SK0-005 Dumps

CompTIA Server+ Certification Exam

https://www.certleader.com/SK0-005-dumps.html

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
A server technician is configuring the IP address on a newly installed server. The documented configuration specifies using an IP address of 10.20.10.15 and a default gateway of 10.20.10.254. Which of the following subnet masks would be appropriate for this setup?

A. 255.255.255.0
B. 255.255.255.128
C. 255.255.255.240
D. 255.255.255.254

Answer: A

Explanation:
The administrator should use a subnet mask of 255.255.255.0 for this setup. A subnet mask is a binary number that defines how many bits of an IP address are used for the network portion and how many bits are used for the host portion. The network portion identifies the specific network that the IP address belongs to, while the host portion identifies the specific device within that network. The subnet mask is usually written in dotted decimal notation, where each octet represents eight bits of the binary number. A 1 in the binary number means that the corresponding bit in the IP address is part of the network portion, while a 0 means that it is part of the host portion. For example, a subnet mask of 255.255.255.0 means that the first 24 bits (three octets) of the IP address are used for the network portion and the last 8 bits (one octet) are used for the host portion. This subnet mask allows up to 254 hosts per network ($2^8 - 2$). In this case, the IP address of 10.20.10.15 and the default gateway of 10.20.10.254 belong to the same network of 10.20.10.0/24 (where /24 indicates the number of bits used for the network portion), which can be defined by using a subnet mask of 255.255.255.0.

NEW QUESTION 3
A server administrator mounted a new hard disk on a Linux system with a mount point of
/newdisk. It was later determined that users were unable to create directories or files on the new mount point. Which of the following commands would successfully mount the drive with the required parameters?

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

Answer: C

Explanation:
The administrator should use the command mount –o remount,rw /newdisk to successfully mount the drive with the required parameters. The mount command is used to mount file systems on Linux systems. The –o option specifies options for mounting file systems. The remount option re-mounts an already mounted file system with different options. The rw option mounts a file system with read-write permissions. In this case,
/newdisk is a mount point for a new hard disk that was mounted with read-only permissions by default. To allow users to create directories or files on /newdisk, the administrator needs to re-mount /
Reference:
https://unix.stackexchange.com/QUESTION NO:s/149399/how-to-remount-as-read-write-a- specific-mount-of-device

NEW QUESTION 4
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 5
An administrator needs to reconfigure a teamed network connection on a server in a remote data center. Which of the following will offer the most resilient connection while performing this change?

A. Use of an 00B solution
B. Use of a crash cart
C. Use of a VNC console
D. Use of an RDP console

Answer: A

Explanation:
An out-of-band (OOB) solution is a method of accessing and managing a server remotely without using the network connection or the operating system of the server. An OOB solution can use a dedicated management port, a serial console, or a KVM switch to provide a resilient connection while performing changes to the network configuration of the server. An OOB solution is more reliable than a VNC or RDP console, which depend on the network and the operating system, and more convenient than a crash cart, which requires physical access to the server.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 2, Lesson 2.3, Objective 2.3

NEW QUESTION 6
A server administrator needs to deploy five VMs, all of which must have the same type of configuration. Which of the following would be the MOST efficient way to perform this task?

A. Snapshot a VM.
B. Use a physical host.
C. Perform a P2V conversion.
D. Use a VM template.

Answer: D

Explanation:
Deploying a virtual machine from a template creates a virtual machine that is a copy of the template. The new virtual machine has the virtual hardware, installed software, and other properties that are configured for the template.
Reference:https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vm_admin.doc/GUID-8254CD05-CC06-491D-BA56- A773A32A8130.html
The most efficient way to perform the task of deploying five VMs with the same type of configuration is to use a VM template. A template is a preconfigured virtual machine image that contains an operating system, applications, settings, and other components. A template can be used to create multiple identical or customized VMs quickly and easily, without having to install and configure each VM from scratch. A template can save time and ensure consistency across VMs.

NEW QUESTION 7
A server administrator is installing a new server that uses 40G0 network connectivity. The administrator needs to find the proper cables to connect the server to the switch. Which of the following connectors should the administrator use?

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

Answer: D

Explanation:
 QSFP+ is a type of connector that should be used to connect a server to a switch that uses 40G network connectivity. QSFP+ (Quad Small Form-factor Pluggable Plus) is a compact, hot-pluggable transceiver module that supports data rates up to 40 Gbps. QSFP+ modules can be used for various network protocols and media types, such as Ethernet, Fibre Channel, InfiniBand, or optical fiber. QSFP+ modules have a 38-pin edge connector and can be inserted into a QSFP+ port on a switch or a server. SFP+ (Small Form-factor Pluggable Plus) is a type of connector that supports data rates up to 10 Gbps, but not 40 Gbps. SFP+ modules have a 20-pin edge connector and can be inserted into an SFP+ port on a switch or a server. GBIC (Gigabit Interface Converter) is an older type of connector that supports data rates up to 1 Gbps, but not 40 Gbps. GBIC modules have an SC duplex connector and can be inserted into a GBIC port on a switch or a server. SFP (Small Form-factor Pluggable) is another older type of connector that supports data rates up to 1 Gbps or 4 Gbps, but not 40 Gbps. SFP modules have an LC duplex connector and can be inserted into an SFP port on a switch or a server. References: https://www.howtogeek.com/190014/virtualization-basics-understanding-techniques-and- fundamentals/ https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and- why-does-it-matter/ https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual-files/

NEW QUESTION 8
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 9
A company is implementing a check-in desk to heighten physical security. Which of the following access controls would be the most appropriate to facilitate this implementation?

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

Answer: D

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

NEW QUESTION 10
A server technician is deploying a server with eight hard drives. The server specifications call for a RAID configuration that can handle up to two drive failures but also allow for the least amount of drive space lost to RAID overhead. Which of the following RAID levels should the technician configure for this drive array?

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

Answer: C

Explanation:
The technician should configure RAID 6 for this drive array to meet the server specifications. RAID 6 is a type of RAID level that provides fault tolerance and performance enhancement by using striping and dual parity. Striping means dividing data into blocks and distributing them across multiple disks to increase speed and capacity. Parity means calculating and storing extra information that can be used to reconstruct data in case of disk failure. RAID 6 uses two sets of parity information foreach stripe, which are stored on different disks. This way, RAID 6 can handle up to two disk failures without losing any data or functionality. RAID 6 also allows for the least amount of drive space lost to RAID overhead compared to other RAID levels that can handle two disk failures, such as RAID 1+0 or RAID 0+1.
Reference:
https://www.booleanworld.com/raid-levels-explained/

NEW QUESTION 10
Which of the following script types would MOST likely be used on a modern Windows server OS?

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

Answer: D

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

NEW QUESTION 14
Which of the following testing exercises for disaster recovery is primarily used to discuss incident response strategies for critical systems without affecting production data?

A. Tabletcp
B. Backup recovery test
C. Lrverail over
D. Hot-site visit audit

Answer: A

Explanation:
A tabletop exercise is a type of disaster recovery testing exercise that is primarily used to discuss incident response strategies for critical systems without affecting production data. A tabletop exercise is a discussion-based session where team members meet in an informal, classroom setting to review their roles and responsibilities during an emergency and their responses to a hypothetical scenario. A facilitator guides the participants through the discussion and evaluates the strengths and weaknesses of the preparedness program. A tabletop exercise does not involve any actual deployment of resources oractivation of systems12. A backup recovery test (B) is a type of disaster recovery testing exercise that involves restoring data from backup media to verify its integrity and availability. A backup recovery test may affect production data if it is not performed on a separate environment. A live failover © is a type of disaster recovery testing exercise that involves switching operations from a primary site to a secondary site in case of a failure or disruption. A live failover may affect production data if it is not performed on a simulated environment. A hot-site visit audit (D) is a type of disaster recovery testing exercise that involves inspecting and evaluating a hot site, which is a backup location that has fully operational equipment and resources to resume business operations in case of a disaster. A hot-site visit audit does not

involve any discussion of incident response strategies or simulation of scenarios. References: 1
https://www.ready.gov/testing-exercises2 https://www.ready.gov/exercises

NEW QUESTION 17
A systems administrator is setting up a server on a LAN that uses an address space that follows the RFC 1918 standard. Which of the following IP addresses should the administrator use to be in compliance with the standard?

A. 11.251.196.241
B. 171.245.198.241
C. 172.16.19.241
D. 193.168.145.241

Answer: C

Explanation:
The administrator should use 172.16.19.241 as an IP address to be in compliance with RFC 1918 standard. RFC 1918 defines three ranges of IP addresses that are reserved for private internets, meaning they are not globally routable on the public Internet and can be used within an enterprise without any risk of conflict or overlap with other networks. These ranges are:
* 10.0.0.0 - 10.255.255.255 (10/8 prefix) 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
* 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
Out of these ranges, only 172.16.19.241 falls within one of them (172.16/12 prefix). The other options are either public IP addresses that belong to other organizations or networks (11.251.196.241, 171.245.198.241) or invalid IP addresses that do not conform to any standard (193.168.145.241).
Reference: https://whatis.techtarget.com/definition/RFC-1918

NEW QUESTION 19
Which of the following actions should a server administrator take once a new backup scheme has been configured?

A. Overwrite the backups
B. Clone the configuration
C. Run a restore test
D. Check the media integrity

Answer: C

Explanation:
The action that the server administrator should take once a new backup scheme has been configured is to run a restore test. A restore test is a process of verifying that the backup data can be successfully recovered and restored to its original location or a different location. A restore test can help ensure that the backup scheme is working properly, that the backup data is valid and consistent, and that there are no errors or issues during the recovery process. A restore test should be performed periodically and after any changes to the backup configuration or environment.

NEW QUESTION 21
A technician is laying out a filesystem on a new Linux server. Which of the following tools would work BEST to allow the technician to increase a partition's size in the future without reformatting it?

A. LVM
B. DiskPart
C. fdisk
D. Format

Answer: A

Explanation:
LVM (Logical Volume Manager) is a tool that allows the technician to increase a partition's size in the future without reformatting it on a Linux server. LVM creates logical volumes that can span across multiple physical disks or partitions and can be resized dynamically without losing data. LVM also provides other features such as snapshots, encryption, and RAID. DiskPart, fdisk, and Format are tools that can be used to partition and format disks, but they do not allow increasing a partition's size without reformatting it. References: https://www.howtogeek.com/howto/40702/how-to-manage-and- use-lvm-logical-volume-management-in-ubuntu/ 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
A server administrator needs to harden a server by only allowing secure traffic and DNS inquiries. A port scan reports the following ports are open:

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

Answer: D

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

NEW QUESTION 25
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 27
A server room contains ten physical servers that are running applications and a cluster of three dedicated hypervisors. The hypervisors are new and only have 10% utilization. The Chief Financial Officer has asked that the IT department do what it can to cut back on power consumption and maintenance costs in the data center. Which of the following would address the request with minimal server downtime?

A. Unplug the power cables from the redundant power supplies, leaving just the minimum required.
B. Convert the physical servers to the hypervisors and retire the ten servers.
C. Reimage the physical servers and retire all ten servers after the migration is complete.
D. Convert the ten servers to power-efficient core editions.

Answer: B

Explanation:
This option would reduce power consumption and maintenance costs by consolidating the physical servers into virtual machines on the hypervisors. This would also free up space and resources in the data center. The other options would either not address the request, increase power consumption, or require more maintenance.

NEW QUESTION 31
Users have noticed a server is performing below Baseline expectations. While diagnosing me server, an administrator discovers disk drive performance has degraded. The administrator checks the diagnostics on the RAID controller and sees the battery on me controller has gone bad. Which of the following is causing the poor performance on the RAID array?

A. The controller has disabled the write cache.
B. The controller cannot use all the available channels.
C. The drive array is corrupt.
D. The controller has lost its configuration.

Answer: A

Explanation:
The write cache is a feature of some RAID controllers that allows them to temporarily store data in a fast memory buffer before writing it to the disk drives. This improves the performance and efficiency of write operations, especially for random and small writes. However, if the battery on the controller goes bad, the controller may disable the write cache to prevent data loss in case of a power failure. This can degrade the disk drive performance significantly, as every write operation will have to wait for the disk drives to complete. References: https://www.dell.com/support/kbdoc/en-us/000131486/understanding-raid-controller-battery-learn-cyclehttps://www.techrepublic.com/article/understanding-raid-controller-write-cache/

NEW QUESTION 36
A technician needs to provide a VM with high availability. Which of the following actions should the technician take to complete this task as efficiently as possible?

A. Take a snapshot of the original VM
B. Clone the original VM
C. Convert the original VM to use dynamic disks
D. Perform a P2V of the original VM

Answer: B

Explanation:
Cloning the original VM is the most efficient way to provide a VM with high availability. Cloning is the process of creating an exact copy of a VM, including its configuration, operating system, applications, and data. A cloned VM can be used as a backup or a replica of the original VM, and can be powered on and run independently. Cloning can be done quickly and easily using vSphere tools or other third-party software. By cloning the original VM and placing it on a different host server or availability zone, the
technician can ensure that if the original VM fails, the cloned VM can take over its role and provide uninterrupted service to the users and applications.

NEW QUESTION 41
A technician noted the RAID hard drives were functional while troubleshooting a motherboard failure. The technician installed a spare motherboard with similar specifications and used the original components. Which of the following should the technician do to restore operations with minimal downtime?

A. Reinstall the OS and programs.

B. Configure old drives to RAID.
C. Reconfigure the RAID.
D. Install from backup.

Answer: C

Explanation:
RAID (Redundant Array of Independent Disks) is a technology that combines multiple hard drives into a logical unit that provides improved performance, reliability, or capacity. RAID can be implemented by hardware, software, or a combination of both. Hardware RAID uses a dedicated controller to manage the RAID array, while software RAID uses the operating system or a driver to do the same1.
In this scenario, the technician noted that the RAID hard drives were functional while troubleshooting a motherboard failure. This means that the data on the drives was not corrupted or lost. However, the technician installed a spare motherboard with similar specifications and used the original components. This means that the new motherboard may not have the same RAID configuration as the old one, or it may not recognize the existing RAID array at all. Therefore, the technician needs to reconfigure the RAID in order to restore operations with minimal downtime.

NEW QUESTION 42
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 44
A server is only able to connect to a gigabit switch at 100Mb. Other devices are able to access the network port at full gigabit speeds, and when the server is brought to another location, it is able to connect at full gigabit speed. Which of the following should an administrator check first?

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

Answer: C

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

NEW QUESTION 47
An organization recently experienced power outages. The administrator noticed the server did not have enough time to shut down properly. After the outages, the administrator had additional batteries installed in the UPS. Which of the following best describes the solution the administrator implemented?

A. The solution reduced shutdown time.
B. The solution improved load balancing,
C. The solution increased power out.
D. The solution extended runtime.

Answer: D

Explanation:
The solution the administrator implemented extended runtime. Runtime is the amount of time that a UPS can provide backup power to a server in case of a power outage. By installing additional batteries in the UPS, the administrator increased the capacity and duration of the backup power, allowing the server more time to shut down properly. References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 1, Lesson 1.4, Objective 1.4

NEW QUESTION 48
An organization is donating its outdated server equipment to a local charity. Which of the following describes what the organization should do BEFORE donating the equipment?

A. Remove all the data from the server drives using the least destructive method.
B. Repurpose and recycle any usable server components.
C. Remove all the components from the server.
D. Review all company polices.

Answer: D

Explanation:
Before donating the outdated server equipment to a local charity, the organization should review all company policies regarding data security, asset disposal, and social responsibility. This can help ensure that the donation complies with the legal and ethical standards of the organization and does not pose any risk to its reputation or operations. Verified References: [Data security], [Asset disposal], [Social responsibility]

NEW QUESTION 51
An administrator is configuring a server to communicate with a new storage array. To do so, the administrator enters the WWPN of the new array in the server's storage configuration. Which of the following technologies is the new connection using?

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

Answer: A

Explanation:
Reference:https://docs.oracle.com/cd/E26996_01/E18549/html/BABHBFHA.html

NEW QUESTION 56
After configuring IP networking on a newly commissioned server, a server administrator installs a straight- through network cable from the patch panel to the switch. The administrator then returns to the server to test network connectivity using the ping command. The partial output of the ping and ipconfig commands are displayed below:

```
ipconfig/all

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

Pinging 192.168.1.2 with 32 bytes of data:

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

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

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

Answer: D

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

NEW QUESTION 57
A server technician has received reports of database update errors. The technician checks the server logs and determines the database is experiencing synchronization errors. To attempt to correct the errors, the technician should FIRST ensure:

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

Answer: C

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

NEW QUESTION 58
Users cannot access a new server by name, but the server does respond to a ping request using its IP address. All the user workstations receive their IP information from a DHCP server. Which of the following would be the best step to perform NEXT?

A. Run the tracert command from a workstation.
B. Examine the DNS to see if the new server record exists.
C. Correct the missing DHCP scope.
D. Update the workstation hosts file.

Answer: B

Explanation:
If users cannot access a new server by name, but the server does respond to a ping request using its IP address, it means that there is a problem with name resolution. The DNS (Domain Name System) is a service that maps hostnames to IP addresses and vice versa. Therefore, the best step to perform next is to examine the DNS to see if the new server record exists and matches its IP address. If not, the DNS record needs to be added or updated accordingly. Running the tracert command from a workstation would not help with name resolution, as it only shows the route taken by packets to reach a destination by IP address. Correcting the missing DHCP scope would not help either, as DHCP (Dynamic Host Configuration Protocol) only assigns IP addresses and other network settings to clients, but does not resolve names. Updating the workstation hosts file would be a temporary workaround, but not a permanent solution, as it would require manually editing every workstation's hosts file with the new server's name and IP address. References: https://www.howtogeek.com/164981/how-to-use-nslookup-to-check- domain-name-information-in-microsoft-windows/https://www.howtogeek.com/howto/27350/beginner-geek-how-to-edit-your-hosts- file/

NEW QUESTION 59
Users at a company work with highly sensitive data. The security department implemented an administrative and technical control to enforce least-privilege access assigned to files. However, the security department has discovered unauthorized data exfiltration. Which of the following is the BEST way to protect the data from leaking?

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

Answer: C

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

NEW QUESTION 60
A server administrator receives the following output when trying to ping a local host:

```
ping imhrh-vc.net
Reply from imhrh-vc.net. Destination host unreachable.
Reply from imhrh-vc.net. Destination host unreachable.
Reply from imhrh-vc.net. Destination host unreachable.
Reply from imhrh-vc.net. Destination host unreachable.
```

Which of the following is MOST likely the issue?

A. Firewall
B. DHCP
C. DNS
D. VLAN

Answer: A

Explanation:
A firewall is a network device or software that filters and controls the incoming and outgoing traffic based on predefined rules. A firewall can block or allow certain types of packets, ports, protocols, or IP addresses. The output of the ping command shows that the local host is unreachable, which means that there is no network connectivity between the source and the destination. This could be caused by a firewall that is blocking the ICMP (Internet Control Message Protocol) packets that ping uses to test the connectivity.References: https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives (Objective 2.2)

NEW QUESTION 63
A datacenter technician is attempting to troubleshoot a server that keeps crashing. The server runs normally for approximately five minutes, but then it crashes. After restoring the server to operation, the same cycle repeats. The technician confirms none of the configurations have changed, and the load on the server is steady from power-on until the crash. Which of the following will MOST likely resolve the issue?

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

Answer: C

Explanation:
The most likely solution to resolve the issue of the server crashing after running normally for approximately five minutes is to reinstall the heat sink with new thermal paste. A heat sink is a device that dissipates heat from a component, such as a processor or a graphics card, by transferring it to a cooling medium, such as air or liquid. A heat sink is usually attached to the component using thermal paste, which is a substance that fills the gaps between the heat sink and the

component and improves thermal conductivity. Thermal paste can degrade over time and lose its effectiveness, resulting in overheating and performance issues. If a server crashes after running for a short period of time, it may indicate that the processor is overheating due to insufficient cooling. To resolve this issue, the technician should remove the heat sink, clean the old thermal paste, apply new thermal paste, and reinstall the heat sink.

NEW QUESTION 65
Network connectivity to a server was lost when it was pulled from the rack during maintenance. Which of the following should the server administrator use to prevent this situation in the future?

A. Cable management
B. Rail kits
C. A wireless connection
D. A power distribution unit

Answer: A

Explanation:
The server administrator should use cable management to prevent network connectivity loss when pulling a server from the rack during maintenance. Cablemanagement is a practice of organizing and securing the cables that connect various devices and components in a system. Cable management can help improve airflow, reduce clutter, prevent tangling, and avoid accidental disconnection or damage of cables. Cable management can be done using various tools and techniques, such as cable ties, cable trays, cable labels, cable organizers, or cable ducts.

NEW QUESTION 70
A server administrator has connected a new server to the network. During testing, the administrator discovers the server is not reachable via server but can be accessed by IP address. Which of the following steps should the server administrator take NEXT? (Select TWO).

A. Check the default gateway.
B. Check the route tables.
C. Check the hosts file.
D. Check the DNS server.
E. Run the ping command.
F. Run the tracert command

Answer: CD

Explanation:
If the server is not reachable by name but can be accessed by IP address, it means that there is a problem with name resolution. The hosts file and the DNS server are both responsible for mapping hostnames to IP addresses. Therefore, the server administrator should check these two files for any errors or inconsistencies that might prevent the server from being resolved by name. References: https://www.howtogeek.com/662249/how-to-edit-the-hosts-file-on-linux/ https://www.howtogeek.com/164981/how-to-use-nslookup-to-check-domain-name-information-in-microsoft-windows/

NEW QUESTION 73
In which of the following media rotation schemes are daily, weekly, and monthly backup media utilized in a first-in, first-out method?

A. Waterfall
B. Synthetic full
C. Tower of Hanoi
D. Grandfather-father-son

Answer: D

Explanation:
Grandfather-father-son (GFS) is a common backup rotation scheme that uses daily, weekly, and monthly backup media in a first-in, first-out (FIFO) method. The daily backups are rotated on a 3-months basis using a FIFO system as above. The weekly backups are similarly rotated on a bi-yearly basis, and the monthly backups are rotated on an annual basis. The oldest backup media in each cycle are overwritten by the newest ones. This scheme provides multiple versions of backup data at different intervals, allowing for flexible restoration options. Waterfall is another name for GFS. Synthetic full is a backup method that combines an initial full backup with subsequent incremental backups to create a new full backup without transferring all data again. Tower of Hanoi isanother backup rotation scheme that uses an algorithm based on moving disks between three pegs. References:
? https://en.wikipedia.org/wiki/Backup_rotation_scheme

NEW QUESTION 74
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 75
Users ate experiencing issues when trying to access resources on multiple servers. The servers are virtual and run on an ESX server. A systems administrator is investigating but is unable to connect to any of the virtual servers. When the administrator connects to the host, a purple screen with while letters appears. Which

of the following troubleshooting steps should the administrator perform FIRST?

A. Check the power supplies
B. Review the log files.
C. Reinstall the ESX server.
D. Reseat the processors.

Answer: B

Explanation:
A purple screen with white letters on an ESX server indicates a kernel panic, which is a fatal error that causes the system to crash and stop functioning3. The first troubleshooting step that an administrator should perform is to review the log files, which may contain information about the cause of the error, such as hardware failures, software bugs, or configuration issues4. Checking the power supplies (A) may not be relevant, as the system is still displaying a screen. Reinstalling the ESX server © or reseating the processors (D) are drastic measures that may result in data loss or further damage, and should only be attempted after ruling out other possible causes. References: 3
https://kb.vmware.com/s/article/10145084 https://www.altaro.com/vmware/vmware-esxi-purple-screen-death/

NEW QUESTION 80
Which of the following licenses would MOST likely include vendor assistance?

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

Answer: D

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

NEW QUESTION 82
Which of the following is the MOST appropriate scripting language to use for a logon script for a Linux box?

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

Answer: B

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

NEW QUESTION 86
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 89
A server administrator has been asked to implement a password policy that will help mitigate the chance of a successful brute-force attack. Which of the following password policies should the administrator implement first?

A. Lockout
B. Length
C. Complexity
D. Minimum age

Answer: B

Explanation:
Password length is the first password policy that the administrator should implement to help mitigate the chance of a successful brute-force attack. A brute-force attack is a method of guessing passwords by trying all possible combinations of characters until the correct one is found. The longer the password, the more combinations there are, and the more time and resources it takes to crack it. Therefore, password length is a key factor in password strength and security.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.2, Objective 3.2

NEW QUESTION 93
A server administrator needs to create a new folder on a file server that only specific users can access. Which of the following BEST describes how the server administrator can accomplish this task?

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

Answer: C

Explanation:
The top portion of the dialog box lists the users and/or groups that have access to the file or folder.
Reference:https://www.uwec.edu/kb/article/drives-establishing-windows-file-and-folder- level-permissions/

NEW QUESTION 95
A server administrator has configured a web server. Which of the following does the administrator need to install to make the website trusted?

A. PKI
B. SSL
C. LDAP
D. DNS

Answer: B

Explanation:
The administrator needs to install SSL to make the website trusted. SSL stands for Secure Sockets Layer, which is an encryption-based Internet security protocol that ensures privacy, authentication, and data integrity in web communications. SSL enables HTTPS (Hypertext Transfer Protocol Secure), which is a secure version of HTTP (Hypertext Transfer Protocol) that encrypts the data exchanged between a web browser and a web server. SSL also uses digital certificates to verify the identity of the web server and establish trust with the web browser. A web server that implements SSL has HTTPS in its URL instead of HTTP and displays a padlock icon or a green bar in the browser's address bar.

NEW QUESTION 97
A technician recently applied a critical OS patch to a working sever. After rebooting, the technician notices the server Is unable to connect to a nearby database server. The technician validates a connection can be made to thedatabasefrom another host. Which of the following is the best NEXT step to restore connectivity?

A. Enable HIDS.
B. Change the service account permissions.
C. Check the host firewall I rule.
D. Roll back the applied patch.

Answer: C

Explanation:
A host firewall is a software that controls the incoming and outgoing network traffic on a server based on predefined rules and filters. It can block or allow certain ports, protocols, or addresses that are used for communication with other servers or devices. If a server is unable to connect to another server after applying a patch, it is possible that the patch changed or added a firewall rule that prevents the connection. The administrator should check the host firewall rule and modify it if necessary to restore connectivity. Verified References: [Host firewall], [Network connection]

NEW QUESTION 100
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 101
Which of the following BEST describes overprovisioning in a virtual server environment?

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

Answer: A

Explanation:
 This is the best definition of overprovisioning in a virtual server environment because it means allocating more CPU, memory, disk, or network resources to the virtual machines than what is actually available on the physical host. This can lead to performance issues and resource contention.
References:https://www.hpe.com/us/en/insights/articles/10-virtualization-mistakes-everyone-makes-1808.html

NEW QUESTION 102
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 107
A remote physical server is unable to communicate to the network through the available NICs, which were misconfigured. However, the server administrator is still able to configure theserver remotely. Which of the following connection types is the server administrator using to access the server?

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

Answer: A

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

NEW QUESTION 108
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 113
Two developers are working together on a project, and they have built out a set of snared servers that both developers can access over the internet. Which of the following cloud models is this an example of?

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

Answer: B

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

NEW QUESTION 116
An administrator notices nigh traffic on a certain subnetand wouldlike to identify the source of the traffic. Which of the following tools should the administrator utilize?

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

Answer: D

Explanation:
A sniffer is a tool that captures and analyzes network traffic on a subnet or a network interface. It can help identify the source, destination, protocol, and content of the traffic and detect any anomalies or issues on the network. Verified References: [Sniffer], [Network traffic]

NEW QUESTION 118
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 119
A technician is connecting a server's secondary NIC to a separate network. The technician connects the cable to the switch but then does not see any link lights on the NIC. The technician confirms there is nothing wrong on the network or with the physical connection. Which of the following should the technician perform NEXT?

A. Restart the server
B. Configure the network on the server
C. Enable the port on the server
D. Check the DHCP configuration

Answer: C

Explanation:
The next thing that the technician should perform is to enable the port on the server. A port is a logical endpoint that identifies a specific service or application on a network device. A port can be enabled or disabled depending on whether the service or application is running or not. If a port is disabled on a server, it means that the server cannot send or receive any network traffic on that port, which can prevent communication with other devices or services that use that port. In this case, if port 389 is disabled on the server, it means that the server cannot use LDAP to access or modify directory services over a network. To resolve this issue, the technician should enable port 389 on the server using commands such as netsh or iptables.

NEW QUESTION 124
A server administrator wants to run a performance monitor for optimal system utilization. Which of the following metrics can the administrator use for monitoring? (Choose two.)

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

Answer: AE

Explanation:

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

NEW QUESTION 127
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 131
A security analyst completed a port scan of the corporate production-server network. Results of the scan were then provided to a systems administrator for immediate action. The following table represents the requested changes:

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

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

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

Answer: E

Explanation:
Port 53 is the standard port for DNS (Domain Name System) queries and responses. DNS is a service that translates domain names (such as www.example.com) into IP addresses (such as 192.0.2.1) and vice versa. DNS is essential for internet connectivity, as it allows users and applications to access websites and other online resources by using human- readable names instead ofnumerical addresses1.
The DNSSrv server is a DNS server that provides name resolution for the corporate network. If port 53 is blocked on this server, it will not be able to communicate with other DNS servers or clients, and the name resolution will fail. This will prevent users from accessing any websites or online services that rely on domain names, such as web browsers, email clients, or cloud applications. Therefore, port 53 must remain open on DNSSrv to allow DNS traffic to flow.

NEW QUESTION 133
Several new components have been added to a mission-critical server, and corporate policy states all new components must meet server hardening requirements. Which of the following should be applied?

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

Answer: B

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

NEW QUESTION 134
An administrator discovers a Bash script file has the following permissions set in octal notation;
777
Which of the following is the MOST appropriate command to ensure only the root user can modify and execute the script?

A. chmod go-rw>:
B. chmod u=rwx
C. chmod u+wx

D. chmod g-rwx

Answer: A

Explanation:
chmod is a command-line tool that changes the permissions of files and directories in Linux and Unix systems. chmod go-rwx means to remove read, write, and execute permissions for group and other users from a file or directory. This can ensure only the root user can modify and execute the script, since root user has full access to all files and directories regardless of their permissions. References:https://linux.die.net/man/1/chmod

NEW QUESTION 136
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 141
A technician is sizing a new server and, for service reasons, needs as many hot-swappable components as possible. Which of the following server components can most commonly be replaced without downtime? (Select three).

A. Drives
B. Fans
C. CMOSIC
D. Processor
E. Power supplies
F. Motherboard
G. Memory
H. BIOS

Answer: ABE

Explanation:
Drives, fans, and power supplies are server components that can most commonly be replaced without downtime if they are hot-swappable. Hot-swappable components can be removed and inserted while the server is running, without affecting its operation or performance. Drives store data and applications, fans cool down the server components, and power supplies provide electricity to the server. Replacing these components can prevent data loss, overheating, or power failure. References: CompTIA Server+ Certification Exam Objectives, Domain 2.0: Hardware, Objective 2.2: Given a scenario, install, configure and maintain server components.

NEW QUESTION 143
An administrator needs to perform bare-metal maintenance on a server in a remote datacenter. Which of the following should the administrator use to access the server's console?

A. IP KVM
B. VNC
C. A crash cart
D. RDP
E. SSH

Answer: A

Explanation:
The administrator should use an IP KVM to access the server's console remotely for bare-metal maintenance. An IP KVM stands for Internet Protocol Keyboard Video Mouse, which is a device that allows remote control of a server's keyboard, video, and mouse over a network connection, such as LAN or Internet. An IP KVM enables an administrator to perform tasks such as BIOS configuration, boot sequence selection, operating system installation, etc., without being physically present at the server location. The other options are not suitable for bare-metal maintenance because they require either physical access to the server (a crash cart) or an operating system running on the server (VNC, RDP, SSH). A crash cart is a mobile unit that contains a monitor, keyboard, mouse, and cables that can be plugged into a server for direct access to its console. VNC stands for Virtual Network Computing, which is a software that allows remote desktop sharing and control over a network connection using a graphical user interface (GUI). RDP stands for Remote Desktop Protocol, which is a protocol that allows remote desktop access and control over a network connection using a GUI or command-line interface (CLI). SSH stands for Secure Shell, which is a protocol that allows secure remote login and command execution over a network connection using a CLI.

NEW QUESTION 146
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 149
A technician has moved a data drive from a new Windows server to an order 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. Thedisk uses GPT.
B. Thepartition is formatted with ext4.
C. The -partition is formatted with FAT32.
D. Thedisk uses MBn.

Answer: A

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. However, GPT is not compatible with older versions of Windows, such as Windows XP or Windows Server 2003, which use MBR (Master Boot Record) as the partitioning scheme. If a disk uses GPT, it may not be recognized or accessible by an older Windows server. Verified References: [GPT], [MBR]

NEW QUESTION 154
An administrator has been asked to increase the storage capacity of a stand-alone file server but no further expansion slots are available. Whichof the following would be the FASTEST solution to implement with no downtime?

A. Configure a RAID array.
B. Replace the current drives with higher-capacity disks.
C. Implement FCoE for more storage capacity.
D. Connect the server to a SAN

Answer: D

Explanation:
 A SAN (Storage Area Network) is a network of storage devices that can provide shared storage capacity to multiple servers. By connecting the server to a SAN, the administrator can increase the storage capacity of the server without adding any internal disks or expansion cards. This solution can be implemented quickly and without any downtime. Verified References: [What is a SAN and how does it differ from NAS?]
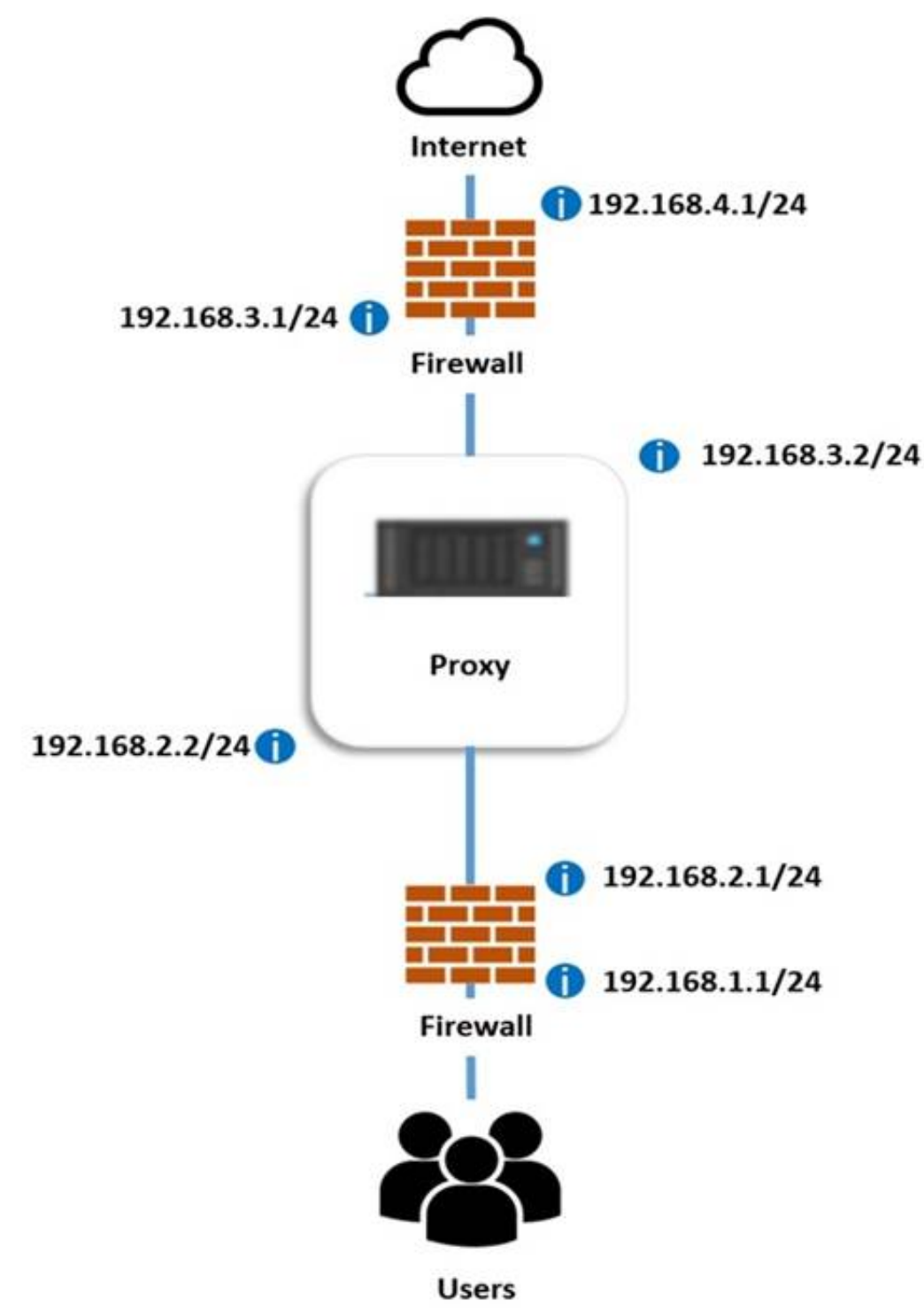
NEW QUESTION 159
HOTSPOT
A systems administrator deployed a new web proxy server onto the network. The proxy server has two interfaces: the first is connected to an internal corporate firewall, and the second is connected to an internet-facing firewall. Many users at the company are reporting they are unable to access the Internet since the new proxy was introduced. Analyze the network diagram and the proxy server's host routing table to resolve the Internet connectivity issues.
INSTRUCTIONS
Perform the following steps:
* 1. Click on the proxy server to display its routing table.
* 2. Modify the appropriate route entries to resolve the Internet connectivity issue.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Proxy Server Routing Table

Destination	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	▼ 192.168.3.0 192.168.4.0 192.168.1.1 192.168.2.0 192.168.1.0 192.168.4.1 192.168.2.1 0.0.0.0 192.168.3.1 255.255.255.0 192.168.3.2 192.168.2.2	▼ 192.168.4.1 192.168.1.1 192.168.3.0 192.168.1.0 192.168.2.2 0.0.0.0 192.168.3.1 255.255.255.0 192.168.3.2 192.168.4.0 192.168.2.1 192.168.2.0
192.168.1.0	255.255.255.0	▼ 192.168.3.0 192.168.4.0 192.168.1.1 192.168.2.0 192.168.1.0 192.168.4.1 192.168.2.1 0.0.0.0 192.168.3.1 255.255.255.0 192.168.3.2 192.168.2.2	▼ 192.168.4.1 192.168.1.1 192.168.3.0 192.168.1.0 192.168.2.2 0.0.0.0 192.168.3.1 255.255.255.0 192.168.3.2 192.168.4.0 192.168.2.1 192.168.2.0

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Proxy Server Routing Table

Destination	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	▼	▼
		192.168.3.0	192.168.4.1
		192.168.4.0	192.168.1.1
		192.168.1.1	192.168.3.0
		192.168.2.0	192.168.1.0
		192.168.1.0	192.168.2.2
		192.168.4.1	0.0.0.0
		0.0.0.0	192.168.3.1
		192.168.3.1	255.255.255.0
		255.255.255.0	192.168.3.2
		192.168.3.2	192.168.4.0
		192.168.2.2	192.168.2.1
			192.168.2.0
192.168.1.0	255.255.255.0	▼	▼
		192.168.3.0	192.168.4.1
		192.168.4.0	192.168.1.1
		192.168.1.1	192.168.3.0
		192.168.2.0	192.168.1.0
		192.168.1.0	192.168.2.2
		192.168.4.1	0.0.0.0
		192.168.2.1	192.168.3.1
		0.0.0.0	255.255.255.0
		192.168.3.1	192.168.3.2
		255.255.255.0	192.168.4.0
		192.168.3.2	192.168.2.1
		192.168.2.2	192.168.2.0

NEW QUESTION 162

A remote, embedded IoT server is having a Linux OS upgrade installed. Which of the following is the best method to stage the new media for the default boot device of the server?

A. Copy and send an SSD to the site.
B. Copy and send a DVD to the site.
C. Copy and send a SATA drive to the site.
D. Copy and send a microSD card to the site.

Answer: D

Explanation:
A microSD card is the best method to stage the new media for the default boot device of a remote embedded IoT server that is having a Linux OS upgrade installed. A microSD card is a small and portable storage device that can store large amounts of data. It can be easily inserted into the slot of an embedded IoT server, which is a small and low-power device that performs specific tasks and connects to other devices over a network. A microSD card can also be formatted with different file systems, such as FAT32 or ext4, which are compatible with Linux OS. References: CompTIA Server+ Certification Exam Objectives, Domain 4.0: Networking, Objective 4.3: Given a scenario, configure servers for IoT applications.

NEW QUESTION 166

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

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

Answer: AC

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

NEW QUESTION 167

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 168
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 172
Hosting data in different regional locations but not moving it for long periods of time describes:

A. a cold site.
B. data at rest.
C. on-site retention.
D. off-site storage.

Answer: B

Explanation:
Data at rest refers to data that is stored in a persistent state on any device or media, such as hard drives, tapes, or cloud storage. Data at rest does not move for long periods of time unless it is accessed or modified by authorized users or applications. A cold site (A) is a backup location that has minimal or no equipment and resources to resume business operations in case of a disaster. On-site retention © is a policy of keeping backup data on premises for a certain period of time before transferring it to an off-site location.
Off-site storage (D) is a method of storing backup data in a remote location that is physically or logically separated from the primary site. References: https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest https://www.techopedia.com/definition/144/cold-site https://www.enterprisestorageforum.com/backup/onsite-offsite- backup.htmlhttps://www.techopedia.com/definition/24195/offsite-storage

NEW QUESTION 174
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 179
A server administrator has a system requirement lo install the virtual OS on Dare metalhardware.Which of the following hypervisor virtualization technologies should the administrator use to BEST meet the system requirements? (Select TWO)

A. Host
B. Template
C. Clone
D. Type1
E. Type2
F. Guest

Answer: BD

Explanation:
A template is a preconfigured virtual machine image that can be used to create new virtual machines quickly and easily. A template can include the operating

system, applications, settings, and data that are required for a specific purpose or role. A type 1 hypervisor is a virtualization technology that runs directly on bare metal hardware, without requiring an underlying operating system. A type 1 hypervisor can providebetter performance, security, and isolation for virtual machines than a type 2 hypervisor, which runs on top of an operating system. Verified References: [Template], [Type 1 hypervisor]

NEW QUESTION 182
After installing a new file server, a technician notices the read times for accessing the same file are slower than the read times for other file servers.
Which of the following is the first step the technician should take?

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

Answer: B

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

NEW QUESTION 183
An administrator is only able to log on to a server with a local account. The server has been successfully joined to the domain and can ping other servers by IP address. Which of the following locally defined settings is MOST likely misconfigured?

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

Answer: C

Explanation:
 This is the most likely misconfigured setting because DNS is the service that resolves hostnames to IP addresses and vice versa. If the DNS server is incorrect or unreachable, the administrator will not be able to log on to the server with a domain account because the server will not be able to authenticate with the domain controller.
References:https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/dns-troubleshooting

NEW QUESTION 186
A hardware technician is installing 19 1U servers in a 42 the following unit sizes should be allocated per server?

A. 1U
B. 2U
C. 3U
D. 4U

Answer: A

Explanation:
 1U stands for one unit and it is a standard unit of measurement for rack- mounted servers. It is equal to 1.75 inches (4.45 cm) in height. A 42U rack can accommodate 42 1U servers or a combination of servers with different unit sizes. Therefore, the unit size per server should be 1U if there are 19 1U servers in a 42U rack.References: https://www.comptia.org/training/resources/exam-objectives/comptia- server-sk0-005-exam-objectives (Objective 1.2)

NEW QUESTION 189
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 190
A backup application is copying only changed files each time it runs. During a restore, however, only a single file is used. Which of the following backup methods does this describe?

A. Open file
B. Synthetic full

C. Full incremental
D. Full differential

Answer: B

Explanation:
 This is the best description of a synthetic full backup method because it creates a full backup by combining previous incremental backups with the latest backup. An incremental backup copies only the files that have changed since the last backup, while a full backup copies all the files. A synthetic full backup reduces the storage space and network bandwidth required for backups, while also simplifying the restore process by using a single file.References:https://www.veritas.com/support/en_US/doc/129705091- 129705095-0/br731_wxrt-tot_v131910378-129705095

NEW QUESTION 192
A server technician is installing a Windows server OS on a physical server. The specifications for the installation call for a 4TB data volume. To ensure the partition is available to the OS, the technician must verify the:

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

Answer: B

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

NEW QUESTION 195
Which of the following is an architectural reinforcement that is used to attempt to conceal the exterior of an organization?

A. Fencing
B. Bollards
C. Camouflage
D. Reflective glass

Answer: C

Explanation:
Camouflage is an architectural reinforcement that is used to attempt to conceal the exterior of an organization. Camouflage is a technique of blending in with the surroundings or disguising the appearance of a building or facility to make it less noticeable or identifiable. Camouflage can reduce the visibility and attractiveness of a target for potential attackers or intruders. 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 197
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 200
A user has been unable to authenticate to the company's external, web-based database after clicking a link in an email that required the user to change the account password. Which of the following steps should the company take next?

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

Answer: A

Explanation:
The user has likely fallen victim to a phishing scam, which is a fraudulent attempt to obtain sensitive information, such as passwords, by disguising as a legitimate entity. The link in the email that required the user to change the account password was probably a fake website that mimicked the company's external database, and captured the user's credentials when they entered them. This could compromise the security and integrity of the company's data, as well as the user's

identity and privacy12.
The company should take immediate action to prevent further damage and investigate the incident. The first step is to disable the user's account and inform the security team. Disabling the user's account can prevent unauthorized access to the external database by the attackers, who may use the stolen credentials to log in and manipulate or steal data. Informing the security team can alert them of the breach and allow them to take appropriate measures, such as scanning for malware, changingpasswords, notifying other users, and reporting the incident34.

NEW QUESTION 203
An administrator has been troubleshooting a server issue. The administrator carefully questioned the users and examined the available logs. Using this information, the administrator was able to rule out several possible causes and develop a theory as to what the issue might be. Through further testing, the administrator's theory proved to be correct. Which of the following should be the next step to troubleshoot the issue?

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

Answer: D

Explanation:
The next step to troubleshoot the issue after developing and testing a theory is to establish an action plan. This involves identifying the steps needed to implement the solution, estimating the time and resources required, and evaluating the potential risks and impacts of the solution. Documenting the findings and actions, escalating the issue to the management team, or implementing the solution are steps that should be done after establishing an action plan. References: [CompTIA Server+ Certification Exam Objectives], Domain 6.0: Disaster Recovery, Objective 6.2: Explain troubleshooting theory and methodologies.

NEW QUESTION 208
Which of the following open ports should be closed to secure the server properly? (Choose two.)

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

Answer: AC

Explanation:
The administrator should close ports 21 and 23 to secure the server properly. Port 21 is used for FTP (File Transfer Protocol), which is an unsecure protocol that allows file transfer between a client and a server over a network connection. FTP does not encrypt the data or the credentials that are transmitted, making them vulnerable to interception or modification by attackers. Port 23 is used for Telnet, which is an unsecure protocol that allows remote login and command execution over a network connection using a CLI. Telnet does not encrypt the data or the credentials that are transmitted, making them vulnerable to interception or modification by attackers.
Reference:
https://www.csoonline.com/article/3191531/securing-risky-network-ports.html

NEW QUESTION 211
A server administrator is installing a new server on a manufacturing floor. Because the server is publicly accessible, security requires the server to undergo hardware hardening. Which of the following actions should the administrator take?

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

Answer: C

Explanation:
 An action that the administrator should take to harden the hardware of a new server is to set a BIOS password. BIOS (Basic Input/Output System) is a firmware that initializes the hardware components and settings of a system before loading the operating system. BIOS password is a security feature that requires a user to enter a password before accessing or modifying the BIOS settings or booting up the system. By setting a BIOS password, the administrator can prevent unauthorized or malicious users from changing the hardware configuration or boot order of the server.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 5, Lesson 5.1, Objective 5.1

NEW QUESTION 215
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 219
Which of the following documents would be useful when trying to restore IT infrastructure operations after a non-planned interruption?

A. Service-level agreement
B. Disaster recovery plan
C. Business impact analysis
D. Business continuity plan

Answer: B

Explanation:
A disaster recovery plan would be useful when trying to restore IT infrastructure operations after a non-planned interruption. A disaster recovery plan is a document that outlines the steps and procedures to recover from a major disruption of IT services caused by natural or man-made disasters, such as fire, flood, earthquake, cyberattack, etc. A disaster recovery plan typically includes:
? A list of critical IT assets and resources that need to be protected and restored
? A list of roles and responsibilities of IT staff and stakeholders involved in the recovery process
? A list of backup and recovery strategies and tools for data, applications, servers, networks, etc.
? A list of communication channels and methods for notifying users, customers, vendors, etc.
? A list of testing and validation methods for ensuring the functionality and integrity of restored systems
? A list of metrics and criteria for measuring the effectiveness and efficiency of the recovery process
A disaster recovery plan helps IT organizations to minimize downtime, data loss, and financial impact of a disaster, as well as to resume normal operations as quickly as possible.

NEW QUESTION 221
A systems administrator needs to back up changes made to a data store on a daily basis during a short time frame. The administrator wants to maximize RTO when restoring data. Which of the following backup methodologies would best fit this scenario?

A. Off-site backups
B. Full backups
C. Differential backups
D. Incremental backups

Answer: D

Explanation:
An incremental backup is a backup method that only backs up the files that have changed since the last backup, whether it was a full or an incremental backup. An incremental backup can save disk space and time, as it only copies the new or modified data. An incremental backup can also improve the RTO (Recovery Time Objective), which is the maximum acceptable time to restore data after a disaster. This is because an incremental backup can restore data faster than a full or a differential backup, as it only needs to apply the latest changes to the previous backup1.

NEW QUESTION 222
Which of the following licensing models allows the greatest number of concurrent Windows VMS to run on a host for the lowest cost?

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

Answer: A

Explanation:
The answer to this question may depend on several factors, such as the number and type of Windows VMs, the number and type of host machines, the number and type of users, and the specific licensing terms and conditions of each licensing model. However, based on the information available from the web search results, one possible answer is per user. Per user licensing model is a licensing model that allows a user to access Windows VMs from any device, regardless of the number of devices or VMs. Per user licensing model is available for Windows 10 Enterprise E3/E5, Windows VDA E3/E5, and Microsoft 365 F3/E3/E5. Per user licensing model may offer the greatest number of concurrent Windows VMs to run on a host for the lowest cost if the following conditions are met:
? The user needs to access multiple Windows VMs from different devices, such as desktops, laptops, tablets, or smartphones.
? The user needs to access Windows VMs that run different versions or editions of Windows, such as Windows 10 Enterprise, Windows 10 Pro, or Windows 7 Enterprise.
? The user needs to access Windows VMs that run on different types of host machines, such as physical servers, virtual servers, or cloud servers.
? The user does not need to access Windows VMs that run on dedicated hardware or have specific performance or security requirements.
According to the web search results1, per user licensing model costs $84 per user per year for Windows 10 Enterprise E3, $168 per user per year for Windows 10 Enterprise E5,
$100.80 per user per year for Windows VDA E3, and $196.80 per user per year for Windows VDA E5.These prices are based on the Open License Program and may vary depending on the volume and agreement level2
Per core licensing model is a licensing model that requires a license for each core of the processor on the host machine that runs Windows VMs. Per core licensing model is available for Windows Server 2022 Datacenter and Standard editions. Per core licensing model may offer a lower cost than per user licensing model if the following conditions are met:
? The host machine has a low number of cores or a high core density.
? The host machine runs a high number of Windows VMs with low resource consumption.
? The host machine runs only Windows Server VMs with the same edition as the host machine.
According to the web search results2, per core licensing model costs $6,155 for 16 core licenses for Windows Server 2022 Datacenter edition and $1,069 for 16 core licenses for Windows Server 2022 Standard edition.These pricesare suggested retail prices and may vary depending on the reseller2
Per instance licensing model is a licensing model that requires a license for each instance of Windows that runs on a host machine or a VM. Per instance licensing model is available for Windows Server 2022 Essentials edition and some older versions of Windows Server. Per instance licensing model may offer a lower cost than per user or per core licensing model if the following conditions are met:
? The host machine runs only one instance of Windows Server with low resource consumption.
? The host machine does not need to run any other VMs or applications.
? The host machine does not need any advanced features or functions that are available in Datacenter or Standard editions.
According to the web search results2, per instance licensing model costs $501 for one server license for Windows Server 2022 Essentials edition.This price is suggested retail price and may vary depending on the reseller2
Per concurrent user licensing model is a licensing model that allows a certain number of users to access Windows VMs at the same time, regardlessof the number of devices or VMs. Per concurrent user licensing model is not available for any current version of Windows or Windows Server. Per concurrent user licensing

model was available for some older versions of Windows Server Terminal Services or Remote Desktop Services, but it was discontinued due to complexity and compliance issues. Therefore, per concurrent user licensing model cannot be used for running Windows VMs on a host.

NEW QUESTION 227
Following a recent power outage, a server in the data center has been constantly going offline and losing its configuration. Users have been experiencing access issues while using the application on the server. The server technician notices the date and time are incorrect when the server is online. All other servers are working. Which of the following would most likely cause this issue? (Select two).

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

Answer: BE

Explanation:
A CMOS battery failure can cause the server to lose its BIOS settings, including the date and time, which can affect the server's functionality and connectivity. The servers have NTP (Network Time Protocol) configured to synchronize their clocks with a reliable time source, which can prevent time drift and ensure consistent timestamps. If one server has a wrong date and time, it can cause conflicts and errors with the other servers that have NTP configured.
References:
? CompTIA Server+ Certification Exam Objectives1, page 9
? Signs or symptoms of a CMOS battery failure2
? NTP: Network Time Protocol

NEW QUESTION 229
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 234
A server administrator receives a report that Ann, a new user, is unable to save a file to her home directory on a server. The administrator checks Ann's home directory permissions and discovers the following:
dr-xr-xr-- /home/Ann
Which of the following commands should the administrator use to resolve the issue without granting unnecessary permissions?

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

Answer: D

Explanation:
The administrator should use the command chmod 754 /home/Ann to resolve the issue without granting unnecessary permissions. The chmod command is used to change the permissions of files and directories on a Linux server. The permissionsare represented by three numbers, each ranging from 0 to 7, that correspond to the read ®, write (w), and execute (x) permissions for the owner, group, and others respectively. The numbers are calculated by adding up the values of each permission: r = 4, w = 2, x = 1. For example, 7 means rwx (4 + 2 + 1), 6 means rw- (4 + 2), 5 means r-x (4 + 1), etc. In this case, Ann's home directory has the permissions dr-xr-xr–, which means that only the owner (d) can read ® and execute (x) the directory, and the group and others can only read ® and execute (x) but not write (w) to it. This prevents Ann from saving files to her home directory. To fix this issue, the administrator should grant write permission to the owner by using chmod 754 /home/Ann, which means that the owner can read ®, write (w), and execute (x) the directory, the group can read ® and execute (x) but not write (w) to it, and others can only read ® but not write (w) or execute (x) it. This way, Ann can save files to her home directory without giving unnecessary permissions to others.
Reference:
https://linuxize.com/post/what-does-chmod-777-mean/

NEW QUESTION 239
A company created a new DR plan. The management team would like to begin performing a review of this plan without endangering company data and with a minimal time commitment. Which of the following testing methods would best allow for this type of review?

A. Simulated
B. Tabletop
C. Live
D. Non-production

Answer: B

Explanation:
Tabletop testing is a method of reviewing a DR plan without endangering company data and with a minimal time commitment. Tabletop testing involves a simulated scenario where the participants discuss their roles and responsibilities, identify potential issues, and evaluate the effectiveness of the plan. Simulated, live, and non-production testing are methods that involve more time and resources, and may pose some risks to company data. References: [CompTIA Server+ Certification Exam Objectives], Domain 6.0: Disaster Recovery, Objective 6.3: Compare and contrast various backup techniques.

NEW QUESTION 241
A new 40GB NIC has just been installed in a server but is not detected within the Windows server OS. Which of the following would most likely fix the issue?

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

Answer: A

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

NEW QUESTION 243
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 246
A server administrator is configuring the IP address on a newly provisioned server in the testing environment. The network VLANs are configured as follows:

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

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

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

Answer: A

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

NEW QUESTION 248

A server technician arrives at a data center to troubleshoot a physical server that is not responding to remote management software. The technician discovers the servers in the data center are not connected to a KVM switch, and their out-of-band management cards have not been configured. Which of the following should the technician do to access the server for troubleshooting purposes?

A. Connect the diagnostic card to the PCIe connector.
B. Connect a console cable to the server NIC.
C. Connect to the server from a crash cart.
D. Connect the virtual administration console.

Answer: C

Explanation:
A crash cart is a mobile device that consists of a monitor, a keyboard, a mouse, and a network connection. It can be used to access a physical server that is not responding to remote management software or does not have out-of-band management cards configured. The technician can connect the crash cart to the server using a VGA or HDMI cable and troubleshoot the server locally. Verified References: [Crash cart], [Out-of-band management]

NEW QUESTION 250
Which of the following server types would benefit MOST from the use of a load balancer?

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

Answer: D

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

NEW QUESTION 253
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: A

Explanation:
A SD card is a type of flash memory card that can be used to store data and run applications. A SD card can be used to install a Type 1 hypervisor on a server, as it provides fast boot time, low power consumption, and high reliability. A Type 1 hypervisor runs directly on the underlying computer's physical hardware, interacting directly with its CPU, memory, and physical storage. For this reason, Type 1 hypervisors are also referred to as bare-metal hypervisors. A Type 1 hypervisor takes the place of a host operating system and VM resources are scheduled directly to the hardware by the hypervisor123. A NAS drive (B) is a type of network-attached storage (NAS) device that provides shared access to files and data over a network. A NAS drive cannot be used to install a Type 1 hypervisor on a server, as it requires a network connection and a host operating system to function. A SATA drive © is a type of hard disk drive (HDD) or solid state drive (SSD) that uses the Serial ATA (SATA) interface to connect to a computer. A SATA drive can be used to install a Type 1 hypervisor on a server, but it may have some disadvantages compared to a SD card, such as slower boot time, higher power consumption, and lower reliability. A SAS drive (D) is a type of hard disk drive (HDD) or solid state drive (SSD) that uses the Serial Attached SCSI (SAS) interface to connect to a computer. A SAS drive can also be used to install a Type 1 hypervisor on a server, but it may have similar disadvantages as a SATA drive, and it may also be more expensive and less compatible than a SD card.References: 1 https://phoenixnap.com/kb/what-is-hypervisor-type-1-22
https://www.ibm.com/topics/hypervisors3 https://www.redhat.com/en/topics/virtualization/what-is-a-hypervisor

NEW QUESTION 254
Which of the following BEST describes a guarantee of the amount of time it will take to restore a downed service?

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

Answer: A

Explanation:
RTO stands for Recovery Time Objective and it is a metric that defines the maximum acceptable amount of time that a system or service can be unavailable after a disaster or disruption. RTO is part of the business continuity planning and disaster recovery planning processes. RTO ensures a guarantee of the amount of time it will take to restore a downed service by setting a target or goal for recovery. RTO can vary depending on the criticality and priority of the service.References:
https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam- objectives (Objective 3.3)

NEW QUESTION 256
A human resources analyst is attempting to email the records for new employees to an outside payroll company. Each time the analyst sends an email containing employee records, the email is rejected with an error message. Other emails outside the company are sent correctly. Which of the following is MOST likely generating the error?

A. DHCP configuration
B. Firewall rules
C. DLP software
D. Intrusion detection system

Answer: C

Explanation:
DLP (Data Loss Prevention) software is a type of security software that monitors and controls the transfer of sensitive or confidential data outside the organization. DLP software can prevent data breaches, data leaks, or data theftby blocking, encrypting, or alerting on unauthorized data transfers. DLP software can be applied to various channels, such as email, web, cloud, or removable devices.
In this scenario, the human resources analyst is attempting to email the records for new employees to an outside payroll company. The records for new employees may contain sensitive or confidential data, such as personal information, tax information, or bank account information. The DLP software may detect this data and block the email from being sent outside the company, as it may violate the company's data protection policy or regulations. The DLP software may also generate an error message to inform the analyst of the reason for the rejection.

NEW QUESTION 260
A Linux server requires repetitive tasks for reconfiguration. Which of the following would be the best scripting language to use?

A. PowerShell
B. Batch command file
C. Bash
D. Visual Basic

Answer: C

Explanation:
Bash is a scripting language that is commonly used in Linux systems to automate tasks and manipulate text. Bash scripts can run commands, variables, functions, loops, and conditional statements. PowerShell is a scripting language that is mainly used in Windows systems, while batch command files are simple text files that contain a series of commands to be executed by the command-line interpreter. Visual Basic is a programming language that is used to create applications, not scripts. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Server Administration, Objective 4.2: Given a scenario, perform proper server maintenance techniques.

NEW QUESTION 265
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 269
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 273
Which of the following access control methodologies can be described BEST as allowing a user the least access based on the jobs the user needs to perform?

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

Answer: B

Explanation:

The access control methodology that can be described best as allowing a user the least access based on the jobs the user needs to perform is role-based access control (RBAC). RBAC is an access control method that assigns permissions to users based on their roles or functions within an organization. RBAC provides fine-grained and manageable access control by defining what actions each role can perform and what resources each role can access. RBAC follows the principle of least privilege, which means that users are only granted the minimum level of access required to perform their tasks. RBAC can reduce security risks, simplify administration, and enforce compliance policies.

NEW QUESTION 275
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 278
A server technician has been asked to upload a few files from the internal web server to the internal FTP server. The technician logs in to the web server using PuTTY, but the connection to the FTP server fails. However, the FTP connection from the technician's workstation is sucessful. To troubleshoot the issue, the technician executes the following command on both the web server and the workstation:
ping ftp.acme.local
The IP address in the command output is different on each machine. Which of the following is the MOST likely reason for the connection failure?

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

Answer: D

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

NEW QUESTION 279
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your SK0-005 Exam with Our Prep Materials Via below:

https://www.certleader.com/SK0-005-dumps.html