CompTIA

Exam Questions SK0-005

CompTIA Server+ Certification Exam

NEW QUESTION 1
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.

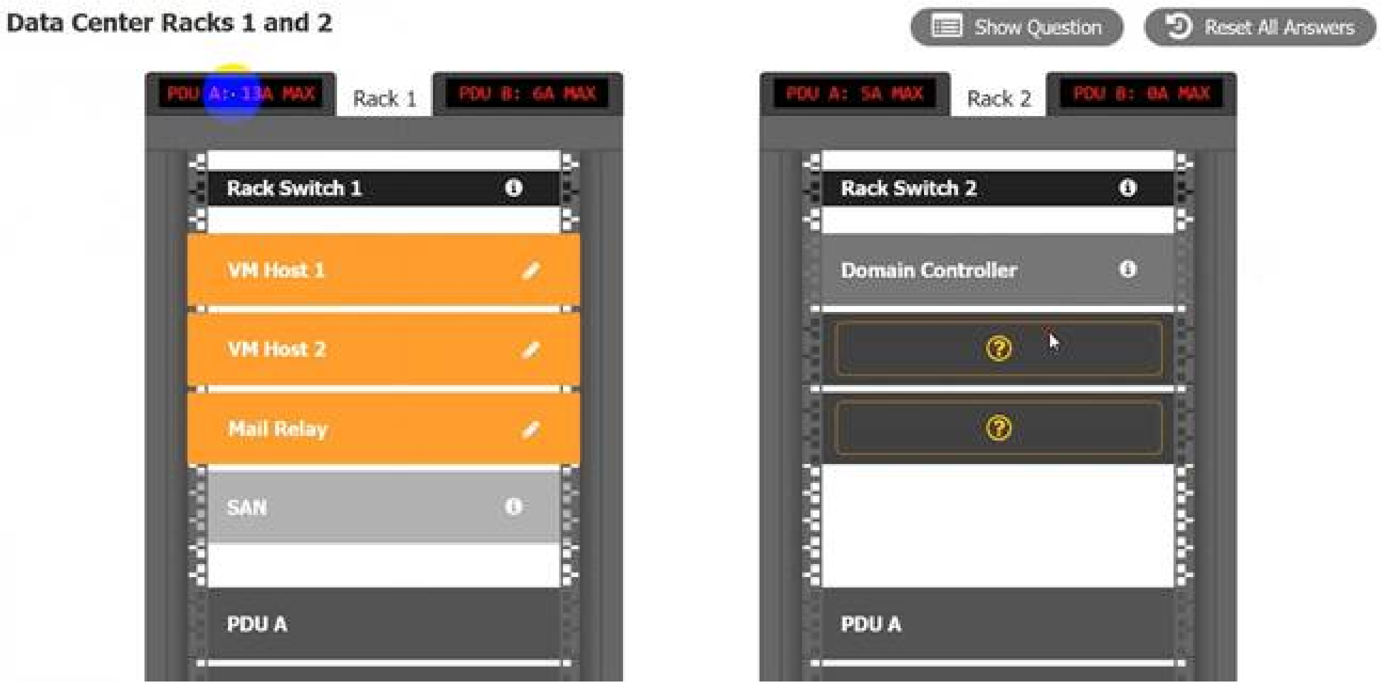
NEW QUESTION 2
An organization purchased six new 4TB drives for a server. An administrator is tasked with creating an efficient RAID given the minimum disk space requirement of 19TBs. Which of the following should the administrator choose to get the most efficient use of space?

A. RAID 1
B. RAID 5
C. RAID 6
D. RAID 10

Answer: B

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

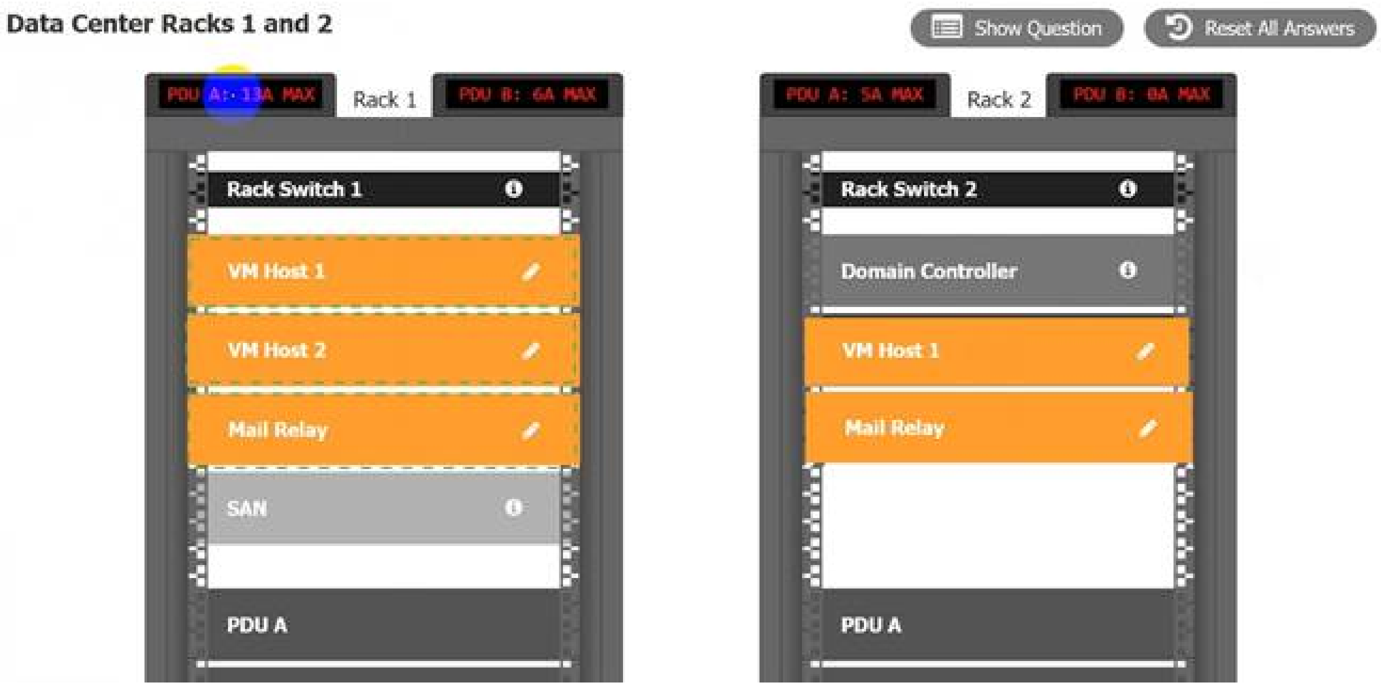
NEW QUESTION 3
DRAG DROP
A recent power Outage caused email services to go down. A sever administrator also received alerts from the datacenter's UPS.
After some investigation, the server administrator learned that each POU was rated at a maximum Of 12A.
INSTRUCTIONS
Ensure power redundancy is implemented throughout each rack and UPS alarms are resolved. Ensure the maximum potential PDU consumption does not exceed 80% or 9.6A).
* a. PDU selections must be changed using the pencil icon.
* b. VM Hosts 1 and 2 and Mail Relay can be moved between racks.
* c. Certain devices contain additional details



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 4
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 5
The management team has mandated the use of data-at-rest encryption for all data. Which of the following forms of encryption best achieves this goal?

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

Answer: A

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

NEW QUESTION 6
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 7
A systems administrator notices a newly added server cannot see any of the LUNs on the SAN. The SAN switch and the local HBA do not display any link lights. Which of the following is most likely the issue?

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

Answer: A

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

NEW QUESTION 8
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 9
A server administrator is installing a new server with multiple NICs on it. The Chief Information Officer has asked the administrator to ensure the new server will have the least amount of network downtime but a good amount of network speed. Which of the following best describes what the administrator should implement on the new server?

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

Answer: C

Explanation:
Link aggregation is the best option to implement on the new server to ensure the least amount of network downtime but a good amount of network speed. Link aggregation is a technique of combining multiple physical network interfaces into one logical interface to increase bandwidth, redundancy, and load balancing. Link aggregation can improve the performance and availability of the server by allowing it to use more than one network path for data transmission and failover in case of link failure. Link aggregation can be implemented using various protocols, such as IEEE 802.3ad (LACP), Cisco EtherChannel, or Linux bonding. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Networking, Objective 4.1: Given a scenario, configure network settings for servers.

NEW QUESTION 10
A technician is installing a variety of servers in a rack. Which of the following is the BEST course of action for the technician to take while loading the rack?

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

Answer: B

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

NEW QUESTION 10
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 14
Which of the following are measures that should be taken when a data breach occurs? (Select TWO).

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

Answer: BE

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

NEW QUESTION 18
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 23
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 26
A server administrator added a new drive to a server. However, the drive is not showing up as available. Which of the following does the administrator need to do to make the drive available?

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

Answer: A

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

NEW QUESTION 27
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

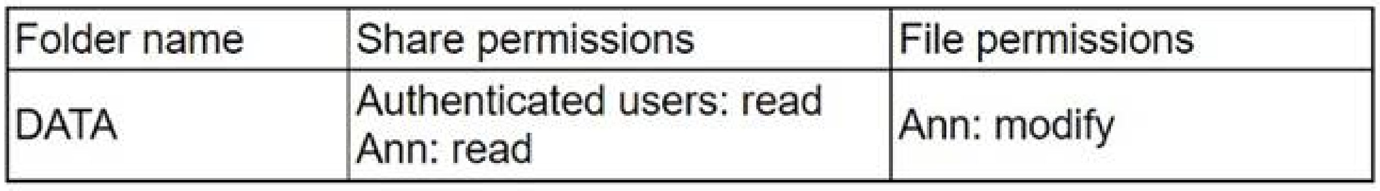
NEW QUESTION 29
An organization implements split encryption keys for sensitive files. Which of the following types of risks does this mitigate?

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

Answer: D

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

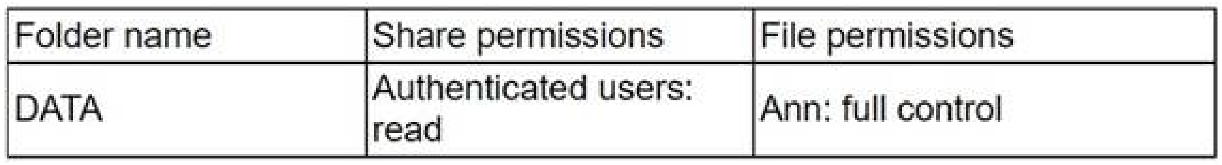
NEW QUESTION 30
An administrator gave Ann modify permissions to a shared folder called DATA, which is located on the company server. Other users need read access to the files in this folder. The current configuration is as follows:



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

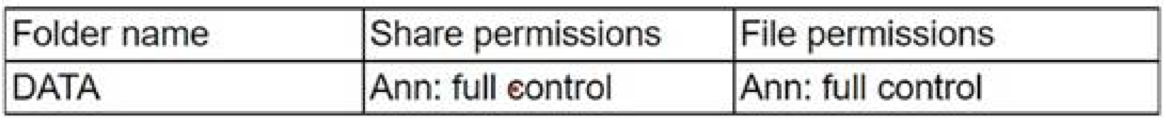
The administrator has determined Ann cannot write anything to the DATA folder using the network. Which of the following would be the best practice to set up Ann's permissions correctly, exposing only the minimum rights required?

A.



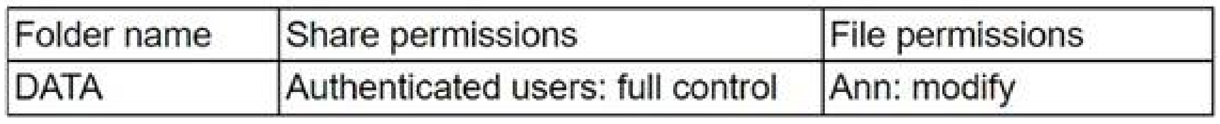
Folder name	Share permissions	File permissions
DATA	Authenticated users: read	Ann: full control

B.



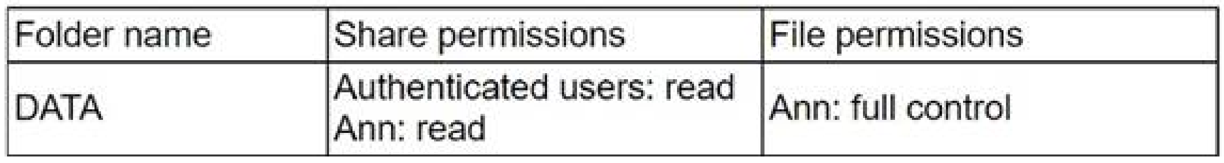
Folder name	Share permissions	File permissions
DATA	Ann: full control	Ann: full control

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 31
Users ate experiencing issues when trying to access resources on multiple servers. The servers are virtual and run on an ESX server. A systems administrator is investigating but is unable to connect to any of the virtual servers. When the administrator connects to the host, a purple screen with while letters appears. Which of the following troubleshooting steps should the administrator perform FIRST?

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

Answer: B

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

NEW QUESTION 35
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 36
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 38
A server administrator has configured a web server. Which of the following does the administrator need to install to make the website trusted?

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

Answer: B

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

NEW QUESTION 40
Two developers are working together on a project, and they have built out a set of snared servers that both developers can access over the internet. Which of the following cloud models is this an example of?

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

Answer: B

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

NEW QUESTION 44
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]

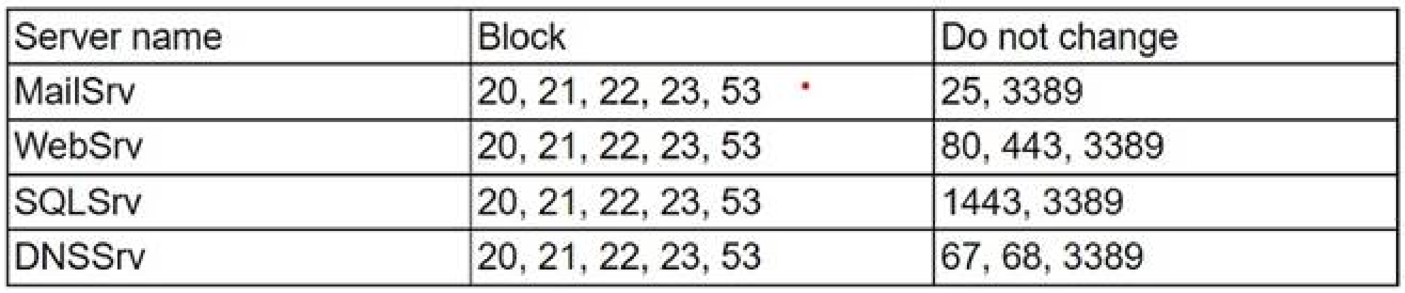
NEW QUESTION 46
A server administrator wants to run a performance monitor for optimal system utilization. Which of the following metrics can the administrator use for monitoring? (Choose two.)

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

Answer: AE

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

NEW QUESTION 48
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 50
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 52
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 57
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 62
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 64
A server administrator recently installed a kernel update to test functionality Upon reboot, the administrator determined the new kernel was not compatible with certain server hardware and was unable to uninstall the update. Which of the following should the administrator do to mitigate further issues with the newly instated kernel version?

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

Answer: A

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

NEW QUESTION 67
After installing a new file server, a technician notices the read times for accessing the same file are slower than the read times for other file servers.
Which of the following is the first step the technician should take?

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

Answer: B

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

NEW QUESTION 69
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 71
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 72
A user has been unable to authenticate to the company's external, web-based database after clicking a link in an email that required the user to change the account password. Which of the following steps should the company take next?

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

Answer: A

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

NEW QUESTION 74
A server administrator deployed a new product that uses a non-standard port for web access on port 8443. However, users are unable to access the new application. The server administrator checks firewall rules and determines 8443 is allowed. Which of the following is most likely the cause of the issue?

A. Intrusion detection is blocking the port.
B. The new application's DNS entry is incorrect.
C. The application should be changed to use port 443.
D. The core switch has a network issue.

Answer: B

Explanation:
A DNS entry is a record that maps a domain name to an IP address. If the DNS entry for the new application is incorrect, users will not be able to resolve the domain name to the correct IP address and port number. This will prevent them from accessing the application, even if the firewall rules allow port 8443. To fix this issue, the server administrator should verify and update the DNS entry for the new application.
References: CompTIA Server+ Study Guide, Chapter 6: Networking, page 230.

NEW QUESTION 76
A server administrator needs to implement load balancing without purchasing any new hardware or implementing any new software. Which of the following will the administrator most likely implement?

A. Round robin
B. Link aggregation
C. Most recently used
D. Heartbeat

Answer: B

Explanation:
Link aggregation is a technique that allows multiple network interfaces to act as one logical interface, increasing the bandwidth and redundancy of the connection. This can improve the load balancing of network traffic without requiring any new hardware or software. Round robin, most recently used, and heartbeat are not load balancing methods, but rather scheduling algorithms or monitoring techniques. References: CompTIA Server+ Certification Exam Objectives, Domain 2.0: Networking, Objective 2.3: Given a scenario, configure NIC teaming.

NEW QUESTION 80

An administrator is researching the upcoming licensing software requirements for an application that usually requires very little technical support. Which of the following licensing models would be the LOWEST cost solution?

A. Open-source
B. Per CPU socket
C. Per CPU core
D. Enterprise agreement

Answer: A

Explanation:
Open-source software is software that is freely available and can be modified and distributed by anyone. It usually requires very little technical support and has no licensing fees. Therefore, it would be the lowest cost solution for an application that does not need much support.References: https://www.comptia.org/training/resources/exam- objectives/comptia-server-sk0-005-exam-objectives (Objective 2.3)

NEW QUESTION 82
A server administrator needs to check remotely for unnecessary running services across 12 servers. Which of the following tools should the administrator use?

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

Answer: B

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

NEW QUESTION 85
A technician recently upgraded several pieces of firmware on a server. Ever since the technician rebooted the server, it no longer communicates with the network. Which of the following should the technician do FIRST to return the server to service as soon as possible?

A. Replace the NIC
B. Make sure the NIC is on the HCL
C. Reseat the NIC
D. Downgrade the NIC firmware

Answer: D

Explanation:
The first thing that the technician should do to return the server to service as soon as possible is downgrade the NIC firmware. Firmware is a type of software that controls the basic functions of hardware devices, such as network interface cards (NICs). Firmware updates can provide bug fixes, performance improvements, or new features for hardware devices. However, firmware updates can also cause compatibility issues, configuration errors, or functionality failures if they are not installed properly or if they are not compatible with the device model or driver version. Downgrading the firmware means reverting to an older version of firmware that was previously working fine on the device. Downgrading the firmware can help resolve any problems caused by a faulty firmware update and restore normal operation of the device.

NEW QUESTION 90
A change in policy requires a complete backup of the accounting server every seven days and a backup of modified data every day. Which of the following would be BEST to restore a full backup as quickly as possible in the event of a complete loss of server data?

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

Answer: D

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

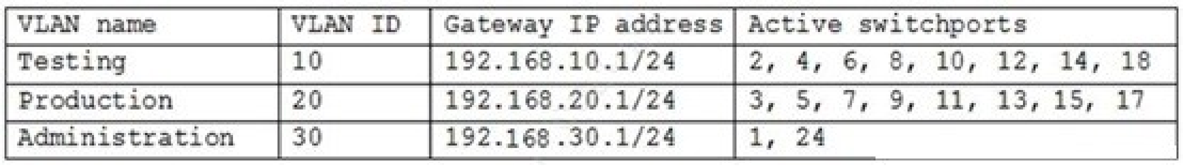
NEW QUESTION 95
A technician runs top on a dual-core server and notes the following conditions: top –- 14:32:27, 364 days, 14 usersload average 60.5 12.4 13.6
Which of the following actions should the administrator take?

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

Answer: C

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

NEW QUESTION 96
A server administrator is configuring the IP address on a newly provisioned server in the testing environment. The network VLANs are configured as follows:



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

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

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

Answer: A

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

NEW QUESTION 98
An administrator is able to ping the default gateway and internet sites byname from a file server. The file server is not able to ping the print server by name. The administrator is able to ping the file server from the print server by both IP address and computer name. When initiating an initiating from the file server for the print server, a different IP address is returned, which of the following is MOST Likely the cause?

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

Answer: D

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

NEW QUESTION 99
A technician has beer tasked to install a new CPU. Prior to the retaliation the server must be configured. Which of the following should the technician update?

A. The RAID card
B. The BIOS
C. The backplane
D. The HBA

Answer: B

Explanation:
The BIOS (Basic Input/Output System) is a firmware that controls the initialization and booting of a server. It also provides settings for the CPU, such as speed, voltage, and temperature. Updating the BIOS can improve the performance and compatibility of the CPU and other hardware components. Verified References: [BIOS], [CPU]

NEW QUESTION 100
A technician needs to install a Type 1 hypervisor on a server. The server has SD card slots, a SAS controller, and a SATA controller, and it is attached to a NAS. On which of the following drive types should the technician install the hypervisor?

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

Answer: A

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

NEW QUESTION 103
A Linux server requires repetitive tasks for reconfiguration. Which of the following would be the best scripting language to use?

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

Answer: C

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

NEW QUESTION 108
An administrator is configuring the storage for a new database server, which will host databases that are mainly used for archival lookups. Which of the following storage types
will yield the fastest database read performance?

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

Answer: B

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

NEW QUESTION 111
Which of the following access control methodologies can be described BEST as allowing a user the least access based on the jobs the user needs to perform?

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

Answer: B

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

NEW QUESTION 113
Which of the following can be BEST described as the amount of time a company can afford to be down during recovery from an outage?

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

Answer: C

Explanation:

The term that best describes the amount of time a company can afford to be down during recovery from an outage is RTO. RTO (Recovery Time Objective) is a metric that defines the maximum acceptable downtime for an application, system, or process after a disaster or disruption. RTO helps determine the level of urgency and resources required for restoring normal business operations. RTO is usuallymeasured in minutes, hours, or days, depending on the criticality and impact of the service.
Reference:
https://whatis.techtarget.com/definition/recovery-time-objective-RTO

NEW QUESTION 115
Which of the following asset management documents is used to identify the location of a serves within a data center?

A. Infrastructure diagram
B. Workflow diagram
C. Rack layout
D. Service manual

Answer: C

Explanation:
A rack layout is a document that shows the physical location and arrangement of servers and other devices within a rack. It can include information such as server names, IP addresses, power consumption, and cable connections. A rack layout can help identify and locate servers easily and efficiently in a data center. Verified References: [Rack layout], [Data center]

NEW QUESTION 118
Users are able to connect to the wireless network, but they are unable to access the internet. The network administrator verifies connectivity to all network devices, and there are no ISP outages. The server administrator removes the old address leases from the active leases pool, which allows users to access the internet. Which of the following is most likely causing the internet issue?

A. THe DHCP exclusion needs to be removed.
B. The DHCP scope is full.
C. The DHCP scope options are misconfigured.
D. The DHCP lease times are too short.
E. The DHCP reservations need to be configured.

Answer: B

Explanation:
The most likely cause of the internet issue is B. The DHCP scope is full.
A DHCP scope is a range of IP addresses that a DHCP server can assign to DHCP clients on a network. A DHCP scope has a start address and an end address, and it can also have some excluded addresses that are not available for lease. A DHCP scope can have various options, such as subnet mask, default gateway, DNS server, etc., that are applied to the DHCP clients along with the IP address. A DHCP scope also has a lease time, which is the duration that a DHCP client can use an IP address before renewing it or releasing it. A DHCP scope can have reservations, which are fixed IP addresses that are assignedto specific DHCP clients based on their MAC addresses12
If a DHCP scope is full, it means that there are no more IP addresses available for lease in the scope. This can happen if the number of DHCP clients exceeds the number of IP addresses in the scope, or if the lease time is too long and the IP addresses are not released or reused frequently enough. If a DHCP scope is full, any new or existing DHCP clients that request an IP address from the DHCP server will not receive one, and they will not be able to access the network or the internet12
In this scenario, users are able to connect to the wireless network, but they are unable to access the internet. The network administrator verifies connectivity to all network devices, and there are no ISP outages. The server administrator removes the old address leases from the active leases pool, which allows users to access the internet. This indicates that the DHCP scope is full, and that removing the old leases frees up some IP addresses for lease in the scope. Therefore, option B is the most likely cause of the internet issue.

NEW QUESTION 122
An administrator notices high traffic on a certain subnet and would like to identify the source of the traffic. Which of the following tools should the administrator utilize?

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

Answer: D

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

NEW QUESTION 125
Which of the following is the MOST secure method to access servers located in remote
branch offices?

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

Answer: A

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

NEW QUESTION 126
A newly hired systems administrator is concerned about fileshare access at the company. The administrator turns on DLP for the fileshare and lets it propagate for a week. Which of the following can the administrator perform now?

A. Manage the fileshare from an RDP session.
B. Audit the permissions of the fileshare.
C. Audit the access to the physical fileshare.
D. Manage the permissions from the fileshare.

Answer: B

Explanation:
DLP, or Data Loss Prevention, is a type of security measure that aims to prevent unauthorized access, use, or transfer of sensitive data. DLP can be applied to various types of data, such as email, cloud storage, network traffic, or fileshares1. DLP for fileshares can help monitor and control who can access, modify, or share files on a network share2. By turning on DLP for the fileshare and letting it propagate for a week, the administrator can audit the permissions of the fileshare and see if there are any violations
or anomalies in the access patterns. This can help the administrator identify and remediate any potential risks or compliance issues related to the fileshare2. The other options are incorrect because they are not directly related to DLP for fileshares. Managing the fileshare from an RDP session or from the fileshare itself are administrative tasksthat do not require DLP. Auditing the access to the physical fileshare is a physical security measure that is not affected by DLP.

NEW QUESTION 130
The Chief Information Officer of a data center is concerned that transmissions from the building can be detected from the outside. Which of the following would resolve this concern? (Select TWO).

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

Answer: CD

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

NEW QUESTION 133
A server is reporting a hard drive S.M.A.R.T. error. When a technician checks on the drive, however, it appears that all drives in the server are functioning normally. Which of the following is the reason for this issue?

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

Answer: A

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

NEW QUESTION 138
An administrator has deployed a new virtual server from a template. After confirming access to the subnet's gateway, the administrator is unable to log on with the domain credentials. Which of the following is the most likely cause of the issue?

A. The server has not been joined to the domain.
B. An IP address has not been assigned to the server.

C. The server requires a reboot to complete the deployment process.
D. The domain credentials are invalid.

Answer: A

Explanation:
The most likely cause of the issue is that the server has not been joined to the domain. A domain is a logical group of computers and devices that share a common directory service and security policy. A domain controller is a server that manages the domain and authenticates users and computers that want to access domain resources. To log on with domain credentials, a server must be joined to the domain and registered in the directory service. If a server has not been joined to the domain, it will not be recognized or authorized by the domain controller.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 4, Lesson 4.3, Objective 4.3

NEW QUESTION 143
Which of the following is the most effective way to mitigate risks associated with privacy- related data leaks when sharing with a third party?

A. Third-party acceptable use policy
B. Customer data encryption and masking
C. Non-disclosure and indemnity agreements
D. Service- and operational-level agreements

Answer: B

Explanation:
The most effective way to mitigate risks associated with privacy-related data leaks when sharing with a third party is customer data encryption and masking. Encryption is a process of transforming data into an unreadable format that can only be decrypted with a key or password. Masking is a process of hiding or replacing sensitive data with fake or meaningless data. By encrypting and masking customer data, the organization can protect the confidentiality and integrity of the data and prevent unauthorized access or disclosure by the third party.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.3, Objective 3.3

NEW QUESTION 147
Which of the following technologies would allow an administrator to build a software RAID on a Windows server?

A. Logical volume management
B. Dynamic disk
C. GPT
D. UEFI

Answer: B

Explanation:
Dynamic disk is a technology that allows an administrator to build a software RAID on a Windows server. Dynamic disk is a type of disk management that supports creating volumes that span multiple disks, stripe data across disks, mirror data between disks, or use parity for fault tolerance. Dynamic disk can be used to create RAID 0 (striping), RAID 1 (mirroring), RAID 5 (striping with parity), or spanned volumes on Windows servers. Logical volume management is a technology that allows creating and resizing logical volumes on Linux servers. GPT (GUID Partition Table) is a standard for defining the partition structure on a disk. UEFI (Unified Extensible Firmware Interface) is a specification for the interface between the operating system and the firmware. References: https://www.howtogeek.com/school/using-windows-admin-tools-like-a-pro/lesson2/ https://www.howtogeek.com/howto/40702/how-to-manage-and-use-lvm-logical-volume-management-in-ubuntu/ https://www.howtogeek.com/193669/whats-the-difference-between-gpt-and-mbr-when-partitioning-a-drive/https://www.howtogeek.com/56958/htg- explains-how-uefi-will-replace-the-bios/

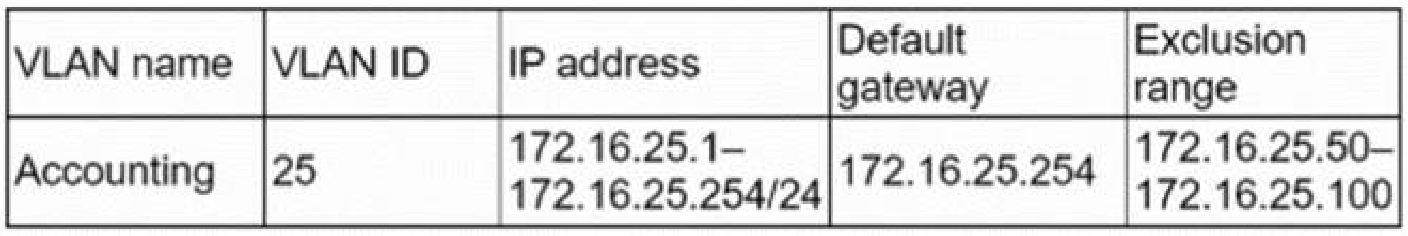
NEW QUESTION 151
A technician needs to install a Type 1 hypervisor on a server. The server has SD card slots, a SAS controller, and a SATA controller, and it is attached to a NAS. On which of the following drive types should the technician install the hypervisor?

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

Answer: D

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

NEW QUESTION 152
A server technician is placing a newly configured server into a corporate environment. The server will be used by members of the accounting department, who are currently assigned by the VLAN identified below:



VLAN name	VLAN ID	IP address	Default gateway	Exclusion range
Accounting	25	172.16.25.1–172.16.25.254/24	172.16.25.254	172.16.25.50–172.16.25.100

Which of the following IP address configurations should the technician assign to the new server so the members of the accounting group can access the server?

A. IP address: 172.16.25.90/24 Default gateway: 172.16.25.254
B. IP address: 172.16.25.101/16 Default gateway: 172.16.25.254
C. IP address: 172.16.25.254/24 Default gateway: 172.16.25.1
D. IP address: 172.16.26.101/24 Default gateway: 172.16.25.254

Answer: A

Explanation:
The IP address configuration that the technician should assign to the new server so the members of the accounting group can access the server is 172.16.25.90/24 for the IP address and 172.16.25.254 for the default gateway. This configuration matches the VLAN identified in the image, which has a network address of 172.16.25.0/24 and a subnet mask of 255.255.255.0. The IP address of the server must be within the same network range as the VLAN, which is from 172.16.25.1 to 172.16.25.254, excluding the network and broadcast addresses (172.16.25.0 and 172.16.25.255). The default gateway of the server must be the same as the VLAN, which is 172.16.25.254, to allow communication with other networks or devices outside the VLAN. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Networking, Objective 4.1: Given a scenario, configure network settings for servers.

NEW QUESTION 154
A server is performing slowly, and users are reporting issues connecting to the application on that server. Upon investigation, the server administrator notices several unauthorized services running on that server that are successfully communicating to an external site. Which of the following are MOST likely causing the issue?
(Choose two.)

A. Adware is installed on the users' devices
B. The firewall rule for the server is misconfigured
C. The server is infected with a virus
D. Intrusion detection is enabled on the network
E. Unnecessary services are disabled on the server
F. SELinux is enabled on the server

Answer: CF

Explanation:
The server is infected with a virus and SELinux is enabled on the server are most likely causing the issue of unauthorized services running on the server. A virus is a type of malicious software that infects a system and performs unwanted or harmful actions, such as creating, modifying, deleting, or executing files. A virus can also create backdoors or open ports on a system to allow remote access or communication with external sites. SELinux (Security-Enhanced Linux) is a security module for Linux systems that enforces mandatory access control policies on processes and files. SELinux can prevent unauthorized services from running on a server by restricting their access to resources based on their security context. However, SELinux can also cause problems if it is not configured properly or if it conflicts with other security tools.

NEW QUESTION 159
Users at a company are licensed to use an application that is restricted by the number of active sessions. Which of the following best describes this licensing model?

A. Per-server
B. per-seat
C. Per-concurrent user
D. per-core

Answer: C

Explanation:
The per-concurrent user licensing model is a type of licensing model that restricts the number of active sessions or connections to a software application at any given time. This means that multiple users can share the same license, as long as they do not access the application simultaneously. This model is often used for applications that are accessed intermittently or for a short duration by different users, such as remote access software, web-based applications, or testing tools12.

NEW QUESTION 164
Which of the following licensing models is MOST appropriate tor a data center that has a variable daily equipment count?

A. Pet site
B. Per server
C. Per user
D. Per core

Answer: D

Explanation:
A per core licensing model is based on the number of processor cores in a server. This model is suitable for a data center that has a variable daily equipment count, as it allows for scaling up or down the number of cores as needed. A per core licensing model also provides better performance and efficiency than other models. Verified References: [Per Core Licensing and Basic Definitions]

NEW QUESTION 166
A systems administrator has several different types of hard drives. The administrator is setting up a MAS that will allow end users to see all the drives within the NAS. Which of the following storage types should the administrator use?

A. RAID array
B. Serial Attached SCSI
C. Solid-state drive
D. Just a bunch of disks

Answer: D

Explanation:
JBOD (Just a Bunch Of Disks) is a storage configuration that combines different types and sizes of hard drives into one logical unit without any RAID level or redundancy. It allows users to see all the drives within the unit as one large storage space. JBOD can utilize all the available capacity of the drives but does not provide any performance or fault tolerance benefits. Verified References: [JBOD], [RAID]

NEW QUESTION 170
A server administrator wants to check the open ports on a server. Which of the following commands should the administrator use to complete the task?

A. nslookup
B. nbtstat
C. telnet
D. netstat -a

Answer: D

Explanation:
netstat is a command-line tool that displays network connections, routing tables, interface statistics, and more. The -a option shows all listening and non-listening sockets on the server. This can help check the open ports on a server and identify any unwanted or malicious connections.References:https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat

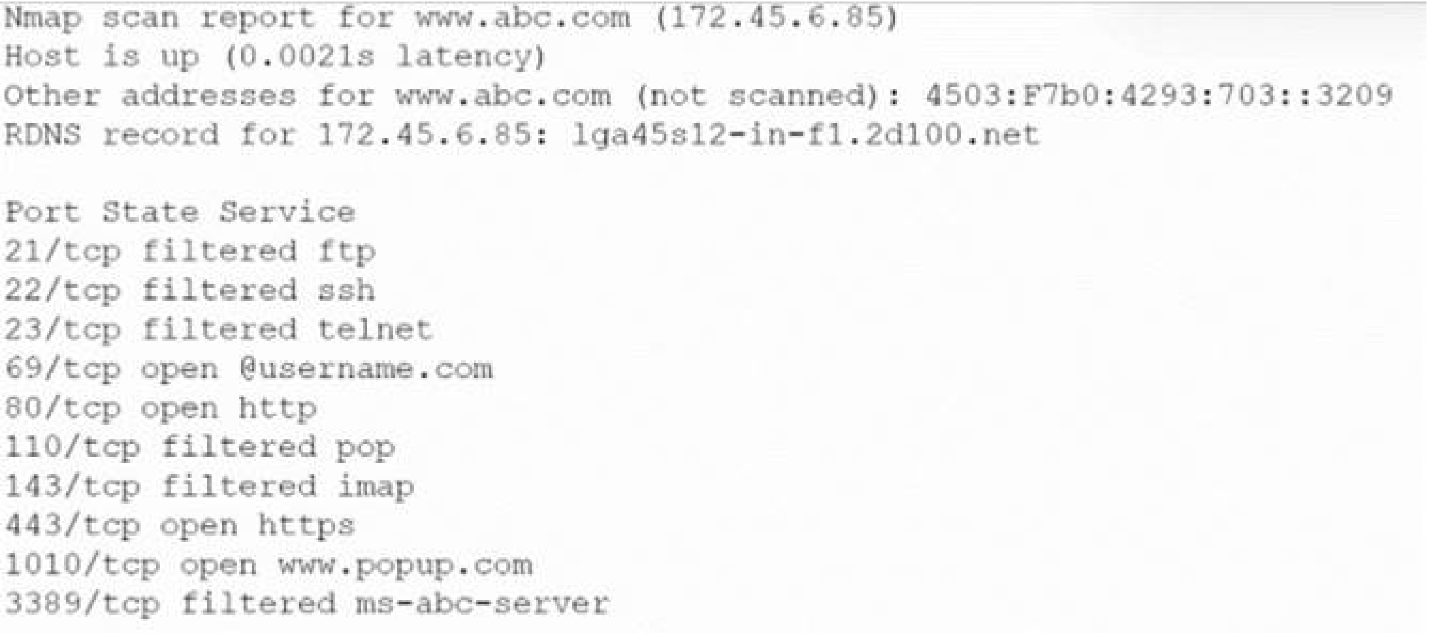
NEW QUESTION 174
A server administrator is implementing an authentication policy that will require users to use a token during login. Which of the following types of authentication is the administrator implementing?

A. Something you are
B. Something you know
C. Something you have
D. Something you do

Answer: C

Explanation:
Something you have is one of the types of authentication methods that relies on a physical object or device that the user possesses to verify their identity. A token is an example of something you have, as it is a small device that generates a one-time password or code that the user enters during login. A token can be a hardware device, such as a key fob or a smart card, or a software application, such as an app on asmartphone or a browser extension. A token provides an additional layer of security to the authentication process, as it prevents unauthorized access even if the user's username and password are compromised1.

NEW QUESTION 178
Which of the following actions should the server administrator perform on the server?



```
Nmap scan report for www.abc.com (172.45.6.85)
Host is up (0.0021s latency)
Other addresses for www.abc.com (not scanned): 4503:F7b0:4293:703::3209
RDNS record for 172.45.6.85: lga45s12-in-f1.2d100.net

Port State Service
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
69/tcp open @username.com
80/tcp open http
110/tcp filtered pop
143/tcp filtered imap
443/tcp open https
1010/tcp open www.popup.com
3389/tcp filtered ms-abc-server
```

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

Answer: C

Explanation:
The server administrator should close port 3389 and rerun the scan. Port 3389 is used for Remote Desktop Protocol (RDP), which allows remote access and

control of a server. RDP is vulnerable to brute-force attacks, credential theft, and malware infection. Closing port 3389 can prevent unauthorized access and improve the security of the server. The other ports are not as risky as port 3389 and can be left open for legitimate purposes. References: CompTIA Server+ Certification Exam Objectives, Domain 5.0: Security, Objective 5.4: Given a scenario, implement proper environmental controls and techniques.

NEW QUESTION 179
A company is running an application on a file server. A security scan reports the application has a known vulnerability. Which of the following would be the company's BEST course of action?

A. Upgrade the application package
B. Tighten the rules on the firewall
C. Install antivirus software
D. Patch the server OS

Answer: A

Explanation:
The best course of action for the company is to upgrade the application package to fix the known vulnerability. A vulnerability is a weakness or flaw in an application that can be exploited by an attacker to compromise the security or functionality of the system. Upgrading the application package means installing a newer version of the application that has patched or resolved the vulnerability. This way, the company can prevent potential attacks that may exploit the vulnerability and cause damage or loss.

NEW QUESTION 181
A storage administrator is investigating an issue with a failed hard drive. A technician replaced the drive in the storage array; however, there is still an issue with the logical volume. Which of the following best describes the NEXT step that should be completed to restore the volume?

A. Initialize the volume
B. Format the volume
C. Replace the volume
D. Rebuild the volume

Answer: D

Explanation:
The administrator should rebuild the volume to restore it after replacing the failed hard drive. A volume is a logical unit of storage that can span across multiple physical disks. A volume can be configured with different levels of RAID (Redundant Array of Independent Disks) to provide fault tolerance and performance enhancement. When a hard drive in a RAID volume fails, the data on that drive can be reconstructed from the remaining drives using parity or mirroring techniques. However, this process requires a new hard drive to replace the failed one and a rebuild operation to copy the data from the existing drives to the new one. Rebuilding a volume can take a long time depending on the size and speed of the drives and the RAID level.

NEW QUESTION 184
Which of the following tools will analyze network logs in real time to report on suspicious log events?

A. Syslog
B. DLP
C. SIEM
D. HIPS

Answer: C

Explanation:
SIEM is the tool that will analyze network logs in real time to report on suspicious log events. SIEM stands for Security Information and Event Management, which is a software solution that collects, analyzes, and correlates log data from various sources, such as servers, firewalls, routers, antivirus software, etc. SIEM can detect anomalies, patterns, trends, and threats in the log data and generate alerts or reports for security monitoring and incident response. SIEM can also provide historical analysis and compliance reporting for audit purposes.
Reference:
https://www.manageengine.com/products/eventlog/syslog-server.html

NEW QUESTION 189
A very old PC is running a critical, proprietary application in MS-DOS. Administrators are concerned about the stability of this computer. Installation media has been lost, and the vendor is out of business. Which of the following would be the BEST course of action to preserve business continuity?

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

Answer: B

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

NEW QUESTION 191
An upper management team is investigating a security breach of the company's filesystem. It has been determined that the breach occurred within the human resources department. Which of the following was used to identify the breach in the human resources department?

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

Answer: B

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

NEW QUESTION 193
An administrator is troubleshooting a failure in the data center in which a server shut down/turned off when utility power was lost The server had redundant power supplies. Which of the following is the MOST likely cause of this failure?

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

Answer: C

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

NEW QUESTION 197
A global organization keeps personnel application servers that are local to each country. However, a security audit shows these application servers are accessible from sites in other countries. Which of the following hardening techniques should the organization use to restrict access to only sites that are in the same country?

A. Configure a firewall
B. Close the unneeded ports
C. Install a HIDS
D. Disable unneeded services.

Answer: A

Explanation:
Monitors Network Traffic Reference:https://www.fortinet.com/resources/cyberglossary/benefits-of-firewall

NEW QUESTION 202
Which of the following life-cycle management phases deals with a server that is no longer in operation?

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

Answer: A

Explanation:
End-of-life is the phase of lifecycle management that deals with a server that is no longer in operation. End-of-life means that the server has reached the end of its useful life and is no longer supported by the manufacturer or the service provider. End-of-life may also imply that the serveris obsolete, incompatible, or inefficient for the current needs and standards1. End-of-life servers may be decommissioned, recycled, donated, or disposed of according to the organizational policies and environmental regulations

NEW QUESTION 207
Which of me following is the BEST action to perform before applying patches to one of the hosts in a high availability cluster?

A. Disable the heartbeat network.
B. Fallback cluster services.
C. Set the cluster to active-active.
D. Failover all VMs.

Answer: D

Explanation:
This is the best action to perform before applying patches to one of the hosts in a high availability cluster. A high availability cluster is a group of hosts that act like a single system and provide continuous uptime. A high availability cluster is often used for load balancing, backup, and failover purposes. Failover is a process of

transferring workloads from one host to another in case of a failure or maintenance. By failing over all VMs (Virtual Machines) from the host that needs to be patched to another host in the cluster, the technician can ensure that there is no downtime or data loss during the patching process. Disabling the heartbeat network is not a good action to perform, as this would disrupt the communication and synchronization between the hosts in the cluster. Fallback cluster services is not a valid term, but it may refer to restoring cluster services after a failover, which is not relevant before applying patches. Setting the cluster to active- active is not a good action to perform, as this would increase the load on both hosts and reduce redundancy. References: https://www.howtogeek.com/190014/virtualization-basics-understanding-techniques-and-fundamentals/https://www.howtogeek.com/428483/what-is- end-to-end-encryption-and-why-does-it-matter/

NEW QUESTION 209
A developer is creating a web application that will contain five web nodes. The developer's main goal is to ensure the application is always available to the end users. Which ofthe following should the developer use when designing the web application?

A. Round robin
B. Link aggregation
C. Network address translation
D. Bridged networking

Answer: A

Explanation:
Round robin is a load balancing technique that distributes requests among multiple web nodes in a circular order. It ensures that each web node receives an equal amount of requests and improves the availability and performance of the web application. Verified References: [Round robin], [Load balancing]

NEW QUESTION 214
Which of the following describes the installation of an OS contained entirely within another OS installation?

A. Host
B. Bridge
C. Hypervisor
D. Guest

Answer: D

Explanation:
The installation of an OS contained entirely within another OS installation is described as a guest. A guest is a term that refers to a virtual machine (VM) that runs on top of a host operating system (OS) using a hypervisor or a virtualization software. A guest can have a different OS than the host, and can run multiple applications or services independently from the host. A guest can also be isolated from the host and other guests for security or testing purposes.

NEW QUESTION 219
Which of the following concepts is in use when dual power supplies are connected to different power sources?

A. Fault tolerance
B. Active-passive
C. Component redundancy
D. Heartbeat
E. Link aggregation

Answer: A

Explanation:
The concept in use when dual power supplies are connected to different power sources is fault tolerance. Fault tolerance is the ability of a system to continue operating without interruption or loss of data in the event of a failure of one or more components. By connecting dual power supplies to different power sources, the system can switch to the alternative power supply or source if one fails, ensuring continuous availability and reliability.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 1, Lesson 1.3, Objective 1.3

NEW QUESTION 222
An administrator is troubleshooting a failed NIC in an application server. The server uses DHCP to get all IP configurations, and the server must use a specific IP address. The administrator replaces the NIC, but then the server begins to receive a different and incorrect IP address. Which of the following will enable the server to get the proper IP address?

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

Answer: A

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

? Static IP vs DHCP Reservation - The Tech Journal
? How to Configure DHCP Server Reservation in Windows … - ITIngredients

NEW QUESTION 226

......