site, corporate users are redirected to cloud services where they will be required to be authenticated just once in order to use all cloud services.
Which of the following types of authentications is described in this scenario?

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

**Answer:** D

**NEW QUESTION 144**
A server administrator needs to check remotely for unnecessary running services across 12 servers. Which of the following tools should the administrator use?

A. DLP
B. A port scanner
C. Anti-malware
D. A sniffer

**Answer:** B

**Explanation:**
The tool that the administrator should use to check for unnecessary running services across 12 servers is a port scanner. A port scanner is a tool that scans a network device for open ports and identifies the services or applications that are running on those ports. A port scanner can help detect any unauthorized or unwanted services that may pose a security risk or consume network resources. A port scanner can also help troubleshoot network connectivity issues or verify firewall rules.
Reference: https://www.getsafeonline.org/business/articles/unnecessary-services/

**NEW QUESTION 146**
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 149**
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 150**
A systems administrator is investigating a server with a RAID array that will not boot into the OS. The administrator notices all the hard drives are reporting to be offline. The administrator checks the RAID controller and verifies the configuration is correct. The administrator then replaces one of the drives with a known-good drive, but it appears to be unavailable as well. Next, the administrator takes a drive out of the server and places it in a spare server, and the drive is available and functional. Which of the following is MOST
likely causing the issue?

A. The kernel is corrupt.
B. Resources are misallocated.
C. The backplane has failed.
D. The drives need to be reseated.

**Answer:** C

**Explanation:**
The backplane is a circuit board that connects multiple hard drives to a RAID controller and provides power and data transfer between them. If the backplane has failed, it may cause all the hard drives to be offline and prevent the server from booting into the OS. The fact that replacing one of the drives with a known-good drive did not work, and that taking a drive out of the server and placing it in a spare server made it functional, suggests that the problem is not with the drives themselves but with the backplane. A corrupt kernel (A) would not affect the status of the hard drives, as it is a software component of the OS. Resource misallocation (B) would not cause all the hard drives to be offline, as it is a configuration issue that affects how resources are assigned to processes or applications. Reseating the drives (D) would not help, as it would not fix a faulty backplane.References:https://www.dell.com/support/kbdoc/en-us/000130114/how-to-troubleshoot-a-faulty-backplane

**NEW QUESTION 153**
An administrator is troubleshooting performance issues on a server that was recently upgraded. The administrator met with users/stakeholders and documented recent changes in an effort to determine whether the server is better or worse since the changes. Which of the following would BEST help answer the server performance question9

A. Server performance thresholds
B. A server baseline
C. A hardware compatibility list
D. An application service-level agreement

**Answer:** B

**Explanation:**
A server baseline is a set of metrics that represents the normal performance and behavior of a server under a specific workload and configuration. A server baseline can help answer the server performance question by comparing the current performancewith the previous performance before the upgrade. This can help identify any changes or issues that may have affected the server performance.References: https://www.comptia.org/training/resources/exam-objectives/comptia-

server-sk0-005-exam- objectives (Objective 4.2)

**NEW QUESTION 154**
A technician runs top on a dual-core server and notes the following conditions: top –- 14:32:27, 364 days, 14 usersload average 60.5 12.4 13.6
Which of the following actions should the administrator take?

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

**Answer:** C

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

**NEW QUESTION 159**
A company has implemented a requirement to encrypt all the hard drives on its servers as part of a data loss prevention strategy. Which of the following should the company also perform as a data loss prevention method?

A. Encrypt all network traffic
B. Implement MFA on all the servers with encrypted data
C. Block the servers from using an encrypted USB
D. Implement port security on the switches

**Answer:** B

**Explanation:**
The company should also implement MFA on all the servers with encrypted data as a data loss prevention method. MFA stands for multi-factor authentication, which is a method of verifying a user's identity by requiring two or more pieces of evidence, such as something they know (e.g., a password), something they have (e.g., a token), or something they are (e.g., a fingerprint). MFA adds an extra layer of security to prevent unauthorized access to sensitive data, even if the user's password is compromised or stolen. Encrypting the hard drives on the servers protects the data from being read or copied if the drives are physically removed or stolen, but it does not prevent unauthorized access to the data if the user's credentials are valid.

**NEW QUESTION 163**
An administrator is able to ping the default gateway and internet sites byname from a file server. The file server is not able to ping the print server by name. The administrator is able to ping the file server from the print server by both IP address and computer name. When initiating an initiating from the file server for the print server, a different IP address is returned, which of the following is MOST Likely the cause?

A. A firewall blockingthe ICMP echo reply.
B. The DHCP scope option is incorrect
C. The DNS entriesforthe print server are incorrect.
D. The hosts file misconfigured.

**Answer:** D

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

**NEW QUESTION 167**
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 172**
A server administrator is setting up a new payroll application. Compliance regulations require that all financial systems logs be stored in a central location. Which of the following should the administrator configure to ensure this requirement is met?

A. Alerting
B. Retention
C. Shipping
D. Rotation

**Answer:** C

**Explanation:**
Shipping is a process of sending logs from one system to another system for centralized storage and analysis. Shipping can help ensure compliance with regulations that require financial systems logs to be stored in a central location. Shipping can also help improve security, performance, and scalability of log management.References: https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam- objectives (Objective 3.4)

**NEW QUESTION 175**
An application server's power cord was accidentally unplugged. After plugging the cord back in the server administrator notices some transactions were not written to the disk array. Which of the following is the MOST likely cause of the issue?

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

**Answer:** D

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

**NEW QUESTION 177**
An administrator notices high traffic on a certain subnet and would like to identify the source of the traffic. Which of the following tools should the administrator utilize?

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

**Answer:** D

**Explanation:**
Application consistent backup is a method of backing up data that ensures the integrity and consistency of the application state. It involves notifying the application to flush its data from memory to disk and quiescing any write operations before taking a snapshot of the data. If the databases were not backed up to be application consistent, they might contain incomplete or corrupted data that cannot be restored properly.
References:
CompTIA Server+ Certification Exam Objectives1, page 12 What is Application Consistent Backup and How to Achieve It2 Application-Consistent Backups3

**NEW QUESTION 178**
Which of the following is the MOST secure method to access servers located in remote branch offices?

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

**Answer:** A

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

**NEW QUESTION 183**
An organization stores backup tapes of its servers at cold sites. The organization wants to ensure the tapes are properly maintained and usable during a DR scenario. Which of the following actions should the organization perform?

A. Have the facility inspect and inventory the tapes on a regular basis.
B. Have duplicate equipment available at the cold site.
C. Retrieve the tapes from the cold site and test them.
D. Use the test equipment at the cold site to read the tapes.

**Answer:** C

**Explanation:**
The organization should retrieve the tapes from the cold site and test them to ensure they are properly maintained and usable during a DR scenario. A cold site is a location that has space and power for backup equipment, but no actual equipment installed or configured. The organization stores backup tapes of its servers at cold sites as a precaution in case of a disaster that affects its primary site. However, backup tapes can degrade over time due to environmental factors such as

temperature, humidity, dust, or magnetic fields. Therefore, the organization should periodically retrieve the tapes from the cold site and test them on compatible equipment to verify their integrity and readability. References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 6, Lesson 6.4, Objective 6.4

**NEW QUESTION 184**
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 189**
A server is reporting a hard drive S.M.A.R.T. error. When a technician checks on the drive, however, it appears that all drives in the server are functioning normally. Which of the following is the reason for this issue?

A. A S.M.A.R.
B. error is a predictive failure notic
C. The drive will fail in the near future and should be replaced at the next earliest time possible
D. A S.M.A.R.
E. error is a write operation erro
F. It has detected that the write sent to the drive was incorrectly formatted and has requested a retransmission of the write from the controller
G. A S.M.A.R.
H. error is simply a bad secto
I. The drive has marked the sector as bad and will continue to function properly
J. A S.M.A.R.
K. error is an ECC erro
L. Due to error checking and correcting, the drive has corrected the missing bit and completed the write operation correctly.

**Answer:** A

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

**NEW QUESTION 192**
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 196**
A server administrator is testing a disaster recovery plan. The test involves creating a downtime scenario and taking the necessary steps. Which of the following testing methods is the administrator MOST likely performing?

A. Backup recovery
B. Simulated
C. Tabletop
D. Live failover

**Answer:** D

**Explanation:**
The live failover testing method is the most likely one that the server administrator is performing when creating a downtime scenario and taking the necessary

steps. A live failover test involves switching from the primary system to the secondary system (or backup site) in a real environment, without any simulation or preparation. A live failover test can evaluate the effectiveness and readiness of the disaster recovery plan, but it also carries a high risk of data loss, corruption, or disruption.Reference:https://www.ibm.com/cloud/learn/disaster-recovery-testing

**NEW QUESTION 198**
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 203**
Which of the following, if properly configured, would prevent a user from installing an OS on a server? (Select TWO).

A. Administrator password
B. Group Policy Object
C. Root password
D. SELInux
E. Bootloader password
F. BIOS/UEFI password

**Answer:** EF

**Explanation:**
These are two methods that can prevent a user from installing an OS on a server if properly configured. A bootloader password is a password that protects the bootloader from unauthorized access or modification. The bootloader is a program that loads the operating system into memory when the system boots up. If a user does not know the bootloader password, they cannot change the boot order or boot from another device such as a CD-ROM or USB drive that contains an OS installation media. A BIOS/UEFI password is a password that protects the BIOS (Basic Input Output System) or UEFI (Unified Extensible Firmware Interface) from unauthorized access or modification. The BIOS or UEFI is a firmware that initializes and configures the hardware components of the system before loading

**NEW QUESTION 205**
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 206**
A technician needs to install a Type 1 hypervisor on a server. The server has SD card slots, a SAS controller, and a SATA controller, and it is attached to a NAS. On which of the following drive types should the technician install the hypervisor?

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

**Answer:** D

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

**NEW QUESTION 211**

Which of the following describes a configuration inwinch both nodes of a redundant system respond to service requests whenever possible?

A. Active-passive
B. Failover
C. Active-active
D. Fallback

**Answer:** C

**Explanation:**
Active-active is a configuration in which both nodes of a redundant system respond to service requests whenever possible. It can improve the performance, availability, and load balancing of the system by distributing the workload among the nodes. However, it also requires more synchronization and coordination between the nodes to avoid conflicts or errors. Verified References: [Active-active], [Redundant system]

**NEW QUESTION 213**
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 217**
A server administrator is racking new servers in a cabinet with multiple connections from the servers to power supplies and the network. Which of the following should the administrator recommend to the organization to best address this situation?

A. Rack balancing
B. Cable management
C. Blade enclosure
D. Rail kits

**Answer:** B

**Explanation:**
Cable management is the process of organizing, securing, and labeling cables in a server rack or cabinet. Cable management can help improve airflow and cooling, reduce clutter and confusion, prevent damage and interference, and enhance safety and aesthetics123. Cable management can be achieved by using various tools and accessories, such as cable trays, ties, hooks, clips, labels, ducts, and organizers12.

**NEW QUESTION 220**
When configuring networking on a VM, which of the following methods would allow multiple VMs to share the same host IP address?

A. Bridged
B. NAT
C. Host only
D. vSwitch

**Answer:** B

**Explanation:**
The method that would allow multiple VMs to share the same host IP address is NAT. NAT (Network Address Translation) is a technique that allows multiple devices to use a single public IP address by mapping their private IP addresses to different port numbers. NAT can be used for VM networking to enable multiple VMs on the same host to access the internet or other networks using the host’s IP address. NAT can also provide security benefits by hiding the VMs’ private IP addresses from external networks.
Reference: https://www.virtualbox.org/manual/ch06.html

**NEW QUESTION 221**
A company has a data center that is located at its headquarters, and it has a warm site that is located 20mi (32km) away, which serves as a DR location. Which of the following should the company design and implement to ensure its DR site is adequate?

A. Set up the warm site as a DR cold site.
B. Set up a DR site that is in the cloud and in the same region.
C. Set up the warm site as a DR hot site.
D. Set up a DR site that is geographically located in another region.

**Answer:** D

**Explanation:**
A DR site is a backup site that can be used to restore business operations in case of a disaster that affects the primary site. A warm site is a DR site that has some equipment and data ready to be activated quickly, but not as fast as a hot site that has fully operational systems and data. A cold site is a DR site that has only basic infrastructure and no equipment or data. The location of a DR site is an important factor to consider when designing and implementing a DR plan. A DR site that is too close to the primary site may be affected by the same disaster, such as a power outage, a flood, or an earthquake. A DR site that is too far away from the primary site may incur higher costs and latency issues. Therefore, a good practice is to set up a DR site that is geographically located in another region that has different risk factors and environmental conditions than the primary site. This can help ensure that the DR site is available and accessible when needed.
References:https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives (Objective 3.3)

**NEW QUESTION 222**
An administrator is deploying a new secure web server. The only administration method that is permitted is to connect via RDP. Which of the following ports should be allowed?
(Select two).

A. 53
B. 80
C. 389
D. 443
E. 445
F. 3389
G. 8080

**Answer:** DF

**Explanation:**
Port 443 is used for HTTPS, which is a secure version of HTTP that encrypts the data between the web server and the client. Port 3389 is used for RDP, which is a protocol that allows remote desktop connections to a server. These ports should be allowed for a secure
web server that can be administered via RDP. References:
? CompTIA Server+ Certification Exam Objectives1, page 15
? Common Ports Cheat Sheet: The Ultimate Ports & Protocols List2

**NEW QUESTION 226**
The management team has mandated the use of data-at-rest encryption for all data. Which of the following forms of encryption best achieves this goal?

A. Drive
B. Database
C. Folder
D. File

**Answer:** A

**Explanation:**
Drive encryption is a form of encryption that best achieves the goal of data-at-rest encryption for all data. Drive encryption encrypts the entire hard drive, including the operating system, applications, and files. This prevents unauthorized access to the data if the drive is lost or stolen. Database, folder, and file encryption are forms of encryption that only encrypt specific data sets, not all data. References: [CompTIA Server+Certification Exam Objectives], Domain 5.0: Security, Objective 5.3: Given a scenario involving a security threat/vulnerability/risk, implement appropriate mitigation techniques.

**NEW QUESTION 228**
A server administrator is setting up a disk with enforcement policies on how much data each home share can hold. The amount of data that is redundant on the server must also be minimized. Which of the following should the administrator perform on the server? (Select two).

A. Partitioning
B. Deduplication
C. Disk quotas
D. Compression
E. Cloning
F. Provisioning

**Answer:** BC

**Explanation:**
Deduplication is a process that eliminates redundant data blocks and reduces the amount of storage space needed. Disk quotas are policies that limit the amount of disk space that each user or group can use on a volume.
References:
? CompTIA Server+ Certification Exam Objectives1, page 8
? Data Deduplication interoperability2

**NEW QUESTION 229**
Which of the following BEST describes the concept of right to downgrade?

A. It allows for the return of a new OS license if the newer OS is not compatible with the currently installed software and is returning to the previously used OS
B. It allows a server to run on fewer resources than what is outlined in the minimum requirements document without purchasing a license
C. It allows for a previous version of an OS to be deployed in a test environment for each current license that is purchased
D. It allows a previous version of an OS to be installed and covered by the same license as the newer version

**Answer:** D

**Explanation:**
The concept of right to downgrade allows a previous version of an OS to be installed and covered by the same license as the newer version. For example, if a

customer has a license for Windows 10 Pro, they can choose to install Windows 8.1 Pro or Windows 7 Professional instead and still be compliant with the license terms. Downgrade rights are granted by Microsoft for certain products and programs, such as Windows and Windows Server software acquired through Commercial Licensing, OEM, or retail channels. Downgrade rights are intended to provide customers with flexibility and compatibility when using Microsoft software.

**NEW QUESTION 230**
A systems administrator recently installed a new virtual server. After completing the installation, the administrator was only able to reach a few of the servers on the network. While testing, the administrator discovered only servers that had similar IP addresses were reachable. Which of the following is the most likely cause of the issue?

A. The jumbo frames are not enabled.
B. The subnet mask is incorrect.
C. There is an IP address conflict.
D. There is an improper DNS configuration.

**Answer:** B

**Explanation:**
A subnet mask is a number that distinguishes the network address and the host address within an IP address1. A subnet mask allows network traffic to understand IP addresses by splitting them into the network and host addresses. If the subnet mask is incorrect, the network traffic may not be able to determine the correct destination for the packets, and only reach some of the servers that have similar IP addresses. For example, if the new virtual server has an IP address of 192.168.1.100 and a subnet mask of 255.255.0.0, it can only communicate with servers that have IP addressesin the range of 192.168.0.0 to 192.168.255.2552. To fix this issue, the systems administrator needs to check and correct the subnet mask of the new virtual server according to the network configuration.

**NEW QUESTION 233**
A server administrator is taking advantage of all the available bandwidth of the four NICs on the server. Which of the following NIC-teaming technologies should the server administrator utilize?

A. Fail over
B. Fault tolerance
C. Load balancing
D. Link aggregation

**Answer:** D

**Explanation:**
Link aggregation is a technique that combines multiple physical network links into one logical link with higher bandwidth and redundancy. It can take advantage of all the available bandwidth of the NICs (Network Interface Cards) on the server and provide load balancing and failover capabilities for network traffic. Verified References: [Link aggregation], [NIC]

**NEW QUESTION 236**
A server technician downloaded new firmware from the manufacturer's website. The technician then attempted to install the firmware on the server, but the installation failed, stating the file is potentially corrupt. Which of the following should the technician have checked prior to installing the firmware?

A. DLF configuration
B. MBR failure
C. ECC support
D. MD5 checksum

**Answer:** D

**Explanation:**
A MD5 checksum is a value that is calculated from a file using a cryptographic hash function. A MD5 checksum is used to verify the integrity of a file by comparing it with the original value provided by the manufacturer or the source. If the MD5 checksums match, it means that the file is authentic and has not been corrupted or tampered with. If the MD5 checksums do not match, it means that the file is potentially corrupt or malicious and should not be installed12. A DLF configuration (A) is a setting that determines how a dynamic link library (DLL) is loaded into memory and executed by an application. A DLF configuration does not check the integrity of a file. A MBR failure (B) is a problem that occurs when the master boot record (MBR) of a disk is damaged or corrupted, preventing the system from booting. A MBR failure does not check the integrity of a file. ECC support © is a feature that enables error-correcting code (ECC) memory to detect and correct data errors inRAM. ECC support does not check the integrity of a file. References:
1 https://www.comparitech.com/net-admin/file-integrity-monitoring-tools2/ https://csrc.nist.gov/CSRC/media/Presentations/Firmware-Integrity-Verification-Monitoring-and-Re/images-media/day2_demonstration_330-420.pdf

**NEW QUESTION 239**
An administrator is configuring a host-based firewall tor a server. The server needs to allow SSH, FTP, and LDAP traffic. Which of the following ports must be configured so this traffic will be allowed? (Select THREE).

A. 21
B. 22
C. 53
D. 67
E. 69
F. 110
G. 123
H. 389

**Answer:** ABH

**Explanation:**
These are the port numbers that must be configured on a host-based firewall for a server that needs to allow SSH, FTP, and LDAP traffic. A port number is a

numerical identifier that specifies a communication endpoint for a network protocol or an application. A host-based firewall is a software tool that monitors and controls incoming and outgoing network traffic on a single host based on predefined rules. SSH (Secure Shell) is a protocol that allows secure remote access and file transfer over an encrypted connection. The default port number for SSH is 22. FTP (File Transfer Protocol) is a protocol that allows transferring files between hosts over a network connection. The default port number for FTP is 21. LDAP (Lightweight Directory Access Protocol) is a protocol that allows accessing and managing directory services over a network connection. The default port number for LDAP is 389. References: https://www.howtogeek.com/190014/virtualization-basics-understanding-techniques-and-fundamentals/ https://www.howtogeek.com/220152/what-is-the-difference-between-127.0.0.1-and-0.0.0.0/https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does- it-matter/

**NEW QUESTION 240**
A very old PC is running a critical, proprietary application in MS-DOS. Administrators are concerned about the stability of this computer. Installation media has been lost, and the vendor is out of business. Which of the following would be the BEST course of action to preserve business continuity?

A. Perform scheduled chkdsk tests.
B. Purchase matching hardware and clone the disk.
C. Upgrade the hard disk to SSD.
D. Perform quarterly backups.

**Answer:** B

**Explanation:**
The best course of action to preserve business continuity for a very old PC that is running a critical, proprietary application in MS-DOS is to purchase matching hardware and clone the disk. This way, the technician can create an exact copy of the PC's configuration and data on another PC that has the same specifications and compatibility. This will ensure that the application can run smoothly on the new PC without any installation or configuration issues. Performing scheduled chkdsk tests would not help, as chkdsk is a tool that checks and repairs disk errors, but does not prevent hardware failures or software compatibility issues. Upgrading the hard disk to SSD would not help either, as
SSDs may not be compatible with the old PC or the MS-DOS operating system. Performing quarterly backups would help with data protection, but not with hardware availability or software compatibility. References: https://www.howtogeek.com/199068/how-to-upgrade-your-existing-hard-drive-in-under-an-hour/https://www.howtogeek.com/66776/how-to- repair-disk-errors-in-windows-7/

**NEW QUESTION 242**
An upper management team is investigating a security breach of the company's filesystem. It has been determined that the breach occurred within the human resources department. Which of the following was used to identify the breach in the human resources department?

A. User groups
B. User activity reports
C. Password policy
D. Multifactor authentication

**Answer:** B

**Explanation:**
User activity reports were used to identify the security breach in the human resources department. User activity reports are records of the actions and events performed by users on a system or network, such as login/logout times, files accessed or modified, commands executed, or websites visited. User activity reports can help monitor and audit user behavior, detect and investigate security incidents, and enforce policies and compliance. User activity reports can be generated by various tools, such as log management software, security information and event management (SIEM) systems, or user and entity behavior analytics (UEBA) solutions. References: [CompTIA Server+ Certification Exam Objectives],
Domain 5.0: Security, Objective 5.2: Given a scenario, apply logical access control methods.

**NEW QUESTION 244**
A server administrator was asked to build a storage array with the highest possible capacity. Which of the following RAID levels should the administrator choose?

A. RAID 0
B. RAID 1
C. RAID 5
D. RAID 6

**Answer:** A

**Explanation:**
The RAID level that provides the highest possible capacity for a storage array is RAID 0. RAID 0 is a type of RAID level that provides performance enhancement by using striping. Striping means dividing data into blocks and distributing them across multiple disks to increase speed and capacity. RAID 0 does not provide any fault tolerance or redundancy, as it does not use any parity or mirroring techniques. RAID 0 uses all of the available disk space for data storage, without losing any space for overhead. Therefore, RAID 0 provides the highest possible capacity for a storage array, but also has the highest risk of data loss.
Reference: https://www.thinkmate.com/inside/articles/what-is-raid

**NEW QUESTION 248**
A server technician notices several of the servers in a data center are making loud noises. The servers are still working correctly, and no indicator lights show any issues. Which of the following should the technician do first to ensure the issues are corrected and the servers remain online?

A. Replace the drives.
B. Upgrade the firmware.
C. Establish a remote connection to the server.
D. Replace the fans.

**Answer:** A

**Explanation:**
The loud noises from the servers are most likely caused by failing hard disk drives, which can produce clicking or grinding sounds. Replacing the drives with new ones can prevent data loss and downtime. Replacing the drives can be done without shutting down the server if they are hot-swappable, which means they can be

removed and inserted while the server is running. References: CompTIA Server+ Certification Exam Objectives, Domain 3.0: Storage, Objective 3.1: Given a scenario, install, deploy, configure and update physical storage devices.

**NEW QUESTION 253**
A system administrator has been alerted to a zero-day vulnerability that is impacting a service enabled on a server OS. Which of the following would work BEST to limit an attacker from exploiting this vulnerability?

A. Installing the latest patches
B. Closing open ports
C. Enabling antivirus protection
D. Enabling a NIDS

**Answer:** A

**Explanation:**
The best way to limit an attacker from exploiting a zero-day vulnerability that is impacting a service enabled on a server OS is to install the latest patches. Patches are updates that fix bugs, improve security, or add features to software. Installing patches can help prevent attackers from exploiting known vulnerabilities that have been fixed by the software vendor. A zero-day vulnerability is a vulnerability that is unknown to the vendor or the public until it is exploited by an attacker. Therefore, installing patches as soon as they are available can reduce the window of opportunity for attackers to exploit zero-day vulnerabilities.Reference: https://www.ibm.com/cloud/learn/patch-management

**NEW QUESTION 257**
The network's IDS is giving multiple alerts that unauthorized traffic from a critical application server is being sent to a known-bad public IP address.
One of the alerts contains the following information: Exploit Alert
Attempted User Privilege Gain 2/2/07-3: 09:09 10.1.200.32
--> 208.206.12.9:80
This server application is part of a cluster in which two other servers are also servicing clients. The server administrator has verified the other servers are not sending out traffic to that public IP address. The IP address subnet of the application servers is 10.1.200.0/26. Which of the following should the administrator perform to ensure only authorized traffic is being sent from the application server and downtime is minimized? (Select two).

A. Disable all services on the affected application server.
B. Perform a vulnerability scan on all the servers within the cluster and patch accordingly.
C. Block access to 208.206.12.9 from all servers on the network.
D. Change the IP address of all the servers in the cluster to the 208.206.12.0/26 subnet.
E. Enable GPO to install an antivirus on all the servers and perform a weekly reboot.
F. Perform an antivirus scan on all servers within the cluster and reboot each server.

**Answer:** BF

**Explanation:**
The administrator should perform an antivirus scan on all servers within the cluster and reboot each server, and block access to 208.206.12.9 from all servers on the network. These actions will help to remove any malware that may have infected the application server and prevent any further unauthorized traffic to the known-bad public IP address. An antivirus scan can detect and remove malicious software that may be sending data to an external source, and a reboot can clear any temporary files or processes that may be related to the malware. Blocking access to 208.206.12.9 from all servers on the network can prevent any future attempts to communicate with the malicious IP address.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.4, Objective 3.4; Chapter 6, Lesson 6.2, Objective 6.2

**NEW QUESTION 258**
An administrator is troubleshooting a failure in the data center in which a server shut down/turned off when utility power was lost The server had redundant power supplies. Which of the following is the MOST likely cause of this failure?

A. The UPS batteries were overcharged.
B. Redundant power supplies require 220V power
C. Both power supplies were connected to the same power feed
D. The power supplies werenot cross-connected

**Answer:** C

**Explanation:**
The most likely cause of this failure is that both power supplies were connected to the same power feed, which means that they both lost power when utility power was lost. To prevent this from happening, redundant power supplies should be connected to different power feeds, preferably from different sources, such as a UPS or a generator. Verified References: [Redundant Power Supply Best Practices]

**NEW QUESTION 261**
A user logs in to a Linux server and attempts to run the following command: sudo emacs /root/file
However the user gets the following message:
User userid is not allowed to execute Temacs' on this server. Which of the following would BEST allow the user to find out which commands can be used?

A. visudo I grep userid
B. sudo -1 -U userid
C. cat /etc/passwd
D. userlist I grep userid

**Answer:** B

**Explanation:**
This is the best command to find out which commands can be used by a user with sudo privileges because it lists the allowed and forbidden commands for a given user or role. The -l option stands for list, and the -U option specifies the user name. The output of this command will show what commands can be executed with sudo by that user on that server.

References:https://www.sudo.ws/man/1.8.13/sudo.man.html

**NEW QUESTION 264**
Which of the following will correctly map a script to a home directory for a user based on username?

A. \\server\users$\username
B. \\server\%username%
C. \\server\FirstInitialLastName
D. \\server\$username$

**Answer:** B

**Explanation:**
The administrator should use \server%username% to correctly map a script to a home directory for a user based on username. %username% is an environment variable that represents the current user's name on a Windows system. By using this variable in the path of the script, the administrator can dynamically map the script to the user's home directory on the server. For example, if the user's name is John, the script will be mapped to \server\John.
Reference:
https://social.technet.microsoft.com/Forums/windows/en-US/07cfcb73-796d-48aa-96a9- 08280a1ef25a/ mapping-home-directory-with-username-variable?forum=w7itprogeneral

**NEW QUESTION 265**
A server administrator is instating a new server in a data center. The administrator connects the server to a midplane but does not connect any cables Which of the following types of servers is the administrator MOST likely installing?

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

**Answer:** D

**Explanation:**
A blade server is a type of server that is installed in a chassis or an enclosure that provides power, cooling, networking, and management features. The blade server does not have any cables attached to it, as it connects to the chassis through a midplane or a backplane. A blade server can save space, energy, and cost compared to other types of servers. Verified References: [Blade server], [Chassis]

**NEW QUESTION 268**
Which of the following is a system that scans outgoing email for account numbers, sensitive phrases, and other forms of Pll?

A. SIEM
B. DLP
C. HIDS
D. IPS

**Answer:** B

**Explanation:**
DLP stands for Data Loss Prevention and it is a system that scans outgoing email for account numbers, sensitive phrases, and other forms of PII (Personally Identifiable Information). DLP can help prevent data breaches, comply with regulations, and protect the privacy of customers and employees. DLP can also block, encrypt, or quarantine emails that contain sensitive data.References: https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives (Objective 3.2)

**NEW QUESTION 272**
A server shut down after an extended power outage. When power was restored, the system failed to start. A few seconds into booting, the Num Lock, Scroll Lock, and Caps Lock LEDs flashed several times, and the system stopped. Which of the following is the MOST likely cause of the issue?

A. The keyboard is defective and needs to be replaced.
B. The system failed before the display card initialized.
C. The power supply is faulty and is shutting down the system.
D. The NIC has failed, and the system cannot make a network connection.

**Answer:** B

**Explanation:**
This is the most likely cause of the issue because the keyboard LED flash indicates a POST error code. If the display card is not initialized, the system cannot show any error messages on the screen and will stop booting. References:https://www.computerhope.com/beep.htm#04

**NEW QUESTION 274**
An administrator is troubleshooting a failed NIC in an application server. The server uses DHCP to get all IP configurations, and the server must use a specific IP address. The administrator replaces the NIC, but then the server begins to receive a different and incorrect IP address. Which of the following will enable the server to get the proper IP address?

A. Modifying the MAC used on the DHCP reservation
B. Updating the local hosts file with the correct IP address
C. Modifying the WWNN used on the DHCP reservation
D. Updating the NIC to use the correct WWNN

**Answer:**

A

**Explanation:**
A DHCP reservation is a way to assign a specific IP address to a device based on its MAC address, which is a unique identifier for each network interface card (NIC). When the administrator replaced the NIC, the MAC address of the server changed, and the DHCP server no longer recognized it as the same device. Therefore, the DHCP server assigned a different IP address to the server, which was incorrect for the application. To fix this problem, the administrator needs to modify the DHCP reservation to use the new MAC address of the NIC, so that the server can get the proper IP address.
A WWNN (World Wide Node Name) is a unique identifier for a Fibre Channel node, which is a device that can communicate over a Fibre Channel network. A WWNN is not related to DHCP or IP addresses, and it is not used for DHCP reservations. Therefore, options B and D are incorrect.
Updating the local hosts file with the correct IP address (option C) is also incorrect, because it does not solve the problem of getting the correct IP address from the DHCP server. The hosts file is a local file that maps hostnames to IP addresses, and it is used to override DNS queries. However, it does not affect how the DHCP server assigns IP addresses to devices. Moreover, updating the hosts file manually on every device that needs to communicate with the server is not a scalable or efficient solution.
References:
? How to reserve IP Address in DHCP Server - Ask Ubuntu
? Static IP vs DHCP Reservation - The Tech Journal
? How to Configure DHCP Server Reservation in Windows … - ITIngredients

**NEW QUESTION 277**
.....

# 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