CompTIA.SK0-005.v2025-07-24.q192

Exam Code:	SK0-005
Exam Name:	CompTIA Server+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	192
Version:	v2025-07-24
# of views:	1011
# of Questions views:	5534
https://www.dumpsfiles.com/files/CompTIA/SK0-005/CompTIA.SK0-005.v2025-07-24.q192	

NEW QUESTION: 1
Which of the following BEST measures now much downtime an organization can tolerate Curing an unplanned outage?
A. SLA
B. BIA
C. RTO
D. MTTR
Answer: C (LEAVE A REPLY)
RTO (Recovery Time Objective) is a measure of how much downtime an organization can tolerate during an unplanned outage. It is the maximum time allowed for restoring normal operations after a disaster. RTO is one of the key metrics for disaster recovery planning and testing. SLA (Service Level Agreement) is a contract that defines the expected level of service and performance between a provider and a customer. BIA (Business Impact Analysis) is a process that identifies and evaluates the potential effects of a disaster on critical business functions and processes. MTTR (Mean Time To Repair) is a measure of how long it takes to fix a failed component or system. References: https://parachute.cloud/rto-vs-rpo/ https://www.techopedia.com /definition/13622/service-level-agreement-sla https://www.techopedia.com/definition/1032/business-impact- analysis-biahttps://www.techopedia.com/definition/8239/mean-time-to-repair-mttr

NEW QUESTION: 2
A company's servers are all displaying the wrong time. The server administrator confirms the time source is correct. Which of the following is MOST likely preventing the servers from obtaining the correct time?
A. A firewall
B. An antivirus
C. AHIDS
D. User account control

Answer: A (LEAVE A REPLY)
The most likely cause of the servers displaying the wrong time is A. A firewall. A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predefined rules. A firewall can block or allow certain ports, protocols, or applications that are used for network communication.
One of the protocols that is used for time synchronization is the Network Time Protocol (NTP), which requires the use of UDP port 123 for all time synchronization1. If a firewall blocks this port, it can prevent the servers from obtaining the correct time from the time source. Therefore, the server administrator should check the firewall settings and make sure that UDP port 123 is allowed for NTP traffic.

NEW QUESTION: 3
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: E,F (LEAVE A REPLY)
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: 4
Which of the following describes the installation of an OS contained entirely within another OS installation?
A. Host
B. Bridge
C. Hypervisor
D. Guest
Answer: (SHOW ANSWER)
The installation of an OS contained entirely within another OS installation is described as a guest. A guest is a term that refers to a virtual machine (VM) that runs on top of a host operating system (OS)

using a hypervisor or a virtualization software. A guest can have a different OS than the host, and can run multiple applications or services independently from the host. A guest can also be isolated from the host and other guests for security or testing purposes.

NEW QUESTION: 5
A company uses a hot-site, disaster-recovery model. Which of the following types of data replication is required?
A. Asynchronous
B. Incremental
C. Application consistent
D. Constant
Answer: D (LEAVE A REPLY)
The type of data replication that is required for a hot-site disaster recovery model is constant. A hot site is a type of disaster recovery site that has fully operational IT infrastructure and equipment that can take over the primary site's functions immediately in case of a disaster or disruption. A hot site requires constant data replication between the primary site and the hot site to ensure that the data is up-to-date and consistent.
Constant data replication means that any changes made to the data at the primary site are immediately copied to the hot site without any delay or lag.

NEW QUESTION: 6
A server administrator created a new script and included the path to the script binary as the first line of the script. Which of the following scripting languages did the administrator most likely use?
A. Batch
B. Java
C. Bash
D. PowerShell
Answer: C (LEAVE A REPLY)
In Bash (a Unix/Linux shell scripting language), it is common to include the shebang (#!) followed by the path to the interpreter (e.g., #!/bin/bash) on the first line of the script. This tells the operating system which interpreter to use to execute the script.
* Bash (Answer C): Bash scripts often start with a shebang line that specifies the path to the binary (#! /bin/bash).
* Batch (Option A): Batch scripts (used in Windows) do not require a path to the interpreter on the first line.
* Java (Option B): Java is a compiled language, not a scripting language, so this does not apply.
* PowerShell (Option D): PowerShell scripts (.ps1 files) do not typically require specifying the interpreter path on the first line.
CompTIA Server+ Reference:This topic is related to SK0-005 Objective 1.1: Understand scripting basics and the use of interpreters.

NEW QUESTION: 7
A technician replaces a single faulted disk in the following array RAID 10, Four 15K SAS HDD The technician replaces it from a disk in spare parts, and the array rebuilds the data in a few minutes. After the array rebuild is complete, the system reports the IOPS on the disk array have dropped by almost 60% Which of the following should the technician investigate first?
A. Check the RAID controller (or background rebuild tasks
B. Check the firmware version on the newly replaced disk.
C. Check the RPM speed on the newly replaced disk-
D. Check the cache settings on the RAID controller.
Answer: C (LEAVE A REPLY)
In RAID 10 arrays, disk performance is crucial, especially if they are high-speed 15K RPM SAS HDDs, as each disk in the array is part of a mirrored pair that also stripes data with another pair. When replacing a disk, it's essential that the new disk matches the specifications of the others, especially in terms of rotational speed (RPM). If the replaced disk is slower, it can significantly reduce the Input/Output operations per second (IOPS) of the entire array. This is because all disks need to work in tandem, and the slowest disk can become a bottleneck. Thus, checking the RPM of the newly replaced disk is a sensible first step to ensure it matches the performance of the other disks in the array.

NEW QUESTION: 8
A security analyst suspects a remote server is running vulnerable network applications. The analyst does not have administrative credentials for the server. Which of the following would MOST likely help the analyst determine if the applications are running?
A. User account control
B. Anti-malware
C. A sniffer
D. A port scanner
Answer: (SHOW ANSWER)
A port scanner is the tool that would most likely help the analyst determine if the applications are running on a remote server. A port scanner is a software tool that scans a network device for open ports. Ports are logical endpoints for network communication that are associated with specific applications or services. By scanning the ports on a remote server, the analyst can identify what applications or services are running on that server and what protocols they are using. A port scanner can also help detect potential vulnerabilities or misconfigurations on a server.

NEW QUESTION: 9
Which of the following asset management documents is used to identify the location of a serves within a data center?
A. Infrastructure diagram
B. Workflow diagram
C. Rack layout

D. Service manual

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 10

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

A. Disable the heartbeat network.

B. Fallback cluster services.

C. Set the cluster to active-active.

D. Failover all VMs.

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 11

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: 12
Alter rack mounting a server, a technician must install four network cables and two power cables for the server. Which of the following is the MOST appropriate way to complete this task?
A. Wire the four network cables and the two power cables through the cable management arm using appropriate-length cables.
B. Run the tour network cables up the left side of the rack to the top of the rack switch. Run the two power cables down the right side of the rack toward the UPS.
C. Use the longest cables possible to allow for adjustment of the server rail within the rack.
D. Install an Ethernet patch panel and a PDU to accommodate the network and power cables.
Answer: (SHOW ANSWER)
This is the most appropriate way to complete the task because it follows the best practices of cable management. Cable management is a process of organizing and securing cables in a rack or a server room to improve airflow, accessibility, safety, and aesthetics. Running the network cables up the left side and the power cables down the right side of the rack helps to avoid cable clutter, interference, and confusion. It also makes it easier to trace and troubleshoot cables if needed. Using appropriate-length cables also helps to reduce cable slack and excess. Wiring the cables through the cable management arm may cause stress and damage to the cables when moving the server in or out of the rack. Using the longest cables possible may create cable loops and tangles that can block airflow and increase fire hazards. Installing an Ethernet patch panel and a PDU (Power Distribution Unit) may be useful for accommodating more network and power cables, but not necessary for a single server. References: https://www.howtogeek.com/303282/how-to-manage-your-pcs-fans-for-optimal-airflow-and-cooling/ https://www.howtogeek.com/303290/how-to-properly-manage-your-cables/

NEW QUESTION: 13
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: (SHOW ANSWER)
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: 14
A company stores extremely sensitive data on an alt-gapped system. Which of the following can Be Implemented to increase security against a potential insider threat?
A. Two-person Integrity
B. SSO
C. SIEM
D. Faraday cage
E. MFA
Answer: A (LEAVE A REPLY)
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: 15
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: 16
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: 17
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: (SHOW ANSWER)
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: 18
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: (SHOW ANSWER)
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: 19
Corporate policy mandates that logs from all servers be available for review regardless of the state of the server. Which of the following must be configured to comply with this policy?
A. Aggregation
B. Subscription
C. Merging
D. Collection
Answer: A (LEAVE A REPLY)
Aggregation is the process of collecting, standardizing, and consolidating log data from multiple sources into a central location. Aggregation makes it easier to search, analyze, and report on log data, as well as to comply with security policies and regulations. By aggregating logs from all servers, regardless of their state, the corporate policy can ensure that no log data is lost or inaccessible in case of a server failure or outage

NEW QUESTION: 20
A server administrator set up a monitoring application on various servers to keep track of CPU usage, memory consumption, and disk space utilization. Which of the following should be configured on the application so it can send email alerts about a specific issue?
A. Event logs
B. Thresholds
C. Disk quotas
D. Uptime lengths
Answer: B (LEAVE A REPLY)
Comprehensive Detailed Explanation with all CompTIA Server+ SK0-005 Study Guide References:
Configuring thresholds allows the monitoring application to define limits (e.g., CPU usage > 90%, disk space
< 10%) that trigger email alerts when exceeded. This proactive measure helps administrators address issues before they escalate.
* Event logs: Provide historical data but do not send alerts.
* Disk quotas: Restrict user disk usage but are unrelated to alerts.
* Uptime lengths: Measure server runtime but do not trigger alerts.

NEW QUESTION: 21
Users in an office lost access to a file server following a short power outage. The server administrator noticed the server was powered off. Which of the following should the administrator do to prevent this situation in the future?

A. Connect the server to a KVM
B. Use cable management
C. Connect the server to a redundant network
D. Connect the server to a UPS
Answer: D (LEAVE A REPLY)
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: 22
An administrator receives an alert that one of the virtual servers has suddenly crashed. The administrator confirms the data center does not have any power failures and then connects to the remote console of the crashed server After connecting to the server console, which of the following should the administrator complete first?
A. Use the keyboard command AH+F12 to switch to the kernel log screen
B. Perform a hard reboot on the server and monitor the server startup
C. Collect a screenshot of the PSOD and note the details after the line detailing the OS version
D. Collect a core dump from the server and store locally before rebooting the hardware
Answer: C (LEAVE A REPLY)
When a virtual server crashes and presents a Purple Screen of Death (PSOD), the immediate response should be to document the incident. Collecting a screenshot of the PSOD is crucial as it contains error codes and state information that can be used for diagnosing the root cause of the crash. Noting the details, especially those that come after the line detailing the OS version, can provide specific clues to what might have caused the server to crash. This is a standard best practice before rebooting the server, as it ensures that there is a record of the event to investigate and potentially prevent future occurrences. A hard reboot should only be done after this critical information has been recorded.

NEW QUESTION: 23
A server administrator is completing an OS installation for a new server. The administrator patches the server with the latest vendor-suggested software, configures DHCP, and verifies all network cables are properly connected in the IDF, but there is no network connectivity. Which of the following is the MOST likely reason for the lack of connectivity?
A. The VLAN Is improperly configured.
B. The DNS configuration Is invalid.
C. The OS version is not compatible with the network switch vendor.
D. The HIDS is preventing the connection.

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

NEW QUESTION: 24
A company needs a media server set up that provides the highest availability with a minimum requirement of at least 10TB. The company purchased five HDDs, each with a 4TB capacity. Which of the options would provide the highest fault tolerance and meet the requirements?
A. RAID 0
B. RAID 5
C. RAID 6
D. RAID 10
Answer: C (LEAVE A REPLY)
RAID 6 is a RAID level that uses disk striping with two parity blocks distributed across all member disks. It can tolerate the failure of up to two disks without losing any data. RAID 6 can provide a minimum of 10TB of usable storage space with five 4TB disks, as the formula for calculating the RAID 6 capacity is (n-2) x Smin, where n is the number of disks and Smin is the smallest disk size. In this case, the RAID 6 capacity is (5-2) x
4TB = 12TB.
References:
* CompTIA Server+ Certification Exam Objectives1, page 8
* RAID Levels and Types Explained: Advantages and Disadvantages2
* RAID Levels & Fault Tolerance3

NEW QUESTION: 25

A technician needs to set up a server backup method for some systems. The company's management team wants to have quick restores but minimize the amount of backup media required. Which of the following are the BEST backup methods to use to support the management's priorities? (Choose two.)

A. Differential

B. Synthetic full

C. Archive

D. Full

E. Incremental

F. Open file

Answer: A,E (LEAVE A REPLY)

The best backup methods to use to support the management's priorities are differential and incremental. A backup is a process of copying data from a source to a destination for the purpose of restoring it in case of data loss or corruption. There are different types of backup methods that vary in terms of speed, efficiency, and storage requirements. Differential and incremental backups are two types of partial backups that only copy the data that has changed since the last full backup. A full backup is a type of backup that copies all the data from the source to the destination. A full backup provides the most complete and reliable restore option, but it also takes the longest time and requires the most storage space. A differential backup copies only the data that has changed since the last full backup. A differential backup provides a faster restore option than an incremental backup, but it also takes more time and requires more storage space than an incremental backup.

An incremental backup copies only the data that has changed since the last backup, whether it was a full or an incremental backup. An incremental backup provides the fastest and most efficient backup option, but it also requires multiple backups to restore the data completely.

NEW QUESTION: 26

A data center has 4U rack servers that need to be replaced using VMs but without losing any data. Which of the following methods will MOST likely be used to replace these servers?

A. Unattended scripted OS installation

B. P2V

C. VM cloning

Answer: (SHOW ANSWER)

P2V (Physical to Virtual) is a method of converting a physical server into a virtual machine that can run on a hypervisor. This method can be used to replace 4U rack servers with VMs without losing any data, as it preserves the configuration and state of the original server. P2V can also reduce hardware costs, power consumption, and space requirements. Verified References: [What is P2V?]

NEW QUESTION: 27

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: 28
A server administrator is swapping out the GPU card inside a server. Which of the following actions should the administrator take FIRST?
A. Inspect the GPU that is being installed.
B. Ensure the GPU meets HCL guidelines.
C. Shut down the server.
D. Disconnect the power from the rack.
Answer: C (LEAVE A REPLY)
The first action that the administrator should take before swapping out the GPU card inside a server is to shut down the server. This is to ensure that the server is not running any processes that might be using the GPU card, and to prevent any damage to the hardware or data loss due to sudden power loss. Shutting down the server also reduces the risk of electrostatic discharge (ESD) that might harm the components. Reference:
https://pcgearhead.com/installing-a-new-gpu/

NEW QUESTION: 29
A systems administrator is setting up a server farm for a new company. The company has a public range of IP addresses and uses the addresses internally. Which of the following IP addresses best fits this scenario?
A. 10.3.7.27
B. 127.0.0.1
C. 192.168.7.1
D. 216,176,128.10
Answer: D (LEAVE A REPLY)
The IP address that best fits this scenario is 216.176.128.10. This is a public IP address that belongs to a range of addresses that are assigned and registered by an Internet service provider (ISP) and can be accessed from anywhere on the Internet. The company has a public range of IP addresses and uses them internally, which means that they do not use private IP addresses or network address translation (NAT) to communicate within their network.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 2, Lesson 2.2, Objective 2.2

NEW QUESTION: 30
A server administrator needs to ensure all Window-based servers within a data center have RDP disabled.
There are thousands of servers performing various roles. Which of the following is the best way to meet this requirement?
A. Run chkconfig --1eve1 345 RDP off.
B. Create a PowerShell script to disable the RDP service.
C. Run chkconfig -- list RDP.
D. Create a Bash shell script to disable the Windows Remote Management service.
E. Create a GPO to disable the Windows Remote Management service.
Answer: B (LEAVE A REPLY)
The best way to meet this requirement is to create a PowerShell script to disable the RDP service on all Windows-based servers within a data center. PowerShell is a scripting language and command-line tool that can be used to automate tasks and manage Windows systems remotely. A PowerShell script can use cmdlets (commands) and parameters to perform actions on multiple servers at once, such as disabling a service or changing a configuration setting. RDP (Remote Desktop Protocol) is a service that allows remote access and control of a Windows system through a graphical user interface. Disabling RDP can improve security by preventing unauthorized or malicious access to the servers.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 4, Lesson 4.3, Objective 4.3; Chapter 7, Lesson 7.1, Objective 7.1

NEW QUESTION: 31
An administrator gave Ann modify permissions to a shared folder called DATA, which is located on the company server. Other users need read access to the files in this folder. The current configuration is as follows:
The administrator has determined Ann cannot write anything to the DATA folder using the network. Which of the following would be the best practice to set up Ann's permissions correctly, exposing only the minimum rights required?
A. Option A
B. Option B
C. Option C
D. Option D
Answer: D (LEAVE A REPLY)
Option D is the best practice to set up Ann's permissions correctly, exposing only the minimum rights required. Option D shows that the share permissions on the DATA folder grant Ann Change access, which allows her to read, write, and delete files in the shared folder. The file permissions grant Ann Modify access, which allows her to read, write, execute, and delete files in the folder. This combination of permissions gives Ann the ability to write anything to the DATA folder using the network, as well as to modify and delete existing files. This meets the requirement of giving Ann modify permissions to the shared folder.

NEW QUESTION: 32
A human resources analyst is attempting to email the records for new employees to an outside payroll company. Each time the analyst sends an email containing employee records, the email is rejected with an error message. Other emails outside the company are sent correctly. Which of the following is MOST likely generating the error?
A. DHCP configuration
B. Firewall rules
C. DLP software
D. Intrusion detection system
Answer: C (LEAVE A REPLY)
DLP (Data Loss Prevention) software is a type of security software that monitors and controls the transfer of sensitive or confidential data outside the organization. DLP software can prevent data breaches, data leaks, or data theft by blocking, encrypting, or alerting on unauthorized data transfers. DLP software can be applied to various channels, such as email, web, cloud, or removable devices. In this scenario, the human resources analyst is attempting to email the records for new employees to an outside payroll company. The records for new employees may contain sensitive or confidential data, such as personal information, tax information, or bank account information. The DLP software may detect this data and block the email from being sent outside the company, as it may violate the company's data protection policy or regulations. The DLP software may also generate an error message to inform the analyst of the reason for the rejection.

NEW QUESTION: 33
Which of the following licensing models was created by software companies in response to the increasing density of processors?
A. Per-instance
B. Per-server
C. per-user
D. per-core
Answer: (SHOW ANSWER)
The correct answer is D. per-core.

The per-core licensing model was created by software companies in response to the increasing density of processors. This model is used for software that runs on servers with multi-core processors, and the licensing fee is based on the number of cores. This way, the software vendors can charge more for software that runs on servers with more processing power1

NEW QUESTION: 34
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: (SHOW ANSWER)
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: 35
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: 36
A server technician is installing a Windows server OS on a physical server. The specifications for the installation call for a 4TB data volume. To ensure the partition is available to the OS, the technician must verify the:
A. hardware is UEFI compliant
B. volume is formatted as GPT
C. volume is formatted as MBR
D. volume is spanned across multiple physical disk drives
Answer: (SHOW ANSWER)
To ensure the partition is available to the OS, the technician must verify that the volume is formatted as GPT.
GPT (GUID Partition Table) is a partitioning scheme that defines how data is organized on a hard disk drive (HDD) or a solid state drive (SSD). GPT uses globally unique identifiers (GUIDs) to identify partitions and supports up to 128 primary partitions per disk. GPT also supports disks larger than 2 TB and has a backup copy of the partition table at the end of the disk for data recovery. GPT is required for installing Windows on UEFI-based PCs, which offer faster boot time and better security than legacy BIOS-based PCs.

NEW QUESTION: 37
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: 38
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: 39
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: (SHOW ANSWER)

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: 40
Users have noticed a server is performing below Baseline expectations. While diagnosing me server, an administrator discovers disk drive performance has degraded. The administrator checks the diagnostics on the RAID controller and sees the battery on me controller has gone bad. Which of the following is causing the poor performance on the RAID array?
A. The controller has disabled the write cache.
B. The controller cannot use all the available channels.
C. The drive array is corrupt.
D. The controller has lost its configuration.
Answer: A (LEAVE A REPLY)
The write cache is a feature of some RAID controllers that allows them to temporarily store data in a fast memory buffer before writing it to the disk drives. This improves the performance and efficiency of write operations, especially for random and small writes. However, if the battery on the controller goes bad, the controller may disable the write cache to prevent data loss in case of a power failure. This can degrade the disk drive performance significantly, as every write operation will have to wait for the disk drives to complete. References: https://www.dell.com/support/kbdoc/en-us/000131486/understanding-raid-controller- battery-learn-cyclehttps://www.techrepublic.com/article/understanding-raid-controller-write-cache/

NEW QUESTION: 41
An administrator is alerted to a hardware failure in a mission-critical server. The alert states that two drives have failed. The administrator notes the drives are in different RAID 1 arrays, and both are hot-swappable.
Which of the following steps will be the MOST efficient?
A. Replace one drive, wait for a rebuild, and replace the next drive.
B. Shut down the server and replace the drives.
C. Replace both failed drives at the same time.
D. Replace all the drives in both degraded arrays.
Answer: C (LEAVE A REPLY)
Since both drives are in different RAID 1 arrays and both are hot-swappable, the most efficient step is to replace both failed drives at the same time. This can minimize the downtime and avoid unnecessary reboots.

RAID 1 provides mirroring, which means that data is duplicated on both drives in the array. Therefore, replacing one drive will not affect the data on the other drive or the functionality of the array.
References:
https://en.wikipedia.org/wiki/Standard_RAID_levels#RAID_1

NEW QUESTION: 42
An organization implements split encryption keys for sensitive files. Which of the following types of risks does this mitigate?
A. Hardware failure
B. Marware
C. Data corruption
D. Insider threat
Answer: (SHOW ANSWER)
An insider threat is a type of risk that can be mitigated by implementing split encryption keys for sensitive files. An insider threat is a malicious actor who has authorized access to an organization's system or data and uses it for unauthorized or harmful purposes. An insider threat can cause data breaches, sabotage, fraud, theft, espionage, or other damages to the organization. Split encryption keys are a method of encrypting data using multiple keys that are stored separately and require collaboration to decrypt. Split encryption keys can prevent an insider threat from accessing or compromising sensitive data without being detected by another authorized party who holds another key. Hardware failure is a type of risk that involves physical damage or malfunction of hardware components such as hard drives, memory modules, power supplies, or fans. Hardware failure can cause data loss, system downtime, performance issues, or other problems for the organization. Hardware failure cannot be mitigated by split encryption keys, but by backup, redundancy, monitoring, and maintenance measures.

NEW QUESTION: 43
Users report they ate unable to access an application after a recent third-party patch update. The physical server that is hosting the application keeps crashing on reboot. Although the update was installed directly from the manufacturer's support website as recommended it has now been recalled and removed from the website as the update unintentionally installed unauthorized software after a reboot. Which of the following steps should the administrator perform to restore access to the application while minimizing downtime?
(Select TWO)
A. Uninstall recent updates.
B. Reimage the server with a different OS.
C. Run a port scan to verify open ports.
D. Enable a GPO to uninstall the update.
E. Scan and remove any malware.
F. Reformat the server and restore the image from the latest backup.
Answer: E,F (LEAVE A REPLY)

The most likely cause of the server crashing and the application being inaccessible is that the unauthorized software installed by the update is malware that corrupted the system files or compromised the security of the server. To restore access to the application while minimizing downtime, the administrator should scan and remove any malware from the server, and then reformat the server and restore the image from the latest back- up. This will ensure that the server is clean and has a working configuration of the application. Verified References: [How to Remove Malware from a Server]

NEW QUESTION: 44
A server administrator needs to configure a server on a network that will have no more than 30 available IP addresses. Which of the following subnet addresses will be the MOST efficient for this network?
A. 255.255.255.0
B. 255.255.255.128
C. 255.255.255.224
D. 255.255.255.252
Answer: (SHOW ANSWER)
The most efficient subnet address for a network that will have no more than 30 available IP addresses is
255.255.255.224. This subnet mask corresponds to a /27 prefix length, which means that 27 bits are used for the network portion and 5 bits are used for the host portion of an IP address. With 5 bits for hosts, there are
2^5 - 2 = 30 possible host addresses per subnet, which meets the requirement. The other options are either too large or too small for the network size. Reference: https://www.ibm.com/cloud/learn/subnet-mask

NEW QUESTION: 45
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: 46
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: (SHOW ANSWER)
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: 47
An administrator is working on improving the security of a new domain controller. A report indicates several open ports on the server. Which of the following ports should the administrator disable?
A. 135
B. 636
C. 3268
D. 3389
Answer: D (LEAVE A REPLY)

The port that should be disabled on the firewall is port 3389. Port 3389 is used by Remote Desktop Protocol (RDP), which is a protocol that allows remote access and control of a Windows system through a graphical user interface. RDP can pose a security risk if it is not properly configured or secured, as it can expose the system to unauthorized or malicious access from external sources. Therefore, port 3389 should be disabled on the firewall unless it is needed for legitimate purposes. References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.3, Objective 3.3

NEW QUESTION: 48
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: (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. 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: 49
Which of the following refers to the requirements that dictate when to delete data backups?
A. Retention policies.
B. Cloud security impact
C. Off-site storage
D. Life-cycle management
Answer: A (LEAVE A REPLY)
Retention policies are the guidelines that dictate when to delete data backups based on operational or compliance needs. They specify how long, how, where, and in what format the data backups are stored, and who has authority over them. The other options are not directly related to the deletion of data backups.
https://backup.ninja/news/Database-Backups-101-Backup-Retention-Policy-Considerations

NEW QUESTION: 50
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: 51
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: 52
A server technician is deploying a server with eight hard drives. The server specifications call for a RAID configuration that can handle up to two drive failures but also allow for the least amount of drive space lost to RAID overhead. Which of the following RAID levels should the technician configure for this drive array?
A. RAID 0
B. RAID 5
C. RAID 6
D. RAID 10
Answer: C (LEAVE A REPLY)
The technician should configure RAID 6 for this drive array to meet the server specifications. RAID 6 is a type of RAID level that provides fault tolerance and performance enhancement by using striping and dual parity. Striping means dividing data into blocks and distributing them across multiple disks to increase speed and capacity. Parity means calculating and storing extra information that can be used to reconstruct data in case of disk failure. RAID 6 uses two sets of parity information for each stripe, which are stored on different disks. This way, RAID 6 can handle up to two disk failures without losing any data or functionality. RAID 6 also allows for the least amount of drive space lost to RAID

overhead compared to other RAID levels that can handle two disk failures, such as RAID 1+0 or RAID 0+1.
Reference:
https://www.booleanworld.com/raid-levels-explained/

NEW QUESTION: 53
An administrator restores several database files without error while participating in a mock disaster recovery exercise. Later, the administrator reports that the restored databases are corrupt and cannot be used. Which of the following would best describe what caused this issue?
A. The databases were not backed up to be application consistent.
B. The databases were asynchronously replicated
C. The databases were mirrored
D. The database files were locked during the restoration process.
Answer: A (LEAVE A REPLY)
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: 54
Which of the following should a server administrator use when writing a script with a function that needs to be run ten times?
A. Loop
B. Variable
C. Comparator
D. Conditional
Answer: A (LEAVE A REPLY)
Aloopis a programming construct used to repeat a block of code multiple times. In this case, if a function needs to run ten times, a loop (such as afor looporwhile loop) would be the appropriate choice.
* Loop (Answer A):This allows the function to be executed repeatedly without writing redundant code.
* Variable (Option B):A variable is used to store data, but it doesn't handle repetition.
* Comparator (Option C):Comparators are used to compare values, not for repeating code.
* Conditional (Option D):Conditionals (if, else) are used for decision-making, not repeating actions multiple times.

CompTIA Server+ Reference:This topic is related toSK0-005 Objective 1.1: Understand basic scripting and automation concepts.

NEW QUESTION: 55
A storage administrator is investigating an issue with a failed hard drive. A technician replaced the drive in the storage array; however, there is still an issue with the logical volume. Which of the following best describes the NEXT step that should be completed to restore the volume?
A. Initialize the volume
B. Format the volume
C. Replace the volume
D. Rebuild the volume
Answer: D (LEAVE A REPLY)
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: 56
An administrator connects a server to an external gigabit switch, but the server can only get a speed of
100Mbps. Which of the following is the most likely cause of this issue?
A. Defective network cable
B. Port security
C. Incorrect IP subnet
D. Wrong VLAN
Answer: A (LEAVE A REPLY)
Comprehensive Detailed Explanation with all CompTIA Server+ SK0-005 Study Guide References:The most likely cause of a speed mismatch (100Mbps instead of 1Gbps) is a defective or incompatible network cable. Gigabit Ethernet requires at least Cat5e or Cat6 cables; using older cables (e.g., Cat5) or damaged cables can limit speeds to 100Mbps.
* Port security and VLAN misconfiguration would typically prevent communication entirely, not reduce speed.
* Incorrect IP subnet does not affect link speed.Checking and replacing the network cable is a logical first troubleshooting step in this scenario.

NEW QUESTION: 57

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)

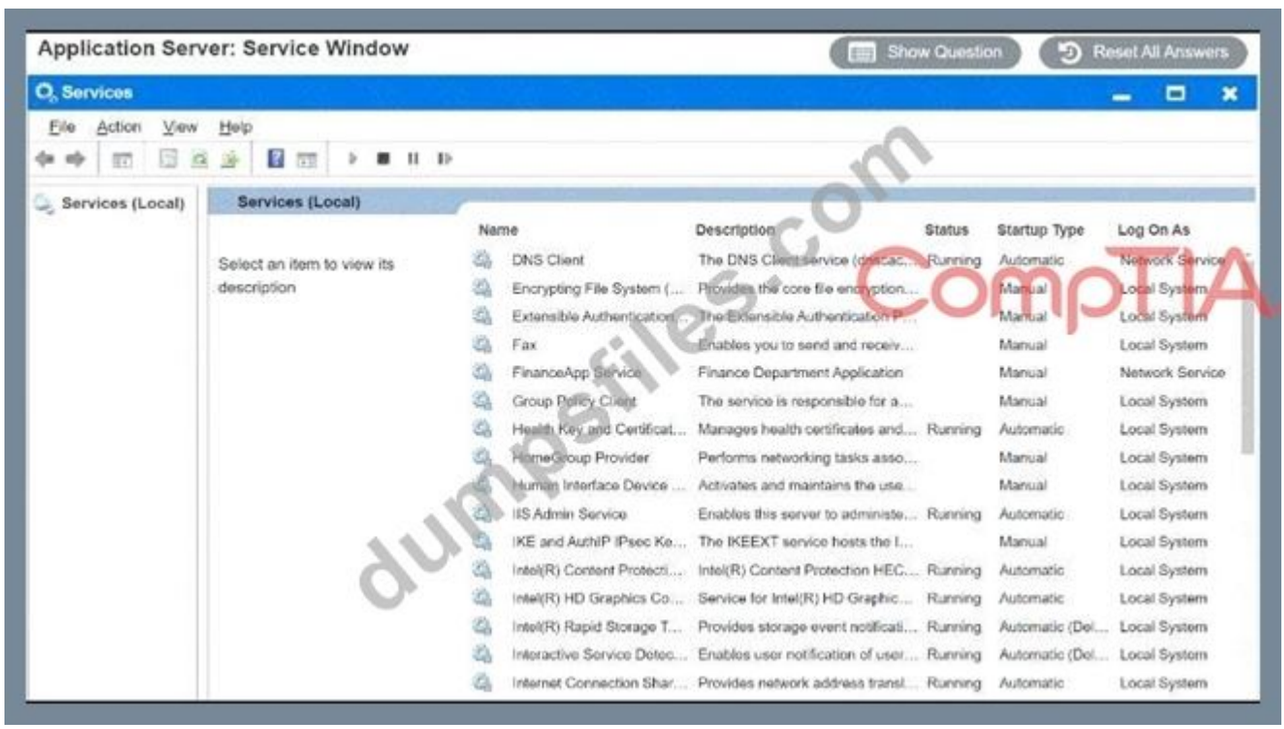
The most appropriate native protocol to use for connecting a Linux server to a share on a NAS is NFS. NFS (Network File System) is a protocol that allows file sharing and remote access over a network. NFS is designed for Unix-like operating systems, such as Linux, and supports features such as symbolic 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: 58

Users report that the FinanceApp software is not running, and they need immediate access. Issues with the FinanceApp software occur every week after the IT team completes server system updates. The users, however, do not want to contact the help desk every time the issue occurs. The users also report the new MarketApp software is not usable when it crashes, which can cause significant downtime. The technician who restarted the MarketApp software noticed it is running under a test account, which is a likely cause of the crashes.

INSTRUCTIONS

Using the Services menu provided, modify the appropriate application services to remedy the stated issues.



Answer:

FinanceApp software is running as a service named "FinanceApp Service". The service description says
"Provides financial data and calculations for the FinanceApp software". The service status is "Stopped", which means that the service is not running and the software is not functional. The service startup type is
"Manual", which means that the service needs to be started manually by the user or the administrator. The service log on as is "Local System", which means that the service runs under a predefined local account that has extensive privileges on the local computer.

To fix the issue with the FinanceApp software, you need to do two things:

* First, you need to start the service, so that the software can run. To do this, you can right-click on the service name and select "Start" from the menu. Alternatively, you can select the service name and click on the "Start" button on the toolbar. You should see a message saying that the service has started successfully.
* Second, you need to change the service startup type, so that the service can start automatically every time the server boots up. This way, you don't have to contact the help desk every time the issue occurs.

To do this, you can right-click on the service name and select "Properties" from the menu. Alternatively, you can select the service name and click on the "Properties" button on the toolbar. You should see a window with several tabs and options. On the "General" tab, under "Startup type", you can select "Automatic" from the drop-down list. Then, click on "OK" to save your changes.

By doing these two steps, you should be able to use the FinanceApp software without any problems.

The MarketApp software is running as a service named "MarketApp Service". The service description says
"Provides market data and analysis for the MarketApp software". The service status is "Running", which means that the service is running and the software is functional. However, as you reported, the software may crash sometimes, which can cause significant downtime. The service startup type is "Automatic", which means that the service starts automatically every time the server boots up. The service log on as is
"TestAccount", which is a test account that was probably used for development or testing purposes.

To fix the issue with the MarketApp software, you need to do one thing:

* You need to change the service log on as, so that the service runs under a proper account that has sufficient permissions and security settings for production use. To do this, you can right-click on the service name and select "Properties" from the menu. Alternatively, you can select the service name and click on the "Properties" button on the toolbar. You should see a window with several tabs and options.

On the "Log On" tab, under "Log on as", you can select either "Local System account" or "This account". If you choose "Local System account", then the service will run under a predefined local account that has extensive privileges on the local computer. If you choose "This account", then you will need to enter a valid username and password for an account that has appropriate permissions and security settings for running the service. You may need to consult with your IT team or your

software vendor to determine which option is best for your situation. Then, click on "OK" to save your changes.

NEW QUESTION: 59
A server administrator mounted a new hard disk on a Linux system with a mount point of /newdisk. It was later determined that users were unable to create directories or files on the new mount point. Which of the following commands would successfully mount the drive with the required parameters?
A. echo /newdisk >> /etc/fstab
B. net use /newdisk
C. mount -o remount, rw /newdisk
D. mount -a
Answer: C (LEAVE A REPLY)
The administrator should use the command mount -o remount,rw /newdisk to successfully mount the drive with the required parameters. The mount command is used to mount file systems on Linux systems. The -o option specifies options for mounting file systems. The remount option re-mounts an already mounted file system with different options. The rw option mounts a file system with read-write permissions. In this case,
/newdisk is a mount point for a new hard disk that was mounted with read-only permissions by default. To allow users to create directories or files on /newdisk, the administrator needs to re-mount /
Reference:
https://unix.stackexchange.com/questions/149399/how-to-remount-as-read-write-a-specific-mount-of-device

NEW QUESTION: 60
Which of the following technologies can successfully back up files that are used by other processes without stopping those processes?
A. Differential
B. Archive
C. Synthetic full
D. Open file
Answer: D (LEAVE A REPLY)
Comprehensive Detailed Explanation with all CompTIA Server+ SK0-005 Study Guide References:An Open file backup solution allows files that are in use by other processes to be backed up without stopping those processes. This is especially important in environments where critical applications and services must remain operational while backup operations occur. Technologies like VSS (Volume Shadow Copy Service) in Windows provide this functionality, enabling the backup of open files such as databases or system files without disrupting the processes.
* Differential and Archive backups are types of backup strategies but do not specifically address backing up open or in-use files.
* Synthetic full backups refer to a method of creating a full backup by combining incremental backups and a full backup, but it does not specifically address open files.

NEW QUESTION: 61
Which of the following concepts refers to prioritizing a connection that had previously worked successfully?
A. Round robin
B. SCP
C. MRU
D. Link aggregation
Answer: C (LEAVE A REPLY)
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: 62
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: (SHOW ANSWER)
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: 63
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: 64
An organization is donating its outdated server equipment to a local charity. Which of the following describes what the organization should do BEFORE donating the equipment?
A. Remove all the data from the server drives using the least destructive method.
B. Repurpose and recycle any usable server components.
C. Remove all the components from the server.
D. Review all company polices.
Answer: (SHOW ANSWER)

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

NEW QUESTION: 65
A technician recently upgraded several pieces of firmware on a server. Ever since the technician rebooted the server, it no longer communicates with the network. Which of the following should the technician do FIRST to return the server to service as soon as possible?
A. Replace the NIC
B. Make sure the NIC is on the HCL
C. Reseat the NIC
D. Downgrade the NIC firmware
Answer: (SHOW ANSWER)
The first thing that the technician should do to return the server to service as soon as possible is downgrade the NIC firmware. Firmware is a type of software that controls the basic functions of hardware devices, such as network interface cards (NICs). Firmware updates can provide bug fixes, performance improvements, or new features for hardware devices. However, firmware updates can also cause compatibility issues, configuration errors, or functionality failures if they are not installed properly or if they are not compatible with the device model or driver version. Downgrading the firmware means reverting to an older version of firmware that was previously working fine on the device. Downgrading the firmware can help resolve any problems caused by a faulty firmware update and restore normal operation of the device.

NEW QUESTION: 66
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: 67
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: 68
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: A,E (LEAVE A REPLY)
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: 69
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: 70
An administrator needs to reconfigure a teamed network connection on a server in a remote data center.
Which of the following will offer the most resilient connection while performing this change?
A. Use of an 00B solution
B. Use of a crash cart
C. Use of a VNC console
D. Use of an RDP console
Answer: A (LEAVE A REPLY)
An out-of-band (OOB) solution is a method of accessing and managing a server remotely without using the network connection or the operating system of the server. An OOB solution can use a dedicated management port, a serial console, or a KVM switch to provide a resilient connection while performing changes to the network configuration of the server. An OOB solution is more reliable than

a VNC or RDP console, which depend on the network and the operating system, and more convenient than a crash cart, which requires physical access to the server.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 2, Lesson 2.3, Objective 2.3

NEW QUESTION: 71
A technician installed a kernel upgrade to a Linux server. The server now crashes regularly. Which of the following is the most likely cause?
A. Necessary dependencies were installed for multiple architectures.
B. There is not enough hard drive space.
C. The server is infected with a virus.
D. Some modules are not compatible.
Answer: D (LEAVE A REPLY)
A kernel upgrade is a process of updating the core component of a Linux operating system that manages the hardware, memory, processes, and drivers. A kernel upgrade can improve the performance, security, and compatibility of the system, but it can also introduce errors if some modules are not compatible with the new kernel version. Modules are pieces of code that can be loaded and unloaded into the kernel to provide additional functionality or support for specific devices. If a module is not compatible with the kernel, it can cause crashes or instability.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 4, Lesson 4.2, Objective 4.2

NEW QUESTION: 72
A user cannot save large files to a directory on a Linux server that was accepting smaller files a few minutes ago. Which of the following commands should a technician use to identify the issue?
A. pvdisplay
B. mount
C. df -h
D. fdisk -l
Answer: C (LEAVE A REPLY)
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: 73
A server administrator noticesthe/var/log/audit/audit.logfileon a Linux server is rotating loo frequently. The administrator would like to decrease the number of times the leg rotates without losing any of the information in the logs. Which of the following should the administrator configure?

A. increase theaudit. log file size in the appropriate confutation file.
B. Decrease the duration of the log rotate cycle tor theaudit. log file.
C. Remove the tog rotate directive from the audit .log We configuration.
D. Move the audit. leg files to a remote syslog server.
Answer: A (LEAVE A REPLY)
The audit.log file is a file that records security-related events on a Linux server, such as user login, file access, and system commands. The logrotate utility is a tool that rotates, compresses, and deletes old log files based on certain criteria, such as size, time, or frequency. To decrease the number of times the log rotates without losing any information, the administrator should increase the audit.log file size in the appropriate configuration file, such as /etc/logrotate.conf or /etc/logrotate.d/auditd. Verified References: [audit.log],
[logrotate]

NEW QUESTION: 74
A system administrator has been alerted to a zero-day vulnerability that is impacting a service enabled on a server OS. Which of the following would work BEST to limit an attacker from exploiting this vulnerability?
A. Installing the latest patches
B. Closing open ports
C. Enabling antivirus protection
D. Enabling a NIDS
Answer: A (LEAVE A REPLY)
The best way to limit an attacker from exploiting a zero-day vulnerability that is impacting a service enabled on a server OS is to install the latest patches. Patches are updates that fix bugs, improve security, or add features to software. Installing patches can help prevent attackers from exploiting known vulnerabilities that have been fixed by the software vendor. A zero-day vulnerability is a vulnerability that is unknown to the vendor or the public until it is exploited by an attacker. Therefore, installing patches as soon as they are available can reduce the window of opportunity for attackers to exploit zero-day vulnerabilities. Reference:
https://www.ibm.com/cloud/learn/patch-management

NEW QUESTION: 75
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: 76
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: 77

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: 78

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

A. Something you are

B. Something you know

C. Something you have

D. Something you do

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 79

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

A. Perform scheduled chkdsk tests.

B. Purchase matching hardware and clone the disk.

C. Upgrade the hard disk to SSD.

D. Perform quarterly backups.

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 80
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: 81
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: 82
A server technician has been asked to upload a few files from the internal web server to the internal FTP server. The technician logs in to the web server using PuTTY, but the connection to the FTP server fails.
However, the FTP connection from the technician's workstation is sucessful. To troubleshoot the issue, the technician executes the following command on both the web server and the workstation:
ping ftp.acme.local
The IP address in the command output is different on each machine. Which of the following is the MOST likely reason for the connection failure?
A. A misconfigured firewall
B. A misconfigured hosts.deny file
C. A misconfigured hosts file
D. A misconfigured hosts.allow file
Answer: (SHOW ANSWER)
A misconfigured hosts file can cause name resolution issues on a server. A hosts file is a text file that maps hostnames to IP addresses on a local system. It can be used to override DNS settings or provide custom name resolution for testing purposes. However, if the hosts file contains incorrect or outdated entries, it can prevent the system from resolving hostnames properly and cause connectivity problems. To fix this issue, the administrator should check and edit the hosts file accordingly.

NEW QUESTION: 83
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: (SHOW ANSWER)
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: 84
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: (SHOW ANSWER)

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: 85

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: D (LEAVE A REPLY)

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: 86

While a technician is troubleshooting a performance issue on a database server, users are disconnected from the database. An administrator is asked to intervene and restore access. Which of the following steps should the administrator take first?

A. Revert any patches or updates on the server from the past 24 hours

B. Reproduce the issue in a test environment and confirm the database fails in the same manner

C. Perform a root cause analysis and report the issue to management

D. Collect all logs from the system and review the actions the technician performed

E. Perform a quick backup of the system to prevent any further issues

Answer: D (LEAVE A REPLY)

The first step when addressing an urgent issue like a database disconnection should be to gather information to understand what actions caused the problem. Collecting all logs and reviewing the technician's actions (Answer D) will help identify what went wrong and guide appropriate remediation. Restoring access quickly is the priority, and without reviewing logs, it would be hard to identify the root cause or prevent further damage.
* Reverting patches (Option A): Reverting patches might cause more issues if the problem isn't directly related to a recent update.
* Reproducing the issue (Option B): Reproduction is useful in a controlled environment but not practical as an immediate first step in production.
* Root cause analysis (Option C): This is necessary but should come after restoring access.
* Performing a quick backup (Option E): While backups are crucial, this step might not help resolve the current access problem and can delay troubleshooting.
CompTIA Server+ Reference:This topic relates to SK0-005 Objective 3.4: Explain troubleshooting theory and methodologies.

NEW QUESTION: 87
The internal IT department policy for monitoring server health requires that evidence of server reboots be collected and reviewed on a regular basis. Which of the following should be monitored to best provide this evidence?
A. Uptime
B. IOPS
C. CPU utilization
D. Event logs
Answer: D (LEAVE A REPLY)
Comprehensive Detailed Explanation with all CompTIA Server+ SK0-005 Study Guide References:
Event logs are the primary source for tracking server reboots and other system events. Logs such as the system log in Linux (/var/log/syslog or /var/log/messages) or the Event Viewer in Windows provide timestamps and details about shutdowns, restarts, and boot processes. Regular monitoring ensures that unplanned reboots or system errors are identified and addressed.
* Uptime: Indicates how long the server has been running since the last reboot but does not provide detailed reboot evidence.
* IOPS: Refers to input/output operations per second, unrelated to reboots.
* CPU utilization: Reflects processor activity but offers no reboot evidence.

NEW QUESTION: 88
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: (SHOW ANSWER)

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 extra overhead 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: 89

A technician is decommissioning a server from a production environment. The technician removes the server from the rack but then decides to repurpose the system as a lab server instead of decommissioning it. Which of the following is the most appropriate NEXT step to recycle and reuse the system drives?

A. Reinstall the OS.

B. Wipe the drives.

C. Degauss the drives.

D. Update the IP schema.

Answer: B (LEAVE A REPLY)

Wiping the drives is the most appropriate step to recycle and reuse the system drives. Wiping the drives means erasing all the data on the drives and overwriting them with random or meaningless data. This can help prevent data leakage, comply with regulations, and prepare the drives for a new installation or configuration.

Wiping the drives is different from deleting or formatting the drives, which only remove the references to the data but not the data itself. References: https://www.comptia.org/training/resources/exam-objectives/comptia- server-sk0-005-exam-objectives (Objective 1.3)

NEW QUESTION: 90

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: B,F (LEAVE A REPLY)

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: 91

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

A. Drive

B. Database

C. Folder

D. File

Answer: A (LEAVE A REPLY)

Drive encryption is a form of encryption that best achieves the goal of data-at-rest encryption for all data.

Drive encryption encrypts the entire hard drive, including the operating system, applications, and files. This prevents unauthorized access to the data if the drive is lost or stolen. Database, folder, and file encryption are forms of encryption that only encrypt specific data sets, not all data. References: [CompTIA Server+ Certification Exam Objectives], Domain 5.0: Security, Objective 5.3: Given a scenario involving a security threat/vulnerability/risk, implement appropriate mitigation techniques.

NEW QUESTION: 92
A site is considered a warm site when it:
A. has basic technical facilities connected to it.
B. has faulty air conditioning that is awaiting service.
C. is almost ready to take over all operations from the primary site.
D. is fully operational and continuously providing services.
Answer: C (LEAVE A REPLY)
A warm site is a backup site that has some of the necessary hardware, software, and network resources to resume operations, but not all of them. A warm site requires some time and effort to become fully operational.
A warm site is different from a cold site, which has minimal or no resources, and a hot site, which has all the resources and is ready to take over immediately.
References: CompTIA Server+ Study Guide, Chapter 10: Disaster Recovery, page 403.

NEW QUESTION: 93
A company is reviewing options for its current disaster recovery plan and potential changes to it. The security team will not allow customer data to egress to non-company equipment, and the company has requested recovery in the shortest possible time. Which of the following will BEST meet these goals?
A. A warm site
B. A hot site
C. Cloud recovery
D. A cold site
Answer: (SHOW ANSWER)
A hot site is a type of disaster recovery site that has all the equipment and data ready to resume operations as soon as possible after a disaster. A hot site is usually located in a different geographic area than the primary site and has redundant power, cooling, network, and security systems. A hot site is best for the company that wants to recover in the shortest possible time and does not want customer data to egress to non-company equipment. A warm site is a type of disaster recovery site that has some equipment and data ready, but requires some configuration and restoration before resuming operations. A cold site is a type of disaster recovery site that has only basic infrastructure and space available, but requires significant setup and installation before resuming operations. Cloud

recovery is a type of disaster recovery service that uses cloud- based resources and platforms to store backups and restore data and applications after a disaster. References:
https://www.techopedia.com/definition/11172/hot-site
https://www.techopedia.com/definition/11173/warm- site
https://www.techopedia.com/definition/11174/cold-sitehttps://www.techopedia.com/definition/29836/cloud-recovery

NEW QUESTION: 94
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: 95
A Windows server has experienced a BSOD, and the administrator needs to monitor the reboot. The server is in a datacenter with no OOB management. Which of the following tools should the administrator use to complete this task?
A. Crash cart
B. IP KVM
C. Virtual administration console
D. Serial connection
Answer: A (LEAVE A REPLY)
Comprehensive Detailed Explanation with all CompTIA Server+ SK0-005 Study Guide References:A Crash cart is a physical console that can be connected directly to the server's video output and keyboard

/mouse ports. This is useful in situations where remote management (OOB) is unavailable, allowing the administrator to directly view the server's display and interact with the system during the reboot process.
* IP KVM (Keyboard, Video, Mouse) is used for remote management, but the scenario specifically mentions no OOB management.
* Virtual administration console and Serial connections can be used for remote management or console access, but since OOB management is unavailable, a physical crash cart is the appropriate choice.

NEW QUESTION: 96
A company is running an application on a file server. A security scan reports the application has a known vulnerability. Which of the following would be the company's BEST course of action?
A. Upgrade the application package
B. Tighten the rules on the firewall
C. Install antivirus software
D. Patch the server OS
Answer: (SHOW ANSWER)
The best course of action for the company is to upgrade the application package to fix the known vulnerability. A vulnerability is a weakness or flaw in an application that can be exploited by an attacker to compromise the security or functionality of the system. Upgrading the application package means installing a newer version of the application that has patched or resolved the vulnerability. This way, the company can prevent potential attacks that may exploit the vulnerability and cause damage or loss.

NEW QUESTION: 97
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: (SHOW ANSWER)
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: 98
A developer is creating a web application that will contain five web nodes. The developer's main goal is to ensure the application is always available to the end users. Which of the following should the developer use when designing the web application?
A. Round robin
B. Link aggregation
C. Network address translation
D. Bridged networking
Answer: A (LEAVE A REPLY)
Round robin is a load balancing technique that distributes requests among multiple web nodes in a circular order. It ensures that each web node receives an equal amount of requests and improves the availability and performance of the web application. Verified References: [Round robin], [Load balancing]

NEW QUESTION: 99
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: 100
The HIDS logs on a server indicate a significant number of unauthorized access attempts via USB devices at startup. Which of the following steps should a server administrator take to BEST secure the server without limiting functionality?

A. Set a BIOS/UEFI password on the server.
B. Change the boot order on the server and restrict console access.
C Configure the host OS to deny login attempts via USB.
C. Disable all the USB ports on the server.
Answer: B (LEAVE A REPLY)
Changing the boot order on the server and restricting console access would prevent unauthorized access attempts via USB devices at startup, as the server would not boot from any external media and only authorized users could access the console. Setting a BIOS/UEFI password on the server would also help, but it could be bypassed by resetting the CMOS battery or using a backdoor password. Configuring the host OS to deny login attempts via USB would not prevent booting from a malicious USB device that could compromise the system before the OS loads. Disabling all the USB ports on the server would limit functionality, as some peripherals or devices may need to use them.
References:
https://www.pcmag.com/how-to/dont-plug-it-in-how-to-prevent-a-usb-attack
https://www.techopedia.com/definition/10362/boot-order
https://www.techopedia.com/definition/10361/console-access
https://www.techopedia.com/definition/102/bios-password
https://www.techopedia.com/definition/10363/cmos-battery

NEW QUESTION: 101
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: 102
The management team has mandated the use of data-at-rest encryption for all data. Which of the following forms of encryption best achieves this goal?

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

NEW QUESTION: 103
A data center environment currently hosts more than 100 servers that include homegrown and commercial software. The management team has asked the server administrator to find a way to eliminate all company-owned data centers. Which of the following models will the administrator most likely choose to meet this need?
A. SaaS
B. Private
C. Public
D. Hybrid
Answer: C (LEAVE A REPLY)
A public cloud model will most likely meet the need of eliminating all company-owned data centers. A public cloud is a type of cloud computing service that is provided by a third-party vendor over the internet. A public cloud offers scalability, flexibility, and cost-effectiveness for hosting servers and applications, as the customers only pay for the resources they use and do not have to maintain their own infrastructure. A public cloud can also provide high availability, security, and performance for the servers and applications, as the vendor manages the underlying hardware and software. A public cloud can support various types of services, such as software as a service (SaaS), platform as a service (PaaS), or infrastructure as a service (IaaS). References: [CompTIA Server+ Certification Exam Objectives], Domain 1.0: Server Administration, Objective 1.2: Given a scenario, compare and contrast server roles and requirements for each.

NEW QUESTION: 104
A company's security team has noticed employees seem to be blocking the door in the main data center when they are working on equipment to avoid having to gain access each time. Which of the following should be implemented to force the employees to enter the data center properly?
A. A security camera

B. A mantrap
C. A security guard
D. A proximity card
Answer: B (LEAVE A REPLY)
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: 105
A technician is sizing a new server and, for service reasons, needs as many hot-swappable components as possible. Which of the following server components can most commonly be replaced without downtime?
(Select three).
A. Drives
B. Fans
C. CMOSIC
D. Processor
E. Power supplies
F. Motherboard
G. Memory
H. BIOS
Answer: A,B,E (LEAVE A REPLY)
Drives, fans, and power supplies are server components that can most commonly be replaced without downtime if they are hot-swappable. Hot-swappable components can be removed and inserted while the server is running, without affecting its operation or performance. Drives store data and applications, fans cool down the server components, and power supplies provide electricity to the server. Replacing these components can prevent data loss, overheating, or power failure.
References: CompTIA Server+ Certification Exam Objectives, Domain 2.0: Hardware, Objective 2.2: Given a scenario, install, configure and maintain server components.

NEW QUESTION: 106
An administrator notices nigh traffic on a certain subnet and would like to identify the source of the traffic.
Which of the following tools should the administrator utilize?
A. Anti-malware
B. Nbtstat
C. Port scanner
D. Sniffer
Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 107
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: 108
A VLAN needs to be configured within a virtual environment for a new VM. Which of the following will ensure the VM receives a correct IP address?
A. A virtual router
B. A host NIC
C. A VPN
D. A virtual switch
E. A vNIC
Answer: (SHOW ANSWER)
The correct answer is D. A virtual switch.
A virtual switch is a software-based network device that connects the virtual machines (VMs) in a virtual environment and allows them to communicate with each other and with the physical network. A virtual switch can also create and manage virtual LANs (VLANs), which are logical segments of a

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

NEW QUESTION: 109
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: 110

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: (SHOW ANSWER)

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: 111

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

A. Connect the diagnostic card to the PCIe connector.

B. Connect a console cable to the server NIC.

C. Connect to the server from a crash cart.

D. Connect the virtual administration console.

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 112

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 to have access without granting excessive access to others?

A. chmod 777 filename
B. chown Joe filename
C. Chmod g+w filename
D. chgrp IT filename
Answer: C (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: 113
A server administrator implemented a new backup solution and needs to configure backup methods for remote sites. These remote sites have low bandwidth and backups must not interfere with the network during normal business hours. Which of the following methods can be used to meet these requirements? (Select two).
A. Open file
B. Archive
C. Cloud
D. Snapshot
E. Differential
F. Synthetic full
Answer: B,E (LEAVE A REPLY)
Archive is a method of storing historical data that is not frequently accessed or modified. Archive can reduce the amount of data that needs to be backed up and save bandwidth and storage space. Differential is a method of backing up only the data that has changed since the last full backup. Differential can also save bandwidth and storage space, as well as speed up the backup process. References:
CompTIA Server+ Certification Exam Objectives1, page 12
Server Management: Server Hardware Installation and Management2, Module 2, Lesson 5

NEW QUESTION: 114
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: 115
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: 192.168.10.2/24
Default gateway: 192.168.10.1
B. IP address: 192.168.1.2/24
Default gateway: 192.168.10.1
C. IP address: 192.168.10.3/24
Default gateway: 192.168.20.1
D. IP address: 192.168.10.24/24
Default 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. The subnet mask determines how many bits of the IP address are used for the network prefix and how many bits are used for the host identifier. A /24 subnet mask means that the first 24 bits of the IP address are used for the network prefix and the last 8 bits are used for the host identifier. Therefore, any IP address that has the same first 24 bits as the default gateway belongs to the same subnet. In this case, the default gateway has an IP address of 192.168.10.1/24, which means that any IP address that starts with 192.168.10.x/24 belongs to the same subnet. The new server has an IP address of 192.168.1.1/24, which does not match the first 24 bits of the default gateway, so it belongs to a different subnet and cannot communicate with the default gateway. To fix this issue, the administrator should change the IP address of the new server to an unused IP address that starts with 192.168.10.x/24, such as
192.168.10.2/24.

NEW QUESTION: 116
An administrator notices high traffic on a certain subnet and would like to identify the source of the traffic.
Which of the following tools should the administrator utilize?
A. Anti-malware
B. Nbtstat
C. Port scanner
D. Sniffer
Answer: D (LEAVE A REPLY)
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: 117
An administrator receives an alert stating a S.MAR.T. error has been detected. Which of the following should the administrator run FIRST to determine the issue?
A. A hard drive test
B. A RAM test
C. A power supply swap
D. A firmware update
Answer: (SHOW ANSWER)
A S.M.A.R.T. error is an indication of a potential failure of a hard drive. S.M.A.R.T. stands for Self-Monitoring, Analysis and Reporting Technology and it is a feature that monitors the health and performance of hard drives. A hard drive test can help diagnose the issue and determine if the drive needs to be replaced.
References: https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam- objectives (Objective 1.1)

NEW QUESTION: 118
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: A (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.

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: 119

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: 120

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: (SHOW ANSWER)

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

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

NEW QUESTION: 121
A company has implemented a requirement to encrypt all the hard drives on its servers as part of a data loss prevention strategy. Which of the following should the company also perform as a data loss prevention method?
A. Encrypt all network traffic
B. Implement MFA on all the servers with encrypted data
C. Block the servers from using an encrypted USB
D. Implement port security on the switches
Answer: B (LEAVE A REPLY)
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: 122
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: C (LEAVE A REPLY)
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: 123
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: B (LEAVE A REPLY)
* 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: 124
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: C,D (LEAVE A REPLY)

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: 125
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: A (LEAVE A REPLY)
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: 126
An administrator needs to disable root login over SSH. Which of the following tiles should be edited to complete this task?
A. /root.ssh/sshd/config
B. /etc.ssh/sshd_config
C. /root/.ssh/ssh_config
D. /etc.sshs_shd_config
Answer: B (LEAVE A REPLY)
To disable root login over SSH, the server administrator needs to edit the SSH configuration file located at /etc
/ssh/sshd_config. This file contains various settings for the SSH daemon that runs on the server and accepts incoming SSH connections. The administrator needs to find the line that says

PermitRootLogin and change it to no or comment it out with a # symbol. Then, the administrator needs to restart the SSH service for the changes to take effect. References: https://www.howtogeek.com/828538/how-and-why-to-disable-root-login- over-ssh-on-linux/

NEW QUESTION: 127
A data center employee shows a driver's license to enter the facility Once the employee enters, the door immediately doses and locks, triggering a scale that then weighs the employee before granting access to another locked door. This is an example of.
A. mantrap.
B. a bollard
C. geofencing
D. RFID.
Answer: A (LEAVE A REPLY)
A mantrap is a security device that consists of a small space with two sets of interlocking doors, such that the first set of doors must close before the second one opens. A mantrap can be used to control access to a data center by verifying the identity and weight of the person entering. A bollard is a sturdy post that prevents vehicles from entering a restricted area. Geofencing is a technology that uses GPS or RFID to create a virtual boundary around a location and trigger an action when a device crosses it. RFID is a technology that uses radio waves to identify and track objects or people.
References:
* https://www.techopedia.com/definition/16293/mantrap
* https://www.techopedia.com/definition/1437/bollard
* https://www.techopedia.com/definition/23961/geofencing
* https://www.techopedia.com/definition/506/radio-frequency-identification-rfid

NEW QUESTION: 128
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: (SHOW ANSWER)
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: 129
A technician is monitoring a server and notices there is only one NIC plugged in. but the server has two. The NIC is oversaturated, and the technician would like to increase the available bandwidth. Which of the following solutions would be the BEST option to increase the speed of this NIC?
A. Link aggregation
B. Heartbeat
C. Most recently used
D. Active-active
Answer: A (LEAVE A REPLY)
This is the best solution to increase the speed of the NIC because link aggregation is a technique that combines multiple physical network interfaces into a single logical interface. This can increase the bandwidth, redundancy, and load balancing of network traffic. Link aggregation requires both the server and the switch to support it and be configured accordingly. References: https://www.cisco.com/c/en/us/support/docs/lan- switching/etherchannel/12023-4.html

NEW QUESTION: 130
A server administrator needs to deploy five VMs, all of which must have the same type of configuration.
Which of the following would be the MOST efficient way to perform this task?
A. Snapshot a VM.
B. Use a physical host.
C. Perform a P2V conversion.
D. Use a VM template.
Answer: D (LEAVE A REPLY)
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: 131
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: 132
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: 133
Due to a disaster incident on a primary site, corporate users are redirected to cloud services where they will be required to be authenticated just once in order to use all cloud services.
Which of the following types of authentications is described in this scenario?
A. NTLM
B. Kerberos
C. SSO
D. MFA
Answer: C (LEAVE A REPLY)

NEW QUESTION: 134
An application server cannot communicate with a newly installed database server. The database server, which has static IP information, is reading the following output from ipconf ig:
The application server is reading the following output from ipconf ig:
Which of the following most likely contains an error?

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

NEW QUESTION: 135
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: (SHOW ANSWER)
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: 136
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: 137
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: 138
An administrator has deployed a new virtual server from a template. After confirming access to the subnet's gateway, the administrator is unable to log on with the domain credentials. Which of the following is the most likely cause of the issue?
A. The server has not been joined to the domain.
B. An IP address has not been assigned to the server.
C. The server requires a reboot to complete the deployment process.
D. The domain credentials are invalid.
Answer: A (LEAVE A REPLY)
The most likely cause of the issue is that the server has not been joined to the domain. A domain is a logical group of computers and devices that share a common directory service and security policy. A domain controller is a server that manages the domain and authenticates users and computers that want to access domain resources. To log on with domain credentials, a server must be joined to the domain and registered in the directory service. If a server has not been joined to the domain, it will not be recognized or authorized by the domain controller.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 4, Lesson 4.3, Objective 4.3

NEW QUESTION: 139
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: 140
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: 141
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: 142
A technician is attempting to reboot a remote physical Linux server. However, attempts to command a shutdown -----now result in the loss of the SSH connection. The server still responds to pings. Which of the following should the technician use to command a remote shutdown?
A. virtual serial console
B. A KVM
C. An IDRAC
D. A crash cart
Answer: C (LEAVE A REPLY)
An IDRAC (Integrated Dell Remote Access Controller) is a tool that can be used to command a remote shutdown of a physical Linux server. An IDRAC is a hardware device that provides out-of-band management for Dell servers. It allows the technician to access the server's console, power

cycle, reboot, or shut down the server remotely using a web interface or a command-line interface. An IDRAC does not depend on the operating system or network connectivity of the server. A virtual serial console is a tool that can be used to access a remote virtual machine's console using a serial port connection. A KVM (Keyboard, Video, Mouse) switch is a device that allows the technician to switch between different computer sources using the same keyboard, monitor, and mouse. A crash cart is a mobile unit that contains a keyboard, monitor, mouse, and other tools that can be connected to a physical server for troubleshooting purposes. References: https://www.
dell.com/support/kbdoc/en-us/000131486/understanding-the-idrac
https://www.howtogeek.com/799968/what- is-a-kvm-
switch/https://www.techopedia.com/definition/1032/business-impact-analysis-bia

NEW QUESTION: 143
Which of the following technologies would allow an administrator to build a software RAID on a Windows server?
A. Logical volume management
B. Dynamic disk
C. GPT
D. UEFI
Answer: B (LEAVE A REPLY)
Dynamic disk is a technology that allows an administrator to build a software RAID on a Windows server.
Dynamic disk is a type of disk management that supports creating volumes that span multiple disks, stripe data across disks, mirror data between disks, or use parity for fault tolerance. Dynamic disk can be used to create RAID 0 (striping), RAID 1 (mirroring), RAID 5 (striping with parity), or spanned volumes on Windows servers. Logical volume management is a technology that allows creating and resizing logical volumes on Linux servers. GPT (GUID Partition Table) is a standard for defining the partition structure on a disk. UEFI (Unified Extensible Firmware Interface) is a specification for the interface between the operating system and the firmware. References:
https://www.howtogeek.com/school/using-windows-admin-tools-like-a- pro/lesson2/
https://www.howtogeek.com/howto/40702/how-to-manage-and-use-lvm-logical-volume- management-in-ubuntu/ https://www.howtogeek.com/193669/whats-the-difference-between-gpt-and-mbr- when-partitioning-a-drive/ https://www.howtogeek.com/56958/htg-explains-how-uefi-will-replace-the-bios/

NEW QUESTION: 144
Which of the following commands should a systems administrator use to create a batch script to map multiple shares'?
A. nbtstat
B. netuse
C. tracert
D. netstst
Answer: (SHOW ANSWER)

The net use command is a Windows command that can be used to create a batch script to map multiple shares.
The net use command can connect or disconnect a computer from a shared resource, such as a network drive or a printer, or display information about computer connections. The syntax of the net use command is:
net use [devicename | *] [\\computername\sharename[\u0003volume] [password | *]] [/user:[domainname\] username] [/user:[dotted domain name\]username] [/user:[[username@dotted domain name] [/savecred] [
/smartcard] [{/delete | /persistent:{yes | no}}]
where:
devicename = the drive letter or printer port to assign to the shared resource computername = the name of the computer that provides access to the shared resource sharename = the name of the shared resource password = the password needed to access the shared resource /user = specifies a different username to make the connection /savecred = stores the provided credentials for future use /smartcard = uses a smart card for authentication /delete = cancels a network connection and removes the connection from the list of persistent connections /persistent = controls whether the connection is restored at logon To create a batch script to map multiple shares, you can use the net use command with different drive letters and share names, for example:
net use W: \\computer1\share1 net use X: \\computer2\share2 net use Y: \\computer3\share3 You can also add other options, such as passwords, usernames, or persistence, as needed. To save the batch script, you can use Notepad or any text editor and save the file with a .bat extension12.
References: 1 https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/net-use 2
https://www.watchingthenet.com/create-a-batch-file-to-map-drives-folders.html

NEW QUESTION: 145
A company is building a new datacenter next to a busy parking lot. Which of the following is the BEST strategy to ensure wayward vehicle traffic does not interfere with datacenter operations?
A. Install security cameras
B. Utilize security guards
C. Install bollards
D. Install a mantrap
Answer: C (LEAVE A REPLY)
The best strategy to ensure wayward vehicle traffic does not interfere with datacenter operations is to install bollards. Bollards are sturdy posts that are installed around a perimeter to prevent vehicles from entering or crashing into a protected area. Bollards can provide physical security and deterrence for datacenters that are located near busy roads or parking lots. Bollards can also prevent accidental damage or injury caused by vehicles that lose control or have faulty brakes.

NEW QUESTION: 146

A systems administrator is installing Windows on an 8TB drive and would like to create a single 8TB partition on the disk. Which of the following options should the administrator use?

A. VMFS

B. ZFS

C. GPT

D. MBR

E. LVM

Answer: C (LEAVE A REPLY)

* Scenario: Installing Windows on an 8TB drive, aiming for a single 8TB partition.
* Solution: Use the GPT (GUID Partition Table) option (Option C):
* GPT supports larger partitions (up to 18.4 million TB) compared to MBR (limited to 2TB).
* VMFS, ZFS, and LVM are unrelated to the partitioning scheme in Windows.

Reference: CompTIA Server+ Guide, Chapter 3: Hardware, Section 3.3.1 (Partitioning)

NEW QUESTION: 147

Which of the following BEST describes a warm site?

A. The site has all infrastructure and live data.

B. The site has all infrastructure and some data

C. The site has partially redundant infrastructure and no network connectivity

D. The site has partial infrastructure and some data.

Answer: (SHOW ANSWER)

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

NEW QUESTION: 148

A startup is migrating a stand-alone application that stores PII to the cloud. Which of the following should be encrypted?

A. Datain transit

B. Dataat rest

C. Databackups

D. Dataarchives

Answer: B (LEAVE A REPLY)

* Scenario: Migrating a stand-alone application storing PII to the cloud.
* Data to Encrypt: Data at rest (Option B) should be encrypted:

* Data in transit (Option A) and backups (Option C) are also important but not the primary concern here.
* Data archives (Option D) may or may not contain sensitive data.
Reference: CompTIA Server+ Guide, Chapter 5: Security, Section 5.3.1 (Data Encryption)

NEW QUESTION: 149
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: 150
A server administrator notices drive C on a critical server does not have any available space, but plenty of unallocated space is left on the disk. Which of the following should the administrator perform to address the availability issue while minimizing downtime?
A. Decrease the size of the page/swap file
B. Reformat drive C to use all the disk space
C. Enable whole disk encryption on the hard drive
D. Enforce disk quotas on shares within that server
E. Partition the unallocated space to provide more available space
Answer: E (LEAVE A REPLY)
If drive C is running out of space and there is unallocated space available on the disk, the best solution is to partition the unallocated space and extend drive C to include the new partition. This can be done without significant downtime and will immediately provide more space for the system.
* Partition the unallocated space (Answer E): This is the simplest and least disruptive method to increase the available space on drive C.
* Decreasing the page/swap file (Option A): This may free up some space but can negatively impact system performance.
* Reformatting (Option B): Reformatting would result in significant downtime and data loss, making it an impractical option.
* Whole disk encryption (Option C): This does not solve the issue of disk space.

* Enforcing disk quotas (Option D): Disk quotas manage space usage but won't free up space on drive C:
CompTIA Server+ Reference:This topic is covered under SK0-005 Objective 3.3: Troubleshoot common server problems.

NEW QUESTION: 151
Which of the following backup methods can be performed while a server is running, will not interrupt files in use, and can be used to fully restore the server if needed?
A. Snapshot
B. Archive
C. Open file
D. Differential
Answer: A (LEAVE A REPLY)
Asnapshotis a point-in-time image of a system's state that can be created while the system is running, without interrupting operations. Snapshots can be used to restore the entire system to the exact state at the time of the snapshot. They are commonly used in virtualized environments and allow administrators to roll back to a previous state if needed.
* Snapshot (Answer A):Captures the entire system's state and can be taken without downtime.
* Archive (Option B):Refers to long-term storage, not necessarily something that supports live backups.
* Open file (Option C):Refers to a method that handles open files during backup but doesn't provide full system restoration capabilities.
* Differential (Option D):Backs up only the data changed since the last full backup but still requires a full backup for complete system restoration.
CompTIA Server+ Reference:This topic is related toSK0-005 Objective 4.1: Explain backup and recovery methods.

NEW QUESTION: 152
Which of the following BEST describes overprovisioning in a virtual server environment?
A. Committing more virtual resources to virtual machines than there are physical resources present
B. Installing more physical hardware than is necessary to run the virtual environment to allow for future expansion

C. Allowing a virtual machine to utilize more resources than are allocated to it based on the server load
D. Ensuring there are enough physical resources to sustain the complete virtual environment in the event of a host failure
Answer: A (LEAVE A REPLY)
This is the best definition of overprovisioning in a virtual server environment because it means allocating more CPU, memory, disk, or network resources to the virtual machines than what is actually available on the physical host. This can lead to performance issues and resource contention.
References: https://www.hpe.com
/us/en/insights/articles/10-virtualization-mistakes-everyone-makes-1808.html

NEW QUESTION: 153
A server administrator needs to create a new folder on a file server that only specific users can access. Which of the following BEST describes how the server administrator can accomplish this task?
A. Create a group that includes all users and assign it to an ACL.
B. Assign individual permissions on the folder to each user.
C Create a group that includes all users and assign the proper permissions.
C. Assign ownership on the folder for each user.
Answer: C (LEAVE A REPLY)
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: 154
A datacenter has ten 40U racks in a hot/cold aisle configuration. The room has adequate air conditioning, but servers located near the top of the racks are shutting down due to issues with heat. Which of the following should be used to reduce issues with heat?
A. Rack balancing
B. Higher-capacity PDUs
C. Rail kits
D. Blanking panels
Answer: D (LEAVE A REPLY)
Comprehensive Detailed Explanation with all CompTIA Server+ SK0-005 Study Guide References:
Blanking panels are used to fill empty spaces in server racks. By blocking airflow gaps between servers, blanking panels help to direct airflow properly, ensuring that the cold air from the cold aisle is not wasted and that the hot air from the hot aisle is contained. This is crucial for maintaining the efficiency of cooling systems in a hot/cold aisle configuration.
* Rack balancing addresses the physical distribution of equipment, but it does not directly address thermal issues.

* Higher-capacity PDUs (Power Distribution Units) provide more power, but they do not address cooling or airflow problems.
* Rail kits are used for mounting servers and are unrelated to cooling efficiency.

NEW QUESTION: 155
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: (SHOW ANSWER)
* 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: 156
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:
* 500GB, 10,000rpm
* 600GB, 10,000rpm
* 500GB, 7,200rpm
* 500GB, 10,000rpm
* 600GB, 15,000rpm
* 600GB, 10,000rpm
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: (SHOW ANSWER)
The goal is to achieve2TB total storage,high performance, andsupport for one drive failure. Using RAID 5 or RAID 10 can provide redundancy while maximizing performance.
* 1, 2, 4, 5, and 6 (Answer C):This selection includes the highest-capacity and highest-performance drives (600GB and 500GB at high RPM speeds). Using these drives will provide the necessary capacity (500GB + 600GB + 500GB + 600GB + 600GB = 2.8TB) and performance with one drive redundancy (RAID 5 or 10).
* Other options (A, B, D):These combinations either lack the necessary capacity or mix slower drives (7,200rpm), reducing overall performance.

CompTIA Server+ Reference:This topic is covered underSK0-005 Objective 1.5: Explain storage technologies and RAID configurations.

NEW QUESTION: 157
Which of the following are measures that should be taken when a data breach occurs? (Select TWO).
A. Restore the data from backup.
B. Disclose the incident.
C. Disable unnecessary ports.
D. Run an antivirus scan.
E. Identify the exploited vulnerability.
F. Move the data to a different location.
Answer: (SHOW ANSWER)
These are two measures that should be taken when a data breach occurs. A data breach is an unauthorized or illegal access to confidential or sensitive data by an internal or external actor. A data breach can result in financial losses, reputational damage, legal liabilities, and regulatory penalties for the affected organization.
Disclosing the incident is a measure that involves informing the relevant stakeholders, such as customers, employees, partners, regulators, and law enforcement, about the nature, scope, and impact of the data breach.
Disclosing the incident can help to mitigate the negative consequences of the data breach, comply with legal obligations, and restore trust and confidence. Identifying the exploited vulnerability is a measure that involves investigating and analyzing the root cause and source of the data breach. Identifying the exploited vulnerability can help to prevent further data loss, remediate the security gaps, and improve the security posture of the organization. Restoring the data from backup is a measure that involves recovering the lost or corrupted data from a secondary storage device or location. However, this does not address the underlying issue of how the data breach occurred or prevent future breaches. Disabling unnecessary ports is a measure that involves closing or blocking network communication endpoints that are not required for legitimate purposes. However, this does not address how the data breach occurred or what vulnerability was exploited.
Running an antivirus scan is a measure that involves detecting and removing malicious software from a system or network. However, this does not address how the data breach occurred or what vulnerability was exploited. Moving the data to a different location is a measure that involves transferring the data to another storage device or location that may be more secure or less accessible. However, this does not address how the data breach occurred or what vulnerability was exploited. References: https://www.howtogeek.com/428483 /what-is-end-to-end-encryption-and-why-does-it-matter/ https://www.howtogeek.com/202794/what-is-the- difference-between-127.0.0.1-and-0.0.0.0/ https://www.howtogeek.com/443611/how-to-encrypt-your-macs- system-drive-removable-devices-and-individual-files/

NEW QUESTION: 158

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: 159

An administrator notices a server is offline. Upon checking the console, the administrator discovers the server is stuck at:

Configuring Memory.....

After a reboot, the server still exhibits the same behavior. The administrator is able to log in to the OOB remote management but is unable to log in to the server. Which of the following is the most likely cause of this issue?

A. A DIMM has failed

B. The VRAM is insufficient

C. The RAID cache has failed

D. The BIOS needs to be updated

Answer: A (LEAVE A REPLY)

The error message "Configuring Memory..." and the fact that the server is stuck at this point strongly suggest thata DIMM (memory module) has failed. Memory issues are commonly diagnosed when servers hang during the memory configuration phase of boot.

* DIMM failure (Answer A):When a memory module fails, the server can get stuck at the memory initialization process during boot.
* VRAM insufficiency (Option B):VRAM (video memory) issues would typically cause display-related errors, not memory configuration issues.

* RAID cache failure (Option C):RAID cache issues would lead to storage errors but not prevent the system from configuring memory.
* BIOS update (Option D):While BIOS issues can cause boot failures, the error message suggests a memory-specific issue.
CompTIA Server+ Reference:This topic relates toSK0-005 Objective 3.3: Diagnose hardware problems.

NEW QUESTION: 160
A technician runs top on a dual-core server and notes the following conditions:
top -- 14:32:27, 364 days, 14 usersload average 60.5 12.4 13.6
Which of the following actions should the administrator take?
A. Schedule a mandatory reboot of the server
B. Wait for the load average to come back down on its own
C. Identify the runaway process or processes
D. Request that users log off the server
Answer: C (LEAVE A REPLY)
The administrator should identify the runaway process or processes that are causing high load average on the server. Load average is a metric that indicates how many processes are either running on or waiting for the CPU at any given time. A high load average means that there are more processes than available CPU cores, resulting in poor performance and slow response time. A runaway process is a process that consumes excessive CPU resources without terminating or releasing them. A runaway process can be caused by various factors, such as programming errors, infinite loops, memory leaks, etc. To identify a runaway process, the administrator can use tools such as top, ps, or htop to monitor CPU usage and process status. To stop a runaway process, the administrator can use commands such as kill, pkill, or killall to send signals to terminate it.

NEW QUESTION: 161
Which of the following should a technician verify first before decommissioning and wiping a file server?
A. The media destruction method
B. The recycling policy
C. Asset management documentation
D. Document retention policy
Answer: C (LEAVE A REPLY)
Before decommissioning and wiping a file server, it's crucial to verify the asset management documentation.
This documentation provides detailed records of the server's lifecycle, including procurement, usage, maintenance, and decommissioning information. Ensuring that asset management documentation is up-to-date and accurate is essential before proceeding with the server's decommissioning to maintain proper inventory control, comply with regulatory and organizational policies, and facilitate any potential audits. While the media destruction method, recycling policy, and document retention policy

are important considerations in the decommissioning process, verifying asset management documentation is the first step to ensure the server is correctly identified and accounted for in the organization's asset registry.

NEW QUESTION: 162
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: 163
Which of the following types of physical security controls would most likely be a target of a social engineering attack?
A. A security guard
B. An access control vestibule
C. Perimeter fencing
D. Biometric locks
E. Bollards
Answer: A (LEAVE A REPLY)
Asecurity guardis a human element in physical security, making them susceptible tosocial engineering attacks. Social engineering exploits human behavior, and a guard can be tricked into allowing unauthorized access through persuasion, manipulation, or deception.
* Security guard (Answer A):Human elements are the most vulnerable to social engineering techniques like impersonation or manipulation.
* Access control vestibule (Option B):This is a physical security barrier, which is harder to exploit through social engineering.
* Perimeter fencing (Option C):This is a static physical barrier, not susceptible to social engineering.

* Biometric locks (Option D):These rely on biological data and are not susceptible to social engineering in the same way a human would be.
* Bollards (Option E):Physical barriers that are not vulnerable to social engineering.
CompTIA Server+ Reference:This topic relates toSK0-005 Objective 4.4: Implement physical security controls.

NEW QUESTION: 164
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 is blocking the ICMP (Internet Control Message Protocol) packets that ping uses to test the connectivity. References:
https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives (Objective 2.2)

NEW QUESTION: 165
An administrator is configuring a server to communicate with a new storage array. To do so, the administrator enters the WWPN of the new array in the server's storage configuration. Which of the following technologies is the new connection using?
A. iSCSI
B. eSATA
C. NFS
D. FcoE
Answer: A (LEAVE A REPLY)
Reference:https://docs.oracle.com/cd/E26996_01/E18549/html/BABHBFHA.html

NEW QUESTION: 166

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: 167

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: 168
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: 169
Hackers recently targeted a company with an attack that resulted in a system breach, which compromised the organization's dat a. Because of the system breach, the administrator had to bypass normal change management procedures. Which of the following change management activities was necessary?
A. Cancelled change request
B. Change request postponement
C. Emergency change request
D. Privilege change request
E. User permission change request
Answer: C (LEAVE A REPLY)
An emergency change request is a type of change management activity that is used to address urgent issues that pose a significant risk to the organization, such as a system breach. An emergency change request requires immediate action and approval, and it may bypass some of the normal change management procedures, such as testing, documentation, or stakeholder communication12.
References = 1: Change Management Plans: A Definitive Guide - Indeed(https://www.indeed.com/career-advice/career-development/change-management-activities) 2:

The 10 Best Change Management Activities - Connecteam(https://connecteam.com/top-10-change-management-activities/)

NEW QUESTION: 170
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: (SHOW ANSWER)
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: 171
A technician is attempting to update a server's firmware. After inserting the media for the firmware and restarting the server, the machine starts normally into the OS. Which of the following should the technician do NEXT to install the firmware?
A. Press F8 to enter safe mode
B. Boot from the media
C. Enable HIDS on the server
D. Log in with an administrative account
Answer: B (LEAVE A REPLY)
The technician should boot from the media to install the firmware on the server. Firmware is a type of software that controls the low-level functions of hardware devices, such as BIOS (Basic Input/Output System), RAID controllers, network cards, etc. Firmware updates are often provided by hardware manufacturers to fix bugs, improve performance, or add new features to their devices. To install firmware updates on a server, the technician needs to boot from a media device (such as a CD-ROM, DVD-ROM, USB flash drive, etc.) that contains the firmware files and installation program. The technician cannot install firmware updates from within the operating system because firmware updates often require restarting or resetting the hardware devices.

NEW QUESTION: 172
A technician is deploying a single server to monitor and record me security cameras at a remote site, which of the following architecture types should be used to minimize cost?
A. Virtual
B. Blade

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

NEW QUESTION: 173
A server located in an IDF of a paper mill reboots every other day at random times. Which of the following should the technician perform on the server first?
A. Check the power cables
B. Clean the fans.
C. Replace the RAM.
D. Reattach the CPU heat sink
Answer: (SHOW ANSWER)
In a situation where a server reboots randomly, the first step should be to check for any issues with the power supply. Random reboots can often be caused by intermittent power supply issues, which can be due to faulty power cables, loose connections, or problems with the power source itself. This is especially pertinent in environments like a paper mill where dust and debris might affect cable integrity. Since the issue occurs every other day and at random times, it's less likely to be caused by components that would typically fail due to overheating or other gradual issues (like RAM or CPU heat sink problems). Therefore, checking the power cables is the simplest and most direct first step to troubleshoot the issue.

NEW QUESTION: 174
A junior administrator reported that the website used for anti-malware updates is not working. The senior administrator then discovered all requests to the anti-malware site are being redirected to a malicious site.

Which of the following tools should the senior administrator check first to identify the potential cause of the issue?

A. Data loss prevention

B. File integrity monitor

C. Port scanner

D. Sniffer

Answer: (SHOW ANSWER)

A sniffer (also known as a packet analyzer) is a tool that captures and inspects data packets traveling across the network. In this case, using a sniffer would help identify suspicious or malicious redirection of traffic, possibly caused by a man-in-the-middle attack, DNS hijacking, or malware.

* Sniffer (Answer D): This tool will allow the senior administrator to inspect the network traffic and identify if and how requests to the anti-malware website are being intercepted or redirected.

* Data loss prevention (Option A): DLP tools focus on preventing data leakage rather than analyzing traffic redirection.

* File integrity monitor (Option B): This checks for unauthorized changes to files, which may not directly address network traffic redirection.

* Port scanner (Option C): A port scanner would only identify open ports on devices, which is unrelated to the redirection issue.

CompTIA Server+ Reference:This topic is addressed under SK0-005 Objective 4.2: Explain server roles and their purposes.

NEW QUESTION: 175

An administrator is receiving reports that users in a remote office are unable to log in to the domain. The network appears to be up between the sites, which are in different states. Which of the following is the most likely cause of the issue?

A. The user accounts are locked out

B. The NTP on the client side is misconfigured

C. MFA is not working

D. The wrong time zone was set in the remote office

Answer: B (LEAVE A REPLY)

A misconfiguredNTP (Network Time Protocol)on the client side can cause authentication issues because Active Directory relies on accurate time synchronization between clients and domain controllers for security purposes. If the clocks are out of sync, even by a few minutes, it can prevent users from authenticating to the domain.

* NTP misconfiguration (Answer B):If the client machines have incorrect time settings, it can disrupt Kerberos-based authentication, which is time-sensitive.

* Locked user accounts (Option A):While it can prevent login, it would affect individual users rather than a whole office.

* MFA (Option C):Multi-factor authentication not working would typically cause a login issue but is less likely across an entire remote office.

* Wrong time zone (Option D):While incorrect time zones can cause confusion, they usually don't prevent logins as long as the NTP server synchronizes the actual time correctly.
CompTIA Server+ Reference:This topic is covered underSK0-005 Objective 2.4: Troubleshoot common server problems.

NEW QUESTION: 176
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: 177
A systems administrator is attempting to install a package on a server. After downloading the package from the internet and trying to launch it, the installation is blocked by the antivirus on the server.
Which of the following must be completed before launching the installation package again?
A. Creating an exclusion to the antivirus for the application
B. Disabling real-time scanning by the antivirus
C. Validating the checksum for the downloaded installation package
D. Checking for corruption of the downloaded installation package
Answer: C (LEAVE A REPLY)
A checksum is a value that is calculated from a data set to verify its integrity and authenticity. A checksum can be used to compare a downloaded installation package with the original source to ensure that the package has not been corrupted or tampered with during the download or transmission process. If the checksums match, then the package is safe to install. If the checksums do not match, then the package may be infected with malware or contain errors that could cause installation problems. Therefore, validating the checksum for the downloaded installation package is a necessary step before launching the installation again12
1: CompTIA Server+ Certification Exam Objectives 2: How to Verify File Integrity Using Checksums on Linux

NEW QUESTION: 178
A large number of connections to port 80 is discovered while reviewing the log files on a server. The server is not functioning as a web server. Which of the following represent the BEST immediate actions to prevent unauthorized server access? (Choose two.)
A. Audit all group privileges and permissions

B. Run a checksum tool against all the files on the server
C. Stop all unneeded services and block the ports on the firewall
D. Initialize a port scan on the server to identify open ports
E. Enable port forwarding on port 80
F. Install a NIDS on the server to prevent network intrusions
Answer: (SHOW ANSWER)
The best immediate actions to prevent unauthorized server access are to stop all unneeded services and block the ports on the firewall. Stopping unneeded services reduces the attack surface of the server by eliminating potential entry points for attackers. For example, if the server is not functioning as a web server, there is no need to run a web service on port 80. Blocking ports on the firewall prevents unauthorized network traffic from reaching the server. For example, if port 80 is not needed for any legitimate purpose, it can be blocked on the firewall to deny any connection attempts on that port.

NEW QUESTION: 179
Which of the following supports virtualization?
A. Type 1 hypervisor
B. Bare-metal installation
C. Server-level redundancy
D. Active-active load balancing
Answer: A (LEAVE A REPLY)
A Type 1 hypervisor (also known as a bare-metal hypervisor) is installed directly on the hardware and is designed to manage multiple virtual machines. It is the most common type of hypervisor used in virtualization environments.
* Type 1 hypervisor (Answer A): This is a core technology that enables virtualization by running virtual machines directly on the physical hardware.
* Bare-metal installation (Option B): Refers to installing an OS or hypervisor directly on hardware, but doesn't inherently support virtualization unless it's a hypervisor.
* Server-level redundancy (Option C): This provides fault tolerance but is not related to virtualization.
* Active-active load balancing (Option D): Refers to distributing workloads across multiple servers, not directly tied to virtualization.
CompTIA Server+ Reference:This topic is covered under SK0-005 Objective 1.3: Explain virtualization concepts.

NEW QUESTION: 180
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: 181
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: (SHOW ANSWER)
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: 182
A Linux server was recently updated. Now, the server stops during the boot process with a blank screen and an £s> prompt. When of the following is the MOST likely cause of this issue?
A. The system is booting to a USB flash drive
B. The UEFI boot was interrupted by a missing Linux boot file
C. The BIOS could not find a bootable hard disk
D. The BIOS firmware needs to be upgraded
Answer: (SHOW ANSWER)
The most likely cause of this issue is that the UEFI boot was interrupted by a missing Linux boot file, such as grub.cfg or vmlinuz, which are essential for loading the Linux kernel and booting the system. The £s> prompt indicates that the system entered into UEFI Shell mode, which is a command-line interface for troubleshooting UEFI boot issues. The administrator can use UEFI Shell commands to locate and restore the missing boot file or change the boot order. Verified References: [UEFI Shell Guide]

NEW QUESTION: 183
Which of the following security risks provides unauthorized access to an application?
A. Backdoor
B. Data corruption
C. Insider threat
D. Social engineering
Answer: A (LEAVE A REPLY)
A backdoor is a security risk that provides unauthorized access to an application. A backdoor is a hidden or undocumented way of bypassing the normal authentication or encryption mechanisms of an application, allowing an attacker to gain remote access, execute commands, or steal data. A backdoor can be created intentionally by the developer, maliciously by an attacker, or unintentionally by a programming error. References: CompTIA Server+ Certification Exam Objectives, Domain 5.0: Security, Objective 5.2:
Given a scenario, apply logical access control methods.

NEW QUESTION: 184
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: 185
A snapshot is a feature that can be used in hypervisors to:
A. roll back firmware updates.
B. restore to a previous version.
C. roll back application drivers.
D. perform a backup restore.
Answer: B (LEAVE A REPLY)
A snapshot is a feature that can be used in hypervisors to restore to a previous version. A snapshot is a point-in-time copy of a virtual machine (VM) that captures the state and data of the VM at a specific moment. A snapshot can be created instantly and with minimal overhead, as it only stores the changes made to the VM after the snapshot was taken. A snapshot can be used to restore the VM to its previous state in case of data loss or corruption.

NEW QUESTION: 186
Which of the following describes the concept of allocating more resources than what is available on a hypervisor?
A. Direct access
B. Overprovisioning
C. Link aggregation
D. Component redundancy
E. Scalability
Answer: B (LEAVE A REPLY)
Overprovisioning: Involves allocating more virtual resources (e.g., CPU, RAM, storage) to virtual machines than the total physical resources available on a hypervisor. The idea is for resources to be dynamically shared, assuming not all VMs will demand their maximum allocation simultaneously.
Direct Access: This usually refers to technologies like RDMA (Remote Direct Memory Access) that allow for very low-latency, direct access to the memory of another computer over a network.
Link Aggregation: The practice of combining multiple physical network links to create a single logical link with increased bandwidth.
Component Redundancy: Refers to having multiple hardware components (e.g., power supplies, hard drives) to provide fault tolerance.
Scalability: The ability of a system to adapt and handle increased workloads by adding resources.
References:
CompTIA Server+ Objectives (Exam codes SK0-004 or SK0-005): Review the sections on virtualization concepts.

Virtualization Technology Documentation: Refer to documentation for popular hypervisors like VMware vSphere, Microsoft Hyper-V, or open-source solutions.

NEW QUESTION: 187
After configuring IP networking on a newly commissioned server, a server administrator installs a straight- through network cable from the patch panel to the switch. The administrator then returns to the server to test network connectivity using the ping command. The partial output of the ping and ipconfig commands are displayed below:

```
ipconfig/all

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

Pinging 192.168.1.2 with 32 bytes of data:

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


The administrator returns to the switch and notices an amber link light on the port where the server is connected. Which of the following is the MOST likely reason for the lack of network connectivity?
A. Network port security
B. An improper VLAN configuration
C. A misconfigured DHCP server
D. A misconfigured NIC on the server
Answer: D (LEAVE A REPLY)
A misconfigured NIC on the server is the most likely reason for the lack of network connectivity. The output of the ping command shows that the server is unable to reach its default gateway (10.0.0.1) or any other IP address on the network. The output of the ipconfig command shows that the server has a valid IP address (10.0.0.10) and subnet mask (255.255.255.0) but no default gateway configured. This indicates that there is a problem with the NIC settings on the server, such as an incorrect IP address, subnet mask, default gateway, DNS server, etc. A misconfigured NIC can also cause an amber link light on the switch port, which indicates a speed or duplex mismatch between the NIC and the switch.

NEW QUESTION: 188
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: 189
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: 190
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: C (LEAVE A REPLY)
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: 191
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: A (LEAVE A REPLY)
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: 192
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: D (LEAVE A REPLY)
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)