CompTIA.SK0-005.v2025-06-06.q195

Exam Code:	SK0-005
Exam Name:	CompTIA Server+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	195
Version:	v2025-06-06
# of views:	13741
# of Questions views:	5321
https://www.dumpsfiles.com/files/CompTIA/SK0-005/CompTIA.SK0-005.v2025-06-06.q195	

NEW QUESTION: 1
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 (LEAVE A REPLY)
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: 2
Which of the following server types would benefit MOST from the use of a load balancer?
A. DNS server
B. File server
C. DHCP server
D. Web server
Answer: D (LEAVE A REPLY)
The server type that would benefit most from the use of a load balancer is web server. A web server is a server that hosts web applications or websites and responds to requests from web browsers or clients. A load balancer is a device or software that distributes network traffic across multiple servers based on various criteria, such as availability, capacity, or performance. A load balancer can improve the scalability, reliability, and performance of web servers by balancing the workload and preventing any single server from being overloaded or unavailable.

Reference:
https://www.dnsstuff.com/what-is-server-load-balancing

NEW QUESTION: 3
A server administrator is configuring a new server that will hold large amounts of information. The server will need to be accessed by multiple users at the same time. Which of the following server roles will the administrator MOST likely need to install?
A. Messaging
B. Application
C. Print
D. Database
Answer: D (LEAVE A REPLY)
Few people are expected to use the database at the same time and users don't need to customize the design of the database.
Reference: https://support.microsoft.com/en-us/office/ways-to-share-an-access-desktop-database-03822632- da43-4d8f-ba2a-68da245a0446 The server role that the administrator will most likely need to install for a server that will hold large amounts of information and will need to be accessed by multiple users at the same time is database. A database is a collection of structured data that can be stored, queried, manipulated, and analyzed using various methods and tools. A database server is a server that hosts one or more databases and provides access to them over a network. A database server can handle large amounts of information and support concurrent requests from multiple users or applications.

NEW QUESTION: 4
Which of the following should be configured in pairs on a server to provide network redundancy?
A. MRU
B. SCP
C. DLP
D. CPU
E. NIC
Answer: E (LEAVE A REPLY)
NIC stands for network interface card, which is a hardware component that allows a server to connect to a network. Configuring NICs in pairs on a server would provide network redundancy, meaning that if one NIC fails, the other one can take over and maintain network connectivity. The other options are not related to network redundancy.

NEW QUESTION: 5
A systems administrator is setting up a second VLAN for end users. Which of the following should be provisioned for a DHCP server to be able to receive client requests from a different subnet?
A. Relay agent
B. NIC teaming
C. VLAN ID
D. Zone transfers
E. DHCP options
Answer: A (LEAVE A REPLY)

NEW QUESTION: 6

A server administrator needs to deploy five VMs, all of which must have the same type of configuration.
Which of the following would be the MOST efficient way to perform this task?
A. Snapshot a VM.
B. Use a physical host.
C. Perform a P2V conversion.
D. Use a VM template.
Answer: (SHOW ANSWER)
Deploying a virtual machine from a template creates a virtual machine that is a copy of the template. The new virtual machine has the virtual hardware, installed software, and other properties that are configured for the template.
Reference: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vm_admin.doc/GUID-8254CD05-CC06-491D-BA56-A773A32A8130.html
The most efficient way to perform the task of deploying five VMs with the same type of configuration is to use a VM template. A template is a preconfigured virtual machine image that contains an operating system, applications, settings, and other components. A template can be used to create multiple identical or customized VMs quickly and easily, without having to install and configure each VM from scratch. A template can save time and ensure consistency across VMs.

NEW QUESTION: 7
A user logs in to a Linux server and attempts to run the following command:
sudo emacs /root/file
However the user gets the following message:
User userid is not allowed to execute Temacs' on this server. Which of the following would BEST allow the user to find out which commands can be used?
A. visudo I grep userid
B. sudo -1 -U userid
C. cat /etc/passwd
D. userlist I grep userid
Answer: B (LEAVE A REPLY)
This is the best command to find out which commands can be used by a user with sudo privileges because it lists the allowed and forbidden commands for a given user or role. The -l option stands for list, and the -U option specifies the user name. The output of this command will show what commands can be executed with sudo by that user on that server. References: https://www.sudo.ws/man/1.8.13/sudo.man.html

NEW QUESTION: 8
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 (LEAVE A REPLY)
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: 9
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: (SHOW ANSWER)
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: 10
A technician noted the RAID hard drives were functional while troubleshooting a motherboard failure. The technician installed a spare motherboard with similar specifications and used the original components. Which of the following should the technician do to restore operations with minimal downtime?
A. Reinstall the OS and programs.
B. Configure old drives to RAID.
C. Reconfigure the RAID.
D. Install from backup.
Answer: C (LEAVE A REPLY)
RAID (Redundant Array of Independent Disks) is a technology that combines multiple hard drives into a logical unit that provides improved performance, reliability, or capacity. RAID can be implemented by hardware, software, or a combination of both. Hardware RAID uses a dedicated controller to manage the RAID array, while software RAID uses the operating system or a driver to do the same1.
In this scenario, the technician noted that the RAID hard drives were functional while troubleshooting a motherboard failure. This means that the data on the drives was not corrupted or lost. However, the technician installed a spare motherboard with similar specifications and used the original components. This means that the new motherboard may not have the same RAID configuration as the old one, or it may not recognize the existing RAID array at all. Therefore, the technician needs to reconfigure the RAID in order to restore operations with minimal downtime.

NEW QUESTION: 11
A technician is preparing a deployment of servers to be used by staff at a remote location. Which of the following should the technician do to prevent access to the hardware configuration?
A. Enable an administrator account
B. Enable a UEFI password
C. Disable WOL
D. Enable encryption at rest

Answer: B (LEAVE A REPLY)
Enabling a UEFI (Unified Extensible Firmware Interface) password prevents unauthorized users from making changes to the server's hardware configuration settings, such as boot order or device settings. This is crucial for protecting the integrity of the server at a remote location where physical security might be more difficult to enforce.
* UEFI password (Answer B): It provides security at the firmware level, preventing changes to low- level configurations unless the correct password is provided.
* Administrator account (Option A): While important for OS-level access, it doesn't prevent someone with physical access from altering hardware settings via UEFI/BIOS.
* Disabling WOL (Option C): Wake-on-LAN (WOL) allows a device to be powered on remotely.
Disabling it can help with security but does not prevent hardware configuration changes.
* Encryption at rest (Option D): Encryption protects data on the server but does not prevent hardware configuration access.
CompTIA Server+ Reference:This topic is covered under SK0-005 Objective 2.1: Install and configure server operating systems.

NEW QUESTION: 12
After a technician upgrades the firmware on a database server that is connected to two external storage arrays, the server prompts the technician to configure RAID. The technician knows the server had several configured RAID sets and thinks the firmware upgrade cleared the RAID configurations. Which of the following should the technician do to troubleshoot this issue?
A. Power cycle the storage arrays and rescan RAID on the server.
B. Boot the OS into recovery mode and rescan the disks.
C. Restore the default RAID configuration and reboot.
D. Perform a rescan on the server's RAID controller.
Answer: D (LEAVE A REPLY)
A rescan on the server's RAID controller is a possible troubleshooting step to detect the existing RAID configurations on the connected storage arrays. A firmware upgrade may cause the RAID controller to lose the RAID metadata or settings, and a rescan may restore them. A rescan is preferable to restoring the default RAID configuration, as the latter may erase the existing data on the arrays. Power cycling the storage arrays or booting the OS into recovery mode may not help if the RAID controller does not recognize the RAID sets.
References: CompTIA Server+ Study Guide, Chapter 7: Storage, page 287.

NEW QUESTION: 13
An administrator is troubleshooting connectivity to a remote server. The goal is to remotely connect to the server to make configuration changes. To further troubleshoot, a port scan revealed the ports on the server as follows:
Port 22: Closed
Port 23: Open
Port 990: Closed
Which of the following next steps should the administrator take?
Reboot the workstation and then the server.
A. Open port 990 and close port 23.
B. Open port 22 and close port 23.
C. Open all of the ports listed.
D. Close all of the ports listed.
Answer: B (LEAVE A REPLY)

Port 22 is used for SSH (Secure Shell), which is a secure and encrypted protocol for remote access to a server.
Port 23 is used for Telnet, which is an insecure and unencrypted protocol for remote access. Port 990 is used for FTPS (File Transfer Protocol Secure), which is a secure and encrypted protocol for file transfer. The administrator should open port 22 and close port 23 to enable SSH and disable Telnet, as SSH is more secure and reliable than Telnet. The administrator does not need to open port 990, as FTPS is not required for making configuration changes123.
References = 1: Remote Desktop - Allow access to your PC from outside your network(https://learn.microsoft.
com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-allow-outside-access) 2:
Test remote network port connectionin Windows 10 - Winaero(https://winaero.com/test-remote-network-port- connection-in-windows-10/) 3: Windows Command to check if a remote server port is opened?
(https://superuser.com/questions/1035018/windows-command-to-check-if-a-remote-server-port-is-opened)

NEW QUESTION: 14
A technician has been asked to check on a SAN. Upon arrival, the technician notices the red LED indicator shows a disk has failed. Which of the following should the technician do NEXT, given the disk is hot swappable?
A. Stop sharing the volume
B. Replace the disk
C. Shut down the SAN
D. Stop all connections to the volume
Answer: B (LEAVE A REPLY)
The next thing that the technician should do, given the disk is hot swappable, is to replace the disk. A hot swappable disk is a disk that can be removed and replaced without shutting down the system or affecting its operation. A hot swappable disk is typically used in a storage array that has RAID (Redundant Array of Independent Disks) configuration that provides fault tolerance and redundancy. If a disk fails in a RAID array, it can be replaced by a new disk without interrupting the service or losing any data. The new disk will automatically rebuild itself using the data from the other disks in the array.

NEW QUESTION: 15
The management team has requested that new software licenses be purchased out of the capital budget as one- time, non-renewing expenses this year. Which of the following types of software licenses would most likely be used to meet this request?
A. Open-source
B. Subscription
C. Volume
D. Perpetual
Answer: D (LEAVE A REPLY)
Aperpetual licenseis a one-time purchase that allows the software to be used indefinitely without recurring costs. This meets the requirement of a non-renewing, one-time capital expense.
* Perpetual (Answer D):This is a one-time purchase and does not require renewal, making it ideal for capital expenditure.
* Open-source (Option A):Open-source software is usually free but may not meet specific licensing requirements.
* Subscription (Option B):This typically involves recurring payments, which contradicts the non- renewing expense requirement.
* Volume (Option C):Volume licenses are used for purchasing multiple licenses at a discount but may still involve subscription-based renewals.
CompTIA Server+ Reference:This topic is covered underSK0-005 Objective 2.1: Explain licensing concepts for software.

NEW QUESTION: 16
An administrator discovers a Bash script file has the following permissions set in octal notation;
777
Which of the following is the MOST appropriate command to ensure only the root user can modify and execute the script?
A. chmod go-rw>:
B. chmod u=rwx
C. chmod u+wx
D. chmod g-rwx
Answer: A (LEAVE A REPLY)
chmod is a command-line tool that changes the permissions of files and directories in Linux and Unix systems. chmod go-rwx means to remove read, write, and execute permissions for group and other users from a file or directory. This can ensure only the root user can modify and execute the script, since root user has full access to all files and directories regardless of their permissions. References:https://linux.die.net/man/1
/chmod

NEW QUESTION: 17
A technician recently replaced a NIC that was not functioning. Since then, no device driver is found when starting the server, and the network card is not functioning. Which of the following should the technician check first?
A. The boot log
B. The BIOS
C. The HCL
D. The event log
Answer: C (LEAVE A REPLY)
The technician should check the hardware compatibility list (HCL) first to see if the new NIC is supported by the server's operating system. The HCL is a list of hardware devices that have been tested and verified to work with a specific operating system. If the NIC is not on the HCL, it means that there is no device driver available or compatible for it, and the NIC will not function properly.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 5, Lesson 5.2, Objective 5.2

NEW QUESTION: 18
The network's IDS is giving multiple alerts that unauthorized traffic from a critical application server is being sent to a known-bad public IP address. One of the alerts contains the following information:
Exploit Alert
Attempted User Privilege Gain
2/2/07-3: 09:09 10.1.200.32
--> 208.206.12.9:80

This server application is part of a cluster in which two other servers are also servicing clients. The server administrator has verified the other servers are not sending out traffic to that public IP address. The IP address subnet of the application servers is 10.1.200.0/26. Which of the following should the administrator perform to ensure only authorized traffic is being sent from the application server and downtime is minimized? (Select two).

A. Disable all services on the affected application server.

B. Perform a vulnerability scan on all the servers within the cluster and patch accordingly.

C. Block access to 208.206.12.9 from all servers on the network.

D. Change the IP address of all the servers in the cluster to the 208.206.12.0/26 subnet.

E. Enable GPO to install an antivirus on all the servers and perform a weekly reboot.

F. Perform an antivirus scan on all servers within the cluster and reboot each server.

Answer: (SHOW ANSWER)

The administrator should perform an antivirus scan on all servers within the cluster and reboot each server, and block access to 208.206.12.9 from all servers on the network. These actions will help to remove any malware that may have infected the application server and prevent any further unauthorized traffic to the known-bad public IP address. An antivirus scan can detect and remove malicious software that may be sending data to an external source, and a reboot can clear any temporary files or processes that may be related to the malware. Blocking access to 208.206.12.9 from all servers on the network can prevent any future attempts to communicate with the malicious IP address.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.4, Objective 3.4; Chapter 6, Lesson 6.2, Objective 6.2

NEW QUESTION: 19

Which of the following would a systems administrator implement to ensure all web traffic is secure?

A. SSH

B. SSL

C. SMTP

D. PGP

Answer: B (LEAVE A REPLY)

Secure Sockets Layer (SSL): SSL and its successor Transport Layer Security (TLS) enable client and server computers to establish a secure connection session and manage encryption and decryption activities.

Reference: https://paginas.fe.up.pt/~als/mis10e/ch8/chpt8-4bullettext.htm

NEW QUESTION: 20

Winch of the following is a type of replication in which all files are replicated, all the time?

A. Constant

B. Application consistent

C. Synthetic full

D. Full

Answer: (SHOW ANSWER)

Constant replication is a type of replication in which all files are replicated, all the time. Replication is a process of copying data from one location to another for backup, recovery, or distribution purposes. Constant replication is also known as real-time replication or synchronous replication. It ensures that any changes made to the source data are immediately reflected on the target data without any delay or lag. Constant replication provides high availability and consistency, but it requires high bandwidth and low latency. Application consistent replication is a type of replication that ensures that the replicated data is consistent with the state of the application that uses it. It involves quiescing or pausing the application before taking a snapshot of the data and resuming the application after the snapshot is taken. Application consistent replication provides better recovery point objectives than crash

consistent replication, which does not quiesce the application before taking a snapshot. Synthetic full replication is a type of replication that involves creating a new full backup by using the previous full backup and related incremental backups. It reduces the backup window and network bandwidth consumption by transferring only changed data from the source to the target. Full replication is a type of replication that involves copying all data from the source to the target regardless of whether it has changed or not. It provides a complete backup of the data, but it requires more storage space and network bandwidth than incremental or differential replication. References: https://www.howtogeek.com /199068/how-to-upgrade-your-existing-hard-drive-in-under-an-hour/ 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: 21
A technician is setting up a repurposed server. The minimum requirements are 2TB while ensuring the highest performance and providing support for one drive failure.The technician has the following six drives available:
Which of the following drive selections should the technician utilize to best accomplish this goal?
A. 1,2, 4, and 6
B. 1, 2, 3, 5, and 6
C. 1, 2, 4, 5, and 6
D. 1, 2, 3, 4, and 6
Answer: C (LEAVE A REPLY)
* RAID 5 configuration: Using five of the available drives in a RAID 5 configuration meets the requirements for:
* Storage capacity: Four 600GB drives (2, 5, and 6) provide a total usable capacity of 2.4TB (4 * 600 * 0.8), exceeding the minimum requirement of 2TB. RAID 5 introduces parity data for fault tolerance, sacrificing some usable space (one drive's worth).
* Performance: The combination of multiple drives in a RAID 5 array improves read performance compared to a single drive setup.
* Fault tolerance: Even with a single drive failure (any of the five drives used in the RAID 5), the remaining drives can reconstruct the lost data, allowing the server to continue operating.

NEW QUESTION: 22
A server administrator was asked to build a storage array with the highest possible capacity. Which of the following RAID levels should the administrator choose?
A. RAID 0
B. RAID 1
C. RAID 5
D. RAID 6
Answer: A (LEAVE A REPLY)
The RAID level that provides the highest possible capacity for a storage array is RAID 0. RAID 0 is a type of RAID level that provides performance enhancement by using striping. Striping means dividing data into blocks and distributing them across multiple disks to increase speed and capacity. RAID 0 does not provide any fault tolerance or redundancy, as it does not use any parity or mirroring techniques. RAID 0 uses all of the available disk space for data storage, without losing any space for overhead. Therefore, RAID 0 provides the highest possible capacity for a storage array, but also has the highest risk of data loss.
Reference: https://www.thinkmate.com/inside/articles/what-is-raid

NEW QUESTION: 23
A server administrator has received calls regarding latency and performance issues with a file server. After reviewing all logs and server features the administrator discovers the server came with four Ethernet ports, out only one port is currently in use. Which of the following features will enable the use of all available ports using a single IP address?
A. Network address translation
B. in-band management
C. Round robin
D. NIC teaming
Answer: (SHOW ANSWER)
NIC teaming is a feature that allows the use of multiple network interface cards (NICs) as a single logical interface with a single IP address. It can improve the network performance, bandwidth, and redundancy of a server. Verified References: [NIC teaming], [Network interface card]

NEW QUESTION: 24
Due to a recent application migration, a company's current storage solution does not meet the necessary requirements tor hosting data without impacting performance when the data is accessed in real time by multiple users. Which of the following is the BEST solution for this Issue?
A. Install local external hard drives for affected users.
B. Add extra memory to the server where data is stored.
C. Compress the data to increase available space.
D. Deploy a new Fibre Channel SAN solution.
Answer: D (LEAVE A REPLY)
A Fibre Channel SAN solution is a type of storage area network (SAN) that uses high-speed optical fiber cables to connect servers and storage devices. A SAN allows for hosting data without impacting performance when the data is accessed in real time by multiple users, as it provides fast data transfer rates, low latency, high availability, and scalability12. A local external hard drive (A) would not be suitable for multiple users, as it would limit the accessibility and security of the data. Adding extra memory to the server (B) would not solve the problem of data access performance, as it would not increase the bandwidth or reduce the congestion of the network. Compressing the data would not improve the performance either, as it would add extraoverhead and complexity to the data processing and retrieval. References: 1 https://www.techradar.com /best/best-cloud-storage 2 https://solutionsreview.com/data-storage/the-best-enterprise-data-storage-solutions/

NEW QUESTION: 25
A company stores extremely sensitive data on an alt-gapped system. Which of the following can Be Implemented to increase security against a potential insider threat?
A. Two-person Integrity
B. SSO
C. SIEM
D. Faraday cage
E. MFA
Answer: (SHOW ANSWER)
Two-person integrity is a security measure that can be implemented to increase security against a potential insider threat on an air-gapped system. An air-gapped system is a system that is isolated from any network connection and can only be accessed physically. An insider threat is a malicious actor who has authorized access to an organization's system or data and uses it for unauthorized or harmful purposes. Two-person integrity is a system of storage and handling that requires the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security

procedures, for accessing certain sensitive data or material. This way, no single person can compromise the security or integrity of the data or material without being noticed by another person. SSO (Single Sign-On) is a feature that allows users to access multiple applications or systems with one set of credentials, but it does not prevent insider threats. SIEM (Security Information and Event Management) is a tool that collects and analyzes log data from various sources to detect and respond to security incidents, but it does not work on air-gapped systems. A Faraday cage is a structure that blocks electromagnetic signals from entering or leaving, but it does not prevent physical access or insider threats. MFA (Multi-Factor Authentication) is a method that requires users to provide two or more pieces of evidence to verify their identity, such as something they know, something they have, or something they are, but it does not prevent insider threats. References: https://www.howtogeek.com/169080/air-gap-how- to-isolate-a-computer-to-protect-it-from-hackers/ https://www.howtogeek.com/428483/what-is-end-to-end- encryption-and-why-does-it-matter/ https://www.howtogeek.com/202794/what-is-the-difference-between-127.0.0.1-and-0.0.0.0/ https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive- removable-devices-and-individual-files/

NEW QUESTION: 26
Which of the following allows for a connection of devices to both sides inside of a blade enclosure?
A. Midplane
B. Active backplane
C. Passive backplane
D. Management module
Answer: A (LEAVE A REPLY)
The component that allows for a connection of devices to both sides inside of a blade enclosure is midplane.
A midplane is a board or panel that connects two sets of connectors or devices in parallel with each other. A midplane is typically used in blade enclosures or chassis to provide power and data connections between blade servers on one side and power supplies, cooling fans, switches, or management modules on the other side. A midplane can also act as a backplane by providing bus signals or communication channels between devices.

NEW QUESTION: 27
A systems administrator needs to create a data volume out of four disks with the MOST redundancy. Which of the following is the BEST solution?
A. RAID 0
B. RAID 1
C. RAID 5
D. RAID 6
Answer: D (LEAVE A REPLY)
RAID 6 is a type of RAID level that uses two parity blocks to provide fault tolerance and redundancy for data storage. RAID 6 can withstand the failure of up to two disks in the array without losing any data. RAID 6 requires a minimum of four disks to operate, and it distributes the data and parity blocks across all the disks in the array. RAID 6 has a high write penalty, which means that it takes more time and resources to write data to the disks than to read data from them. However, RAID 6 offers a high level of data protection and reliability, which makes it suitable for applications that require high availability and durability1.
RAID 1 provides redundancy and fault tolerance by mirroring the data from one disk to another disk. RAID 1 offers high read performance and data security, but it has low capacity and write performance. RAID 1 requires a minimum of two disks to operate, and it can only tolerate the failure of one disk in the array. If more than one disk fails, all the data in the array is lost2.
RAID 5 provides redundancy and fault tolerance by using one parity block to store information that can be used to reconstruct the data in case of a disk failure. RAID 5 requires a minimum of three disks to operate, and it distributes the data and parity blocks across all the disks in the array. RAID 5 offers

a balance between performance, capacity, and data protection, but it can only tolerate the failure of one disk in the array. If more than one disk fails, all the data in the array is lost2.
Therefore, among these options, RAID 6 is the best solution for creating a data volume out of four disks with the most redundancy.

NEW QUESTION: 28
Joe. a user m the IT department cannot save changes to a sensitive file on a Linux server. An 1s -1& snows the following listing; Which of the following commands would BEST enable the server technician to allow Joe tohaveaccess without granting excessive access to others?
A. Chmod g+w filename
B. chgrp IT filename
C. chown Joe filename
D. chmod 777 filename
Answer: A (LEAVE A REPLY)
The chmod command is used to change the permissions of files and directories. The g+w option means to grant write permission to the group owner of the file. Since Joe is a member of the IT group, which is also the group owner of the file, this command will allow him to save changes to the file without affecting the permissions of other users. Verified References: [Linux chmod command]

NEW QUESTION: 29
An administrator restores several database files without error while participating in a mock disaster recovery exercise. Later, the administrator reports that the restored databases are corrupt and cannot be used. Which of the following would best describe what caused this issue?
A. The databases were not backed up to be application consistent.
B. The databases were asynchronously replicated
C. The databases were mirrored
D. The database files were locked during the restoration process.
Answer: (SHOW ANSWER)
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: 30
A company has a data center that is located at its headquarters, and it has a warm site that is located 20mi (32km) away, which serves as a DR location. Which of the following should the company design and implement to ensure its DR site is adequate?
A. Set up the warm site as a DR cold site.
B. Set up a DR site that is in the cloud and in the same region.
C. Set up the warm site as a DR hot site.
D. Set up a DR site that is geographically located in another region.
Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 31
Which of the following should an administrator use to transfer log files from a Linux server to a Windows workstation?
A. Telnet
B. Robocopy
C. XCOPY
D. SCP
Answer: D (LEAVE A REPLY)
The administrator should use SCP to transfer log files from a Linux server to a Windows workstation. SCP (Secure Copy Protocol) is a protocol that allows secure file transfer between two devices using SSH (Secure Shell) encryption. SCP can transfer files between different operating systems, such as Linux and Windows, as long as both devices have an SSH client installed. SCP can also preserve file attributes, such as permissions and timestamps, during the transfer.

NEW QUESTION: 32
A staff member who a monitoring a data center reports one rack is experiencing higher temperatures than the racks next to it, despite the hardware in each rack being the same. Which of the following actions would MOST likely remediate the heal issue?
A. Installing blanking panels in all the empty rack spaces
B. installing an additional POU and spreading out the power cables
C. Installing servers on the shelves instead of sliding rails
D. installing front bezels on all the server's m the rack
Answer: (SHOW ANSWER)
Blanking panels are metal or plastic plates that are installed in the empty spaces of a rack to prevent hot air from recirculating back to the front of the rack. This can improve the airflow and cooling efficiency of the rack and reduce the heat generated by the servers. Verified References: [Blanking panel], [Rack cooling]

NEW QUESTION: 33

Which of the following backup types should be chosen for database servers?
A. Differential
B. Incremental
C. Synthetic full
D. Open file
Answer: C (LEAVE A REPLY)
A synthetic full backup is a type of backup that combines a full backup with one or more incremental backups to create a new full backup without accessing the source data. This type of backup is suitable for database servers, as it reduces the backup window, minimizes the impact on the server performance, and provides faster recovery time. Verified References: [Synthetic Full Backup]

NEW QUESTION: 34
A technician set up a new multifunction printer. After adding the printer to the print server, the technician configured the printer on each user's machine. Several days later, users reported that they were no longer able to print, but scanning to email worked. Which of the following is most likely causing this issue?
A. The gateway is no longer being reached.
B. The network firewall was enabled.
C. The printer's network interface failed.
D. The printer had DHCP enabled.
Answer: D (LEAVE A REPLY)
The most likely cause of this issue is that the printer had DHCP enabled, which changed its IP address after adding it to the print server and configuring it on each user's machine. DHCP (Dynamic Host Configuration Protocol) is a network protocol that assigns IP addresses and other network configuration parameters to devices automatically, without manual intervention. DHCP can simplify network management and avoid IP conflicts, but it can also cause problems if the devices are not configured to use static or reserved IP addresses. If the printer had DHCP enabled, it might have received a different IP address from the DHCP server after rebooting or reconnecting to the network, which would make it unreachable by the print server and the users' machines that were configured with the previous IP address. Scanning to email would still work, as it does not depend on the print server or the users' machines, but on the printer's SMTP settings and internet connection. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0:
Networking, Objective 4.l: Given a scenario, configure network settings for servers.

NEW QUESTION: 35
A technician has several possible solutions to a reported server issue. Which of the following BEST represents how the technician should proceed with troubleshooting?
A. Determine whether there is a common element in the symptoms causing multiple problems.
B. Perform a root cause analysis.
C. Make one change at a time and test.
D. Document the findings, actions, and outcomes throughout the process.
Answer: C (LEAVE A REPLY)
This is the best way to proceed with troubleshooting when the technician has several possible solutions to a reported server issue. Making one change at a time and testing allows the technician to isolate the cause and effect of each solution and determine which one works best. It also helps to avoid introducing new problems or complicating existing ones by making multiple changes at once. Determining whether there is a common element in the symptoms causing multiple problems is a good step to perform before identifying possible solutions, but not after. Performing a root cause analysis is a

good step to perform after resolving the issue, but not during. Documenting the findings, actions, and outcomes throughout the process is a good practice to follow at every step of troubleshooting, but not a specific way to proceed with testing possible solutions.
References: https://www.howtogeek.com/174288/how-to-tell-if-your-computer-is-overheating-and-what-to- do-about-it/
https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-it-matter/

NEW QUESTION: 36
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: C,F (LEAVE A REPLY)
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: 37
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 were not cross-connected
Answer: C (LEAVE A REPLY)
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: 38
A server administrator just installed a new physical server and needs to harden the OS. Which of the following best describes the OS hardening method?
A. Apply security updates.
B. Disable unneeded hardware.

C. Set a BIOS password.
D. Configure the boot order.
Answer: A (LEAVE A REPLY)
Applying security updates is one of the common operating system hardening methods that can help protect the OS from cyberattacks and vulnerabilities. Security updates are released by the OS developer to fix bugs, patch security holes, and improve performance. By installing the latest updates, the server administrator can ensure that the OS is up to date and secure12.

NEW QUESTION: 39
A technician is connecting a Linux server to a share on a NAS. Which of the following is the MOST appropriate native protocol to use for this task?
A. CIFS
B. FTP
C. SFTP
D. NFS
Answer: D (LEAVE A REPLY)
The most appropriate native protocol to use for connecting a Linux server to a share on a NAS is NFS. NFS (Network File System) is a protocol that allows file sharing and remote access over a network. NFS is designed for Unix-like operating systems, such as Linux, and supports features such as symbolic links, hard links, file locking, and file permissions. NFS uses mount points to attach remote file systems to local file systems, making them appear as if they are part of the local file system. NFS can provide fast and reliable access to files stored on a NAS (Network Attached Storage), which is a device that provides centralized storage for network devices.

NEW QUESTION: 40
A server administrator has received tickets from users who report the system runs very slowly and various unrelated messages pop up when they try to access an internet-facing web application using default ports. The administrator performs a scan to check for open ports and reviews the following report:
Starting Nmap 7.70 https://nmap.org) at 2019-09-19 14:30 UTC
Nmap scan report for www.abc.com (172.45.6.85)
Host is up (0.0021s latency)
Other addresses for www.abc.com (not scanned) : 4503 : F7b0 : 4293: 703: : 3209 RDNS record for 172.45.6.85: 1ga45s12-in-f1.2d100.net Port State Service
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
69/tcp open @username.com
80/tcp open http
110/tcp filtered pop
143/tcp filtered imap
443/tcp open https
1010/tcp open www.popup.com
3389/tcp filtered ms-abc-server
Which of the following actions should the server administrator perform on the server?
A. Close ports 69 and 1010 and rerun the scan.

B. Close ports 80 and 443 and rerun the scan.
C. Close port 3389 and rerun the scan.
D. Close all ports and rerun the scan.
Answer: A (LEAVE A REPLY)
Port 69 is used for TFTP (Trivial File Transfer Protocol), which is an insecure and unencrypted protocol for file transfer. Port 1010 is used for a malicious website that generates pop-up ads. Both of these ports are likely to be exploited by hackers or malware to compromise the server or the web application. The server administrator should close these ports and rerun the scan to verify that they are no longer open12.
References = 1: Why Are Some Network Ports Risky, And How Do You Secure Them? - How-To Geek (https://www.howtogeek.com/devops/why-are-some-ports-risky-and-how-do-you-secure-them/) 2: Switchport Port Security Explained With Examples - ComputerNetworkingNotes(https://www.computernetworkingnotes.com/ccna-study-guide/switchport-port-security-explained-with-examples.html)

NEW QUESTION: 41
A new application server has been configured in the cloud to provide access to all clients within the network.
On-site users are able to access all resources, but remote users are reporting issues connecting to the new application. The server administrator verifies that all users are configured with the appropriate group memberships. Which of the following is MOST likely causing the issue?
A. Telnet connections are disabled on the server.
B. Role-based access control is misconfigured.
C. There are misconfigured firewall rules.
D. Group policies have not been applied.
Answer: C (LEAVE A REPLY)
This is the most likely cause of the issue because firewall rules can block or allow traffic based on source, destination, port, protocol, or other criteria. If the firewall rules are not configured properly, they can prevent remote users from accessing the cloud application server, while allowing on-site users to access it. References:
https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

NEW QUESTION: 42
A server room contains ten physical servers that are running applications and a cluster of three dedicated hypervisors. The hypervisors are new and only have 10% utilization. The Chief Financial Officer has asked that the IT department do what it can to cut back on power consumption and maintenance costs in the data center. Which of the following would address the request with minimal server downtime?
A. Unplug the power cables from the redundant power supplies, leaving just the minimum required.
B. Convert the physical servers to the hypervisors and retire the ten servers.
C. Reimage the physical servers and retire all ten servers after the migration is complete.
D. Convert the ten servers to power-efficient core editions.
Answer: B (LEAVE A REPLY)
Explanation: This option would reduce power consumption and maintenance costs by consolidating the physical servers into virtual machines on the hypervisors. This would also free up space and resources in the data center. The other options would either not address the request, increase power consumption, or require more maintenance.

NEW QUESTION: 43
Which of the following environmental controls must be carefully researched so the control itself does not cause the destruction of the server equipment?

A. Humidity control system
B. Sensors
C. Fire suppression
D. Heating system
Answer: C (LEAVE A REPLY)
Fire suppression systems are designed to extinguish or contain fires in a server room, but they can also damage the server equipment if they are not carefully researched and selected. For example, water-based fire suppression systems can cause electrical shorts and corrosion, while gas-based fire suppression systems can create thermal shock and reduce oxygen levels. Therefore, fire suppression systems must be compatible with the server environment and equipment.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 1, Lesson 1.5, Objective 1.5

NEW QUESTION: 44
Which of the following should be created to understand how long data is stored and how frequently data backups should be scheduled?
A. Retention policies
B. Service-level agreement
C. Life-cycle management
D. Mean time to recover
Answer: A (LEAVE A REPLY)
Retention policiesdefine how long data should be kept before being archived or deleted and help in determining the frequency of backups to ensure data is available when needed. These policies are crucial for compliance, storage management, and disaster recovery planning.
* Retention policies (Answer A):These directly address how long data is kept and how often it should be backed up.
* Service-level agreement (Option B):SLAs define performance expectations and uptime, not specific data retention or backup schedules.
* Life-cycle management (Option C):This refers to managing data from creation to disposal but doesn't specifically address backup frequency or retention periods.
* Mean time to recover (Option D):This metric measures how long it takes to restore services after a failure, not backup scheduling.
CompTIA Server+ Reference:This topic relates toSK0-005 Objective 4.2: Explain the importance of data security concepts.

NEW QUESTION: 45
A server administrator receives a report that Ann, a new user, is unable to save a file to her home directory on a server. The administrator checks Ann's home directory permissions and discovers the following:
dr-xr-xr-- /home/Ann
Which of the following commands should the administrator use to resolve the issue without granting unnecessary permissions?
A. chmod777/home/Ann
B. chmod666/home/Ann
C. chmod711/home/Ann
D. chmod754/home/Ann
Answer: D (LEAVE A REPLY)
The administrator should use the command chmod 754 /home/Ann to resolve the issue without granting unnecessary permissions. The chmod command is used to change the permissions of files and directories on a Linux server. The permissions are represented by three numbers, each ranging from 0 to 7, that correspond to the read , write (w), and execute (x) permissions for the owner, group, and others respectively. The numbers are calculated by adding up the values of each permission: r = 4, w = 2, x = 1. For example, 7 means rwx (4 +

2 + 1), 6 means rw- (4 + 2), 5 means r-x (4 + 1), etc. In this case, Ann's home directory has the permissions dr-xr-xr-, which means that only the owner (d) can read and execute (x) the directory, and the group and others can only read and execute (x) but not write (w) to it. This prevents Ann from saving files to her home directory. To fix this issue, the administrator should grant write permission to the owner by using chmod 754 /home/Ann, which means that the owner can read , write (w), and execute (x) the directory, the group can read and execute (x) but not write (w) to it, and others can only read but not write (w) or execute (x) it. This way, Ann can save files to her home directory without giving unnecessary permissions to others.
Reference:
https://linuxize.com/post/what-does-chmod-777-mean/

NEW QUESTION: 46
A server administrator is deploying a new server that has two hard drives on which to install the OS. Which of the following RAID configurations should be used to provide redundancy for the OS?
A. RAID 0
B. RAID 1
C. RAID 5
D. RAID 6
Answer: B (LEAVE A REPLY)
RAID 1 (mirroring) is a RAID configuration that should be used to provide redundancy for the OS on a server that has two hard drives on which to install the OS. RAID 1 (mirroring) is a configuration that duplicates data across two or more drives. It provides fault tolerance and improves read performance, but reduces storage capacity by half. If one drive fails in RAID 1, the other drive can continue to operate without data loss or system downtime. RAID 0 (striping) is a configuration that splits data across two or more drives without parity or redundancy. It improves performance but offers no fault tolerance. If one drive fails in RAID 0, all data is lost and the system cannot boot. RAID 5 (striping with parity) is a configuration that stripes data across three or more drives with parity information. It provides fault tolerance and improves performance, but reduces storage capacity by one drive's worth of space. RAID 5 can tolerate one drive failure without data loss, but not two ormore. RAID 6 (striping with double parity) is a configuration that stripes data across four or more drives with double parity information. It provides fault tolerance and improves performance, but reduces storage capacity by two drives' worth of space. RAID 6 can tolerate two drive failures without data loss, but not three or more.References:https://www.howtogeek.com/199068/how-to-upgrade-your-existing- hard-drive-in-under-an-hour/

NEW QUESTION: 47
A technician needs to deploy an operating system that would optimize server resources. Which of the following server installation methods would BEST meet this requirement?
A. Full
B. Bare metal
C. Core
D. GUI

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

NEW QUESTION: 48
A Linux server was recently updated. The server now stops during the boot process with a blank screen and an fs> prompt. Which of the following is the most likely cause of this issue?
A. The system is booting to a USB flash drive.
B. The UEFI boot was interrupted by a missing Linux boot file.
C. The BIOS could not find a bootable hard disk.
D. The BIOS firmware needs to be upgraded.
Answer: B (LEAVE A REPLY)
Comprehensive Detailed Explanation with all CompTIA Server+ SK0-005 Study Guide References:The fs> prompt typically indicates that the Unified Extensible Firmware Interface (UEFI) has entered the EFI shell due to a failure in locating the bootloader or a critical Linux boot file. This often occurs after an update where boot files are moved, renamed, or deleted. To resolve:
* Verify the bootloader configuration (e.g., GRUB) and ensure the correct partition is set for booting.
* Recreate or repair the bootloader files if necessary.
* Ensure the boot sequence in UEFI settings points to the correct disk and partition.
Other options:
* A. USB flash drive booting: Unlikely unless the boot order was unintentionally altered.
* C. BIOS not finding a bootable hard disk: Would generally result in a different error message.
* D. BIOS firmware upgrade: Not typically required for this specific issue.

NEW QUESTION: 49
A technician is checking a server rack. Upon entering the room, the technician notices the tans on a particular server in the rack are running at high speeds. This is the only server in the rack that is experiencing this behavior. The ambient temperature in the room appears to be normal. Which of the following is the MOST likely reason why the fans in that server are operating at full speed?
A. The server is In the process of shutting down, so fan speed operations have been defaulted to high.
B. An incorrect fan size was inserted into the server, and the server has had to Increase the fan speed to compensate.
C. A fan failure has occurred, and the other fans have increased speed to compensate.
D. The server is utilizing more memory than the other servers, so it has increased the fans to compensate.
Answer: (SHOW ANSWER)
This is the most likely reason why the fans in that server are operating at full speed while the ambient temperature in the room is normal and the other servers in the rack are not experiencing this behavior. A fan failure is a situation where one or more fans in a server stop working or malfunction due to wear and tear, dust, or other factors. This can cause overheating and performance issues on the server. To prevent this, most servers have a fan redundancy feature that allows the other fans to increase their speed and airflow to compensate for the failed fan and maintain a safe temperature level. The server is not likely to be in the process of shutting down, as this would not cause the fans to run at high speeds. An incorrect fan size is not likely to

be inserted into the server, as most fans are standardized and compatible with the server chassis and motherboard. The server is not likely to be utilizing more memory than the other servers, as this would not cause a significant increase in temperature or fan speed. References: https://www.howtogeek.com/303282 /how-to-manage-your-pcs-fans-for-optimal-airflow-and-cooling/https://www.howtogeek.com/174288/how-to- tell-if-your-computer-is-overheating-and-what-to-do-about-it/

NEW QUESTION: 50
A server administrator is racking new servers in a cabinet with multiple connections from the servers to power supplies and the network. Which of the following should the administrator recommend to the organization to best address this situation?
A. Rack balancing
B. Cable management
C. Blade enclosure
D. Rail kits
Answer: B (LEAVE A REPLY)
Cable management is the process of organizing, securing, and labeling cables in a server rack or cabinet. Cable management can help improve airflow and cooling, reduce clutter and confusion, prevent damage and interference, and enhance safety and aesthetics123. Cable management can be achieved by using various tools and accessories, such as cable trays, ties, hooks, clips, labels, ducts, and organizers12.

NEW QUESTION: 51
A systems administrator notices that a SAN is running out of space. There is no additional funding in the budget to upgrade the storage space. Which of the following will significantly reduce the storage space with the least effort? (Select two).
A. Configuring compression
B. Deleting old and unused files
C. Increasing the number of IOPS
D. Decreasing the RAID level
E. Enabling deduplication
F. Upgrading the filesystem type
Answer: (SHOW ANSWER)
To free up storage space on a SAN with minimal effort and no additional cost, the following methods can be used:
* Configuring compression (Answer A):Compression reduces the size of files stored on the SAN, allowing more data to be stored in the same space.
* Enabling deduplication (Answer E):Deduplication identifies and removes duplicate copies of data, reducing the amount of space required for storage.
* Deleting old and unused files (Option B):While effective, this requires manual effort and may not be the best long-term solution.
* Increasing the number of IOPS (Option C):This relates to improving performance, not reducing storage space.
* Decreasing the RAID level (Option D):Lowering the RAID level could reduce redundancy, which may free up space but also decreases fault tolerance.
* Upgrading the filesystem type (Option F):This is a complex process that doesn't directly reduce storage usage.
CompTIA Server+ Reference:This topic is covered underSK0-005 Objective 3.2: Summarize storage technologies and solutions.

NEW QUESTION: 52
After installing an OS on a new server, the administrator realizes the server does not have any network connectivity. The administrator checks the network cable, and it seems to be transferring data. Which of the following should be checked next?
A. NIC firmware

B. IPv4 options
C. DHCP options
D. Firewall options
E. DNS settings
Answer: B (LEAVE A REPLY)
If the network cable is functioning but there is no network connectivity, the next step would be to check the IPv4 options. This includes verifying that the server has a correct IP address, subnet mask, and gateway configuration.
* IPv4 options (Answer B): Incorrect IP configuration is a common reason for network connectivity issues.
* NIC firmware (Option A): Firmware issues are less likely if the NIC is detecting the cable and appears operational.
* DHCP options (Option C): DHCP could be checked if automatic IP assignment is being used, but verifying IPv4 options manually is the first step.
* Firewall options (Option D): Firewalls can block connectivity but should be checked after confirming IP settings.
* DNS settings (Option E): DNS issues usually affect domain name resolution, not basic network connectivity.
CompTIA Server+ Reference:This topic is covered under SK0-005 Objective 3.1: Install and configure server components.

NEW QUESTION: 53
Which of the following physical security concepts would most likely be used to limit personnel access to a restricted area within a data center?
A. An access control vestibule
B. Video surveillance
C. Bollards
D. Data center camouflage
Answer: A (LEAVE A REPLY)
An access control vestibule is a physical security concept that limits personnel access to a restricted area within a data center. It is a small room or hallway that has two doors: one that leads to the outside and one that leads to the restricted area. The doors are controlled by an electronic lock that requires authentication, such as a card reader, biometric scanner, or keypad. Only authorized personnel can enter the vestibule and access the restricted area. References: CompTIA Server+ Certification Exam Objectives, Domain 5.0:
Security, Objective 5.1: Given a scenario, apply physical security methods to a server.

NEW QUESTION: 54
Which of the following BEST measures how much downtime an organization can tolerate during an unplanned outage?
A. SLA
B. BIA
C. RTO
D. MTTR
Answer: C (LEAVE A REPLY)
RTO (Recovery Time Objective) is a metric that measures how much downtime an organization can tolerate during an unplanned outage before it affects its business continuity and reputation. RTO is usually expressed in hours or minutes and is determined by the criticality of the business processes and the impact of the outage on the revenue, customers, and stakeholders. RTO helps to define the recovery strategy and the resources needed to restore the normal operations as quickly as possible. Verified References: [RTO vs RPO]

NEW QUESTION: 55

While running a local network security scan an administrator discovers communication between clients and one of the web servers is happening in cleartext. Company policy requires all communication lo be encrypted.
Which of the following ports should be closed to stop the deartext communication?
A. 21
B. 22
C. 443
D. 3389
Answer: A (LEAVE A REPLY)
Port 21 is used for FTP (File Transfer Protocol), which is a protocol that transfers files between servers and clients in cleartext, meaning that anyone can intercept and read the data. To stop this communication, port 21 should be closed on the web server and replaced with a secure protocol, such as SFTP (Secure File Transfer Protocol) or FTPS (File Transfer Protocol Secure), which use encryption to protect the data. Verified References: [FTP vs SFTP vs FTPS]

NEW QUESTION: 56
A server administrator is connecting a new storage array to a server. The administrator has obtained multiple IP addresses for the array. Which of the following connection types is the server most likely using to connect to the array?
A. eSATA
B. USB
C. FC
D. iSCSI
Answer: D (LEAVE A REPLY)
iSCSI is a protocol that allows SCSI commands to be transmitted over IP networks, enabling remote access to storage devices. iSCSI uses IP addresses to identify and communicate with the storage array, so having multiple IP addresses for the array indicates that iSCSI is being used. eSATA, USB, and FC are other types of connections that use different protocols and connectors than iSCSI. References: CompTIA Server+ Certification Exam Objectives, Domain 3.0: Storage, Objective 3.1: Given a scenario, install and deploy primary storage devices based on given specifications and interfaces.

NEW QUESTION: 57
Which of the following is a system that scans outgoing email for account numbers, sensitive phrases, and other forms of Pll?
A. SIEM
B. DLP
C. HIDS
D. IPS
Answer: B (LEAVE A REPLY)
DLP stands for Data Loss Prevention and it is a system that scans outgoing email for account numbers, sensitive phrases, and other forms of PII (Personally Identifiable Information). DLP can help prevent data breaches, comply with regulations, and protect the privacy of customers and employees. DLP can also block, encrypt, or quarantine emails that contain sensitive data.References: https://www.comptia.org/training /resources/exam-objectives/comptia-server-sk0-005-exam-objectives (Objective 3.2)

NEW QUESTION: 58

An administrator is upgrading a group of legacy blade servers to the latest version of the hypervisor. After restarting the server, the upgrade is interrupted. The hypervisor is not available, and the update is not successful. Which of the following should the administrator do next to accomplish this upgrade?

A. Change the upgrade to a new installation and overwrite the boot drive.

B. Upgrade the blade server's firmware to support the new hypervisor.

C. Increase the blade server's onboard RAM.

D. Upgrade the blade server's hardware.

Answer: B (LEAVE A REPLY)

Comprehensive Detailed Explanation with all CompTIA Server+ SK0-005 Study Guide References:Firmware incompatibility is a common issue when upgrading hypervisors, especially on legacy hardware. Upgrading the firmware ensures that the hardware is compatible with the new hypervisor version. This includes updating BIOS, RAID controllers, and network adapters to the latest supported versions.

* A. New installation:Risks data loss and is unnecessary if the issue is firmware-related.
* C. Increasing RAM:May enhance performance but does not resolve compatibility issues.
* D. Hardware upgrade:A last resort if firmware updates do not resolve the problem.

NEW QUESTION: 59

A security administrator ran a port scanning tool against a virtual server that is hosting a secure website. A list of open ports was provided as documentation. The management team has requested that non- essential ports be disabled on the firewall. Which of the following ports must remain open?

A. 25

B. 53

C. 443

D. 3389

E. 8080

Answer: C (LEAVE A REPLY)

* HTTPS (Secure Web Traffic): Port 443 is the standard port for HTTPS, which is essential for encrypting communication between web browsers and a secure website. (CompTIA Server+ Objectives SK0-004: 4.1)
* Why other options are not essential:
* 25 (SMTP): Used for email transmission
* 53 (DNS): Used for domain name resolution
* **3389 (RDP): ** Used for remote desktop connections
* **8080 (Alternate HTTP): ** Sometimes used for web servers, but not the standard secure port

NEW QUESTION: 60

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

A. /28

B. /29

C. /30

D. /32

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

NEW QUESTION: 61
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 (LEAVE A REPLY)
DLP, or Data Loss Prevention, is a type of security measure that aims to prevent unauthorized access, use, or transfer of sensitive dat a. 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 tasks that do not require DLP. Auditing the access to the physical fileshare is a physical security measure that is not affected by DLP.

NEW QUESTION: 62
A systems administrator is trying to determine why users in the human resources department cannot access an application server. The systems administrator reviews the application logs but does not see any attempts by the users to access the application. Which of the following is preventing the users from accessing the application server?
A. NAT
B. ICMP
C. VLAN
D. NIDS
Answer: C (LEAVE A REPLY)
This is the most likely cause of preventing the users from accessing the application server because a VLAN is a logical segmentation of a network that isolates traffic based on certain criteria. If the human resources department and the application server are on different VLANs, they will not be able to communicate with each other unless there is a router or a switch that can route between VLANs.References:https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html

NEW QUESTION: 63
Which of the following documents would be useful when trying to restore IT infrastructure operations after a non-planned interruption?
A. Service-level agreement
B. Disaster recovery plan
C. Business impact analysis
D. Business continuity plan
Answer: B (LEAVE A REPLY)
A disaster recovery plan would be useful when trying to restore IT infrastructure operations after a non-planned interruption. A disaster recovery plan is a document that outlines the steps and procedures to recover from a major disruption of IT services caused by natural or man-made disasters, such as fire, flood, earthquake, cyberattack, etc. A disaster recovery plan typically includes:
* A list of critical IT assets and resources that need to be protected and restored
* A list of roles and responsibilities of IT staff and stakeholders involved in the recovery process
* A list of backup and recovery strategies and tools for data, applications, servers, networks, etc.
* A list of communication channels and methods for notifying users, customers, vendors, etc.
* A list of testing and validation methods for ensuring the functionality and integrity of restored systems
* A list of metrics and criteria for measuring the effectiveness and efficiency of the recovery process A disaster recovery plan helps IT organizations to minimize downtime, data loss, and financial impact of a disaster, as well as to resume normal operations as quickly as possible.

NEW QUESTION: 64

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: A,E (LEAVE A REPLY)

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: 65

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

A. BIA.

B. RTO.

C. MTTR.

D. SLA.

Answer: (SHOW ANSWER)

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

NEW QUESTION: 66

Following a recent power outage, a server on a server farm has been running slowly. A technician receives a ticket with a request to check for anything out of the ordinary. The technician sees an orange light on the front console of the server, indicating an error. Which of the following should the technician check next?

A. RAM

B. Power supply

C. CPU

D. RAID battery

Answer: (SHOW ANSWER)

NEW QUESTION: 67

A server room with many racks of servers is managed remotely with occasional on-site support. Which of the following would be the MOST cost-effective option to administer and troubleshoot network problems locally on the servers?

A. Management port

B. Crash cart

C. IP KVM
D. KVM
Answer: C (LEAVE A REPLY)
An IP KVM (keyboard, video, mouse) is a device that allows remote access and control of multiple servers over a network using a web browser or a client software. An IP KVM is a cost-effective option to administer and troubleshoot network problems locally on the servers, as it eliminates the need for physical presence or dedicated hardware for each server. A management port (A) is a network interface that is used for out-of-band management of network devices, such as routers or switches. A management port does not provide local access to servers. A crash cart (B) is a mobile unit that contains a monitor, keyboard, mouse, and other tools for troubleshooting servers in a data center. A crash cart requires physical access to each server and may not be cost-effective for many racks of servers. A KVM (D) is a device that allows switching between multiple servers using a single keyboard, video, and mouse. A KVM does not provide remote access over a network and requires physical connection to each server. References:
https://www.enterprisestorageforum.com
/management/best-data-storage-solutions-and-software-2021/ https://www.microsoft.com/en-us/microsoft-365
/business-insights-ideas/resources/cloud-storage-vs-on-premises-servers

NEW QUESTION: 68
An administrator is configuring a server that will host a high-performance financial application. Which of the following disk types will serve this purpose?
A. SAS SSD
B. SATA SSD
C. SAS drive with 10000rpm
D. SATA drive with 15000rpm
Answer: A (LEAVE A REPLY)
The best disk type for a high-performance financial application is a SAS SSD. A SAS SSD (Serial Attached SCSI Solid State Drive) is a type of storage device that uses flash memory chips to store data and has a SAS interface to connect to a server or a storage array. A SAS SSD offers high speed, low latency, high reliability, and high durability compared to other types of disks, such as SATA SSDs, SAS HDDs, or SATA HDDs. A SAS SSD can handle high I/O workloads and deliver consistent performance for applications that require fast data access and processing.
Reference:
https://www.hp.com/us-en/shop/tech-takes/sas-vs-sata

NEW QUESTION: 69
A technician is installing an OS on ten servers. Which of the following media installation types would allow for the fastest installation time?
A. Network
B. Embedded
C. Optical
D. USB
Answer: A (LEAVE A REPLY)
* Network Installation: Allows the OS image to be deployed from a central server, streamlining deployment across multiple systems simultaneously. This is significantly faster than individual installations from other media. (CompTIA Server+ Objectives SK0-004: 3.1)
* Why other options are less optimal:
* Embedded: Refers to OSes pre-installed on hardware and not intended for mass deployment.
* Optical (CDs/DVDs): Requires physical media insertion on each server, slower than network distribution.
* USB Similar to optical, requires individual installations and can be time-consuming for multiple servers.

NEW QUESTION: 70
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 (LEAVE A REPLY)
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: 71
A server administrator has connected a new server to the network. During testing, the administrator discovers the server is not reachable via server but can be accessed by IP address. Which of the following steps should the server administrator take NEXT? (Select TWO).
A. Check the default gateway.
B. Check the route tables.
C. Check the hosts file.
D. Check the DNS server.
E. Run the ping command.
F. Run the tracert command
Answer: (SHOW ANSWER)
If the server is not reachable by name but can be accessed by IP address, it means that there is a problem with name resolution. The hosts file and the DNS server are both responsible for mapping hostnames to IP addresses. Therefore, the server administrator should check these two files for any errors or inconsistencies that might prevent the server from being resolved by name. References: https://www.howtogeek.com/662249 /how-to-edit-the-hosts-file-on-linux/ https://www.howtogeek.com/164981/how-to-use-nslookup-to-check- domain-name-information-in-microsoft-windows/

NEW QUESTION: 72
A technician has received tickets responding a server is responding slowly during business hours. Which of the following should the technician implement so the team will be informed of this behavior in real time?
A. Log rotation
B. Alerts
C. Reports
D. Log stopping
Answer: (SHOW ANSWER)
Alerts are notifications that inform the technician or the team of any issues or events that occur on a server or a network. Alerts can be configured to trigger based on certain thresholds, such as CPU usage, disk space, memory utilization, or response time. Alerts can help the technician monitor and troubleshoot the server performance in real time. Verified References: [Alerts], [Server performance]

NEW QUESTION: 73
An administrator is investigating several unexpected documents and video files that recently appeared in a network share. The administrator checks the properties of the files and sees the author's name on the documents is not a company employee. The administrator questions the other users, but no one knows anything about the files. The administrator then checks the log files and discovers the FTP protocol was used to copy the files to the server. Which of the following needs to be done to prevent this from happening again?
A. Implement data loss prevention.
B. Configure intrusion detection.
C. Turn on User Account Control.
D. Disable anonymous access.
Answer: D (LEAVE A REPLY)
This is the best solution to prevent unauthorized files from being copied to the server via FTP because anonymous access allows anyone to log in to the FTP server without providing a username or password.
Disabling anonymous access will require users to authenticate with valid credentials before accessing the FTP server. References:
https://docs.microsoft.com/en-us/iis/configuration/system.applicationhost/sites/site
/ftpserver/security/authentication/anonymousauthentication

NEW QUESTION: 74
Which of the following attacks is the most difficult to mitigate with technology?
A. Ransomware
B. Backdoor
C. SQL injection
D. Phishing
Answer: D (LEAVE A REPLY)
Phishing is a type of attack that is the most difficult to mitigate with technology. Phishing is a technique of deceiving users into revealing their personal or confidential information, such as passwords, credit card numbers, or bank accounts, by sending them fraudulent emails or messages that appear to be from legitimate sources. Phishing relies on human factors, such as curiosity, greed, or fear, to trick users into clicking on malicious links or attachments, or entering their credentials on fake websites. Technology solutions, such as antivirus software, firewalls, or spam filters, can help detect and block some phishing attempts, but they cannot prevent users from falling victim to social engineering tactics. References: [CompTIA Server+ Certification Exam Objectives], Domain 5.0: Security, Objective 5.3: Given a scenario, explain methods and techniques to secure data.

NEW QUESTION: 75
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 (LEAVE A REPLY)

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: 76

An administrator reviews a new server that was received from a vendor and notes the OS has been installed to a two-drive array configured with RAID 0. Which of the following best describes what will happen if a drive in that array fails?

A. The server will gracefully shut down.

B. The server will immediately crash.

C. The server will operate but in read-only mode.

D. The server will continue to operate normally.

Answer: (SHOW ANSWER)

RAID 0 is a configuration that splits data evenly across two or more disks without parity or mirroring. This improves performance but offers no fault tolerance. If a drive in a RAID 0 array fails, the data on the array becomes inaccessible and the server will immediately crash. The other options are not applicable to RAID
0. References: [CompTIA Server+ Certification Exam Objectives], Domain 3.0: Storage, Objective 3.2:
Given a scenario, configure RAID using best practices.

NEW QUESTION: 77

Which of the following describes when a site is considered a warm site?

A. It has basic technical facilities connected to it.

B. It has faulty air conditioning that is awaiting service.

C. It is almost ready to take over all operations from the primary site.
D. It is fully operational and continuously providing services.
Answer: C (LEAVE A REPLY)
A warm site is a backup location that has partial infrastructure ready to support operations in the event of a failure at the primary site. It is almost ready to take over but requires some configuration or installation of data backups and software before it can become fully operational.
* Warm site (Answer C): This site has the necessary equipment but requires some setup, making it a middle ground between cold and hot sites.
* Basic technical facilities (Option A): This more accurately describes a cold site.
* Faulty air conditioning (Option B): This is irrelevant to the definition of a warm site.
* Fully operational (Option D): This describes a hot site, which is continuously ready to provide full services.
CompTIA Server+ Reference:This topic is related to SK0-005 Objective 4.1: Summarize disaster recovery methods and concepts.

NEW QUESTION: 78
The management team has mandated the use of data-at-rest encryption on all corporate servers. Using this encryption paradigm will ensure:
A. website traffic is protected while traversing the internet.
B. files stored on the server are protected against physical theft.
C. attachments that are emailed from this server cannot be intercepted.
D. databases in use are protected from remote hackers.
Answer: B (LEAVE A REPLY)
Data-at-rest encryption is a method of encrypting data while it is stored on a storage device, such as a hard drive, an SSD, or a tape library. This ensures that if the data is stolen or lost, it will be unreadable without the encryption key. Data-at-rest encryption does not protect data while it is in transit over the network, in use by the CPU or memory, or attached to an email.

NEW QUESTION: 79
An administrator is troubleshooting an application performance issue on a virtual server with two vCPUs. The application performance logs indicate CPU contention. The administrator adds more vCPU cores to the VM, yet the issue persists. Which of the following is the most likely reason for this issue?
A. The server has high page utilization.
B. The server has high disk latency.
C. The application is single-threaded.
D. The application cannot be virtualized.
Answer: (SHOW ANSWER)
A single-threaded application is an application that can only execute one task or process at a time. A single-threaded application can only utilize one CPU core, regardless of how many cores are available or assigned to the virtual machine. Therefore, adding more vCPU cores to the VM will not improve the performance of the application, as it will still be limited by the speed and capacity of one core12.
To troubleshoot this issue, the administrator should check if the application is single-threaded or multi-threaded. This can be done by using tools such as Task Manager, Performance Monitor, or Process Explorer on Windows, or top, htop, or ps on Linux34. If the application is single-threaded, the administrator should consider the following options:
* Reduce the number of vCPU cores on the VM to match the number of threads that the application can use. This can help avoid CPU contention and co-stop issues that may arise from having too many vCPUs relative to the number of physical cores on the host5.
* Upgrade the physical CPU on the host to a faster or newer model that can provide higher clock speed and performance for the single core that the application uses.
* Optimize the application code or configuration to make it more efficient or multi-threaded, if possible.

This can help the application take advantage of multiple cores and improve its performance.

NEW QUESTION: 80
A company has implemented a requirement to encrypt all the hard drives on its servers as part of a data loss prevention strategy. Which of the following should the company also perform as a data loss prevention method?
A. Encrypt all network traffic
B. Implement MFA on all the servers with encrypted data
C. Block the servers from using an encrypted USB
D. Implement port security on the switches
Answer: (SHOW ANSWER)
The company should also implement MFA on all the servers with encrypted data as a data loss prevention method. MFA stands for multi-factor authentication, which is a method of verifying a user's identity by requiring two or more pieces of evidence, such as something they know (e.g., a password), something they have (e.g., a token), or something they are (e.g., a fingerprint). MFA adds an extra layer of security to prevent unauthorized access to sensitive data, even if the user's password is compromised or stolen. Encrypting the hard drives on the servers protects the data from being read or copied if the drives are physically removed or stolen, but it does not prevent unauthorized access to the data if the user's credentials are valid.

NEW QUESTION: 81
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 (LEAVE A REPLY)
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, or modification of the files1. SCP also preserves the file attributes, such as permissions, timestamps, and ownership2.

NEW QUESTION: 82
An administrator is installing a new file server that has four drive bays available. Which of the following RAID types would provide the MOST storage as well as disk redundancy?
A. RAIDO
B. RAID 1
C. RAID 5
D. RAID 10
Answer: (SHOW ANSWER)
RAID 5 is a RAID level that provides striping with parity, which means that data is distributed across all disks with one disk storing parity information for error correction. RAID 5 can tolerate one disk failure without losing data. RAID 5 provides the most storage as well as disk redundancy out of the four RAID levels given, since it only uses one disk for parity and the rest for data. For example, if four 200GB drives are used in a RAID 5 array, the total storage capacity would be 600GB (200GB x 3), while in RAID 0 it would be 800GB (200GB x 4), in RAID 1 it would be 200GB (200GB x 1), and in RAID 10 it would be 400GB (200GB x 2).

References: https://en.wikipedia.org/wiki/Standard_RAID_levels#RAID_5

NEW QUESTION: 83
A technician retailed a new 4TB hard drive in a Windows server. Which of the following should the technician perform FIRST to provision the new drive?
A. Configure the drive as a base disk.
B. Configure the drive as a dynamic disk.
C. Partition the drive using MBR.
D. Partition the drive using OPT.
Answer: D (LEAVE A REPLY)
GPT (GUID Partition Table) is a partitioning scheme that allows creating partitions on large hard drives (more than 2 TB). It supports up to 128 partitions per drive and uses 64-bit addresses to locate them. MBR (Master Boot Record) is an older partitioning scheme that has limitations on the size and number of partitions (up to 4 primary partitions or 3 primary and 1 extended partition per drive). To provision a new 4 TB drive, the technician should partition it using GPT. Verified References: [GPT], [MBR]

NEW QUESTION: 84
Users cannot access a new server by name, but the server does respond to a ping request using its IP address.
All the user workstations receive their IP information from a DHCP server. Which of the following would be the best step to perform NEXT?
A. Run the tracert command from a workstation.
B. Examine the DNS to see if the new server record exists.
C. Correct the missing DHCP scope.
D. Update the workstation hosts file.
Answer: B (LEAVE A REPLY)
If users cannot access a new server by name, but the server does respond to a ping request using its IP address, it means that there is a problem withname resolution. The DNS (Domain Name System) is a service that maps hostnames to IP addresses and vice versa. Therefore, the best step to perform next is to examine the DNS to see if the new server record exists and matches its IP address. If not, the DNS record needs to be added or updated accordingly. Running the tracert command from a workstation would not help with name resolution, as it only shows the route taken by packets to reach a destination by IP address. Correcting the missing DHCP scope would not help either, as DHCP (Dynamic Host Configuration Protocol) only assigns IP addresses and other network settings to clients, but does not resolve names. Updating the workstation hosts file would be a temporary workaround, but not a permanent solution, as it would require manually editing every workstation's hosts file with the new server's name and IP address.
References: https://www.howtogeek.
com/164981/how-to-use-nslookup-to-check-domain-name-information-in-microsoft-windows/https://www.
howtogeek.com/howto/27350/beginner-geek-how-to-edit-your-hosts-file/

NEW QUESTION: 85
A server administrator is testing a disaster recovery plan. The test involves creating a downtime scenario and taking the necessary steps. Which of the following testing methods is the administrator MOST likely performing?
A. Backup recovery
B. Simulated
C. Tabletop
D. Live failover
Answer: D (LEAVE A REPLY)

The live failover testing method is the most likely one that the server administrator is performing when creating a downtime scenario and taking the necessary steps. A live failover test involves switching from the primary system to the secondary system (or backup site) in a real environment, without any simulation or preparation. A live failover test can evaluate the effectiveness and readiness of the disaster recovery plan, but it also carries a high risk of data loss, corruption, or disruption. Reference: https://www.ibm.com/cloud/learn
/disaster-recovery-testing

NEW QUESTION: 86
Which of the following backup methods protects all the changes that have occurred since the last full backup?
A. Incremental
B. Archive
C. Differential
D. Snapshot
Answer: C (LEAVE A REPLY)
A differential backup is a backup method that protects all the changes that have occurred since the last full backup. A differential backup copies all the files that have been added or modified since the last full backup, regardless of whether they have been backed up before or not. A differential backup does not reset the archive bit of the files, which means they will be backed up again in the next differential backup. A differential backup requires more storage space and time than an incremental backup, but it simplifies the restoration process, as only the last full backup and the last differential backup are needed to restore the data

NEW QUESTION: 87
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: (SHOW ANSWER)
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: 88
Which of the following should a technician verify FIRST before decommissioning and wiping a file server?
A. The media destruction method
B. The recycling poke?
C. Asset management documentation
D. Non-utilization
Answer: D (LEAVE A REPLY)
The first thing that a technician should verify before decommissioning and wiping a file server is non-utilization, which means that no one is using or accessing the server or its data. This can be done by checking logs, monitoring network traffic, or contacting users or stakeholders. Non-utilization

ensures that decommissioning and wiping will not cause any data loss or disruption to business operations. Verified References: [Server Decommissioning Checklist]

NEW QUESTION: 89
A server technician is configuring the IP address on a newly installed server. The documented configuration specifies using an IP address of 10.20.10.15 and a default gateway of 10.20.10.254. Which of the following subnet masks would be appropriate for this setup?
A. 255.255.255.0
B. 255.255.255.128
C. 255.255.255.240
D. 255.255.255.254
Answer: A (LEAVE A REPLY)
The administrator should use a subnet mask of 255.255.255.0 for this setup. A subnet mask is a binary number that defines how many bits of an IP address areused for the network portion and how many bits are used for the host portion. The network portion identifies the specific network that the IP address belongs to, while the host portion identifies the specific device within that network. The subnet mask is usually written in dotted decimal notation, where each octet represents eight bits of the binary number. A 1 in the binary number means that the corresponding bit in the IP address is part of the network portion, while a 0 means that it is part of the host portion. For example, a subnet mask of 255.255.255.0 means that the first 24 bits (three octets) of the IP address are used for the network portion and the last 8 bits (one octet) are used for the host portion.
This subnet mask allows up to 254 hosts per network (2^8 - 2). In this case, the IP address of 10.20.10.15 and the default gateway of 10.20.10.254 belong to the same network of 10.20.10.0/24 (where /24 indicates the number of bits used for the network portion), which can be defined by using a subnet mask of 255.255.255.0.

NEW QUESTION: 90
Which of the following types of locks utilizes key fobs or key cards held against a sensor/reader to gain access?
A. Bolting door lock
B. Combination door lock
C. Electronic door lock
D. Biometric door lock
Answer: C (LEAVE A REPLY)
* Lock Type: The type of lock utilizing key fobs or key cards is an electronic door lock (Option C).
* Explanation: Electronic locks use electronic credentials (such as key cards) for access control.
Reference: CompTIA Server+ Guide, Chapter 5: Security, Section 5.1.2 (Access Control)

NEW QUESTION: 91
Which of the following is an architectural reinforcement that is used to attempt to conceal the exterior of an organization?
A. Fencing
B. Bollards
C. Camouflage
D. Reflective glass
Answer: C (LEAVE A REPLY)
Camouflage is an architectural reinforcement that is used to attempt to conceal the exterior of an organization.

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

NEW QUESTION: 92
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 (LEAVE A REPLY)
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: 93
A technician needs to restore data from a backup. The technician has these files in the backup inventory:

Name	Size
01012020.bak	100MB
01022020.bak	10MB
01032020.bak	5MB
01042020.bak	7MB
01052020.bak	120MB
01062020.bak	8MB
01072020.bak	10MB

Which of the following backup types is being used if the file 01062020.bak requires another file to restore data?
A. Full
B. Incremental

C. Snapshot
D. Differential
Answer: B (LEAVE A REPLY)
An incremental backup only backs up files that have changed since the last backup, whether it was a full or an incremental backup. Therefore, an incremental backup file may require another file to restore data, depending on the sequence of backups. A full backup backs up all files and does not require any other file to restore data.
A snapshot is a point-in-time copy of data that does not depend on other files. A differential backup backs up files that have changed since the last full backup and does not require any other file to restore data.

NEW QUESTION: 94
An administrator is setting up a new employee's read/write access to a document on the file server. Currently, the user can open the file, but edits cannot be saved. Which of the following should the administrator do so the user can save the updated file while maintaining least-privilege access?
A. Give the user "read and execute" rights to the file.
B. Give the user "modify" rights to the file.
C. Give the user "list folder contents" rights to the folder.
D. Give the user "full control" rights to the folder.
Answer: B (LEAVE A REPLY)
To enable a user to both read and write to a file, the administrator needs to provide "modify" rights. This permission level allows the user not only to open and view the file (read) but also to make changes and save those changes back to the file (write). "Read and execute" rights would allow the user to open and run the file but not make any changes. "List folder contents" rights would enable the user to view the files within a folder but not make changes to them. "Full control" rights would provide the user with complete control over the file, including the ability to change permissions and delete the file, which exceeds the principle of least-privilege access necessary for this task.

NEW QUESTION: 95
A company's IDS has identified outbound traffic from one of the web servers coming over port 389 to an outside address. This server only hosts websites. The company's SOC administrator has asked a technician to harden this server. Which of the following would be the BEST way to complete this request?
A. Disable port 389 on the server
B. Move traffic from port 389 to port 443
C. Move traffic from port 389 to port 637
D. Enable port 389 for web traffic
Answer: (SHOW ANSWER)
The best way to complete the request to harden the server is to disable port 389 on the server. Port 389 is the default port used by LDAP (Lightweight Directory Access Protocol), which is a protocol that allows access and modification of directory services over a network. LDAP can be used for authentication, authorization, or information retrieval purposes. However, LDAP does not encrypt its data by default, which can expose sensitive information or credentials to attackers who can intercept or modify the network traffic. Therefore, port 389 should be disabled on a web server that only hosts websites and does not need LDAP functionality.
Alternatively, port 636 can be used instead of port 389 to enable LDAPS (LDAP over SSL/TLS), which encrypts the data using SSL/TLS certificates.

NEW QUESTION: 96

An administrator is troubleshooting a RAID issue in a failed server. The server reported a drive failure, and then it crashed and would no longer boot. There are two arrays on the failed server: a two-drive RAIO 0 set tor the OS, and an eight-drive RAID 10 set for data. Which of the following failure scenarios MOST likely occurred?

A. A drive failed in the OS array.

B. A drive failed and then recovered in the data array.

C. A drive failed in both of the arrays.

D. A drive failed in the data array.

Answer: A (LEAVE A REPLY)

If a server has two arrays on the failed server: a two-drive RAID 0 set for the OS, and an eight-drive RAID 10 set for data, then the most likely failure scenario that caused the server to crash and not boot is that a drive failed in the OS array. RAID 0 is a RAID configuration that stripes data across two or more drives without parity or redundancy. RAID 0 offers high performance but no fault tolerance. If one drive fails in RAID 0, all data is lost and the system cannot boot. RAID 10 is a RAID configuration that combines disk mirroring and disk striping with parity. RAID 10 offers high performance and fault tolerance. RAID 10 can tolerate up to one drive failure per mirrored pair without losing data or functionality.References:https://www.technewstoday.com/what-is-a-raid-0/ https://www.technewstoday.com/what-is-a-raid-10/

NEW QUESTION: 97

A technician is configuring a server that requires secure remote access. Which of the following ports should the technician use?

A. 21

B. 22

C. 23

D. 443

Answer: B (LEAVE A REPLY)

The technician should use port 22 to configure a server that requires secure remote access. Port 22 is the default port for Secure Shell (SSH), which is a protocol that allows secure remote login and command execution over a network connection using a command-line interface (CLI). SSH encrypts both the authentication and data transmission between the client and the server, preventing eavesdropping, tampering, or spoofing. SSH can be used to perform various tasks on a server remotely, such as configuration, administration, maintenance, troubleshooting, etc.

NEW QUESTION: 98

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

A. The keyboard is defective and needs to be replaced.

B. The system failed before the display card initialized.

C. The power supply is faulty and is shutting down the system.

D. The NIC has failed, and the system cannot make a network connection.

Answer: B (LEAVE A REPLY)

This is the most likely cause of the issue because the keyboard LED flash indicates a POST error code. If the display card is not initialized, the system cannot show any error messages on the screen and will stop booting.

References: https://www.computerhope.com/beep.htm#04

NEW QUESTION: 99

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 (LEAVE A REPLY)

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: 100

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 (LEAVE A REPLY)

Monitors Network Traffic

Reference:https://www.fortinet.com/resources/cyberglossary/benefits-of-firewall

NEW QUESTION: 101

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

A. Fibre Channel

B. FCoE

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

NEW QUESTION: 102
Which of the following often-overlooked parts of the asset life cycle can cause the greatest number of issues in relation to PII exposure?
A. Usage
B. End-of-life
C. Procurement
D. Disposal
Answer: (SHOW ANSWER)
Disposal is the part of the asset life cycle that can cause the greatest number of issues in relation to PII exposure. PII stands for personally identifiable information, which is any data that can be used to identify a specific individual, such as name, address, phone number, email, social security number, etc. PII exposure is the unauthorized access or disclosure of PII, which can result in identity theft, fraud, or other harms to the individuals whose data is compromised. Disposal is the process of getting rid of an asset that is no longer needed or useful, such as a server, a hard drive, or a mobile device. If the disposal is not done properly, the PII stored on the asset may still be accessible or recoverable by unauthorized parties, such as hackers, thieves, or competitors. Therefore, it is important to follow best practices for secure disposal of assets that contain PII, such as wiping, encrypting, shredding, or physically destroying the data storage media

NEW QUESTION: 103
A technician is setting up a small office that consists of five Windows 10 computers. The technician has been asked to use a simple IP configuration without manually adding any IP addresses. Which of the following will the technician MOST likely use for the IP address assignment?
A. Static
B. Router-assigned
C. APIPA
D. DHCP
Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 104
A technician has moved a data drive from a new Windows server to an orderWindows server. The hardware recognizes the drive, but the data is not visible to the OS. Which of the following is the MOST Likely cause of the issue?
A. Thedisk uses GPT.
B. Thepartition is formatted with ext4.
C. The -partition is formatted with FAT32.
D. Thedisk uses MBn.
Answer: (SHOW ANSWER)
GPT (GUID Partition Table) is a partitioning scheme that allows creating partitions on large hard drives (more than 2 TB). It supports up to 128 partitions per drive and uses 64-bit addresses to locate them.
However, GPT is not compatible with older versions of Windows, such as Windows XP or Windows Server
2003, which use MBR (Master Boot Record) as the partitioning scheme. If a disk uses GPT, it may not be recognized or accessible by an older Windows server. Verified References: [GPT], [MBR]

NEW QUESTION: 105
A datacenter in a remote location lost power. The power has since been restored, but one ol the servers has not come back online. After some investigation, the server is found to still be powered off. Which of the following is the BEST method to power on the server remotely?
A. Crash cart
B. Out-of-band console
C. IP KVM
D. RDP
Answer: B (LEAVE A REPLY)
Out-of-band console is a tool that can be used to command a remote shutdown of a physical Linux server. Out- of-band console is a method of accessing a server's console through a dedicated management port or device that does not rely on the server's operating system or network connection. Out-of-band console can be used to power cycle, reboot, update firmware, monitor performance, and perform other tasks remotely even if the server is unresponsive or offline. Crash cart is a mobile unit that contains a keyboard, monitor, mouse, and other tools that can be used to troubleshoot a server on-site, but it requires physical access to the server. IP KVM (Internet Protocol Keyboard Video Mouse) switch is a hardware device that allows remote access to multiple servers using a web browser or a client software, but it requires network connectivity and may not work if the SSH connection is lost. RDP (Remote Desktop Protocol) is a protocol that allows remote access to a Windows server's graphical user interface, but it does not work on Linux servers and requires network connectivity. References: https://www.techopedia.com/definition/13623/crash-cart https://www.techopedia. com/definition/13624/kvm-switchhttps://www.techopedia.com/definition/3422/remote-desktop-protocol-rdp

NEW QUESTION: 106
Which of the following script types would MOST likely be used on a modern Windows server OS?
A. Batch

B. VBS
C. Bash
D. PowerShell
Answer: D (LEAVE A REPLY)
PowerShell is a scripting language and a command-line shell that is designed for Windows server administration. It can perform various tasks such as configuration, automation, and management of servers and applications. Verified References: [PowerShell], [Scripting language]

NEW QUESTION: 107
A systems administrator notices the fans are running at full speed in a newly upgraded server. Which of the following should be done to address this issue?
A. Replace the PSU.
B. Reseat the video card.
C. Reseat the RAM.
D. Reattach the heat sink.
Answer: D (LEAVE A REPLY)
Comprehensive Detailed Explanation with all CompTIA Server+ SK0-005 Study Guide References:If the fans are running at full speed, it may indicate that the CPU or system temperature is too high. This is often caused by a poorly attached or improperly seated heat sink, which prevents efficient heat dissipation. Reattaching the heat sink with proper thermal paste resolves the issue.
* A. Replace the PSU:Not relevant to temperature control.
* B. Reseat the video card:Would not affect fan speed unless a GPU temperature issue exists, which is not stated here.
* C. Reseat the RAM:Unrelated to fan operation.

NEW QUESTION: 108
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 (LEAVE A REPLY)
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: 109
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 /mnt. Change to the /mnt/etc directory. Edit the passwd file found in that directory.
B. Reinstall the OS in overlay mode. Reset the root password from the install GUI screen.
C. Adjust the GRUB boot parameters to boot into single-user mode. Run passwd from the command prompt.
D. Boot using a Linux live CD and mount the hard disk to /mnt. SCP the /etc directory from a known accessible server to /mnt/etc.
Answer: (SHOW ANSWER)
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_GRUB

NEW QUESTION: 110
A systems administrator recently upgraded the memory in a server, and now the server does not turn on, and nothing is displayed on the screen.
Which of the following is the next step the administrator should take to diagnose the error without opening the machine?
A. Perform a cold reboot.
B. Listen for POST code beeps.
C. Call technical support.
D. Check the monitor connection.
Answer: B (LEAVE A REPLY)
A power-on self-test (POST) is a diagnostic process that runs when a server is turned on to check the basic functionality of the hardware components and report any errors or faults. A POST code is a series of beeps or flashes that indicate the status of the POST process and identify any problems that prevent the server from booting up. A POST code can be heard through a speaker or seen on a display attached to the server motherboard. A POST code is useful for diagnosing errors without opening the machine or using any software tools.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 5, Lesson 5.1, Objective 5.1

NEW QUESTION: 111
An administrator is tasked with building an environment consisting of four servers that can each serve the same website. Which of the following concepts is described?
A. Load balancing
B. Direct access
C. Overprovisioning
D. Network teaming
Answer: A (LEAVE A REPLY)

Load balancing is a technique used to distribute workloads evenly across multiple servers, ensuring no single server is overwhelmed. This is especially important in environments where high availability and reliability are critical, such as when multiple servers are serving the same website. By doing so, load balancing improves the responsiveness and availability of applications or websites.
Load balancing refers to the process of distributing network or application traffic across multiple servers to ensure no single server becomes overwhelmed, thereby improving responsiveness and availability of applications or websites. In the scenario described, where four servers are set up to each serve the same website, the concept of load balancing is applied. This setup aims to distribute incoming requests evenly among the servers to maximize speed and capacity utilization while ensuring no one server is overburdened, which can lead to improved overall performance of the website. Options B, C, and D do not accurately describe the scenario of distributing traffic for the same website across multiple servers.

NEW QUESTION: 112
A Linux administrator created a script that will run at startup. After successfully writing the script, the administrator received me following output when trying to execute the script:
Bash ./startup,sh:Permission denied
Which of the following commands would BEST resolve the error message?
A. Chmod +w startup.sh
B. Chmod 444 startup.sh
C. Chmod+x startup.sh
D. Chmod 466 startUp,sh
Answer: C (LEAVE A REPLY)
This is the command that would best resolve the error message "Bash ./startup.sh: Permission denied" when trying to execute a script on Linux. Chmod is a command that changes the permissions of files or directories on Linux. +x is an option that adds the execute permission to the file or directory for the owner, group, and others. startup.sh is the name of the script file that needs to be executed. By running chmod +x startup.sh, the technician grants execute permission to the script file and allows it to be run by any user. Chmod +w startup.
sh would add write permission to the file, but not execute permission. Chmod 444 startup.sh would set read- only permission for all users, but not execute permission. Chmod 466 startup.sh would set read and write permission for the owner and write-only permission for group and others, but not execute permission.
References: https://www.howtogeek.com/437958/how-to-use-the-chmod-command-on-linux

NEW QUESTION: 113
A new 40GB NIC has just been installed in a server but is not detected within the Windows server OS. Which of the following would most likely fix the issue?
A. Update the firmware on the NIC.
B. Update the server OS.
C. Update the remote management console.
D. Update the switch firmware.
Answer: A (LEAVE A REPLY)
Updating the firmware on the NIC is the most likely solution to fix the issue of a new 40GB NIC not being detected within the Windows server OS. Firmware is a software program that controls the functionality of a hardware device, such as a NIC (network interface card). A NIC is a device that enables network communication for a server by providing an interface between the server and the network cable or wireless connection. Updating the firmware on the NIC can improve its performance, compatibility, and stability with the server OS and network protocols. References: CompTIA Server+ Certification Exam Objectives, Domain

4.0: Networking, Objective 4.1: Given a scenario, configure network settings for servers.

NEW QUESTION: 114
When a user plugs a USB drive into a workstation and attempts to transfer a file from the server, an error appears that indicates the file cannot be copied. However, the user can copy or create new files from the local workstation. Which of the following is part of this security strategy?
A. HIDS
B. SIEM
C. ACL
D. DLP
Answer: (SHOW ANSWER)
Comprehensive Detailed Explanation with all CompTIA Server+ SK0-005 Study Guide References:Data Loss Prevention (DLP)policies are designed to prevent sensitive data from being copied, moved, or accessed in unauthorized ways. In this scenario, the DLP system is likely configured to block file transfers from the server to external storage devices, such as USB drives, while still allowing local file creation or movement.
* HIDS (Host-Based Intrusion Detection System):Monitors system activities for malicious behavior but does not block file transfers.
* SIEM (Security Information and Event Management):Provides centralized monitoring and analysis of security events but does not directly enforce file transfer restrictions.
* ACL (Access Control List):Manages permissions but does not control data transfer policies.

NEW QUESTION: 115
A backup application is copying only changed files each line it runs. During a restore, however, only a single file is used. Which of the following backup methods does this describe?
A. Open file
B. Synthetic full
C. Full Incremental
D. Full differential
Answer: (SHOW ANSWER)
A synthetic full backup is a backup method that describes copying only changed files each time it runs and using only a single file during a restore. A synthetic full backup is a backup approach that involves creating a new full backup by using the previous full backup and related incremental backups. This means that a backup solution does not have to transfer the full amount of data from the source machine and can synthetize the latest incremental backups with the last full backup to create a new full backup. This reduces the backup window and network bandwidth consumption. During a restore, only the latest synthetic full backup file is needed to recover the data. Open file backup is a backup method that allows backing up files that are in use or locked by applications. Full incremental backup is a backup method that involves performing a full backup first and then backing up only the changed files since the last backup. Full differential backup is a backup method that involves performing a full backup first and then backing up only the changed files since the last full backup. References: https://www.nakivo.com/blog/what-is-synthetic-backup/https://www.howtogeek.com /192115/what-you-need-to-know-about-creating-system-image-backups/

NEW QUESTION: 116
An administrator has been asked to deploy a database server that provides the highest performance with fault tolerance. Which of the following RAID levels will fulfill this request?
A. RAIDO
B. RAID1

C. RAID 5
D. RAID 6
E. RAID 10
Answer: E (LEAVE A REPLY)
RAID 10 is the best option to deploy a database server that provides the highest performance with fault tolerance. RAID 10 is a type of RAID level that combines RAID 1 (mirroring) and RAID 0 (striping) to create an array of mirrored stripes. RAID 10 offers high performance by distributing data across multiple disks in parallel (striping), which improves read/write speed and I/O operations. RAID 10 also offers fault tolerance by duplicating data across two or more disks in each stripe (mirroring), which provides redundancy and data protection in case of disk failure. RAID 10 requires at least four disks to implement and has a high storage overhead, as half of the disk space is used for mirroring. References: [CompTIA Server+ Certification Exam Objectives]

NEW QUESTION: 117
A server administrator purchased a single license key to use for all the new servers that will be imaged this year. Which of the following MOST likely refers to the licensing type that will be used?
A. Per socket
B. Open-source
C. Per concurrent user
D. Volume
Answer: D (LEAVE A REPLY)
This is the most likely licensing type that will be used because volume licensing allows a single license key to be used for multiple installations of a software product. Volume licensing is typically used by organizations that need to deploy software to a large number of devices or users.References:https://www.microsoft.com/en- us/licensing/licensing-programs/volume-licensing-programs

NEW QUESTION: 118
A datacenter technician is attempting to troubleshoot a server that keeps crashing. The server runs normally for approximately five minutes, but then it crashes. After restoring the server to operation, the same cycle repeats. The technician confirms none of the configurations have changed, and the load on the server is steady from power-on until the crash. Which of the following will MOST likely resolve the issue?
A. Reseating any expansion cards in the server
B. Replacing the failing hard drive
C. Reinstalling the heat sink with new thermal paste
D. Restoring the server from the latest full backup
Answer: C (LEAVE A REPLY)
The most likely solution to resolve the issue of the server crashing after running normally for approximately five minutes is to reinstall the heat sink with new thermal paste. A heat sink is a device that dissipates heat from a component, such as a processor or a graphics card, by transferring it to a cooling medium, such as air or liquid. A heat sink is usually attached to the component using thermal paste, which is a substance that fills the gaps between the heat sink and the component and improves thermal conductivity. Thermal paste can degrade over time and lose its effectiveness, resulting in overheating and performance issues. If a server crashes after running for a short period of time, it may indicate that the processor is overheating due to insufficient cooling. To resolve this issue, the technician should remove the heat sink, clean the old thermal paste, apply new thermal paste, and reinstall the heat sink.

NEW QUESTION: 119

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 (LEAVE A REPLY)
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: 120
A server administrator has been asked to implement a password policy that will help mitigate the chance of a successful brute-force attack. Which of the following password policies should the administrator implement first?
A. Lockout
B. Length
C. Complexity
D. Minimum age
Answer: B (LEAVE A REPLY)
Password length is the first password policy that the administrator should implement to help mitigate the chance of a successful brute-force attack. A brute-force attack is a method of guessing passwords by trying all possible combinations of characters until the correct one is found. The longer the password, the more combinations there are, and the more time and resources it takes to crack it. Therefore, password length is a key factor in password strength and security.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.2, Objective 3.2

NEW QUESTION: 121
Several mobile users are reporting intermittent performance issues when attempting to access network shares on the file server. After some investigation, the server administrator notices the server resources are running at maximum capacity, even during non-peak usage times. A recent port scan of the network identified this server as having too many unnecessary ports open to the public. Which of the following is the most likely cause of the performance issues?
A. Incorrect share permissions for mobile users
B. Improper privilege escalation
C. A virus infection
D. A misconfigured firewall rule
Answer: C (LEAVE A REPLY)
The fact that the server is running at maximum capacity, combined with the open ports, suggests that the server may have been compromised bya virus infection. Malware can exploit unnecessary open ports, leading to resource exhaustion and performance issues.
* Virus infection (Answer C):Malware often exploits open ports and consumes system resources, leading to performance degradation.
* Incorrect share permissions (Option A):This would affect access but not resource utilization.
* Improper privilege escalation (Option B):This refers to unauthorized users gaining higher access rights, but it doesn't explain the high resource usage.

* Misconfigured firewall rule (Option D):A misconfigured firewall could allow unnecessary traffic, but it' s less likely to cause performance issues unless combined with malware.
CompTIA Server+ Reference:This topic is covered underSK0-005 Objective 4.2: Explain server security concepts and best practices.

NEW QUESTION: 122
A company wants to find an affordable way to simulate a fail over of a critical application. The company does not currently have a solution for it. The application consists of 15 servers, and the company would like to simulate on production configurations and IP address schemes. Which of the following would be the most cost-effective solution?
A. Build a warm site and perform a fail over of the application.
B. Build a cloud laaS and perform a fail over of the application.
C. Build a hot site and perform a fail over of the application.
D. Build a cold site and perform a fail over of the application.
E. Perform a tabletop fail over of the application.
Answer: B (LEAVE A REPLY)
Cloud IaaS (Infrastructure as a Service) is a service model that allows users to rent virtualized computing resources over the internet, such as servers, storage, network, and software. Cloud IaaS can provide several benefits for disaster recovery and failover scenarios, such as:
Lower cost: Cloud IaaS can reduce the capital and operational expenses of building and maintaining a physical disaster recovery site, as users only pay for the resources they use on demand12.
Scalability: Cloud IaaS can offer flexible and elastic scalability of resources, as users can easily provision or deprovision resources according to their needs and workload12.
Availability: Cloud IaaS can ensure high availability and reliability of the application, as users can leverage the cloud provider's redundant and geographically distributed infrastructure12.
Simplicity: Cloud IaaS can simplify the failover process, as users can use the cloud provider's tools and services to automate and orchestrate the failover operations12.
Therefore, building a cloud IaaS and performing a failover of the application would be the most cost-effective solution for the company, as it would allow them to simulate a failover of a critical application on production configurations and IP address schemes without investing in a physical disaster recovery site.

NEW QUESTION: 123
An administrator needs to increase the size of an existing RAID 6 array that is running out of available space.
Which of the following is the best way the administrator can perform this task?
A. Replace all the array drives at once and then expand the array.
B. Expand the array by changing the RAID level to 6.
C. Expand the array by changing the RAID level to 10.

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

NEW QUESTION: 124
Which of the following, if properly configured, would prevent a user from installing an OS on a server?
(Select TWO).
A. Administrator password
B. Group Policy Object
C. Root password
D. SELInux
E. Bootloader password
F. BIOS/UEFI password
Answer: (SHOW ANSWER)
These are two methods that can prevent a user from installing an OS on a server if properly configured. A bootloader password is a password that protects the bootloader from unauthorized access or modification. The bootloader is a program that loads the operating system into memory when the system boots up. If a user does not know the bootloader password, they cannot change the boot order or boot from another device such as a CD-ROM or USB drive that contains an OS installation media. A BIOS/UEFI password is a password that protects the BIOS (Basic Input Output System) or UEFI (Unified Extensible Firmware Interface) from unauthorized access or modification. The BIOS or UEFI is a firmware that initializes and configures the hardware components of the system before loading

NEW QUESTION: 125
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: (SHOW ANSWER)
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: 126
A server administrator needs to set up active-passive load balancing for an environment with multiple network paths. The traffic should be directed to one path and switched only in the event that the original path becomes unavailable. Which of the following describes this scenario?
A. Most recently used
B. Heartbeat
C. Link aggregation
D. Round robin
Answer: B (LEAVE A REPLY)
In anactive-passive load balancingconfiguration, one path (or server) handles all the traffic while the other remains in standby mode, ready to take over if the active path becomes unavailable. This setup is typically monitored via aheartbeatmechanism, where the standby server checks the availability of the active server and takes over when it detects a failure.
* Heartbeat (Answer B):This term refers to the monitoring process that checks the availability of the active path in an active-passive configuration.
* Most recently used (Option A):This describes a load-balancing method where the most recently used path or server is prioritized, but it doesn't describe an active-passive setup.
* Link aggregation (Option C):This refers to combining multiple network connections for increased throughput, not for failover purposes.
* Round robin (Option D):This load-balancing method alternates traffic between all available paths, which doesn't match the active-passive description.
CompTIA Server+ Reference:This topic is covered underSK0-005 Objective 1.4: Summarize methods used to manage network connections.

NEW QUESTION: 127
A server administrator is tasked with ensuring that information stored on company database systems is secure from bad actors. Which of the following security practices would accomplish this task?
A. Encryption at rest
B. Audit logging
C. BIOS password
D. Signal blocking
Answer: A (LEAVE A REPLY)

NEW QUESTION: 128
An administrate is helping to replicate a large amount of data between two Windows servers. The administrator is unsure how much data has already been transferred. Which of the following will BEST ensure all the data is copied consistently?
A. rsync
B. copy
C. scp
D. robocopy
Answer: D (LEAVE A REPLY)
Robocopy (Robust File Copy) is a command-line tool that can copy files and folders between Windows servers or computers. It has many features and options that can ensure all the data is copied consistently, such as retrying failed copies, resuming interrupted copies, copying permissions and attributes, mirroring source and destination directories, and logging the copy progress and results. Verified References: [Robocopy], [File copy]

NEW QUESTION: 129

A technician needs to replace two RAID controllers on a database server as part of an upgrade. The server has six external storage arrays and eight internal disks that are controlled by the two RAID controllers. The technician completes the replacement and powers the systems back on, but the server OS detects several missing disks in the configuration. Which of the following steps should the technician take first to resolve this issue?

A. Reboot to the RAID controller BIOS and rescan for attached disks and arrays

B. Start the motherboard UEFI and confirm the RAID controller start order is correct

C. Turn off the external arrays and reboot the server to redetect the internal disks first

D. Turn off all components and confirm all external and internal cables before rebooting

Answer: A (LEAVE A REPLY)

When new RAID controllers are installed and disks go missing, the first logical step is toreboot to the RAID controller BIOS and rescan for attached disks and arrays (Answer A). This will allow the RAID controller to detect the connected drives and rebuild the RAID configuration as expected.

* Rebooting to RAID controller BIOS (Answer A):This step ensures that all the attached disks and arrays are properly detected and mapped to the RAID configuration.
* Checking UEFI settings (Option B):This might be useful later, but initially, the RAID controller BIOS should be checked first to verify disk detection.
* Turning off external arrays (Option C):While this could be helpful in some scenarios, it's not the most efficient first step.
* Checking cables (Option D):This could be necessary, but since the controllers were just replaced, software/BIOS configurations should be checked first.

CompTIA Server+ Reference:This topic relates toSK0-005 Objective 3.1: Install and configure server components.

NEW QUESTION: 130

A bad actor leaves a USB drive with malicious code on it in a company's parking lot. Which of the following describes this scenario?

A. Hacking

B. Insider threat

C. Phishing

D. Social engineering

Answer: D (LEAVE A REPLY)

Leaving a USB drive in a company parking lot is a classic example ofsocial engineering, where the bad actor relies on human curiosity to prompt someone to pick up the USB drive and insert it into their computer, potentially infecting the system with malicious code.

* Social engineering (Answer D):The attacker manipulates human behavior (in this case, curiosity) to exploit security weaknesses.
* Hacking (Option A):Hacking refers to directly breaching security systems or exploiting software vulnerabilities, not manipulating humans.
* Insider threat (Option B):This involves a legitimate insider within the organization carrying out malicious activities, which isn't the case here.
* Phishing (Option C):Phishing typically involves emails or messages designed to deceive individuals into providing sensitive information.

CompTIA Server+ Reference:This topic is covered underSK0-005 Objective 4.2: Explain server security concepts and best practices.

NEW QUESTION: 131

A security administrator ran a port scanning tool against a virtual server that is hosting a secure website. A list of open ports was provided as documentation. The management team has requested that non-essential ports be disabled on the firewall. Which of the following ports must remain open?

A. 25

B. 443

C. 3389

D. 8080

Answer: B (LEAVE A REPLY)
The port that must remain open for a secure website is port 443. Port 443 is used by Hypertext Transfer Protocol Secure (HTTPS), which is an extension of HTTP that encrypts and authenticates the communication between a web server and a web browser. HTTPS ensures that the data transmitted over the web is protected from eavesdropping, tampering, or spoofing. Therefore, port 443 must remain open for a secure website to function properly.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 2, Lesson 2.2, Objective 2.2

NEW QUESTION: 132
An administrator has been asked to disable CPU hyperthreading on a server to satisfy a licensing issue. Which of the following best describes how the administrator will likely perform this action?
A. Use a RDP/VNC session.
B. Modify the startup configuration.
C. Use a PowerShell/Bash script.
D. Use the BIOS/UEFI setup.
Answer: D (LEAVE A REPLY)
The BIOS (Basic Input/Output System) or UEFI (Unified Extensible Firmware Interface) setup is a program that allows users to configure the hardware settings of a computer, such as the CPU, memory, disk, and boot options. The BIOS/UEFI setup can be accessed by pressing a specific key (such as F2, F10, or Delete) during the boot process, before the operating system loads12.
One of the settings that can be changed in the BIOS/UEFI setup is the CPU hyperthreading option.
Hyperthreading is a technology that enables a single physical CPU core to execute two threads or tasks simultaneously, improving the performance and efficiency of multi-threaded applications. However, some software licenses may limit the number of CPU cores or threads that can be used, and therefore require disabling hyperthreading on the server34.
To disable hyperthreading on a server, the administrator will likely need to enter the BIOS/UEFI setup and navigate to the processor options menu. There, the administrator will find a setting for Intel Hyperthreading Technology or Hyperthreading Function, which can be enabled or disabled. The administrator will need to disable this setting and save the changes. This will turn off hyperthreading on the server and reduce the number of logical CPUs to match the number of physical cores5.

NEW QUESTION: 133
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 (LEAVE A REPLY)
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 dat a. 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: 134

Which of the following is an architectural reinforcement that attempts to conceal the interior of an organization?

A. Bollards

B. Signal blocking

C. Reflective glass

D. Data center camouflage

Answer: (SHOW ANSWER)

Reflective glass is an architectural reinforcement that attempts to conceal the interior of an organization by reflecting light and preventing outsiders from seeing inside. Reflective glass can also reduce heat and glare, and enhance the aesthetic appearance of a building. Reflective glass is often used in high-security facilities, such as data centers, government buildings, or corporate headquarters12

1: Server Architecture for CompTIA Server+ (SK0-004) | Pluralsight 2: Introducing the CompTIA Infrastructure Career Pathway

NEW QUESTION: 135

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 (LEAVE A REPLY)

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-licensing https://www.techopedia.com/definition/1032/business- impact-analysis-bia

NEW QUESTION: 136

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 (LEAVE A REPLY)

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: 137
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 (LEAVE A REPLY)
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: 138
An administrator is deploying a new secure web server. The only administration method that is permitted is to connect via RDP. Which of the following ports should be allowed?
(Select two).
A. 53
B. 80
C. 389
D. 443
E. 445
F. 3389
G. 8080
Answer: D,F (LEAVE A REPLY)
Port 443 is used for HTTPS, which is a secure version of HTTP that encrypts the data between the web server and the client. Port 3389 is used for RDP, which is a protocol that allows remote desktop connections to a server. These ports should be allowed for a secure web server that can be administered via RDP.
References:
CompTIA Server+ Certification Exam Objectives1, page 15
Common Ports Cheat Sheet: The Ultimate Ports & Protocols List2

NEW QUESTION: 139

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 (LEAVE A REPLY)
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: 140
A server administrator made a change in a server's BIOS in an attempt to fix an issue with the OS not turning on. However, the change did not successfully correct the issue. Which of the following should the server administrator do NEXT?
A. Reinstall the server OS in repair mode while maintaining the data.
B. Flash the BIOS with the most recent version.
C. Reverse the latest change made to the server and reboot.
D. Restart the server into safe mode and roll back changes.
Answer: C (LEAVE A REPLY)
The best practice for troubleshooting is to follow a logical and systematic process that involves identifying the problem, establishing a theory of probable cause, testing the theory, establishing a plan of action, implementing the solution, verifying functionality, and documenting findings. Since the problem occurred after a change in the server's BIOS, the most likely cause is that the change was incompatible or incorrect for the OS. Therefore, the next step should be to reverse the latest change made to the server and reboot to see if that fixes the issue.References:
https://www.comptia.org/training/resources/exam-objectives/comptia-server- sk0-005-exam-objectives (Objective 4.3)

NEW QUESTION: 141
Which of the following is the MOST appropriate scripting language to use for a logon script for a Linux box?
A. VBS
B. Shell
C. Java
D. PowerShell
E. Batch
Answer: B (LEAVE A REPLY)
Shell is the most appropriate scripting language to use for a logon script for a Linux box. Shell is a generic term for a command-line interpreter that allows users to interact with the operating system by typing commands and executing scripts. Shell scripts are files that contain a series of commands and instructions that can be executed by a shell. Shell scripts are commonly used for automating tasks, such as logon scripts that run when a user logs on to a system. There are different types of shells available for Linux systems, such as Bash, Ksh, Zsh, etc., but they all share a similar syntax and functionality.

NEW QUESTION: 142
A technician is attempting to resolve an issue with a file server that is unable to download a file Given the following output:

```
root@server:~$ ls -Z /var/www/html/file
-rw-r--r--  root  root  unconfined_u:object_r:samba_share_t:s0  /var/www/html/file
```

Which of the following would best allow this file to be read?

A. chown

B. sestatus

C. setenforce

D. getenforce

E. chmod

Answer: E (LEAVE A REPLY)

The given output in the image indicates that the file is present, but the permissions may not allow it to be read.

The output indicates '-rw-------', which means that the file is set to be readable and writable by the owner only, with no permissions for group or others.

To allow the file to be read by users other than the owner, the file's permissions will need to be changed. Thechmod(change mode) command is used to change the file's permissions in Linux. For example,chmod 644 filewould change the permissions of the file to be readable by everyone and writable by the owner, which is typically what's required for a file server. It is always recommended to apply the least permissive settings that still allow the required operation to maintain security.

NEW QUESTION: 143

The management team at a healthcare organization is concerned about being able to access the dairy vital records if there is an IT disaster that causes both servers and the network lo be offline. Which of the following backup types can the organization use to mitigate this risk?

A. Tape

B. Cloud

C. Disk

D. Print

Answer: (SHOW ANSWER)

A print backup is a type of backup that can be used to mitigate the risk of being unable to access the daily vital records if there is an IT disaster that causes both servers and the network to be offline. A print backup is a backup that involves printing out the data on paper and storing it in a secure location. A print backup can provide offline access to the data without relying on any hardware or software components that may be affected by the disaster. However, a print backup has some drawbacks such as high cost, low efficiency, low security, and environmental impact. A tape backup is a type of backup that involves storing the data on magnetic tape cartridges that can be accessed using a tape drive or a tape library. A tape backup can provide offline access to the data with high capacity, low cost, and long durability, but it requires special equipment and software that may not be available during a disaster. A cloud backup is a type of backup that involves storing the data on remote servers or platforms that can be accessed over the internet using a web browser or an application. A cloud backup can provide online access to the data with high scalability, flexibility, and security, but it requires network connectivity and bandwidth that may not be available during a disaster. A disk backup is a type of backup that involves storing the data on hard disk drives or solid state drives that can be accessed using a computer or a device. A disk backup can provide online or offline access to the data with high performance, reliability, and portability, but it requires compatible hardware and software that may not be available during a disaster.

References: https://www.howtogeek.com/428483/what-is-end-to-end- encryption-and-why-does-it-matter/ https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system- drive-removable-devices-and-individual-files/ https://www.howtogeek.com/199068/how-to-upgrade-your- existing-hard-drive-in-under-an-hour/ https://www.howtogeek.com/202794/what-is-the-difference-between-

NEW QUESTION: 144

A server administrator needs to create a new folder on a file server that only specific users can access. Which of the following BEST describes how the server administrator can accomplish this task?
A. Create a group that includes all users and assign it to an ACL.
B. Assign individual permissions on the folder to each user.C Create a group that includes all users and assign the proper permissions.
C. Assign ownership on the folder for each user.
Answer: (SHOW ANSWER)
The top portion of the dialog box lists the users and/or groups that have access to the file or folder.
Reference:https://www.uwec.edu/kb/article/drives-establishing-windows-file-and-folder-level-permissions/

NEW QUESTION: 145
An administrator discovers a misconfiguration that impacts all servers but can be easily corrected. The administrator has a list of affected servers and a script to correct the issue. Which of the following scripting principles should the administrator use to cycle through the list of servers to deliver the needed change?
A. Linked list
B. String
C. Loop
D. Constant
Answer: C (LEAVE A REPLY)
A loop is a programming construct that allows a block of code to be executed repeatedly until a certain condition is met1. A loop can be used to cycle through a list of servers and run a script on each one of them.
For example, in Python, a loop can be written as:
Python
This code is AI-generated. Review and use carefully. Visit our FAQ for more information.
Copy
```
# Assume servers is a list of server names
for server in servers:
# Run the script on the server
run_script(server)
```
A loop can help automate the task of correcting the misconfiguration on all servers, saving time and effort.

NEW QUESTION: 146
A server administrator is tasked with upgrading the network on a server to 40Gbps. After installing the card, which of the following connectors should the administrator use?
A. QSFP+
B. 10 GigE
C. SFP
D. SFP+
Answer: A (LEAVE A REPLY)
QSFP+ (Quad Small Form-factor Pluggable Plus) connectors are used in high-density, high-speed networking solutions such as 40 Gigabit Ethernet (40GbE) interfaces. When upgrading a server's network to 40Gbps, QSFP+ is the appropriate choice due to its capability to support such high-speed

data transfer rates. 10 GigE, SFP, and SFP+ connectors are used for lower speed connections (10Gbps and below for SFP+ and 10 GigE, and even less for SFP), making them unsuitable for a 40Gbps network upgrade.

NEW QUESTION: 147
A systems administrator has noticed performance degradation on a company file server, and one of the disks on it has a solid amber light. The administrator logs on to the disk utility and sees the array is rebuild ing.
Which of the following should the administrator do NEXT once the rebuild is finished?
A. Restore the server from a snapshot.
B. Restore the server from backup.
C. Swap the drive and initialize the disk.
D. Swap the drive and initialize the array.
Answer: (SHOW ANSWER)
The next action that the administrator should take once the rebuild is finished is to swap the drive and initialize the disk. This is to replace the faulty disk that has a solid amber light, which indicates a predictive failure or a SMART error. Initializing the disk will prepare it for use by the RAID controller and add it to the array. The administrator should also monitor the array status and performance after swapping the drive.
Reference:https://www.salvagedata.com/how-to-rebuild-a-failed-raid/

NEW QUESTION: 148
A virtual host has four NICs and eight VMs. Which of the following should the technician configure to enable uplink redundancy?
A. VM
B. vNIC
C. vSwitch
D. vCPU
E. vHBA
Answer: C (LEAVE A REPLY)
Uplink redundancy is a method used to ensure that if one physical network interface card (NIC) fails, the network connectivity for the virtual machines (VMs) does not go down. This is typically achieved by configuring multiple NICs to connect to a single virtual switch (vSwitch) and setting up NIC teaming or bonding. The vSwitch manages the internal network traffic between the VMs and the outside network by using the physical NICs assigned to it. By configuring the vSwitch with multiple NICs, you can create redundancy, so if one NIC fails, the other NICs can take over the traffic, ensuring continuous network connectivity.

NEW QUESTION: 149
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: (SHOW ANSWER)

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: 150
Which of the following concepts refers to prioritizing a connection that had previously worked successfully?
A. Round robin
B. SCP
C. MRU
D. Link aggregation
Answer: (SHOW ANSWER)
MRU, or Most Recently Used, is a concept that refers to prioritizing a connection that had previously worked successfully. It is often used in load balancing algorithms to distribute the workload among multiple servers or paths. MRU assumes that the most recently used connection is the most likely to be available and efficient, and therefore assigns the next request to that connection. This can help reduce latency and improve performance12. The other options are incorrect because they do not refer to prioritizing a previous connection. Round robin is a concept that refers to distributing the workload equally among all available connections in a circular order12. SCP, or Secure Copy Protocol, is a concept that refers to transferring files securely between hosts using encryption3. Link aggregation is a concept that refers to combining multiple physical links into a single logical link to increase bandwidth and redundancy4.

NEW QUESTION: 151
A server technician is installing application updates on a Linux server. When the technician tries to install a MySQL update, the GUI displays the following error message: AVC denial. Which of the following should the technician do for the MySQL update to install?
A. Download the update manually and run a checksum utility to verify file integrity.
B. Issue the setenforce 0 command.
C. Create a firewall rule to allow port 3306 through the firewall.
D. Issue the yum -y update mysql command.
Answer: B (LEAVE A REPLY)
The AVC denial error message indicates that SELinux (Security-Enhanced Linux) is preventing the MySQL update from installing. SELinux is a security module that enforces mandatory access control policies on Linux systems. To install the MySQL update, the technician should issue the setenforce 0 command, which temporarily disables SELinux enforcement until the next reboot. Downloading the update manually, creating a firewall rule, or issuing the yum -y update mysql command will not resolve the error. References:
[CompTIA Server+ Certification Exam Objectives], Domain 4.0: Server Administration, Objective 4.3: Given a scenario, troubleshoot server issues using appropriate tools.

NEW QUESTION: 152
A server administrator just installed a new physical server and needs to harden the applications on the server.
Which of the following best describes a method of application hardening?
A. Install the latest patches.
B. Disable unneeded hardware.
C. Set the boot order.
D. Enable a BIOS password.
Answer: A (LEAVE A REPLY)
A method of application hardening is installing the latest patches. Application hardening is a process of reducing the attack surface and vulnerabilities of an application by applying security measures and best practices. Installing the latest patches is one way to harden an application, as patches are updates that fix bugs, errors, or security issues in an application. By installing the latest patches, an application can be protected from known exploits or threats.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.5, Objective 3.5

NEW QUESTION: 153
An organization stores backup tapes of its servers at cold sites. The organization wants to ensure the tapes are properly maintained and usable during a DR scenario. Which of the following actions should the organization perform?
A. Have the facility inspect and inventory the tapes on a regular basis.
B. Have duplicate equipment available at the cold site.
C. Retrieve the tapes from the cold site and test them.
D. Use the test equipment at the cold site to read the tapes.
Answer: C (LEAVE A REPLY)
The organization should retrieve the tapes from the cold site and test them to ensure they are properly maintained and usable during a DR scenario. A cold site is a location that has space and power for backup equipment, but no actual equipment installed or configured. The organization stores backup tapes of its servers at cold sites as a precaution in case of a disaster that affects its primary site. However, backup tapes can degrade over time due to environmental factors such as temperature, humidity, dust, or magnetic fields.
Therefore, the organization should periodically retrieve the tapes from the cold site and test them on compatible equipment to verify their integrity and readability.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 6, Lesson 6.4, Objective 6.4

NEW QUESTION: 154
Which of the following is typical of software licensing in the cloud?
A. Per socket
B. Perpetual
C. Subscription-based
D. Site-based
Answer: (SHOW ANSWER)

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

NEW QUESTION: 155
Which of the following license types most commonly describes a product that incurs a yearly cost regardless of how much it is used?
A. Physical
B. Subscription
C. Open-source
D. Per instance
E. Per concurrent user
Answer: B (LEAVE A REPLY)
A subscription license is a type of license that grants the user the right to use a product or service for a fixed period of time, usually a year. The user pays a recurring fee, regardless of how much they use the product or service. Subscription licenses are common for cloud-based software and services, such as Microsoft 3651 or DocuSign2.
References = 1: Compare All Microsoft 365 Plans (Formerly Office 365) - Microsoft Store(https://www.microsoft.com/en-us/microsoft-365/buy/compare-all-microsoft-365-products) 2: DocuSign Pricing | eSignature Plans for Personal & Business(https://ecom.docusign.com/plans-and-pricing/esignature)

NEW QUESTION: 156
A server administrator receives the following output when trying to ping a local host:

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

Which of the following is MOST likely the issue?
A. Firewall
B. DHCP
C. DNS
D. VLAN
Answer: (SHOW ANSWER)
A firewall is a network device or software that filters and controls the incoming and outgoing traffic based on predefined rules. A firewall can block or allow certain types of packets, ports, protocols, or IP addresses. The output of the ping command shows that the local host is unreachable, which means that there is no network connectivity between the source and the destination. This could be caused by a firewall that isblocking the ICMP (Internet Control Message Protocol) packets that ping uses to test the connectivity.References:

https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives (Objective 2.2)

NEW QUESTION: 157
A server administrator is experiencing difficulty configuring MySQL on a Linux server. The administrator issues the getenforce command and receives the following output:
># Enforcing
Which of the following commands should the administrator issue to configure MySQL successfully?
A. setenforce 0
B. setenforce permissive
C. setenforce 1
D. setenforce disabled
Answer: (SHOW ANSWER)
The command that the administrator should issue to configure MySQL successfully is setenforce 0. This command sets the SELinux (Security-Enhanced Linux) mode to permissive, which means that SELinux will not enforce its security policies and will only log any violations. SELinux is a feature that provides mandatory access control (MAC) for Linux systems, which can enhance the security and prevent unauthorized access or modification of files and processes. However, SELinux can also interfere with some applications or services that require specific permissions or ports that are not allowed by SELinux by default. In this case, MySQL may not be able to run properly due to SELinux restrictions. To resolve this issue, the administrator can either disable SELinux temporarily by using setenforce 0, or permanently by editing the /etc/selinux/config file and setting SELINUX=disabled. Alternatively, the administrator can configure SELinux to allow MySQL to run by using commands such as semanage or setsebool.
Reference:
https://blogs.oracle.com/mysql/selinux-and-mysql-v2

NEW QUESTION: 158
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 (LEAVE A REPLY)
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: 159
A server administrator is configuring the IP address on a newly provisioned server in the testing environment.
The network VLANs are configured as follows:
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: 192.168.1.2/24Default 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 (LEAVE A REPLY)
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. Thesubnet 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: 160
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 (LEAVE A REPLY)
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: 161
Users in an office lost access to a file server following a short power outage. The server administrator noticed the server was powered off. Which of the following should the administrator do to prevent this situation in the future?
A. Connect the server to a KVM
B. Use cable management
C. Connect the server to a redundant network
D. Connect the server to a UPS

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

NEW QUESTION: 162
A technician is troubleshooting a server issue. The technician has determined several possible causes of the issue and has identified various solutions. Which of the following should the technician do next?
A. Consult internet forums to determine which is the most common cause and deploy only that solution.
B. Test each solution individually to determine the root cause, rolling back the changes in between each test.
C. Implement the shortest solution first to identify the issue and minimize downtime.
D. Test each solution in succession and restore the server from the latest snapshot.
Answer: B (LEAVE A REPLY)
According to the CompTIA troubleshooting methodology, the fourth step is to establish a plan of action to resolve the problem and implement the solution1. The best practice is to test each solution individually to determine the root cause, rolling back the changes in between each test. This way, the technician can isolate the cause and avoid introducing new problems or making the situation worse. Testing each solution in succession and restoring the server from the latest snapshot (D) is not a good option because it may not identify the root cause and may overwrite important dat a. Implementing the shortest solution first to identify the issue and minimize downtime is also not a good option because it may not solve the problem or may create new issues. Consulting internet forums to determine which is the most common cause and deploy only that solution (A) is not a good option because it may not apply to the specific situation or may be outdated or inaccurate

NEW QUESTION: 163
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 (LEAVE A REPLY)
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: 164
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 (LEAVE A REPLY)
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: 165
A user cannot save large files to a directory on a Linux server that was accepting smaller files a few minutes ago. Which of the following commands should a technician use to identify the issue?
A. pvdisplay
B. mount
C. df -h
D. fdisk -l
Answer: (SHOW ANSWER)
The df -h command should be used to identify the issue of not being able to save large files to a directory on a Linux server. The df -h command displays disk space usage in human-readable format for all mounted file systems on the server. It shows the total size, used space, available space, percentage of use, and mount point of each file system. By using this command, a technician can check if there is enough free space on the file system where the directory is located or if it has reached its capacity limit.

NEW QUESTION: 166
An administrator is only able to log on to a server with a local account. The server has been successfully joined to the domain and can ping other servers by IP address. Which of the following locally defined settings is MOST likely misconfigured?
A. DHCP
B. WINS
C. DNS
D. TCP
Answer: C (LEAVE A REPLY)
This is the most likely misconfigured setting because DNS is the service that resolves hostnames to IP addresses and vice versa. If the DNS server is incorrect or unreachable, the administrator will not be able to log on to the server with a domain account because the server will not be able to authenticate with the domain controller.References:https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/dns- troubleshooting

NEW QUESTION: 167

A technician is configuring a new server with four disks for the development team. The requirements are disk redundancy and maximum usable disk capacity. Which of the following RAID levels should be used for this server?

A. 0

B. 1

C. 5

D. 10

Answer: (SHOW ANSWER)

RAID 5offers bothdisk redundancyandmaximum usable disk capacityby using block-level striping with parity. RAID 5 allows one drive to fail while still retaining data, and it uses only one disk's worth of space for parity, maximizing the usable capacity.

* RAID 5 (Answer C):Provides redundancy with only one disk's space used for parity, maximizing storage.
* RAID 0 (Option A):Provides no redundancy; if one drive fails, all data is lost.
* RAID 1 (Option B):Mirrors data, so redundancy is provided, but only half the capacity is usable.
* RAID 10 (Option D):Combines RAID 1 and 0 for high performance and redundancy but requires half the disk space for mirroring.

CompTIA Server+ Reference:This topic is covered underSK0-005 Objective 1.5: Explain RAID levels and their benefits.

NEW QUESTION: 168

The management team has mandated the encryption of all server administration traffic. Which of the following should MOST likely be implemented?

A. SSH

B. VPN

C. SELinux

D. FTPS

Answer: A (LEAVE A REPLY)

SSH stands for Secure Shell and it is a network protocol that provides encrypted and authenticated communication between two hosts. SSH can be used to remotely access and administer a server using a command-line interface or a graphical user interface. SSH can ensure the encryption of all server administration traffic, which can prevent eavesdropping, tampering, or spoofing by unauthorized parties.

References: https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam- objectives (Objective 2.4)

NEW QUESTION: 169

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: (SHOW ANSWER)

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: 170

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

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

NEW QUESTION: 171
Which of the following DR testing scenarios is described as verbally walking through each step of the DR plan in the context of a meeting?
A. Live failover
B. Simulated failover
C. Asynchronous
D. Tabletop
Answer: (SHOW ANSWER)
The DR testing scenario that is described as verbally walking through each step of the DR plan in the context of a meeting is tabletop. A tabletop test is a type of disaster recovery (DR) test that involves discussing and reviewing the DR plan with key stakeholders and participants in a simulated scenario. A tabletop test does not involve any actual execution of the DR plan or any disruption of the normal operations. A tabletop test can help identify gaps, issues, or inconsistencies in the DR plan and improve communication and coordination among the DR team members.

NEW QUESTION: 172
A systems administrator is provisioning a large number of virtual Linux machines that will be configured identically. The administrator would like to configure the machines quickly and easily but does not have access to an automation/orchestration platform. Additionally, the administrator would like to set up a system that can be used in the future, even on newer versions of the OS. Which of the following will best meet the administrator's requirements?
A. Deploying each server from a VM template
B. Using a kickstart file during installation
C. Configuring each server manually one at a time
D. Copying/pasting configuration commands into each server through SSH sessions
E. Configuring a single server and then creating clones of it
Answer: (SHOW ANSWER)
* Kickstart Files (Linux): Kickstart files are configuration files that automate the Linux installation process. They contain pre-determined answers to installation prompts, allowing for identical and rapid deployment of multiple systems. (CompTIA Server+ Objectives SK0-004: 3.1, Red Hat documentation on Kickstart: https://access.redhat.com/documentation/)
* Why other options are less ideal:
* VM Template (A): Templates are useful for replicating the OS & some software, but might not capture all configurations.
* Manual Configuration (C): Time-consuming and prone to errors when replicating across many servers.

* Copy/Paste via SSH (D): Tedious, error-prone, and requires servers to be online before configuration.
* Cloning (E): Can work but has version compatibility risks if the OS of the cloned server isn't identical to the new ones.

NEW QUESTION: 173
A technician wants to limit disk usage on a server. Which of the following should the technician implement?
A. Formatting
B. Compression
C. Disk quotas
D. Partitioning
Answer: (SHOW ANSWER)
Reference:https://www.digitalcitizen.life/simple-questions-what-are-disk-quotas-how-set-them-windows/ Explanation: Disk quotas are a way to limit disk usage on a server by setting a maximum amount of space that each user or group can use. Disk quotas can help manage disk space allocation, prevent disk space exhaustion, and enforce fair usage policies. Disk quotas can be set at the volume level or at the folder level, depending on the file system and operating system used.Reference:https://docs.microsoft.com/en-us/windows-server/storage
/ntfs/ntfs-disk-quotas-overview

NEW QUESTION: 174
Following a recent power outage, a server in the datacenter has been constantly going offline and losing its configuration. Users have been experiencing access issues while using the application on the server. The server technician notices the data and time are incorrect when the server is online. All other servers are working. Which of the following would MOST likely cause this issue? (Choose two.)
A. The server has a faulty power supply
B. The server has a CMOS battery failure
C. The server requires OS updates
D. The server has a malfunctioning LED panel
E. The servers do not have NTP configured
F. The time synchronization service is disabled on the servers
Answer: B,F (LEAVE A REPLY)
The server has a CMOS battery failure and the time synchronization service is disabled on the servers. The CMOS battery is a small battery on the motherboard that powers the BIOS settings and keeps track of the date and time when the server is powered off. If the CMOS battery fails, the server will lose its configuration and display an incorrect date and time when it is powered on. This can cause access issues for users and applications that rely on accurate time stamps. The time synchronization service is a service that synchronizes the system clock with a reliable external time source, such as a network time protocol (NTP) server. If the time synchronization service is disabled on the servers, they will not be able to update their clocks automatically and may drift out of sync with each other and with the network. This can also cause access issues for users and applications that require consistent and accurate time across the network.

NEW QUESTION: 175
Following a recent power outage, a server in the data center has been constantly going offline and losing its configuration. Users have been experiencing access issues while using the application on the server. The server technician notices the date and time are incorrect when the server is online. All other servers are working. Which of the following would most likely cause this issue? (Select two).
A. The server has a faulty power supply.
B. The server has a CMOS battery failure.

C. The server requires OS updates.
D. The server has a malfunctioning LED panel.
E. The servers have NTP configured.
F. CPU frequency scaling is set too high.
Answer: B,E (LEAVE A REPLY)
A CMOS battery failure can cause the server to lose its BIOS settings, including the date and time, which can affect the server's functionality and connectivity. The servers have NTP (Network Time Protocol) configured to synchronize their clocks with a reliable time source, which can prevent time drift and ensure consistent timestamps. If one server has a wrong date and time, it can cause conflicts and errors with the other servers that have NTP configured.
References:
* CompTIA Server+ Certification Exam Objectives1, page 9
* Signs or symptoms of a CMOS battery failure2
* NTP: Network Time Protocol

NEW QUESTION: 176
A new virtual server was deployed in a perimeter network. Users have reported the time on the server has been incorrect. The engineer has verified the configuration, and the internal time servers are configured properly. Which of the following should the engineer do to resolve this issue?
A. Check the firewall rules.
B. Replace the CMOS battery in the server.
C. Restart the time servers.
D. Manually correct the time.
Answer: D (LEAVE A REPLY)
* The virtual server's time is incorrect despite proper configuration of internal time servers.
* Resolution: The engineer should manually correct the time (Option D):
* If the internal time servers are configured correctly, manual adjustment is necessary.
* Checking firewall rules would help identify NTP (Network Time Protocol) issues.
* Replacing the CMOS battery is unlikely to be the cause of incorrect time.
Reference: CompTIA Server+ Guide, Chapter 4: Networking, Section 4.2.2 (Time Synchronization)

NEW QUESTION: 177
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 (LEAVE A REPLY)
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-1-2 2 https://www.ibm.
com/topics/hypervisors 3 https://www.redhat.com/en/topics/virtualization/what-is-a-hypervisor

NEW QUESTION: 178
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 initial install.
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 the system.
Answer: A (LEAVE A REPLY)
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: 179
Which of the following BEST describes a guarantee of the amount of time it will take to restore a downed service?
A. RTO
B. SLA
C. MTBF
D. MTTR
Answer: A (LEAVE A REPLY)
RTO stands for Recovery Time Objective and it is a metric that defines the maximum acceptable amount of time that a system or service can be unavailable after a disaster or disruption. RTO is part of the business continuity planning and disaster recovery planning processes. RTO ensures a guarantee of the amount of time it will take to restore a downed service by setting a target or goal for recovery. RTO can vary depending on the criticality and priority of the service.References: https://www.comptia.org/training/resources/exam- objectives/comptia-server-sk0-005-exam-objectives (Objective 3.3)

NEW QUESTION: 180
A server in a remote datacenter is no longer responsive. Which of the following is the BEST solution to investigate this failure?
A. Remote desktop
B. Access via a crash cart

C. Out-of-band management
D. A Secure Shell connection
Answer: C (LEAVE A REPLY)
The best solution to investigate the failure of a server in a remote datacenter is out-of-band management. Out-of-band management is a method of accessing and controlling a server or a device using a dedicated channel that is separate from its normal network connection. Out-of-band management can use various technologies, such as serial ports, modems, KVM switches, or dedicated management cards or interfaces. Out-of-band management can provide remote access to servers or devices even when they are powered off, unresponsive, or disconnected from the network. Out-of-band management can enable troubleshooting, configuration, maintenance, or recovery tasks without requiring physical presence at the server location.
Reference:
https://www.lantronix.com/wp-content/uploads/pdf/Data_Center_Mgmt_WP.pdf

NEW QUESTION: 181
A technician is connecting a server's secondary NIC to a separate network. The technician connects the cable to the switch but then does not see any link lights on the NIC. The technician confirms there is nothing wrong on the network or with the physical connection. Which of the following should the technician perform NEXT?
A. Restart the server
B. Configure the network on the server
C. Enable the port on the server
D. Check the DHCP configuration
Answer: C (LEAVE A REPLY)
The next thing that the technician should perform is to enable the port on the server. A port is a logical endpoint that identifies a specific service or application on a network device. A port can be enabled or disabled depending on whether the service or application is running or not. If a port is disabled on a server, it means that the server cannot send or receive any network traffic on that port, which can prevent communication with other devices or services that use that port. In this case, if port 389 is disabled on the server, it means that the server cannot use LDAP to access or modify directory services over a network. To resolve this issue, the technician should enable port 389 on the server using commands such as netsh or iptables.

NEW QUESTION: 182
After the installation of an additional network card into a server, the server will not boot into the OS. A technician tests the network card in a different server with a different OS and verifies the card functions correctly. Which of the following should the technician do NEXT to troubleshoot this issue?
A. Remove the original network card and attempt to boot using only the new network card.
B. Check that the BIOS is configured to recognize the second network card.
C. Ensure the server has enough RAM to run a second network card.
D. Verify the network card is on the HCL for the OS.
Answer: (SHOW ANSWER)

The HCL stands for Hardware Compatibility List and it is a list of hardware devices that are tested and certified to work with a specific operating system. If a network card is not on the HCL for the OS, it may not function properly or cause compatibility issues. Therefore, verifying the network card is on the HCL for the OS should be the next step to troubleshoot this issue.References: https://www.comptia.org/training/resources /exam-objectives/comptia-server-sk0-005-exam-objectives (Objective 4.1)

NEW QUESTION: 183
An administrator is troubleshooting performance issues on a server that was recently upgraded. The administrator met with users/stakeholders and documented recent changes in an effort to determine whether the server is better or worse since the changes. Which of the following would BEST help answer the server performance question9
A. Server performance thresholds
B. A server baseline
C. A hardware compatibility list
D. An application service-level agreement
Answer: B (LEAVE A REPLY)
A server baseline is a set of metrics that represents the normal performance and behavior of a server under a specific workload and configuration. A server baseline can help answer the server performance question by comparing the current performance with the previous performance before the upgrade. This can help identify any changes or issues that may have affected the server performance.References: https://www.comptia.org /training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives (Objective 4.2)

NEW QUESTION: 184
An administrator is troubleshooting a server that is rebooting and crashing. The administrator notices that the server is making sounds that are louder than usual. Upon closer inspection, the administrator discovers that the noises are coming from the front of the chassis. Which of the following is the most likely reason for this behavior?
A. One of the fans has failed.
B. The power supply has failed.
C. The RAM is malfunctioning.
D. The CPU is overheating.
Answer: A (LEAVE A REPLY)
A server has multiple fans inside the chassis to cool down the components and prevent overheating. If one of the fans fails, it can cause the server to reboot and crash due to thermal issues. A failed fan can also make loud noises due to friction or vibration. The administrator should check the fans and clean them from dust and debris, or replace them if they are damaged12.
References = 1: It's Too Loud! 3 Solutions to Remedy Server Noise - Computerware Blog | DC Metro | Computerware Blog(https://www.cwit.com/blog/it-s-too-loud-3-solutions-to-remedy-server-noise) 2: What factors affect the noise level of a server? - Server Fault(https://serverfault.com/questions/430550/what-factors-affect-the-noise-level-of-a-server)

NEW QUESTION: 185
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: (SHOW ANSWER)

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 dat a. 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: 186

A systems administrator deployed a new web proxy server onto the network. The proxy server has two interfaces: the first is connected to an internal corporate firewall, and the second is connected to an internet- facing firewall. Many users at the company are reporting they are unable to access the Internet since the new proxy was introduced. Analyze the network diagram and the proxy server's host routing table to resolve the Internet connectivity issues.

INSTRUCTIONS

Perform the following steps:

1. Click on the proxy server to display its routing table.
2. Modify the appropriate route entries to resolve the Internet connectivity issue.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Proxy Server Routing Table

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

Answer:

Proxy Server Routing Table

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

Explanation:

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

NEW QUESTION: 187

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

A. The server has an architecture mismatch

B. The system time is not synchronized

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

NEW QUESTION: 188
A systems engineer is configuring a new VLAN for expansion of a campus network. The engineer configures a new DHCP scope on the existing Windows DHCP server cluster and activates the scope for the clients.
However, new clients in the area report they are not receiving any DHCP address information. Which of the following should the engineer do first?
A. Confirm the client PCs are using the correct speed on the NIC
B. Confirm the network uses the same NTP server as the clients
C. Confirm the network has a helper address for the DHCP server
D. Confirm the DHCP server is authorized in Active Directory
Answer: C (LEAVE A REPLY)
When clients on a different VLAN cannot receive DHCP addresses, it's often because there is noDHCP helper addressconfigured on the router or switch. ADHCP relay/helper addressforwards DHCP requests from clients on the VLAN to the DHCP server, which may reside on a different network.
* Confirming the network has a helper address (Answer C):This should be the first step to ensure that DHCP requests from the VLAN are correctly routed to the DHCP server.
* Checking client NIC speed (Option A):While important, incorrect NIC speed wouldn't affect the ability to obtain an IP address from DHCP.
* Checking NTP server (Option B):Time synchronization is unrelated to DHCP issues.
* Authorizing the DHCP server (Option D):This is essential for DHCP operation, but since this is an existing DHCP cluster, the helper address is more likely the issue.
CompTIA Server+ Reference:This topic is related toSK0-005 Objective 1.2: Manage server network connections.

NEW QUESTION: 189
Which of the following would a systems administrator most likely implement to encrypt data in transit for remote administration?
A. Telnet
B. SSH
C. TFTP
D. rlogin
Answer: B (LEAVE A REPLY)

SSH (Secure Shell) is a protocol that would most likely be implemented to encrypt data in transit for remote administration. SSH provides secure communication between two devices over an unsecured network by using public-key cryptography and symmetric encryption. SSH can be used to remotely execute commands, transfer files, or tunnel other protocols. Telnet, TFTP, and rlogin are protocols that do not encrypt data in transit and are considered insecure for remote administration. References: [CompTIA Server+ Certification Exam Objectives], Domain 2.0: Networking, Objective 2.4: Given a scenario involving network security
/access methods, implement an appropriate solution.

NEW QUESTION: 190
Which of the following licensing concepts is based on the number of logical processors a server has?
A. Per core
B. Per socket
C. Per instance
D. Per server
Answer: A (LEAVE A REPLY)
Per core licensing is based on the number of logical processors a server has. A logical processor is either a physical core or a virtual core created by hyperthreading. Per core licensing requires purchasing a license for each logical processor on the server. Verified References: [Per core licensing], [Logical processor]

NEW QUESTION: 191
A technician has moved a data drive from a new Windows server to an older Windows server. The hardware recognizes the drive, but the data is not visible to the OS. Which of the following is the most likely cause of the issue?
A. The disk uses GPT.
B. The partition is formatted with ext4.
C. The partition is formatted with FAT32.
D. The disk uses MBR.
Answer: A (LEAVE A REPLY)
The most likely cause of the issue is that the disk uses GPT. GPT stands for GUID Partition Table, which is a newer standard for disk partitioning that supports larger disks and more partitions than the older MBR (Master Boot Record) standard1. However, GPT is not compatible with some older operating systems, such as Windows XP or Windows Server 20032. Therefore, if the data drive was formatted with GPT on a new Windows server and then moved to an older Windows server, the older server may not be able to recognize the GPT partitions and access the data on the drive.
The partition being formatted with ext4, FAT32, or MBR are not likely causes of the issue. Ext4 is a file system that is commonly used on Linux-based systems, but it can also be read by Windows with some third-party software3. FAT32 is a file system that is widely compatible with most operating systems and devices, but it has some limitations such as a maximum file size of 4 GB and a maximum partition size of 8 TB4. MBR is not a file system, but a partitioning scheme that can support various file systems such as NTFS, FAT32, or exFAT5. However, MBR has some disadvantages compared to GPT, such as a maximum disk size of 2 TB and a maximum number of primary partitions of four1.

NEW QUESTION: 192
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: (SHOW ANSWER)
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: 193
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 (LEAVE A REPLY)
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: 194
Multiple users have reported an issue accessing files on a specific server. Which of the following should be the first step in troubleshooting this issue?
A. Notify the key stakeholders of an outage.
B. Immediately execute a backup of the server.
C. Identify changes made to the environment.
D. Correct the permissions on the folder containing the files.
Answer: C (LEAVE A REPLY)
Comprehensive Detailed Explanation with all CompTIA Server+ SK0-005 Study Guide References:When troubleshooting server access issues, identifying recent changes to the environment is critical. Changes such as updates, patches, configuration modifications, or network adjustments could be the root cause of the issue.
This aligns with the best practices of the ITIL framework and troubleshooting methodologies outlined in the CompTIA Server+ study materials:
* Step 1: Gather information and identify the scope of the problem.
* Step 2: Look for recent changes to identify potential triggers.This approach ensures that corrective actions are based on an understanding of what caused the problem, avoiding unnecessary disruptions or incorrect fixes.

NEW QUESTION: 195
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 (LEAVE A REPLY)
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]