Exam Questions SK0-005

CompTIA Server+ Certification Exam

https://www.2passeasy.com/dumps/SK0-005/

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

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

Answer: B

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

NEW QUESTION 2
An administrator 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
An administrator is rebooting servers manually after a group of updates were deployed through SCCM. The administrator notices several of the servers did not receive the deployed update. Which of the following should the administrator review first?

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

Answer: D

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

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

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

Answer: A

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

NEW QUESTION 5
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.

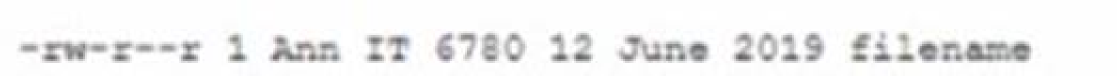
NEW QUESTION 6
A server administrator needs to deploy five VMs, all of which must have the same type of configuration. Which of the following would be the MOST efficient way to perform this task?

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

Answer: D

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

NEW QUESTION 7
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 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 9
A server administrator has noticed that the storage utilization on a file server is growing faster than planned. The administrator wants to ensure that, in the future, there is a more
direct relationship between the number of users using the server and the amount of space that might be used. Which of the following would BEST enable this correlation?

A. Partitioning
B. Deduplication

C. Disk quotas
D. Compression

Answer: C

Explanation:
The best way to ensure that there is a more direct relationship between the number of users using the server and the amount of space that might be used is to implement disk quotas. Disk quotas are a feature that allows a server administrator to limit the amount of disk space that each user or group can use on a file server. Disk quotas can help manage storage utilization, prevent disk space exhaustion, and enforce fair usage policies. Disk quotas can also provide reports and alerts on disk space usage and quota status.

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

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

Answer: C

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

NEW QUESTION 13
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 17

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

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

Answer: D

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

NEW QUESTION 20
Which of the following refers to the requirements that dictate when to delete data backups?

A. Retention policies.
B. Cloud security impact
C. Off-site storage
D. Life-cycle management

Answer: A

Explanation:
Retention policies are the guidelines that dictate when to delete data backups based on operational or compliance needs. They specify how long, how, where, and in what format the data backups are stored, and who has authority over them. The other options are not directly related to the deletion of data backups.
https://backup.ninja/news/Database-Backups-101-Backup-Retention-Policy-Considerations

NEW QUESTION 21
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 25
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 29
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 33
A server administrator is currently working on an incident. Which of the following steps should the administrator perform before resolving the issue?

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

Answer: C

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

NEW QUESTION 35
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 40
A server administrator needs to harden a server by only allowing secure traffic and DNS inquiries. A port scan reports the following ports are open:

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

Answer: D

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

NEW QUESTION 45
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 46
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 51
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 53
Users have noticed a server is performing below Baseline expectations. While diagnosing me server, an administrator discovers disk drive performance has degraded. The administrator checks the diagnostics on the RAID controller and sees the battery on me controller has gone bad. Which of the following is causing the poor performance on the RAID array?

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

Answer: A

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

NEW QUESTION 56
A Linux server was recently updated. Now, the server stops during the boot process with a blank screen and an£s> prompt. When of the following is the MOST likely cause of this issue?

A. The system is booting to a USB flash drive
B. The UEFI boot was interrupted by a missing Linux boot file

C. The BIOS could not find a bootable hard disk
D. The BIOS firmware needs to be upgraded

Answer: B

Explanation:
The most likely cause of this issue is that the UEFI boot was interrupted by a missing Linux
boot file, such as grub.cfg or vmlinuz, which are essential for loading the Linux kernel and booting the system. The £s> prompt indicates that the system entered into UEFI Shell mode, which is a command-line interface for troubleshooting UEFI boot issues. The administrator can use UEFI Shell commands to locate and restore the missing boot file or change the boot order. Verified References: [UEFI Shell Guide]

NEW QUESTION 59
An administrator has been asked to disable CPU hyperthreading on a server to satisfy a licensing issue. Which of the following best describes how the administrator will likely perform this action?

A. Use a RDP/VNC session.
B. Modify the startup configuration.
C. Use a PowerShell/Bash script.
D. Use the BIOS/UEFI setup.

Answer: D

Explanation:
The BIOS (Basic Input/Output System) or UEFI (Unified Extensible Firmware Interface) setup is a program that allows users to configure the hardware settings of a computer, such as the CPU, memory, disk, and boot options. The BIOS/UEFI setup can be accessed by pressing aspecific key (such as F2, F10, or Delete) during the boot process, before the operating system loads12.
One of the settings that can be changed in the BIOS/UEFI setup is the CPU hyperthreading option. Hyperthreading is a technology that enables a single physical CPU core to execute two threads or tasks simultaneously, improving the performance and efficiency of multi- threaded applications. However, some software licenses may limit the number of CPU cores or threads that can be used, and therefore require disabling hyperthreading on the server34.
To disable hyperthreading on a server, the administrator will likely need to enter the BIOS/UEFI setup and navigate to the processor options menu. There, the administrator will find a setting for Intel ® Hyperthreading Technology or Hyperthreading Function, which can be enabled or disabled. The administrator will need to disable this setting and save the changes. This will turn off hyperthreading on the server and reduce the number of logical CPUs to match the number of physical cores5.

NEW QUESTION 63
A technician wants to limit disk usage on a server. Which of the following should the technician implement?

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

Answer: C

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

NEW QUESTION 66
An administrator is deploying a new secure web server. The only administration method that is permitted is to connect via RDP. Which of the following ports should be allowed? (Select TWO).

A. 53
B. 80
C. 389
D. 443
E. 45
F. 3389
G. 8080

Answer: DF

Explanation:
Port 443 is the default port for HTTPS, which is the protocol used for secure web communication. HTTPS uses SSL/TLS certificates to encrypt the data between the web server and the browser. Port 443 is commonly used for web servers that need to provide secure services, such as online banking, e-commerce, or email. By allowing port 443, the administrator can access the web server’s interface and manage its settings1.
Port 3389 is the default port for RDP, which is the protocol used for remote desktop connection. RDP allows a user to remotely access and control another computer over a network. Port 3389 is commonly used for remote administration, technical support, or remote work. By allowing port 3389, the administrator can connect to the web server’s desktop and perform tasks that require graphical user interface2.

NEW QUESTION 69
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 74
A server is only able to connect to a gigabit switch at 100Mb. Other devices are able to access the network port at full gigabit speeds, and when the server is brought to another location, it is able to connect at full gigabit speed. Which of the following should an administrator check first?

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

Answer: C

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

NEW QUESTION 76
A server administrator is creating a new server that will be used to house customer sales records. Which of the following roles will MOST likely be Installed on the server?

A. Print
B. File
C. Database
D. Messaging

Answer: C

Explanation:
A database server is a server that hosts a database management system (DBMS) that stores, organizes, and manipulates data. A database server is suitable for housing customer sales records, as it can provide fast and secure access, query and analysis capabilities, backup and recovery options, and scalability and performance optimization. Some examples of database servers are Microsoft SQL Server, Oracle Database, MySQL, and PostgreSQL. Verified References: [What is a Database Server?]

NEW QUESTION 79
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 83
An administrator is tasked with building an environment consisting of four servers that can each serve the same website. Which of the following concepts is described?

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

Answer: A

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

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

NEW QUESTION 85
Users in an office lost access to a file server following a short power outage. The server administrator noticed the server was powered off. Which of the following should the administrator do to prevent this situation in the future?

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

Answer: D

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

NEW QUESTION 90
A server administrator is deploying a new server that has two hard drives on which to install the OS. Which of the following RAID configurations should be used to provide redundancy for the OS?

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

Answer: B

Explanation:
RAID 1 (mirroring) is a RAID configuration that should be used to provide redundancy for the OS on a server that has two hard drives on which to install the OS. RAID 1 (mirroring) is a configuration that duplicates data across two or more drives. It provides fault tolerance and improves read performance, but reduces storage capacity by half. If one drive fails in RAID 1, the other drive can continue to operate without data loss or system downtime. RAID 0 (striping) is a configuration that splits data across two or more drives without parity or redundancy. It improves performance but offers no fault tolerance. If one drive fails in RAID 0, all data is lost and the system cannot boot. RAID 5 (striping with parity) is a configuration thatstripes data across three or more drives with parity information. It provides fault tolerance and improves performance, but reduces storage capacity by one drive’s worth of space. RAID 5 can tolerate one drive failure without data loss, but not two or more. RAID 6 (striping with double parity) is a configuration that stripes data across four or more drives with double parity information. It provides fault tolerance and improves performance, but reduces storage capacity by two drives’ worth of space. RAID 6 can tolerate two drive failures without data loss, but not three or more.References:https://www.howtogeek.com/199068/how-to-upgrade-your-existing-hard-drive-in-under-an-hour/

NEW QUESTION 92
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 96
Which of the following commands would MOST likely be used to register a new service on a Windows OS?

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

Answer: C

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

NEW QUESTION 97
A technician is attempting to log in to a Linux server as root but cannot remember the administrator password. Which of the following is the LEAST destructive method of resetting the administrator password?

A. Boot using a Linux live CD and mount the hard disk to /mn
B. Change to the /mnt/etcdirector
C. Edit the passwd file found in that directory.

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

Answer: C

Explanation:
This is the least destructive method of resetting the administrator password because it does not require modifying any files or reinstalling the OS. It only requires changing the boot parameters temporarily and running a command to change the password.References:https://wiki.archlinux.org/title/Reset_lost_root_password#Using_GR UB

NEW QUESTION 98
A server administrator is completing an OS installation for a new server. The administrator patches the server with the latest vendor-suggested software, configures DHCP, and verifies all network cables are properly connected in the IDF, but there is no network connectivity. Which of the following is the MOST likely reason for the lack of connectivity?

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

Answer: A

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

NEW QUESTION 102
An administrator has been asked to verify that all traffic egressing from a company is secured. The administrator confirms all the information that is sent over the network is encrypted. Which of the following describes the type of traffic being encrypted?

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

Answer: D

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

NEW QUESTION 104
Which of the following license types most commonly describes a product that incurs a yearly cost regardless of how much it is used?

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

Answer: B

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

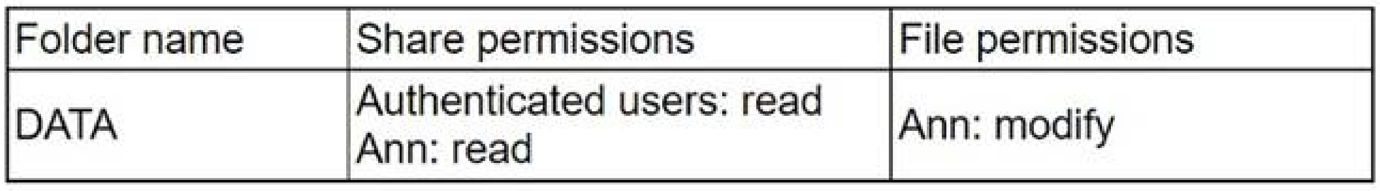
NEW QUESTION 109
A datacenter technician is attempting to troubleshoot a server that keeps crashing. The server runs normally for approximately five minutes, but then it crashes. After restoring the server to operation, the same cycle repeats. The technician confirms none of the configurations have changed, 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.

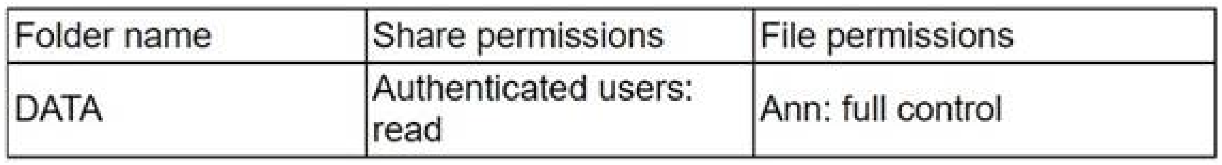
NEW QUESTION 110
An administrator gave Ann modify permissions to a shared folder called DATA, which is located on the company server. Other users need read access to the files in this folder. The current configuration is as follows:



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

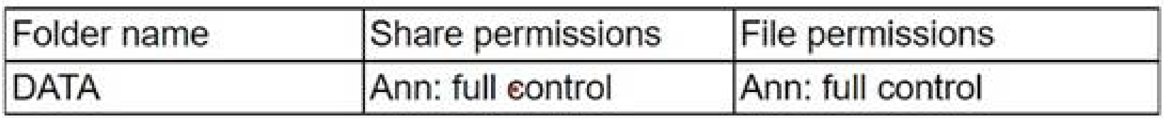
The administrator has determined Ann cannot write anything to the DATA folder using the network. Which of the following would be the best practice to set up Ann's permissions correctly, exposing only the minimum rights required?

A.



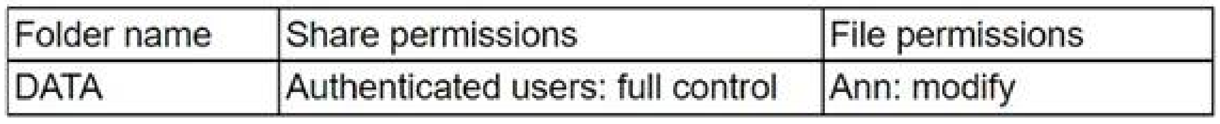
Folder name	Share permissions	File permissions
DATA	Authenticated users: read	Ann: full control

B.



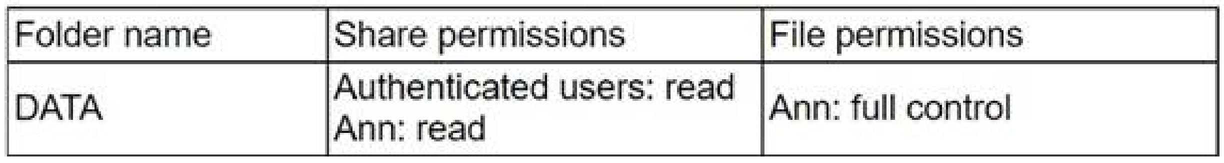
Folder name	Share permissions	File permissions
DATA	Ann: full control	Ann: full control

C.



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

D.



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

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

Answer: D

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

NEW QUESTION 112
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 117
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 122
A server administrator has connected a new server to the network. During testing, the administrator discovers the server is not reachable via server but can be accessed by IP address. Which of the following steps should the server administrator take NEXT? (Select TWO).

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

Answer: CD

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

NEW QUESTION 123
A systems administrator needs to configure a new server and external storage for a new production application environment. Based on end-user specifications, the new solution needs to adhere to the following basic requirements:
* 1. The OS must be installed in a separate disk partition. In case of hard drive failure, it cannot be affected.
* 2. Application data IOPS performance is a must.
* 3. Data availability is a high priority, even in the case of multiple hard drive failures.
Which of the following are the BEST options to comply with the user requirements? (Choose three.)

A. Install the OS on a RAID 0 array.
B. Install the OS on a RAID 1 array.
C. Configure RAID 1 for the application data.
D. Configure RAID 5 for the application data.
E. Use SSD hard drives for the data application array.
F. Use SATA hard drives for the data application array.
G. Use a single JBOD for OS and application data.

Answer: BDE

Explanation:
To comply with the user requirements, the best options are to install the OS on a RAID 1 array, configure RAID 5 for the application data, and use SSD hard drives for the data application array. Here is why:
? RAID 1 is a mirroring technique that creates an exact copy of data on two disks.
This provides redundancy and fault tolerance in case of hard drive failure. RAID 1 also improves read performance since either disk can be read at the same time. Therefore, installing the OS on a RAID 1 array meets the first requirement of separating the OS from the application data and protecting it from hard drive failure.
? RAID 5 is a striping technique with parity that distributes data and parity blocks
across three or more disks. This provides improved performance and storage efficiency compared to RAID 1, as well as fault tolerance in case of a single disk failure. Therefore, configuring RAID 5 for the application data meets the second and third requirements of providing high IOPS performance and data availability.
? SSD hard drives are solid-state drives that use flash memory to store data. They
have no moving parts and offer faster read and write speeds, lower latency, and lower power consumption than traditional HDDs. Therefore, using SSD hard drives for the data application array meets the second requirement of providing high IOPS performance.
References:
? https://phoenixnap.com/kb/raid-levels-and-types
? https://en.wikipedia.org/wiki/Standard_RAID_levels

NEW QUESTION 126
A server administrator must respond to tickets within a certain amount of time. The server administrator needs to adhere to the:

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

Answer: D

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

NEW QUESTION 127
A server administrator just installed a new physical server and needs to harden the applications on the server. Which of the following best describes a method of application hardening?

A. Install the latest patches.
B. Disable unneeded hardware.
C. Set the boot order.
D. Enable a BIOS password.

Answer: A

Explanation:
A method of application hardening is installing the latest patches. Application hardening is a process of reducing the attack surface and vulnerabilities of an application by applying security measures and best practices. Installing the latest patches is one way to harden an application, as patches are updates that fix bugs, errors, or security issues in an application. By installing the latest patches, an application can be protected from known exploits or threats.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.5, Objective 3.5

NEW QUESTION 132
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 136
Which of the following is the MOST appropriate scripting language to use for a logon script for a Linux box?

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

Answer: B

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

NEW QUESTION 140
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 145
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 147
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 148
A server administrator needs to create a new folder on a file server that only specific users can access. Which of the following BEST describes how the server administrator can accomplish this task?

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

Answer: C

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

NEW QUESTION 151
A technician recently applied a critical OS patch to a working sever. After rebooting, the technician notices the server Is unable to connect to a nearby database server. The technician validates a connection can be made to thedatabasefrom another host. Which of the following is the best NEXT step to restore connectivity?

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

Answer: C

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

NEW QUESTION 155
A company is building a new datacenter next to a busy parking lot. Which of the following is the BEST strategy to ensure wayward vehicle traffic does not interfere with datacenter operations?

A. Install security cameras
B. Utilize security guards
C. Install bollards
D. Install a mantrap

Answer: C

Explanation:
The best strategy to ensure wayward vehicle traffic does not interfere with datacenter operations is to install bollards. Bollards are sturdy posts that are installed around a perimeter to prevent vehicles from entering or crashing into a protected area. Bollards can provide physical security and deterrence for datacenters that are located near busy roads or parking lots. Bollards can also prevent accidental damage or injury caused by vehicles that lose control or have faulty brakes.

NEW QUESTION 160
A systems administrator is trying to determine why users in the human resources department cannot access an application server. The systems administrator reviews the application logs but does not see any attempts by the users to access the application. Which of the following is preventing the users from accessing the application server?

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

Answer: C

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

NEW QUESTION 162
A server administrator is creating a script that will move files only if they were created before a date input by the user. Which of the following constructs will allow the script to apply this test until all available files are assessed?

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

Answer: B

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

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

A variable is a script construct that allows the script to store and manipulate data. A variable can be used to store the date input by the user, but it cannot apply a test to each file1
A comparator is a script construct that allows the script to compare two values and determine their relationship. A comparator can be used to check if a file was created before
the date, but it cannot repeat the test for all files1
A conditional is a script construct that allows the script to execute different blocks of code based on certain conditions. A conditional can be used to decide whether to move a file or not, but it cannot iterate over all files1
1: CompTIA Server+ Certification Exam Objectives

NEW QUESTION 166
A remote physical server is unable to communicate to the network through the available NICs, which were misconfigured. However, the server administrator is still able to configure theserver remotely. Which of the following connection types is the server administrator using to access the server?

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

Answer: A

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

NEW QUESTION 168
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 172

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 175
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 178
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

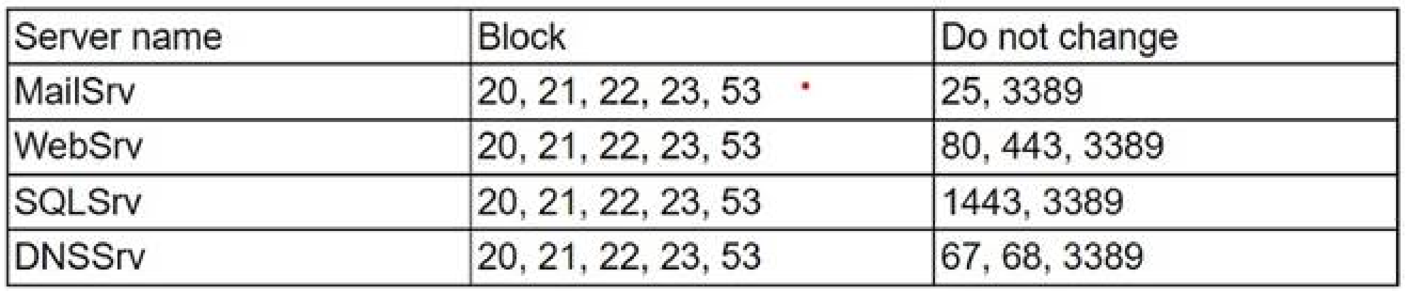
NEW QUESTION 183
A server administrator needs to keep a copy of an important fileshare that can be used to restore the share as quickly as possible. Which of the following is the BEST solution?

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

Answer: D

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

NEW QUESTION 186
A security analyst completed a port scan of the corporate production-server network. Results of the scan were then provided to a systems administrator for immediate action. The following table represents the requested changes:



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

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

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

Answer: E

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

NEW QUESTION 187
A server administrator noticesthe/var/log/audit/audit.logfileon a Linux server is rotating loo frequently. The administrator would like to decrease the number of times the leg rotates without losing any of the information in the logs. Which of the following should the administrator configure?

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

Answer: A

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

NEW QUESTION 190
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 191
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 193
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 198
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 203
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 vNlC

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

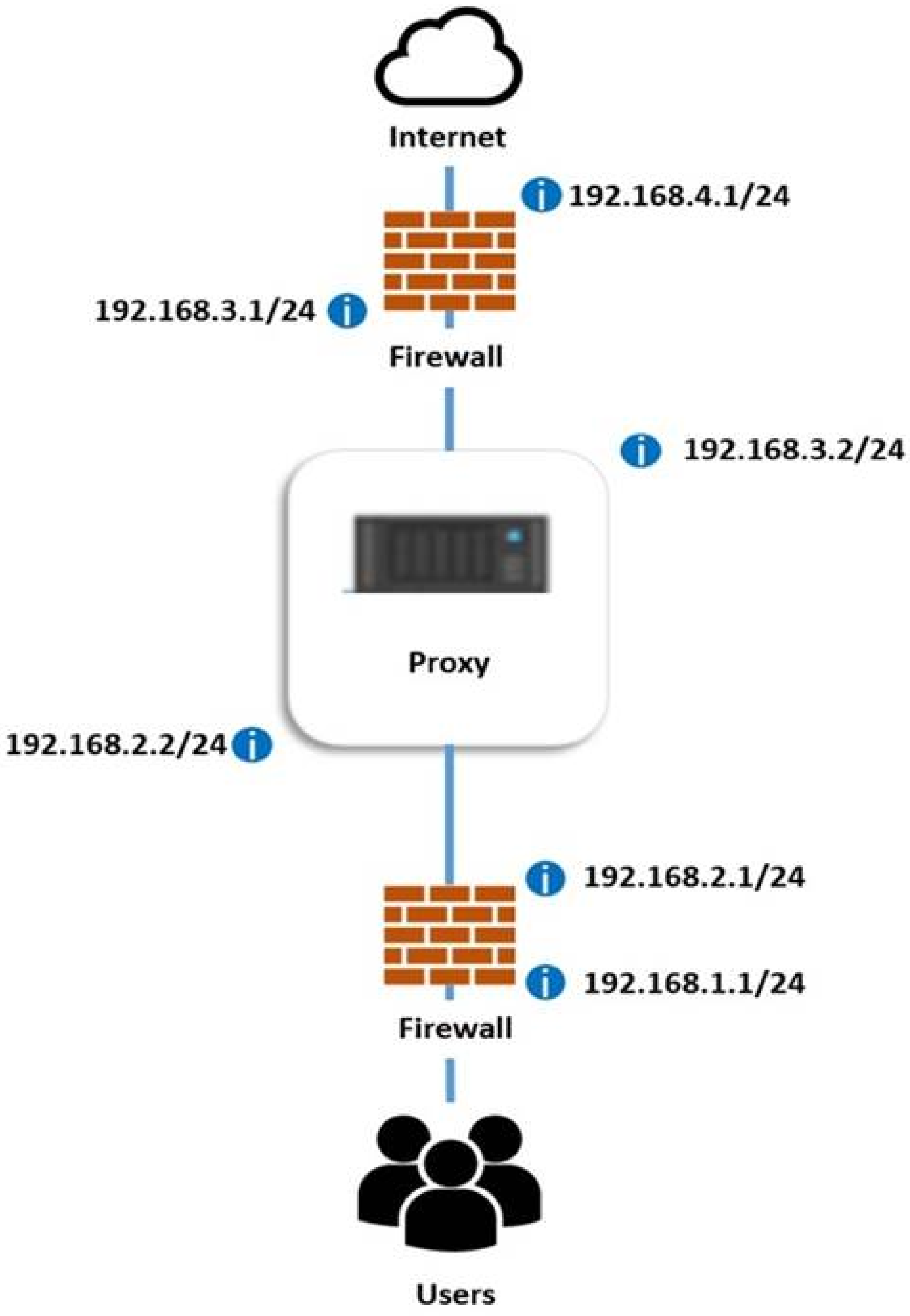
NEW QUESTION 206
An administrator has been asked to increase the storage capacity of a stand-alone file server but no further expansion slots are available. Whichof the following would be the FASTEST solution to implement with no downtime?

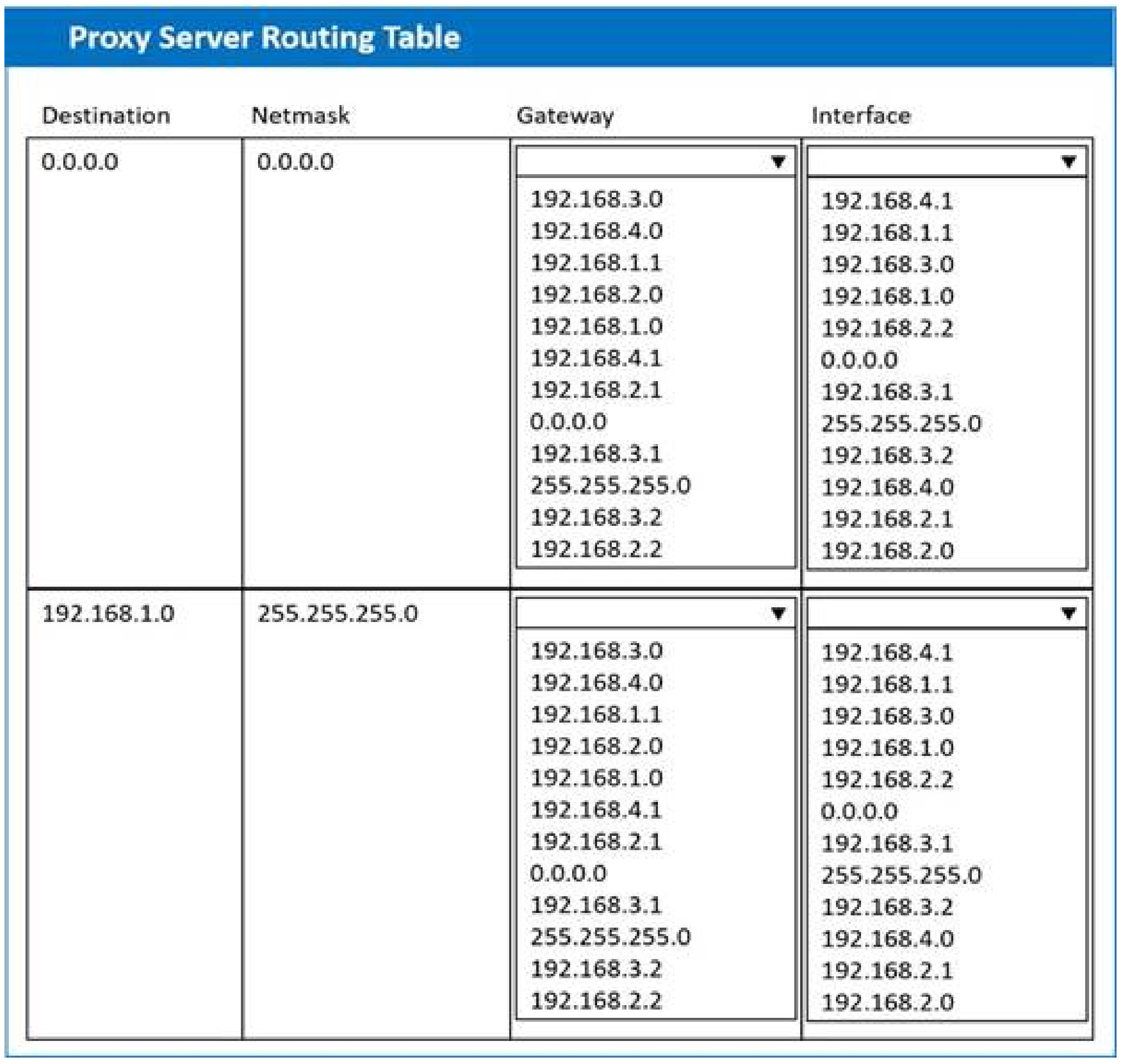
A. Configure a RAID array.
B. Replace the current drives with higher-capacity disks.
C. Implement FCoE for more storage capacity.
D. Connect the server to a SAN

Answer: D

Explanation:
A SAN (Storage Area Network) is a network of storage devices that can provide shared storage capacity to multiple servers. By connecting the server to a SAN, the administrator can increase the storage capacity of the server without adding any internal disks or expansion cards. This solution can be implemented quickly and without any downtime. Verified References: [What is a SAN and how does it differ from NAS?]

NEW QUESTION 208
HOTSPOT
A systems administrator deployed a new web proxy server onto the network. The proxy server has two interfaces: the first is connected to an internal corporate firewall, and the second is connected to an internet-facing firewall. Many users at the company are reporting they are unable to access the Internet since the new proxy was introduced. Analyze the network diagram and the proxy server's host routing table to resolve the Internet connectivity issues.
INSTRUCTIONS
Perform the following steps:
* 1. Click on the proxy server to display its routing table.
* 2. Modify the appropriate route entries to resolve the Internet connectivity issue.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





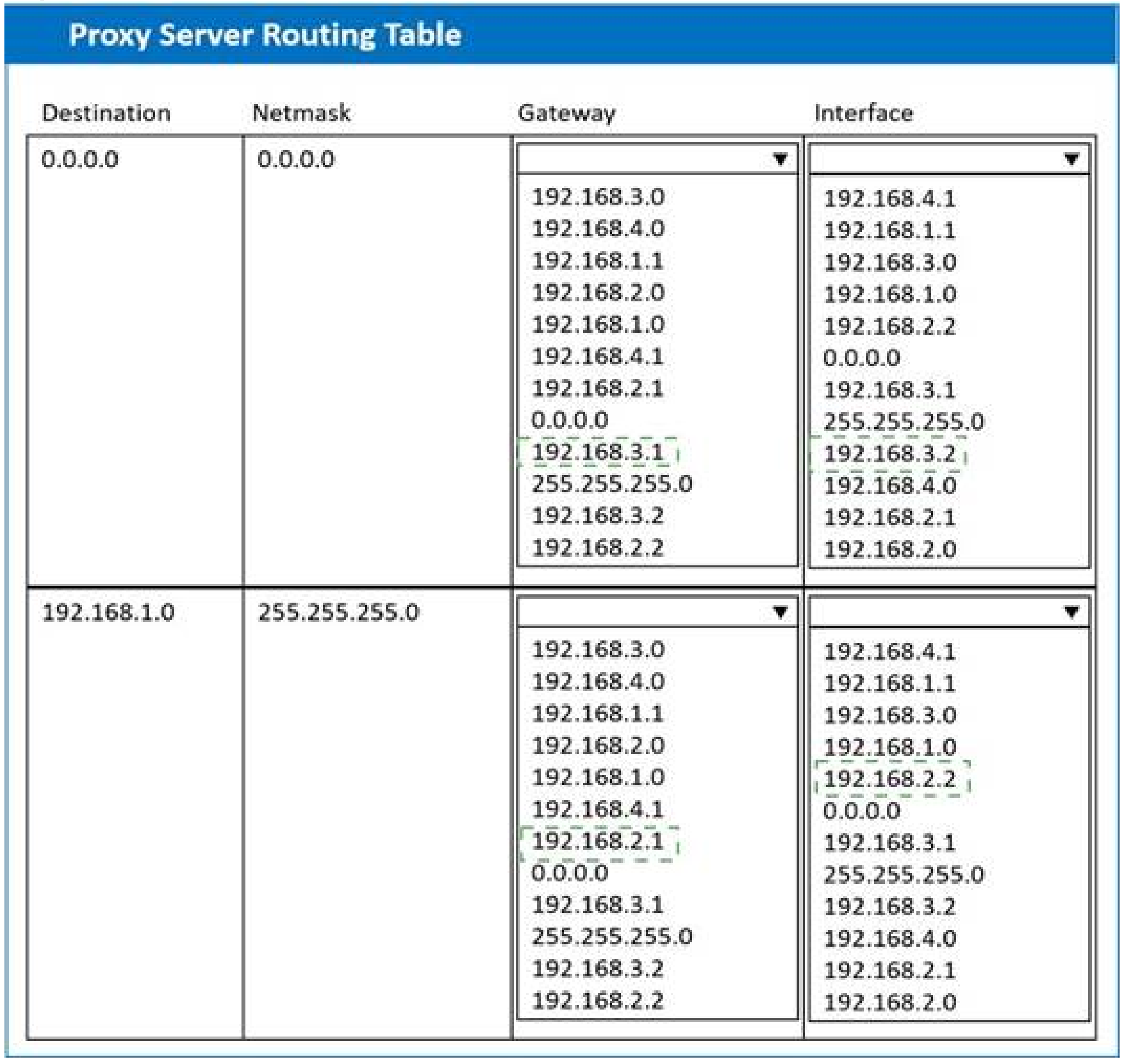
Proxy Server Routing Table

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Proxy Server Routing Table

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

NEW QUESTION 213
An administrator is setting up a new server and has been asked to install an operating system that does not have a GUI because the server has limited resources. Which of the
following installation options should the administrator use?

A. Bare metal
B. Headless
C. Virtualized
D. Slipstreamed

Answer: B

Explanation:
A headless installation is an installation method that does not require a graphical user interface (GUI) or a monitor, keyboard, and mouse. It can be done remotely through a network connection or a command-line interface. A headless installation is suitable for a server that has limited resources and does not need a GUI.
References:
? CompTIA Server+ Certification Exam Objectives1, page 14
? Server Management: Server Hardware Installation and Management2, Module 2, Lesson 5

NEW QUESTION 217
A remote, embedded loT 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 218
A company needs a media server set up that provides the highest availability with a minimum requirement of at least 10TB. The company purchased five HDDs, each with a 4TB
capacity. Which of the options would provide the highest fault tolerance and meet the requirements?

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

Answer: C

Explanation:
RAID 6 is a RAID level that uses disk striping with two parity blocks distributed across all member disks. It can tolerate the failure of up to two disks without losing any data. RAID 6 can provide a minimum of 10TB of usable storage space with five 4TB disks, as the formula for calculating the RAID 6 capacity is (n-2) x Smin, where n is the number of disks and Smin is the smallest disk size. In this case, the RAID 6 capacity is (5-2) x 4TB = 12TB. References:
? CompTIA Server+ Certification Exam Objectives1, page 8
? RAID Levels and Types Explained: Advantages and Disadvantages2
? RAID Levels & Fault Tolerance3

NEW QUESTION 223
A server has experienced several component failures. To minimize downtime, the server administrator wants to replace the components while the server is running. Which of the following can MOST likely be swapped out while the server is still running? (Select TWO).

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

Answer: AC

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

NEW QUESTION 228
A junior administrator needs to configure a single RAID 5 volume out of four 200GB drives attached to the server using the maximum possible capacity. Upon completion, the server reports that all drives were used, and the approximate volume size is 400GB. Which of the following BEST describes the result of this configuration?

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

Answer: B

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

NEW QUESTION 230
An administrate is helping to replicate a large amount of data between two Windows servers. The administrator is unsure how much data has already been transferred. Which of the following will BEST ensure all the data is copied consistently?

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

Answer: D

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

NEW QUESTION 235
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 237
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 239
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 240
Which of the following must a server administrator do to ensure data on the SAN is not compromised if it is leaked?

A. Encrypt the data that is leaving the SAN
B. Encrypt the data at rest
C. Encrypt the host servers
D. Encrypt all the network traffic

Answer: B

Explanation:
The administrator must encrypt the data at rest to ensure data on the SAN is not compromised if it is leaked. Data at rest refers to data that is stored on a device or a medium, such as a hard drive, a flash drive, or a SAN (Storage Area Network). Data at rest can be leaked if the device or the medium is lost, stolen, or accessed by unauthorized parties. Encrypting data at rest means applying an algorithm that transforms the data into an unreadable format that can only be decrypted with a key. Encryption protects data at rest from being exposed or misused by attackers who may obtain the device or the medium.

NEW QUESTION 241
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 244
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 247
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 250
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 251
Due to a recent application migration, a company's current storage solution does not meet the necessary requirements tor hosting data without impacting performance when the data is accessed in real time by multiple users. Which of the following is the BEST solution for this Issue?

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

Answer: D

Explanation:
A Fibre Channel SAN solution is a type of storage area network (SAN) that uses high-speed optical fiber cables to connect servers and storage devices. A SAN allows for hosting data without impacting performance when the data is accessed in real time by multiple users, as it provides fast data transfer rates, low latency, high availability, and scalability12. A local external hard drive (A) would not be suitable for multiple users, as it would limit the accessibility and security of the data. Adding extra memory to the server (B) would not solve the problem of data access performance, as it would not increase the bandwidth or reduce the congestion of the network. Compressing the data © would not improve the performance either, as it would add extraoverhead and complexity to the data processing and retrieval. References: 1 https://www.techradar.com/best/best-cloud- storage 2 https://solutionsreview.com/data-storage/the-best-enterprise-data-storage- solutions/

NEW QUESTION 254
A company deploys antivirus, anti-malware, and firewalls that can be assumed to be functioning properly. Which of the following is the MOST likely system vulnerability?

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

Answer: A

Explanation:
Insider threat is the most likely system vulnerability in a company that deploys antivirus, anti-malware, and firewalls that can be assumed to be functioning properly. An insider threat is a malicious or negligent act by an authorized user of a system or network that compromises the security or integrity of the system or network. An insider threat can include data theft, sabotage, espionage, fraud, or other types of attacks. Antivirus, anti-malware, and firewalls are security tools that can protect a system or network from external threats, such as viruses, worms, ransomware, or open ports. However, these tools cannot prevent an insider threat from exploiting their access privileges or credentials to harm the system or network.

NEW QUESTION 257
Which of the following would MOST likely be part of the user authentication process when implementing SAML across multiple applications?

A. SSO
B. LDAP
C. TACACS
D. MFA

Answer: A

Explanation:
The term that is most likely part of the user authentication process when implementing SAML across multiple applications is SSO. SSO (Single Sign-On) is a way for users to be authenticated for multiple applications and services at once. With SSO, a user signs in at a single login screen and can then use a number of apps without having to enter their credentials again. SSO improves user experience and security by reducing password fatigue and phishing risks. SAML (Security Assertion Markup Language) is a protocol that enables SSO by providing a standardized way to exchange authentication and authorization data between an identity provider (IdP) and a service provider (SP). SAML uses XML-based messages called assertions to communicate user identity and attributes between parties.
Reference:
https://www.onelogin.com/learn/how-single-sign-on-works

NEW QUESTION 259
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 260
A server administrator has received calls regarding latency and performance issues with a file server. After reviewing all logs and server features the administrator discovers the server came with four Ethernet ports, out only one port is currently in use. Which of the following features will enable the use of all available ports using a single IP address?

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

Answer: D

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

NEW QUESTION 261
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 265
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 268
A backup application is copying only changed files each time it runs. During a restore, however, only a single file is used. Which of the following backup methods does this describe?

A. Open file
B. Synthetic full
C. Full incremental
D. Full differential

Answer: B

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

NEW QUESTION 273
Which of the following is an architectural reinforcement that is used to attempt to conceal the exterior of an organization?

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

Answer: C

Explanation:
Camouflage is an architectural reinforcement that is used to attempt to conceal the exterior of an organization. Camouflage is a technique of blending in with the surroundings or disguising the appearance of a building or facility to make it less noticeable or identifiable. Camouflage can reduce the visibility and attractiveness of a target for potential attackers or intruders. References: CompTIA Server+ Certification Exam Objectives, Domain 5.0: Security, Objective 5.1: Given a scenario, apply physical security methods to a server.

NEW QUESTION 277
Which of the following is typical of software licensing in the cloud?

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

Answer: C

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

NEW QUESTION 280
A newly installed server is accessible to local users, but remote users are unable to connect. Which of the following is MOST likely misconfigured?

A. The IP address
B. The default gateway
C. The VLAN
D. The subnet mask

Answer: B

Explanation:
This is the most likely misconfigured setting because the default gateway is the router that connects the local network to other networks. If the default gateway is incorrect, the server will not be able to communicate with remote users or devices outside its own subnet.
References:https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig

NEW QUESTION 285
A company is reviewing options for its current disaster recovery plan and potential changes to it. The security team will not allow customer data to egress to non-company equipment, and the company has requested recovery in the shortest possible time. Which of the following will BEST meet these goals?

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

Answer: B

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

NEW QUESTION 289
An administrator has been troubleshooting a server issue. The administrator carefully questioned the users and examined the available logs. Using this information, the administrator was able to rule out several possible causes and develop a theory as to what the issue might be. Through further testing, the administrator's theory proved to be correct. Which of the following should be the next step to troubleshoot the issue?

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

Answer: D

Explanation:
The next step to troubleshoot the issue after developing and testing a theory is to establish an action plan. This involves identifying the steps needed to implement the solution, estimating the time and resources required, and evaluating the potential risks and impacts of the solution. Documenting the findings and actions, escalating the issue to the management team, or implementing the solution are steps that should be done after establishing an action plan. References: [CompTIA

Server+ Certification Exam Objectives], Domain 6.0: Disaster Recovery, Objective 6.2: Explain troubleshooting theory and methodologies.

NEW QUESTION 293
Which of the following open ports should be closed to secure the server properly? (Choose two.)

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

Answer: AC

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

NEW QUESTION 297
A large number of connections to port 80 is discovered while reviewing the log files on a server. The server is not functioning as a web server. Which of the following represent the BEST immediate actions to prevent unauthorized server access? (Choose two.)

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

Answer: CF

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

NEW QUESTION 298
A server administrator is installing a new server on a manufacturing floor. Because the server is publicly accessible, security requires the server to undergo hardware hardening. Which of the following actions should the administrator take?

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

Answer: C

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

NEW QUESTION 301
A staff memberwho a monitoring a data center reports one rack is experiencing higher temperatures than the racks next to it, despite the hardware in each rack being the same. Which of the following actions would MOST likely remediate the heal issue?

A. Installing blanking panels in all the empty rack spaces
B. installing an additional POU and spreading out the power cables
C. Installing servers on the shelves instead of sliding rails
D. installing front bezels on all the server's m the rack

Answer: A

Explanation:
Blanking panels are metal or plastic plates that are installed in the empty spaces of a rack to prevent hot air from recirculating back to the front of the rack. This can improve the airflow and cooling efficiency of the rack and reduce the heat generated by the servers. Verified References: [Blanking panel], [Rack cooling]

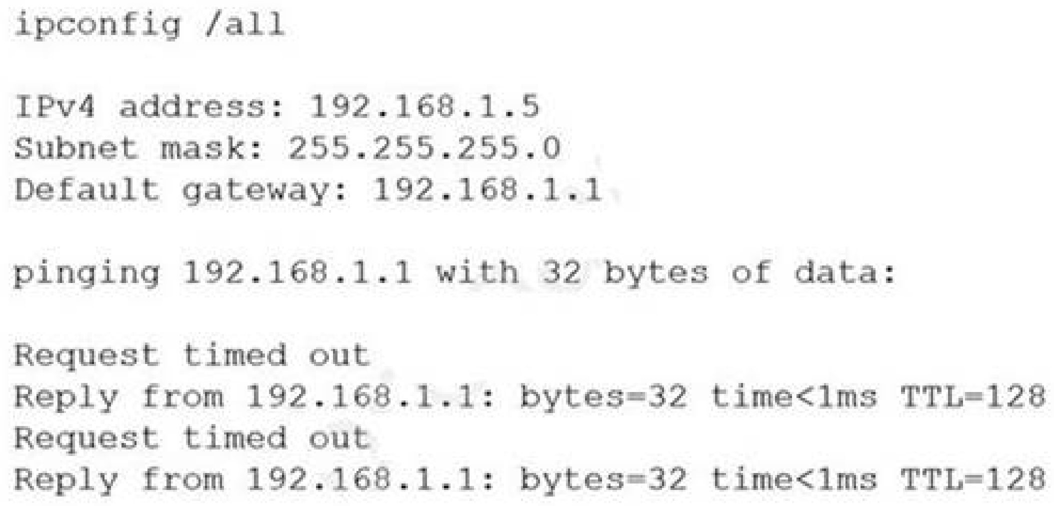
NEW QUESTION 305
A server administrator purchased a single license key to use for all the new servers that will be imaged this year. Which of the following MOST likely refers to the licensing type that will be used?

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

Answer: D

Explanation:
This is the most likely licensing type that will be used because volume licensing allows a single license key to be used for multiple installations of a software product. Volume licensing is typically used by organizations that need to deploy software to a large number of devices or users.References:https://www.microsoft.com/en-us/licensing/licensing-programs/volume-licensing-programs

NEW QUESTION 308
A server technician installs a new NIC on a server and configures the NIC for IP connectivity. The technician then tests the connection using thepingcommand. Given the following partial output of thepingandipconfigcommands:



```
ipconfig /all

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

pinging 192.168.1.1 with 32 bytes of data:

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

Which of the following caused the issue?

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

Answer: A

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

NEW QUESTION 310
Following a recent power outage, a server in the data center has been constantly going offline and losing its configuration. Users have been experiencing access issues while using the application on the server. The server technician notices the date and time are incorrect when the server is online. All other servers are working. Which of the following would most likely cause this issue? (Select two).

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

Answer: BE

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

NEW QUESTION 314
......