CompTIA

Exam Questions SK0-005

CompTIA Server+ Certification Exam

NEW QUESTION 1
A server administrator mounted a new hard disk on a Linux system with a mount point of
/newdisk. It was later determined that users were unable to create directories or files on the new mount point. Which of the following commands would successfully mount the drive with the required parameters?

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

Answer: C

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

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

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

Answer: D

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

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

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

Answer: A

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

NEW QUESTION 4
A server administrator is exporting Windows system files before patching and saving them to the following location:
\\server1\ITDept\
Which of the following is a storage protocol that the administrator is MOST likely using to save this data?

A. eSATA
B. FCoE
C. CIFS
D. SAS

Answer: C

Explanation:
The storage protocol that the administrator is most likely using to save data to the location \server1\ITDept\ is CIFS. CIFS (Common Internet File System) is a protocol that allows file sharing and remote access over a network. CIFS is based on SMB (Server Message Block), which is a protocol that enables communication between devices on a network. CIFS uses UNC (Universal Naming Convention) paths to identify network resources, such as files or folders. A UNC path has the format \servername\sharename\path\filename. In this case, server1 is the name of the server, ITDept is the name of the shared folder, and \ is the path within the shared folder.

NEW QUESTION 5
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 6
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 7
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 8
A systems administrator recently upgraded the memory in a server, and now the server does not turn on, and nothing is displayed on the screen.
Which of the following is the next step the administrator should take to diagnose the error without opening the machine?

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

Answer: B

Explanation:
A power-on self-test (POST) is a diagnostic process that runs when a server is turned on to check the basic functionality of the hardware components and report any errors or faults. A POST code is a series of beeps or flashes that indicate the status of the POST process and identify any problems that prevent the server from booting up. A POST code can be heard through a speaker or seen on a display attached to the server motherboard. A POST code is useful for diagnosing errors without opening the machine or using any software tools.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 5, Lesson 5.1, Objective 5.1

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

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

Answer: AB

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

NEW QUESTION 10
A server administrator is installing an OS on a new server. Company policy states no one is to log in directly to the server. Which of the following Installation methods is BEST suited to meet the company policy?

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

Answer: B

Explanation:
A core installation is a type of installation method that is best suited to meet the company policy that states no one is to log in directly to the server. A core installation is a minimal installation option that is available when deploying some editions of Windows Server. A core installation includes most but not all server roles and features, but does not include a graphical user interface (GUI). A core installation can only be managed remotely using command-line tools such as PowerShell or Windows Admin Center, or using graphical tools such as Server Manager or Remote Desktop from another computer. This reduces the attack surface, resource consumption, and maintenance requirements of the server. A GUI installation is a type of installation method that includes a graphical user interface (GUI) and allows local or remote management using graphical tools or command- line tools. A virtualized installation is a type of installation method that involves creating and running one or more virtual machines on a physical host using a hypervisor such as Hyper- V or VMware. A clone installation is a type of installation method that involves creating an exact copy of an existing server's configuration and data on another server using tools such as Sysprep or Clonezilla.
References: https://www.howtogeek.com/67469/the- beginners-guide-to-shell-scripting-the-basics/ https://www.howtogeek.com/443611/how-to- encrypt-your-macs-system-drive-removable-devices-and-individual-files/
https://www.howtogeek.com/199068/how-to-upgrade-your-existing-hard-drive-in-under-an- hour/

NEW QUESTION 15
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 17
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 20
The management team has mandated the use of data-at-rest encryption for all data. Which of the following forms of encryption best achieves this goal?

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

Answer: A

Explanation:
Drive encryption is a form of data-at-rest encryption that encrypts the entire hard drive or solid state drive. This means that all the data on the drive, including the operating system, applications, and files, are protected from unauthorized access. Drive encryption is usually implemented at the hardware or firmware level, and requires a password, PIN, or biometric authentication to unlock the drive. Drive encryption is the most comprehensive and secure way to achieve data-at-rest encryption, as it prevents anyone from accessing the data without the proper credentials, even if they physically remove the drive from the server.
References: CompTIA Server+ Study Guide, Chapter 9: Security, page 367.

NEW QUESTION 23
Alter rack mounting a server, a technician must install four network cables and two power cables for the server. Which of the following is the MOST appropriate way to complete this task?

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

Answer: B

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

NEW QUESTION 25
A user cannot save large files to a directory on a Linux server that was accepting smaller files a few minutes ago. Which of the following commands should a technician use to identify the issue?

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

Answer: C

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

NEW QUESTION 30

Which of the following backup types resets the archive bit each time it is run?

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

Answer: C

Explanation:
Incremental backup is a type of backup that only backs up the files that have changed since the last backup, whether it was a full or an incremental backup. Incremental backup resets the archive bit each time it is run, which means it clears the flag that indicates whether or not the file has been backed up. Incremental backup can save time and space compared to full backup, but it requires more time and resources to restore data from multiple backups.References: https://www.comptia.org/training/resources/exam- objectives/comptia-server-sk0-005-exam-objectives (Objective 3.1)

NEW QUESTION 34
A server administrator needs to configure a server on a network that will have no more than 30 available IP addresses. Which of the following subnet addresses will be the MOST efficient for this network?

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

Answer: C

Explanation:
The most efficient subnet address for a network that will have no more than 30 available IP addresses is 255.255.255.224. This subnet mask corresponds to a /27 prefix length, which means that 27 bits are used for the network portion and 5 bits are used for the host portion of an IP address. With 5 bits for hosts, there are 2^5 - 2 = 30 possible host addresses per subnet, which meets the requirement. The other options are either too large or too small for the network size. Reference:https://www.ibm.com/cloud/learn/subnet- mask

NEW QUESTION 38
Which of the following concepts refers to prioritizing a connection that had previously worked successfully?

A. Round robin
B. SCP
C. MRU
D. Link aggregation

Answer: C

Explanation:
MRU, or Most Recently Used, is a concept that refers to prioritizing a connection that had previously worked successfully. It is often used in load balancing algorithms to distribute the workload among multiple servers or paths. MRU assumes that the most recently used connection is the most likely to be available and efficient, and therefore assigns the next request to that connection. This can help reduce latency and improve performance12. The other options are incorrect because they do not refer to prioritizing a previous
connection. Round robin is a concept that refers to distributing the workload equally among all available connections in a circular order12. SCP, or Secure Copy Protocol, is a concept that refers to transferring files securely between hosts using encryption3. Link aggregation is a concept that refers to combining multiple physical links into a single logical link to increase bandwidth and redundancy4.

NEW QUESTION 42
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 46
Following a recent power outage, a server in the datacenter has been constantly going offline and losing its configuration. Users have been experiencing access issues while using the application on the server. The server technician notices the data and time are incorrect when the server is online. All other servers are working. Which of the following would MOST likely cause this issue? (Choose two.)

A. The server has a faulty power supply
B. The server has a CMOS battery failure
C. The server requires OS updates
D. The server has a malfunctioning LED panel

E. The servers do not have NTP configured
F. The time synchronization service is disabled on the servers

Answer: BF

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

NEW QUESTION 47
Hackers recently targeted a company with an attack that resulted in a system breach, which compromised the organization's data. Because of the system breach, the administrator had to bypass normal change management procedures. Which of the following change management activities was necessary?

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

Answer: C

Explanation:
An emergency change request is a type of change management activity that is used to address urgent issues that pose a significant risk to the organization, such as a system breach. An emergency change request requires immediate action and approval, and it may bypass some of the normal change management procedures, such as testing, documentation, or stakeholder communication12.
References = 1: Change Management Plans: A Definitive Guide -Indeed(https://www.indeed.com/career-advice/career-development/change-management-activities) 2: The 10 Best Change Management Activities-Connecteam(https://connecteam.com/top-10-change-management-activities/)

NEW QUESTION 52
A systems administrator notices a newly added server cannot see any of the LUNs on the SAN. The SAN switch and the local HBA do not display any link lights. Which of the following is most likely the issue?

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

Answer: A

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

NEW QUESTION 57
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 61
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 62
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 64
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 67
A technician is installing a variety of servers in a rack. Which of the following is the BEST course of action for the technician to take while loading the rack?

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

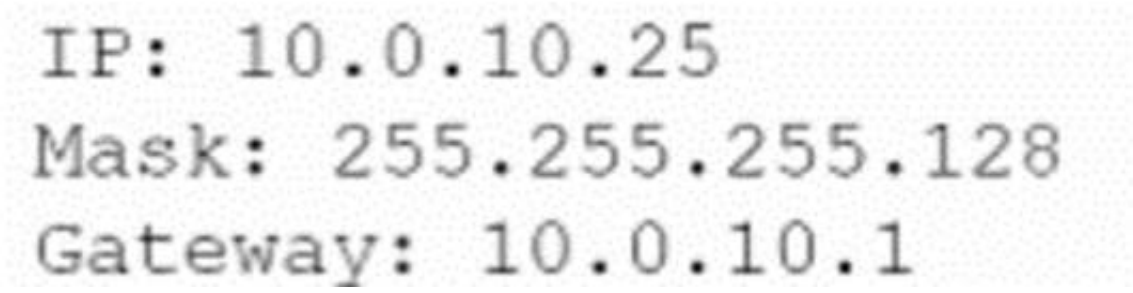
Answer: B

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

NEW QUESTION 70
An application server cannot communicate with a newly installed database server. The database server, which has static IP information, is reading the following output from ipconf ig:

```
IP: 10.0.10.240
Mask: 255.255.255.128
Gateway: 10.0.10.1
```

The application server is reading the following output from ipconf ig:



Which of the following most likely contains an error?

A. IP address
B. DHCP
C. Gateway
D. Subnet mask

Answer: D

Explanation:
The subnet mask is most likely containing an error that prevents the application server from communicating with the newly installed database server. The 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 subnet mask determines which devices belong to the same network or subnet and can communicate directly with each other without routing or switching devices. The subnet mask of the database server is 255.255.O.O, which means that all 32 bits of its IP address are used for the network portion and none for the host portion, which is invalid and makes it unreachable by any other device on any network or subnet. The subnet mask of the application server is 255.O.O.O, which means that only 8 bits of its IP address are used for the network portion and 24 bits are used for the host portion, which is also uncommon and makes it incompatible with most networks or subnets. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Networking, Objective 4.1: Given a scenario, configure network settings for servers.

NEW QUESTION 71
A technician is checking a server rack. Upon entering the room, the technician notices the tans on a particular server in the rack are running at high speeds. This is the only server in the rack that is experiencing this behavior. The ambient temperature in the room appears to be normal. Which of the following is the MOST likely reason why the fans in that server are operating at full speed?

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

Answer: C

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

NEW QUESTION 72
Which of the following are measures that should be taken when a data breach occurs? (Select TWO).

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

Answer: BE

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

NEW QUESTION 73

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

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

Answer: A

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

NEW QUESTION 74
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 75
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 76
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 79
A security technician generated a public/private key pair on a server. The technician needs to copy the key pair to another server on a different subnet. Which of the following is the most secure method to copy the keys?
? HTTP

A. FTP
B. SCP
C. USB

Answer: C

Explanation:

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

NEW QUESTION 82
A server administrator added a new drive to a server. However, the drive is not showing up as available. Which of the following does the administrator need to do to make the drive available?

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

Answer: A

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

NEW QUESTION 83
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 85
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 86
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 88
An organization implements split encryption keys for sensitive files. Which of the following types of risks does this mitigate?

A. Hardware failure
B. Marware
C. Data corruption
D. Insider threat

Answer: D

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

NEW QUESTION 92
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 96
A storage administrator needs to implement SAN-based shared storage that can transmit at 16Gb over an optical connection. Which of the following connectivity options would BEST meet this requirement?

A. Fibre Channel
B. FCoE
C. iSCSI
D. eSATA

Answer: A

Explanation:
Fibre Channel is a connectivity option that can transmit at 16Gb over an optical connection for SAN-based shared storage. Fibre Channel is a high-speed network technology that provides reliable and secure data transfer between servers and storage devices. Fibre Channel uses optical fiber cables to connect devices and supports various topologies and protocols. FCoE is another connectivity option that uses Fibre Channel over Ethernet, which encapsulates Fibre Channel frames into Ethernet packets. FCoE can also transmit at 16Gb over an optical connection, but it requires a converged network adapter (CNA) and a lossless Ethernet network. iSCSI is another connectivity option that uses SCSI commands over IP networks, which can use either copper or optical cables. iSCSI can transmit at 10Gb or 40Gb over an optical connection, but it has higher latency and lower performance than Fibre Channel. eSATA is another connectivity option that uses SATA commands over external cables, which are usually copper. eSATA can transmit at 6Gb over a copper connection, but it has limited cable length and device support compared
to Fibre Channel. References:
? https://www.ibm.com/topics/storage-area-network
? https://www.techopedia.com/definition/1369/fibre-channel-fc
? https://www.techopedia.com/definition/1368/fibre-channel-over-ethernet-fcoe
? https://www.techopedia.com/definition/1367/internet-small-computer-system- interface-iscsi
? https://www.techopedia.com/definition/1366/external-serial-advanced-technology- attachment-esata

NEW QUESTION 98
A security analyst suspects a remote server is running vulnerable network applications. The analyst does not have administrative credentials for the server. Which

of the following would MOST likely help the analyst determine if the applications are running?

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

Answer: D

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

NEW QUESTION 101
A company wants to find an affordable way to simulate a fail over of a critical application. The company does not currently have a solution for it. The application consists of 15 servers, and the company would like to simulate on production configurations and IP address schemes. Which of the following would be the most cost-effective solution?

A. Build a warm site and perform a fail over of the application.
B. Build a cloud laaS and perform a fail over of the application.
C. Build a hot site and perform a fail over of the application.
D. Build a cold site and perform a fail over of the application.
E. Perform a tabletop fail over of the application.

Answer: B

Explanation:
Cloud IaaS (Infrastructure as a Service) is a service model that allows users to rent virtualized computing resources over the internet, such as servers, storage, network, and software. Cloud IaaS can provide several benefits for disaster recovery and failover scenarios, such as:
? Lower cost: Cloud IaaS can reduce the capital and operational expenses of
building and maintaining a physical disaster recovery site, asusers only pay for the resources they use on demand12.
? Scalability: Cloud IaaS can offer flexible and elastic scalability of resources, as
users can easily provision or deprovision resources according to their needs and workload12.
? Availability: Cloud IaaS can ensure high availability and reliability of the
application, as users can leverage the cloud provider's redundant and geographically distributed infrastructure12.
? Simplicity:Cloud IaaS can simplify the failover process, as users can use the cloud provider's tools and services to automate and orchestrate the failover operations12.
Therefore, building a cloud IaaS and performing a failover of the application would be the most cost-effective solution for the company, as it would allow them to simulate a failover of a critical application on production configurations and IP address schemes without investing in a physical disaster recovery site.

NEW QUESTION 102
A technician recently replaced a NIC that was not functioning. Since then, no device driver is found when starting the server, and the network card is not functioning. Which of the following should the technician check first?

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

Answer: C

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

NEW QUESTION 104
A technician is tasked with upgrading 24 hosts simultaneously with a Type 1 hypervisor. Which of the following protocols should the technician use for this upgrade?

A. VPN
B. TFTP
C. SSH
D. HTTP

Answer: B

Explanation:
TFTP (Trivial File Transfer Protocol) is a simple and lightweight protocol that can be used to transfer files over a network. TFTP is often used to upgrade firmware or software on network devices, such as routers, switches, or servers. TFTP can also be used to install a Type 1 hypervisor, such as VMware ESXi, on multiple hosts simultaneously12. References = 1: How to Install VMware ESXi Type 1 Hypervisor - MatthewEaton.net(https://mattheweaton.net/posts/how-to-install-vmware-esxi-type-1- hypervisor/) 2: Explore Type 1 Hypervisors - Set Up Virtual Machines Using VirtualBox and vSphere - OpenClassrooms(https://openclassrooms.com/en/courses/7163136-set-up- virtual-machines-using-virtualbox-and-vsphere/7358546-explore-type-1-hypervisors)

NEW QUESTION 105
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 107
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 108
A data center environment currently hosts more than 100 servers that include homegrown and commercial software. The management team has asked the server administrator to find a way to eliminate all company-owned data centers. Which of the following models will the administrator most likely choose to meet this need?

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

Answer: C

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

NEW QUESTION 113
A company uses a hot-site, disaster-recovery model. Which of the following types of data replication is required?

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

Answer: D

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

NEW QUESTION 116
A server administrator wants to ensure a storage array can survive the failure of two drives without the loss of data. Which of the following RAID levels should the administrator choose?

A. 1
B. 5
C. 6

Answer: D

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

NEW QUESTION 121
Which of the following is an example of load balancing?

A. Round robin
B. Active-active
C. Active-passive
D. Failover

Answer: A

Explanation:
Round robin is an example of load balancing. Load balancing is the method of distributing network traffic equally across a pool of resources that support an application. Load balancing improves application availability, scalability, security, and performance by preventing any single resource from being overloaded or unavailable. Round robin is a simple load balancing algorithm that assigns each incoming request to the next available resource in a circular order. For example, if there are three servers (A, B, C) in a load balancer pool, round robin will send the first request to server A, the second request to server B, the third request to server C, the fourth request to server A again, and so on. Reference: https://simplicable.com/new/load-balancing

NEW QUESTION 126
A company's security team has noticed employees seem to be blocking the door in the main data center when they are working on equipment to avoid having to gain access each time. Which of the following should be implemented to force the employees to enter the data center properly?

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

Answer: B

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

NEW QUESTION 130
A technician is attempting to update a server’s firmware. After inserting the media for the firmware and restarting the server, the machine starts normally into the OS. Which of the following should the technician do NEXT to install the firmware?

A. Press F8 to enter safe mode
B. Boot from the media
C. Enable HIDS on the server
D. Log in with an administrative account

Answer: B

Explanation:
The technician should boot from the media to install the firmware on the server. Firmware is a type of software that controls the low-level functions of hardware devices, such as BIOS (Basic Input/Output System), RAID controllers, network cards, etc. Firmware updates are often provided by hardware manufacturers to fix bugs, improve performance, or add new features to their devices. To install firmware updates on a server, the technician needs to boot from a media device (such as a CD-ROM, DVD-ROM, USB flash drive, etc.) that contains the firmware files and installation program. The technician cannot install firmware updates from within the operating system because firmware updates often require restarting or resetting the hardware devices.

NEW QUESTION 131
An analyst is planning a new point-to-point Ethernet connection between a university campus and a newly acquired space downtown that is about 5mi (8km) away. The analyst would like the fastest possible connection speed. Which of the following would best meet the analyst's needs?

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

Answer: A

Explanation:
A 1000BASE-LX 1Gb single-mode plenum fiber connection would best meet the analyst’s needs for a new point-to-point Ethernet connection between a university campus and a newly acquired space downtown that is about 5mi (8km) away. A 1000BASE-LX is a type of Ethernet standard that supports data transmission at 1 gigabit per second over single- mode fiber cables using long wavelength lasers. A single-mode fiber cable is a type of optical fiber cable that has a small core diameter and allows only one mode of light to propagate through it. A single-mode fiber cable can transmit data over long distances at high speeds, but it requires

more expensive transceivers and connectors than multimode fiber cables. A plenum fiber cable is a type of optical fiber cable that has a special coating that prevents the spread of fire or toxic fumes in case of burning. A plenum fiber cable is suitable for installation in plenum spaces, which are areas used for air circulation in buildings, such as above ceilings or below floors. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Networking, Objective 4.2: Given a scenario involving server networking issues (e.g., network interface card failure), troubleshoot using appropriate tools.

NEW QUESTION 134
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 135
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 137
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 138
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 143
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 145
A server administrator just installed a new physical server and needs to harden the OS. Which of the following best describes the OS hardening method?

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

Answer: A

Explanation:
Applying security updates is one of the common operating system hardening methods that can help protect the OS from cyberattacks and vulnerabilities. Security updates are released by the OS developer to fix bugs, patch security holes, and improve performance. By installing the latest updates, the server administrator can ensure that the OS is up to date and secure12.

NEW QUESTION 149
A technician has moved a data drive from a new Windows server to an older Windows server. The hardware recognizes the drive, but the data is not visible to the OS. Which of the following is the most likely cause of the issue?

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

Answer: A

Explanation:
The most likely cause of the issue is that the disk uses GPT.GPT stands for GUID Partition Table, which is a newer standard for disk partitioning that supports larger disks and more partitions than theolder MBR (Master Boot Record) standard1.However, GPT is not compatible with some older operating systems, such as Windows XP or Windows Server 20032. Therefore, if the data drive was formatted with GPT on a new Windows server and then moved to an older Windows server, the older server may not be able to recognize the GPT partitions and access the data on the drive.
The partition being formatted with ext4, FAT32, or MBR are not likely causes of the issue.Ext4 is a file system that is commonly used on Linux-based systems, but it can also be read by Windows with some third-party software3.FAT32 is a file system that is widely compatible with most operating systems and devices, but it has some limitations such as a maximum file size of 4 GB and a maximum partition size of 8 TB4.MBR is not a file system, but a partitioning scheme that can support various file systems such as NTFS, FAT32, or exFAT5.However, MBR has some disadvantages compared to GPT, such as a maximum disk size of 2 TB and a maximum number of primary partitions of four1.

NEW QUESTION 151
A company needs to increase the security controls on its servers. Anadministrator is implementing MFA on all servers using cost effective techniques. Which of the following should the administrator use to satisfy the MFA requirement?

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

Answer: B

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

NEW QUESTION 156
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 161
Which of the following symbols is used to write a text description per line within a PowerShell script?

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

Answer: D

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

NEW QUESTION 164
An administrator is alerted to a hardware failure in a mission-critical server. The alert states that two drives have failed. The administrator notes the drives are in different RAID 1 arrays, and both are hot-swappable. Which of the following steps will be the MOST efficient?

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

Answer: C

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

NEW QUESTION 169
Which of the following should an administrator use to transfer log files from a Linux server to a Windows workstation?

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

Answer: D

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

NEW QUESTION 170
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 173
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 178
Which ofthefollowingshouldatechnician verify FIRST before decommissioning and wipinga file server?

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

Answer: D

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

NEW QUESTION 181
A senior administrator instructs a technician to run the following script on a Linux server: for i in {1..65536); do echo Si; telnet localhost $i; done
The script mostly returns the following message: Connection refused. However, there are several entries in the console display that look like this:
80
Connected to localhost 443
Connected to localhost
Which of the following actions should the technician perform NEXT?

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

Answer: A

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

NEW QUESTION 185
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 187
A company wants to deploy software to all users, Out very few of men will be using the software at any one point in time. Which of the following licensing models would be BEST lot the company?

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

Answer: B

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

NEW QUESTION 191
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 194
A company stores extremely sensitive data on an alt-gapped system. Which of the following can Be Implemented to increase security against a potential insider threat?

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

Answer: A

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

NEW QUESTION 199
A VLAN needs to be configured within a virtual environment for a new VM. Which of the following will ensure the VM receives a correct IP address?

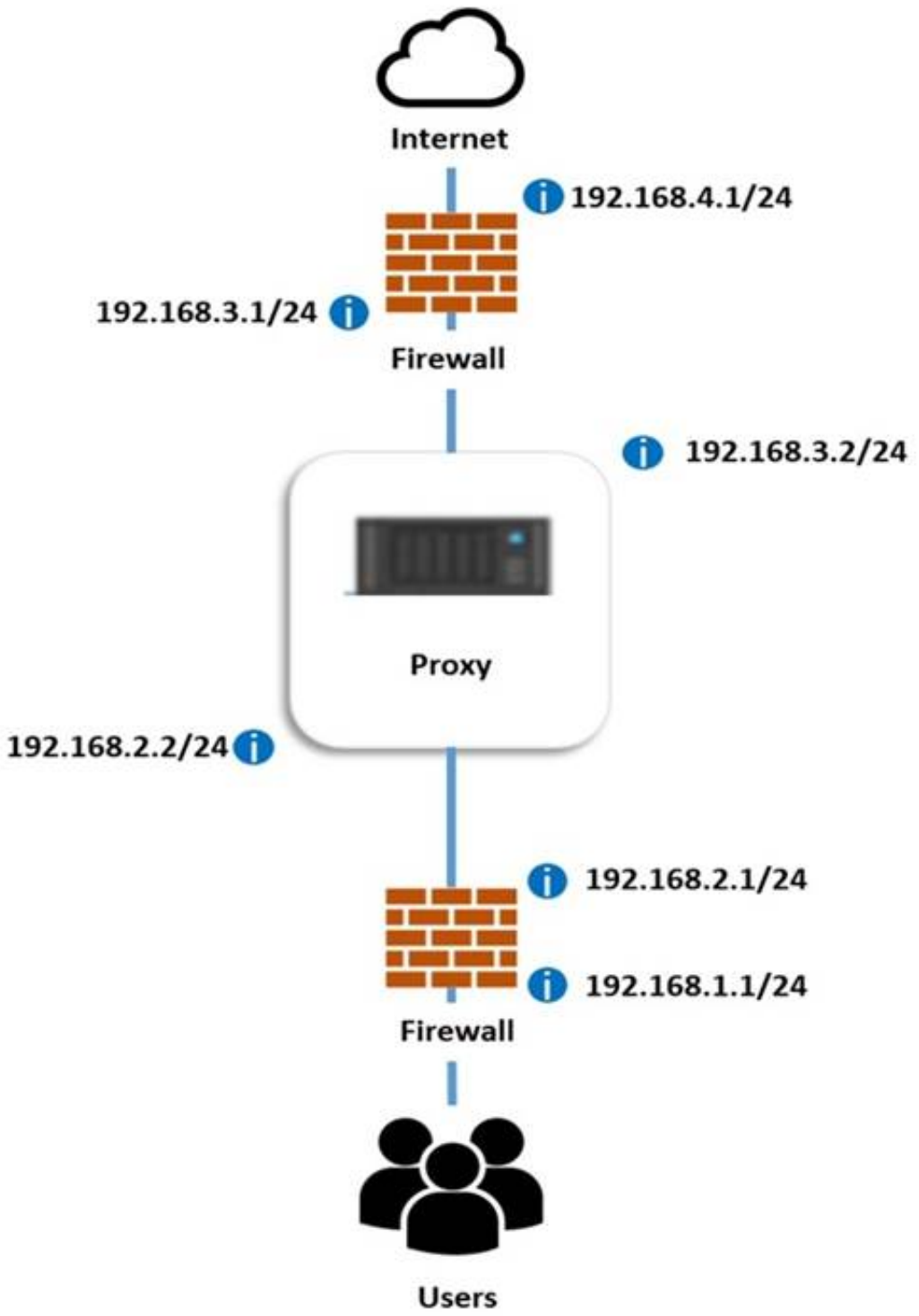
A. A virtual router
B. A host NIC
C. A VPN
D. A virtual switch
E. A vNIC

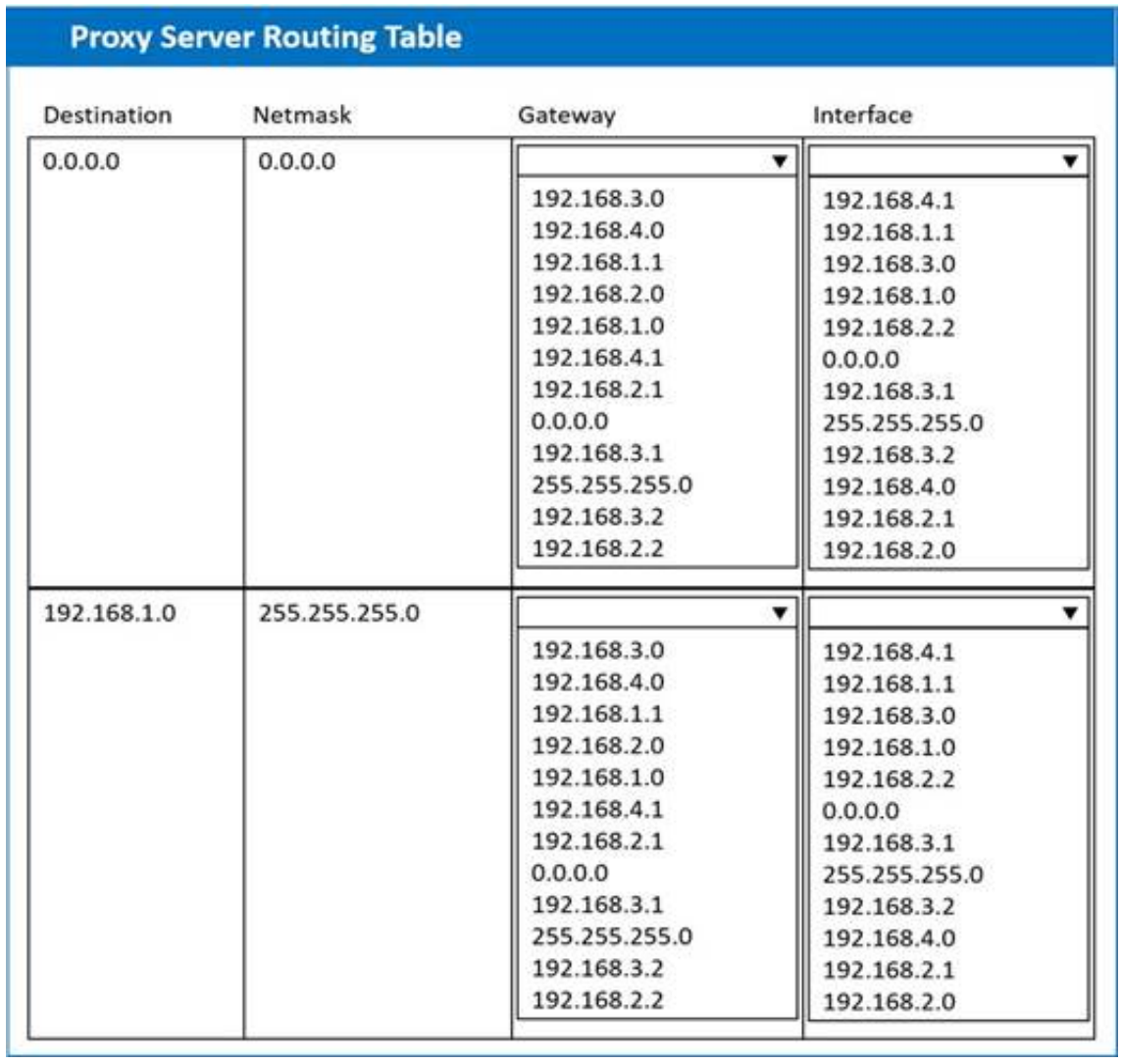
Answer: D

Explanation:
The correct answer is D. A virtual switch.

A virtual switch is a software-based network device that connects the virtual machines (VMs) in a virtual environment and allows them to communicate with each other and with the physical network. A virtual switch can also create and manage virtual LANs (VLANs), which are logical segments of a network that separate the traffic of different VMs or groups of VMs. A VLAN needs a DHCP server to assign IP addresses to the VMs that belong to it. A virtual switch can act as a DHCP relay agent and forward the DHCP requests from the VMs to the DHCP server on the physical network.This way, the VMs can receive correct IP addresses for their VLANs123
A virtual router is a software-based network device that routes packets between different networks or subnets. A virtual router can also create and manage VLANs, but it is not necessary for a VM to receive a correct IP address.A virtual router can be used to provide additional security, redundancy, or load balancing for the VMs12
A host NIC is a physical network interface card that connects the host machine to the physical network. A host NIC can also support VLAN tagging, which allows the host machine to communicate with different VLANs on the network. However, a host NIC alone cannot ensure that a VM receives a correct IP address for its VLAN.The host NIC needs to be connected to a virtual switch that can relay the DHCP requests from the VMs to the DHCP server12
A VPN is a virtual private network that creates a secure tunnel between two or more devices over the internet. A VPN can be used to encrypt and protect the data traffic of the VMs, but it is not related to the configuration of VLANs or IP addresses.A VPN does not affect how a VM receives a correct IP address for its VLAN14
A vNIC is a virtual network interface card that connects a VM to a virtual switch or a virtual router. A vNIC can also support VLAN tagging, which allows the VM to communicate with different VLANs on the network.However, a vNIC alone cannot ensure that a VM receives a correct IP address for its VLAN.The vNIC needs to be connected to a virtual switch or a virtual router that can relay the DHCP requests from the VMs to the DHCP server12

NEW QUESTION 201
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.

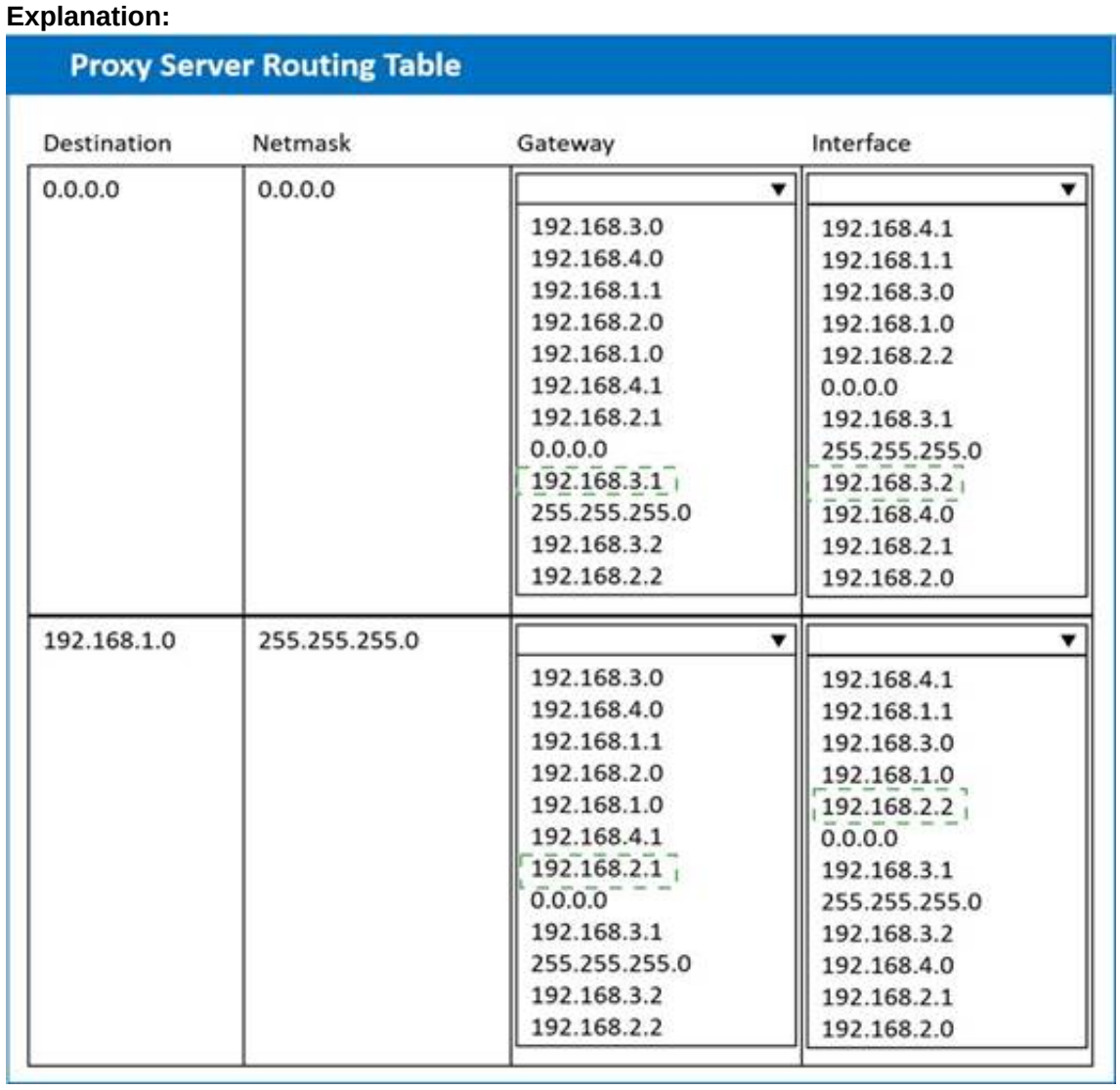




A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 204
A server technician is installing application updates on a Linux server. When the technician tries to install a MySQL update, the GUI displays the following error message: AVC denial. Which of the following should the technician do for the MySQL update to install?

A. Download the update manually and run a checksum utility to verify file integrity.
B. Issue the setenforce 0 command.
C. Create a firewall rule to allow port 3306 through the firewall.
D. Issue the yum -y update mysql command.

Answer: B

Explanation:
The AVC denial error message indicates that SELinux (Security-Enhanced Linux) is preventing the MySQL update from installing. SELinux is a security module that enforces mandatory access control policies on Linux systems. To install the MySQL update, the technician should issue the setenforce 0 command, which temporarily disables SELinux enforcement until the next reboot. Downloading the update manually, creating a firewall rule, or issuing the yum -y update mysql command will not resolve the error. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Server Administration, Objective 4.3: Given a scenario, troubleshoot server issues using appropriate tools.

NEW QUESTION 208
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 210
A technician is configuring a point-to-point heartbeat connection between two servers using IP addressing. Which of the following is the most efficient subnet mask for this connection?

A. /28
B. /29
C. /30
D. /32

Answer: C

Explanation:
The most efficient subnet mask for a point-to-point heartbeat connection between two servers using IP addressing is /30. A /30 subnet mask has 255.255.255.252 as its decimal representation and 11111111.11111111.11111111.11111100 as its binary representation. This means that there are only two bits available for the host portion of the IP address, which allows for four possible combinations: 00, 01, 10, and 11. However, the first and the last combinations are reserved for the network address and the broadcast address, respectively. Therefore, only two IP addresses are usable for the point-to-point connection, which is the minimum required for such a link.A /30 subnet mask is also known as a point- to-point prefix because it is commonly used for point-to-point links between routers or servers1.
A /28 subnet mask has 255.255.255.240 as its decimal representation and 11111111.11111111.11111111.11110000 as its binary representation. This means that there are four bits available for the host portion of the IP address,which allows for 16 possible combinations. However, two of them are reserved for the network address and the broadcast address, respectively. Therefore, 14 IP addresses are usable for the subnet, which is more than needed for a point-to-point connection and would result in wasted addresses.
A /29 subnet mask has 255.255.255.248 as its decimal representation and 11111111.11111111.11111111.11111000 as its binary representation. This means that there are three bits available for the host portion of the IP address, which allows for eight possible combinations. However, two of them are reserved for the network address and the broadcast address, respectively. Therefore, six IP addresses are usable for the subnet, which is still more than needed for a point-to-point connection and would result in wasted addresses.
A /32 subnet mask has 255.255.255.255 as its decimal representation and 11111111.11111111.11111111.11111111 as its binary representation. This means that there are no bits available for the host portion of the IP address, which allows for only one possible combination: all ones. Therefore, only one IP address is usable for the subnet, which is not enough for a point-to-point connection and would result in an invalid configuration.
Therefore, a /30 subnet mask is the most efficient choice for a point-to-point heartbeat connection between two servers using IP addressing because it provides exactly two usable IP addresses without wasting any addresses or creating any conflicts1.

NEW QUESTION 212
A company recently implemented VoIP across a multicampus environment with ten locations. The company uses many network technologies, including fiber, copper, and wireless. Users calling between three of the locations have reported that voices sound strange. Which of the following should be monitored to narrow down the issue?

A. Disk IOPS
B. CPU utilization
C. RAM utilization
D. Network latency

Answer: D

Explanation:
Network latency is the measure of delay in data transmission over a network. It can affect the quality of voice over IP (VoIP) calls by causing echo, jitter, or distortion.
Network latencycan be caused by various factors such as network congestion, distance, routing, or bandwidth. To monitor network latency, you can use tools such as ping, traceroute, or network analyzers.
References: CompTIA Server+ Study Guide, Chapter 6: Networking, page 237.

NEW QUESTION 216
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 220
Which of the following BEST describes a warm site?

A. The site has all infrastructure and live data.
B. The site has all infrastructure and some data
C. The site has partially redundant infrastructure and no network connectivity
D. The site has partial infrastructure and some data.

Answer: D

Explanation:
A warm site is a type of disaster recovery site that has some pre-installed hardware, software, and network connections, but not as much as a hot site. A warm site also has some backup data, but not as current as a hot site. A warm site requires some time and effort to become fully operational in the event of a disaster. A hot site is a disaster recovery site that has all infrastructure and live data, and can take over the primary site's operations immediately. A cold site is a disaster recovery site that has no infrastructure or data, and requires significant time and resources to set up. References:
? https://www.enterprisestorageforum.com/management/disaster-recovery-site/
? https://www.techopedia.com/definition/3780/warm-site

NEW QUESTION 221
A technician is deploying a single server to monitor and record me security cameras at a remote site, which of the following architecture types should be used to minimize cost?

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

Answer: C

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

NEW QUESTION 222
Which of the following encryption methodologies would MOST likely be used to ensure encrypted data cannot be retrieved if a device is stolen?

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

Answer: C

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

NEW QUESTION 227
Which of the following security risks provides unauthorized access to an application?

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

Answer: A

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

NEW QUESTION 230
An administrator is investigating several unexpected documents and video files that recently appeared in a network share. The administrator checks the properties of the files and sees the author's name on the documents is not a company employee. The administrator questions the other users, but no one knows anything about the files. The administrator then checks the log files and discovers the FTP protocol was used to copy the files to the server. Which of the following needs to be done to prevent this from happening again?

A. Implement data loss prevention.
B. Configure intrusion detection.
C. Turn on User Account Control.
D. Disable anonymous access.

Answer: D

Explanation:
This is the best solution to prevent unauthorized files from being copied to the server via FTP because anonymous access allows anyone to log in to the FTP server without providing a username or password. Disabling anonymous access will require users to authenticate with valid credentials before accessing the FTP server.References: https://docs.microsoft.com/en-us/iis/configuration/system.applicationhost/sites/site/ftpserver/security/authentication/anony mousauthentication

NEW QUESTION 234
A technician is setting up a small office that consists of five Windows 10 computers. The technician has been asked to use a simple IP configuration without manually adding any IP addresses. Which of the following will the technician MOST likely use for the IP address assignment?

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

Answer: D

Explanation:
DHCP stands for Dynamic Host Configuration Protocol and it is a network protocol that automatically assigns IP addresses and other network configuration parameters to devices on a network. DHCP can help simplify IP configuration without manually adding any IP addresses. DHCP works by using a DHCP server that maintains a pool of available IP addresses and leases them to devices that request them. The devices can renew or release their IP addresses as needed.References: https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam- objectives (Objective 2.1)

NEW QUESTION 235
Which of the following often-overlooked parts of the asset life cycle can cause the greatest number of issues in relation to Pll exposure?

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

Answer: D

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

NEW QUESTION 239
A technician has received tickets responding a server is responding slowly during business hours. Which of the following should the technician implement so the team will be informed of this behavior in real time?

A. Log rotation
B. Alerts
C. Reports
D. Log stopping

Answer:

B

Explanation:
Alerts are notifications that inform the technician or the team of any issues or events that occur on a server or a network. Alerts can be configured to trigger based on certain thresholds, such as CPU usage, disk space, memory utilization, or response time. Alerts can help the technician monitor and troubleshoot the server performance in real time. Verified References: [Alerts], [Server performance]

NEW QUESTION 241
A server administrator has received tickets from users who report the system runs very slowly and various unrelated messages pop up when they try to access an internet-facing web application using default ports. The administrator performs a scan to check for open ports and reviews the following report:
Starting Nmap 7.70 https://nmap.org) at 2019-09-19 14:30 UTC Nmap scan report for www.abc.com (172.45.6.85)
Host is up (0.0021s latency)
Other addresses for www.abc.com (not scanned) : 4503 : F7b0 : 4293: 703: : 3209 RDNS record for 172.45.6.85: 1ga45s12-in-f1.2d100.net
Port State Service 21/tcp filtered ftp 22/tcp filtered ssh 23/tcp filtered telnet
69/tcp open @username.com 80/tcp open http
110/tcp filtered pop 143/tcp filtered imap 443/tcp open https
1010/tcp open www.popup.com 3389/tcp filtered ms-abc-server
Which of the following actions should the server administrator perform on the server?

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

Answer: A

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

NEW QUESTION 243
A server administrator recently installed a kernel update to test functionality Upon reboot, the administrator determined the new kernel was not compatible with certain server hardware and was unable to uninstall the update. Which of the following should the administrator do to mitigate further issues with the newly instated kernel version?

A. Edit the bootloader configuration file and change the first Kernel stanza to reflect the file location for the last known-good kernel files.
B. Perform a complete OS reinstall on the server using the same media that was used during the initialinstall.
C. Edit the bootloader configuration file and move the newest kernel update stanza lo the end of the file.
D. Set a BIOS password to prevent server technicians from making any changes to thesystem.

Answer: A

Explanation:
The bootloader configuration file is used to specify which kernel version and options to use when booting the system. The first kernel stanza in the file is the default one that is loaded automatically. By editing this stanza and changing it to point to the last known-good kernel files, the administrator can boot the system with a working kernel and avoid any compatibility issues with the new kernel update. Verified References: [How To Change The Linux Kernel Version]

NEW QUESTION 247
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 248
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 252
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 256
A technicianretailed a new4TBharddrive inaWindows server. Which of the following should the technician perform FIRST to provision the newdrive?

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

Answer: D

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

NEW QUESTION 261
A systems administrator has noticed performance degradation on a company file server, and one of the disks on it has a solid amber light. The administrator logs on to the disk utility and sees the array is rebuild ing. Which of the following should the administrator do NEXT once the rebuild is finished?

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

Answer: C

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

NEW QUESTION 262
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 267
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 271
An administrator needs to disable root login over SSH. Which of the following tiles should be edited to complete this task?

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

Answer: B

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

NEW QUESTION 272
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

SK0-005 Practice Exam Features:

* SK0-005 Questions and Answers Updated Frequently

* SK0-005 Practice Questions Verified by Expert Senior Certified Staff

* SK0-005 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SK0-005 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year