CompTIA.SK0-005.v2023-10-07.q117

Exam Code:	SK0-005
Exam Name:	CompTIA Server+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	117
Version:	v2023-10-07
# of views:	3848
# of Questions views:	4436
https://www.dumpsfiles.com/files/CompTIA/SK0-005/CompTIA.SK0-005.v2023-10-07.q117	

NEW QUESTION: 1
A server technician is troubleshooting an issue regarding users who are not able to access a reporting server. The reporting server has a static IP address and is connected to a Windows domain. The technician attempts steps to narrow down the issue:
- Pings the hostname but is not successful
- Pings the IP address and is successful
- Verifies the IP and DNS settings on the NIC card are okay
Which of the following should the technician do NEXT?
A. Perform an ipconfig on the host to verify the IP configurations.
B. Update the DNS configuration on the host NIC card to localhost for lookups.
C. Reboot the computer to apply security updates to the system.
D. Verify the DNS A record for the hostname of the server.
E. Perform a tracert to the hostname and IP address.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 2
A company is reviewing options for its current disaster recovery plan and potential changes to it. The security team will not allow customer data to egress to non-company equipment, and the company has requested recovery in the shortest possible time. Which of the following will BEST meet these goals?
A. A warm site
B. A hot site
C. Cloud recovery
D. A cold site
Answer: B (LEAVE A REPLY)
Explanation
A hot site is a type of disaster recovery site that has all the equipment and data ready to resume operations as soon as possible after a disaster. A hot site is usually located in a different geographic area than the primary site and has redundant power, cooling, network, and security systems. A hot site is best for the company that wants to recover in the shortest possible time and does not want customer data to

egress to non-company equipment. A warm site is a type of disaster recovery site that has some equipment and data ready, but requires some configuration and restoration before resuming operations. A cold site is a type of disaster recovery site that has only basic infrastructure and space available, but requires significant setup and installation before resuming operations. Cloud recovery is a type of disaster recovery service that uses cloud-based resources and platforms to store backups and restore data and applications after a disaster. References:
https://www.techopedia.com/definition/11172/hot-site
https://www.techopedia.com/definition/11173/warm-site
https://www.techopedia.com/definition/11174/cold-site
https://www.techopedia.com/definition/29836/cloud-recovery

NEW QUESTION: 3
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. volume is formatted as MBR
B. volume is formatted as GPT
C. hardware is UEFI compliant
D. volume is spanned across multiple physical disk drives
Answer: C (LEAVE A REPLY)

NEW QUESTION: 4
A systems administrator is investigating a server with a RAID array that will not boot into the OS. The administrator notices all the hard drives are reporting to be offline. The administrator checks the RAID controller and verifies the configuration is correct. The administrator then replaces one of the drives with a known-good drive, but it appears to be unavailable as well. Next, the administrator takes a drive out of the server and places it in a spare server, and the drive is available and functional. Which of the following is MOST likely causing the issue?
A. The kernel is corrupt.
B. The backplane has failed.
C. The drives need to be reseated.
D. Resources are misallocated.
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Which of the following licenses would MOST likely include vendor assistance?
A. Open-source
B. Version compatibility
C. Subscription
D. Maintenance and support
Answer: D (LEAVE A REPLY)
Maintenance and support is a type of license that would most likely include vendor assistance. Maintenance and support is a contract that defines the level and scope of service and assistance that a vendor provides to a customer for using their software product. Maintenance and support may include technical support, bug fixes, patches, updates, upgrades, documentation, training, and other benefits.

Maintenance and support licenses usually have an annual fee based on the number of users or devices covered by the contract. Open-source is a type of license that allows free access to the source code and modification and distribution of the software product, but does not guarantee vendor assistance. Version compatibility is not a type of license, but a feature that ensures software products can work with different versions of operating systems or other software products. Subscription is a type of license that allows access to software products for a limited period of time based on recurring payments, but does not necessarily include vendor assistance. Reference: https://www.techopedia.com/definition/1440/software-licensing https://www.techopedia.com/definition/1032/business-impact-analysis-bia

NEW QUESTION: 6
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. 255.255.255.128
B. 255.255.255.0
C. 255.255.255.224
D. 255.255.255.252
Answer: (SHOW ANSWER)

NEW QUESTION: 7
A technician has received tickets responding a server is responding slowly during business hours. Which of the following should the technician implement so the team will be informed of this behavior in real time?
A. Log rotation
B. Alerts
C. Reports
D. Log stopping
Answer: B (LEAVE A REPLY)
Explanation
Alerts are notifications that inform the technician or the team of any issues or events that occur on a server or a network. Alerts can be configured to trigger based on certain thresholds, such as CPU usage, disk space, memory utilization, or response time. Alerts can help the technician monitor and troubleshoot the server performance in real time. Verified References: [Alerts], [Server performance]

NEW QUESTION: 8
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. Failover all VMs.
D. Set the cluster to active-active.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 9
A server shut down after an extended power outage. When power was restored, the system failed to start. A few seconds into booting, the Num Lock, Scroll Lock, and Caps Lock LEDs flashed several times, and the system stopped. Which of the following is the MOST likely cause of the issue?

A. The keyboard is defective and needs to be replaced.
B. The system failed before the display card initialized.
C. The power supply is faulty and is shutting down the system.
D. The NIC has failed, and the system cannot make a network connection.
Answer: (SHOW ANSWER)
Explanation
This is the most likely cause of the issue because the keyboard LED flash indicates a POST error code. If the display card is not initialized, the system cannot show any error messages on the screen and will stop booting.
References: https://www.computerhope.com/beep.htm#04

NEW QUESTION: 10
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: (SHOW ANSWER)
Explanation
This is the most likely licensing type that will be used because volume licensing allows a single license key to be used for multiple installations of a software product. Volume licensing is typically used by organizations that need to deploy software to a large number of devices or users. References:
https://www.microsoft.com/en-us/licensing/licensing-programs/volume-licensing-programs

NEW QUESTION: 11
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,B (LEAVE A REPLY)
Full Slow backup, fast restore.
Full+Incremental Fast backup, slow restore (compared to Full+Differential).
Full+Differential Slow backup, fast restore (compared to Full+Incremental).

NEW QUESTION: 12

A technician is able to copy a Me to a temporary folder on another partition but is unable to copy it to a network share or a USB flash drive. Which of the following is MOST likely preventing the file from being copied to certain locations?

A. An ACL

B. Antivirus

C. DLP

D. A firewall

Answer: C (LEAVE A REPLY)

Explanation

DLP (Data Loss Prevention) is a security measure that prevents unauthorized copying, transferring, or leaking of sensitive data from a server or a network. It can block or alert the user when they try to copy a file to certain locations, such as a network share or a USB flash drive, based on predefined policies and rules. Verified References: [DLP], [Data loss]

NEW QUESTION: 13

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. eSATA

B. FcoE

C. iSCSI

D. NFS

Answer: (SHOW ANSWER)

NEW QUESTION: 14

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

A. 21

B. 22

C. 23

D. 53

E. 443

F. 636

Answer: (SHOW ANSWER)

Explanation

The administrator should only allow secure traffic and DNS inquiries on the server, which means that only ports 22, 53, and 443 should be open. Port 22 is used for SSH (Secure Shell), which is a protocol that allows secure remote login and command execution over a network connection using a command-line interface (CLI).

Port 53 is used for DNS (Domain Name System), which is a service that translates domain names into IP addresses and vice versa. Port 443 is used for HTTPS (Hypertext Transfer Protocol Secure), which is a secure version of HTTP that encrypts the data exchanged between a web browser and a web server.

NEW QUESTION: 15

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

A. Restore the server from a snapshot.

B. Restore the server from backup.

C. Swap the drive and initialize the disk.

D. Swap the drive and initialize the array.

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 16

An administrator discovers a Bash script file has the following permissions set in octal notation;

777

Which of the following is the MOST appropriate command to ensure only the root user can modify and execute the script?

A. chmod go-rw>:

B. chmod u=rwx

C. chmod u+wx

D. chmod g-rwx

Answer: A (LEAVE A REPLY)

chmod is a command-line tool that changes the permissions of files and directories in Linux and Unix systems. chmod go-rwx means to remove read, write, and execute permissions for group and other users from a file or directory. This can ensure only the root user can modify and execute the script, since root user has full access to all files and directories regardless of their permissions. Reference: https://linux.die.net/man/1/chmod

NEW QUESTION: 17

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

NEW QUESTION: 18
A systems administrator is investigating a server with a RAID array that will not boot into the OS. The administrator notices all the hard drives are reporting to be offline. The administrator checks the RAID controller and verifies the configuration is correct. The administrator then replaces one of the drives with a known-good drive, but it appears to be unavailable as well. Next, the administrator takes a drive out of the server and places it in a spare server, and the drive is available and functional. Which of the following is MOST likely causing the issue?
A. The kernel is corrupt.
B. Resources are misallocated.
C. The backplane has failed.
D. The drives need to be reseated.
Answer: C (LEAVE A REPLY)
The backplane is a circuit board that connects multiple hard drives to a RAID controller and provides power and data transfer between them. If the backplane has failed, it may cause all the hard drives to be offline and prevent the server from booting into the OS. The fact that replacing one of the drives with a known-good drive did not work, and that taking a drive out of the server and placing it in a spare server made it functional, suggests that the problem is not with the drives themselves but with the backplane. A corrupt kernel (A) would not affect the status of the hard drives, as it is a software component of the OS. Resource misallocation (B) would not cause all the hard drives to be offline, as it is a configuration issue that affects how resources are assigned to processes or applications. Reseating the drives (D) would not help, as it would not fix a faulty backplane. Reference: https://www.dell.com/support/kbdoc/en-us/000130114/how-to-troubleshoot-a-faulty-backplane

NEW QUESTION: 19
A server room with many racks of servers is managed remotely with occasional on-site support.
Which of the following would be the MOST cost-effective option to administer and troubleshoot network problems locally on the servers?
A. KVM
B. IP KVM
C. Crash cart
D. Management port
Answer: (SHOW ANSWER)

NEW QUESTION: 20
Which of the following tools will analyze network logs in real time to report on suspicious log events?
A. Syslog
B. DLP
C. SIEM

D. HIPS
Answer: C (LEAVE A REPLY)
Security information and event management (SIEM) software provides a centralized repository for logs, audit events, and security device alerts to detect and notify admins of suspicious activity.
For example, attackers can enable a backdoor on a compromised device that will provide them with undetected access for long periods of time; this problem is often solved by applying patches, but SIEM solutions may detect repeated abnormal login times to a server.

NEW QUESTION: 21
Users ate experiencing issues when trying to access resources on multiple servers. The servers are virtual and run on an ESX server. A systems administrator is investigating but is unable to connect to any of the virtual servers. When the administrator connects to the host, a purple screen with while letters appears. Which of the following troubleshooting steps should the administrator perform FIRST?
A. Check the power supplies
B. Review the log files.
C. Reinstall the ESX server.
D. Reseat the processors.
Answer: (SHOW ANSWER)
A purple screen of death (PSOD) is a diagnostic screen with white type on a purple background that's displayed when the VMkernel of a VMware ESXi host experiences a critical error, becomes inoperative and terminates any virtual machines (VMs) that are running.
The other answers could be the issue but are a bit drastic and definitely not something you do FIRST.
https://www.techtarget.com/searchvmware/definition/Purple-Screen-of-Death-PSOD

NEW QUESTION: 22
A technician is configuring a new server. After using the RAID setup program to create a new RAID array, the OS installer is not able to find storage on which to write. Which of the following is the MOST likely reason this may happen?
A. The OS is not supported on the server hardware.
B. The technician did not provide drivers to support the controller.
C. The technician did not enable UEFI in the server BIOS.
D. The technician did not allow time for the new array to initialize.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
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 hot site
B. Cloud recovery
C. A warm site
D. A cold site
Answer: A (LEAVE A REPLY)

NEW QUESTION: 24

A server administrator is swapping out the GPU card inside a server. Which of the following actions should the administrator take FIRST?
A. Ensure the GPU meets HCL guidelines.
B. Inspect the GPU that is being installed.
C. Shut down the server.
D. Disconnect the power from the rack.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 25
Which of the following steps in the troubleshooting theory should be performed after a solution has been implemented? (Choose two.)
A. Perform a root cause analysis
B. Develop a plan of action
C. Document the findings
D. Escalate the issue
E. Scope the issue
F. Notify the users
Answer: A,C (LEAVE A REPLY)
The following list represents the basic steps in a troubleshooting methodology:
Identify the problem
Determine the scope of the problem
Establish a theory of probable cause/question the obvious
Test the theory to determine the cause
Establish a plan of action
Implement the solution or escalate the issue
Verify full system functionality
Implement preventive measures
Perform a root cause analysis
Document findings, actions, and outcomes throughout the process.

NEW QUESTION: 26
A server room with many racks of servers is managed remotely with occasional on-site support. Which of the following would be the MOST cost-effective option to administer and troubleshoot network problems locally on the servers?
A. Management port
B. Crash cart
C. IP KVM
D. KVM
Answer: C (LEAVE A REPLY)
Explanation
An IP KVM (keyboard, video, mouse) is a device that allows remote access and control of multiple servers over a network using a web browser or a client software. An IP KVM is a cost-effective option to administer and troubleshoot network problems locally on the servers, as it eliminates the need for physical presence or dedicated hardware for each server. A management port (A) is a network interface that is used for out-of-band management of network devices, such as routers or switches. A management port does not provide local access to

servers. A crash cart (B) is a mobile unit that contains a monitor, keyboard, mouse, and other tools for troubleshooting servers in a data center. A crash cart requires physical access to each server and may not be cost-effective for many racks of servers. A KVM (D) is a device that allows switching between multiple servers using a single keyboard, video, and mouse. A KVM does not provide remote access over a network and requires physical connection to each server. References:
https://www.enterprisestorageforum.com/management/best-data-storage-solutions-and-software-2021/
https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/cloud-storage-vs-on-premises

NEW QUESTION: 27
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. Upgrade the hard disk to SSD.
B. Perform quarterly backups.
C. Perform scheduled chkdsk tests.
D. Purchase matching hardware and clone the disk.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 28
A server technician installs a new NIC on a server and configures the NIC for IP connectivity. The technician then tests the connection using the pingcommand. Given the following partial output of the pingand ipconfigcommands:

```
ipconfig /all

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

pinging 192.168.1.1 with 32 bytes of data:

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


Which of the following caused the issue?
A. DHCP misconfiguration
B. Incorrect routing table
C. Duplicate IP address
D. Incorrect default gateway
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29
An administrator is configuring a host-based firewall tor a server. The server needs to allow SSH, FTP, and LDAP traffic. Which of the following ports must be configured so this traffic will be allowed? (Select THREE).
A. 21
B. 22
C. 53
D. 67
E. 69
F. 110
G. 123
H. 389
Answer: A,B,H (LEAVE A REPLY)
These are the port numbers that must be configured on a host-based firewall for a server that needs to allow SSH, FTP, and LDAP traffic. A port number is a numerical identifier that specifies a communication endpoint for a network protocol or an application. A host-based firewall is a software tool that monitors and controls incoming and outgoing network traffic on a single host based on predefined rules. SSH (Secure Shell) is a protocol that allows secure remote access and file transfer over an encrypted connection. The default port number for SSH is 22. FTP (File Transfer Protocol) is a protocol that allows transferring files between hosts over a network connection. The default port number for FTP is 21. LDAP (Lightweight Directory Access Protocol) is a protocol that allows accessing and managing directory services over a network connection. The default port number for LDAP is 389. Reference: https://www.howtogeek.com/190014/virtualization-basics-understanding-techniques-and-fundamentals/ https://www.howtogeek.com/220152/what-is-the-difference-between-127.0.0.1-and-0.0.0.0/ https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-it-matter/

NEW QUESTION: 30
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)
RAID 6 Disk Striping with Double Parity
The RAID 6 design distributes data across a minimum of four HDDs the same way that RAID 0 and RAID 5 do, but it also distributes parity information across two disks. The result is that a RAID 6 array can recover data even with the failure of two HDDs. Reads are quick, like RAID 5, but writes are slower due to the duplication of the parity data. It is a good general solution as long as the performance hit on write tasks is not a problem for your environment.
RAID 6 requires a minimum of four HDDs.

NEW QUESTION: 31

A critical server has stopped responding in a distant location where there are no remote technicians to check the condition of the server. Which of the following can assist in checking the condition of the server? (Choose two.)

A. Remote desktop protocol

B. iDRAC

C. SSH

D. ILO

E. VNC

F. Bootstrap protocol

Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 32

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. mount -a

B. echo /newdisk >> /etc/fstab

C. net use /newdisk

D. mount -o remount, rw /newdisk

Answer: D (LEAVE A REPLY)

NEW QUESTION: 33

A server that recently received hardware upgrades has begun to experience random BSOD conditions. Which of the following are likely causes of the issue? (Choose two.)

A. Faulty memory

B. Data partition error

C. Incorrectly seated memory

D. Incompatible disk speed

E. Uninitialized disk

F. Overallocated memory

Answer: A,C (LEAVE A REPLY)

Faulty memory and incorrectly seated memory are likely causes of the random BSOD conditions on the server. Memory is one of the most common hardware components that can cause BSOD (Blue Screen of Death) errors on Windows systems. BSOD errors occur when the system encounters a fatal error that prevents it from continuing to operate normally. Memory errors can be caused by faulty or incompatible memory modules that have physical defects or manufacturing flaws. Memory errors can also be caused by incorrectly seated memory

modules that are not properly inserted or locked into the memory slots on the motherboard. This can result in loose or poor connections between the memory modules and the motherboard.

NEW QUESTION: 34
Which of the following script types uses commands That start with sec-?
A. Batch
B. Bash
C. PowerShell
D. JavaScript
Answer: C (LEAVE A REPLY)
Explanation
PowerShell is a scripting language and a command-line shell that uses commands that start with sec- to perform security-related tasks. For example, sec-edit is a command that edits security policies, sec-logon is a command that manages logon sessions, and sec-policy is a command that applies security templates. Verified References: [PowerShell security commands], [Security policy]

NEW QUESTION: 35
Which of the following encryption methodologies would MOST likely be used to ensure encrypted data cannot be retrieved if a device is stolen?
A. End-to-end encryption
B. Encryption in transit
C. Encryption at rest
D. Public key encryption
Answer: (SHOW ANSWER)
Encryption at rest is a type of encryption methodology that would most likely be used to ensure encrypted data cannot be retrieved if a device is stolen. Encryption at rest is a process of encrypting stored data on a device such as a hard drive, SSD, USB flash drive, or mobile device. This way, if the device is lost or stolen, the data cannot be accessed without the encryption key or password. Encryption at rest can be implemented using software tools such as BitLocker on Windows or FileVault on Mac OS, or hardware features such as self-encrypting drives or Trusted Platform Module chips. End-to-end encryption is a type of encryption methodology that ensures encrypted data cannot be intercepted or modified by third parties during transmission over a network. Encryption in transit is a type of encryption methodology that protects encrypted data while it is moving from one location to another over a network. Public key encryption is a type of encryption algorithm that uses a pair of keys: a public key that can be shared with anyone and a private key that is kept secret by the owner.
Reference: https://www.howtogeek.com/196541/bitlocker-101-what-it-is-how-it-works-and-how-to-use-it/
https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual-files/
https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-it-matter/ https://www.howtogeek.com/195877/what-is-encryption-and-how-does-it-work/

NEW QUESTION: 36
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: (SHOW ANSWER)
Explanation
The technician should configure RAID 6 for this drive array to meet the server specifications. RAID 6 is a type of RAID level that provides fault tolerance and performance enhancement by using striping and dual parity. Striping means dividing data into blocks and distributing them across multiple disks to increase speed and capacity. Parity means calculating and storing extra information that can be used to reconstruct data in case of disk failure. RAID 6 uses two sets of parity information 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.

NEW QUESTION: 37
An administrator is sizing the CPU requirements of a new application. The application requires 12 guest VMs to run concurrently on the host. If each guest requires 500MHz of CPU and the server has two sockets, which of the following CPUs will ensure there are sufficient host CPU resources for this application?
A. 2.5GHz CPU
B. 3.2GHz CPU
C. 2.0GHz CPU
D. 1.6GHz CPU
Answer: B (LEAVE A REPLY)

NEW QUESTION: 38
A server administrator needs to keep a copy of an important fileshare that can be used to restore the share as quickly as possible. Which of the following is the BEST solution?
A. Copy the fileshare to an LTO-4 tape drive
B. Configure a new incremental backup job for the fileshare
C. Create an additional partition and move a copy of the fileshare
D. Create a snapshot of the fileshare
Answer: (SHOW ANSWER)
Explanation
The best solution to keep a copy of an important fileshare that can be used to restore the share as quickly as possible is to create a snapshot of the fileshare. A snapshot is a point-in-time copy of a file system or a volume that captures the state and data of the fileshare at a specific moment. A snapshot can be created instantly and with minimal overhead, as it only stores the changes made to the fileshare after the snapshot was taken. A snapshot can be used to restore the fileshare to its previous state in case of data loss or corruption.

NEW QUESTION: 39
A technician wants to limit disk usage on a server. Which of the following should the technician implement?
A. Partitioning
B. Disk quotas
C. Compression

D. Formatting
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which of the following is typical of software licensing in the cloud?
A. Per socket
B. Perpetual
C. Subscription-based
D. Site-based
Answer: C (LEAVE A REPLY)
Explanation
Cloud software licensing refers to the process of managing and storing software licenses in the cloud. The benefits of cloud software licensing models are vast. The main and most attractive benefit has to do with the ease of use for software vendors and the ability to provide customizable cloud software license management based on customer needs and desires1. Cloud-based licensing gives software developers and vendors the opportunity to deliver software easily and quickly and gives customers full control over their licenses, their analytics, and more1. Cloud based licensing gives software sellers the ability to add subscription models to their roster of services1. Subscription models are one of the most popular forms of licensing today1. Users sign up for a subscription (often based on various options and levels of use, features, etc.) and receive their licenses instantly1. References: 1 Everything You Need to Know about Cloud Licensing | Thales

NEW QUESTION: 41
Which of the following, if properly configured, would prevent a user from installing an OS on a server?
(Select TWO).
A. Administrator password
B. Group Policy Object
C. Root password
D. SELInux
E. Bootloader password
F. BIOS/UEFI password
Answer: (SHOW ANSWER)
Explanation
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: 42
A technician is unable to access a server's package repository internally or externally. Which of the following are the MOST likely reasons?
(Choose two.)

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

NEW QUESTION: 43
Which of the following techniques can be configured on a server for network redundancy?
A. Clustering
B. Vitalizing
C. Cloning
D. Teaming
Answer: D (LEAVE A REPLY)
Teaming is a technique that can be configured on a server for network redundancy. Teaming involves combining two or more network adapters into a single logical unit that acts as one network interface. This way, if one network adapter fails, another one can take over without disrupting network connectivity. Teaming can also improve network performance by load balancing traffic across multiple network adapters. Clustering is a technique that involves grouping two or more servers together to act as one system for high availability and fault tolerance. Virtualizing is a technique that involves creating multiple virtual machines on a single physical server to optimize resource utilization and flexibility. Cloning is a technique that involves creating an exact copy of a server's configuration and data for backup or migration purposes. Reference: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming/nic-teaming https://www.techopedia.com/definition/19588/clustering https://www.techopedia.com/definition/4790/virtualization https://www.techopedia.com/definition/4776/cloning

NEW QUESTION: 44
A user reports that a server is not accessible. A technician sees the following message on the server: PXE server not found. Which of the following should the technician attempt FIRST to resolve the issue?
A. Eject the disk in the CD-ROM and reboot the server.
B. Enter the BIOS and correct the boot sequence on the server.
C. Ensure the network cable is properly connected and reboot the server.
D. Power down the server and reseat the PCI cards.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 45
Which of me following BEST describes a disaster recovery site with a target storage array that receives replication traffic and servers that are only powered on In the event of a disaster?
A. Cloud
B. Cold
C. Hot
D. Warm
Answer: (SHOW ANSWER)
The difference between a hot site and a warm site is that while the hot site provides a mirror of the production data-center and its environment(s), a warm site will contain only servers ready for the installation of production environments.
https://www.seguetech.com/three-stages-disaster-recovery-sites/#

NEW QUESTION: 46
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: 47
The systems administrator received an alert that one of the servers went offline. The systems administrator logged on remotely to the machine using the IPMI connection and noticed the following message upon boot up: No logical volumes present. Press F1 to continue. Which of the following is the BEST step for the systems administrator to take to resolve the issue?
A. Enter the BIOS and enable the disk.
B. Verify the array controller to determine if it is seen by the BIOS.

C. Check the array controller to see if the disks are visible.
D. Resume the server reboot by pressing F1.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 48
Users cannot access a new server by name, but the server does respond to a ping request using its IP address. All the user workstations receive their IP information from a DHCP server. Which of the following would be the best step to perform NEXT?
A. Run the tracert command from a workstation.
B. Correct the missing DHCP scope.
C. Examine the DNS to see if the new server record exists.
D. Update the workstation hosts file.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 49
A recent power Outage caused email services to go down. A sever administrator also received alerts from the datacenter's UPS.
After some investigation, the server administrator learned that each POU was rated at a maximum Of 12A.
INSTRUCTIONS
Ensure power redundancy is implemented throughout each rack and UPS alarms are resolved. Ensure the maximum potential PDU consumption does not exceed 80% or 9.6A).
a. PDU selections must be changed using the pencil icon.
b. VM Hosts 1 and 2 and Mail Relay can be moved between racks.
c. Certain devices contain additional details


Data Center Racks 1 and 2
Show Question
Reset All Answers
PDU A: 13A MAX
Rack 1
PDU B: 6A MAX
Rack Switch 1
VM Host 1
VM Host 2
Mail Relay
SAN
PDU A
PDU A: 5A MAX
Rack 2
PDU B: 0A MAX
Rack Switch 2
Domain Controller
PDU A
dumpsfiles.com
CompTIA.

Answer:

Data Center Racks 1 and 2
Show Question
Reset All Answers
PDU A: 13A MAX
Rack 1
PDU B: 6A MAX
Rack Switch 1
VM Host 1
VM Host 2
Mail Relay
SAN
PDU A
PDU A: 5A MAX
Rack 2
PDU B: 0A MAX
Rack Switch 2
Domain Controller
VM Host 1
Mail Relay
PDU A
dumpsfiles.com
CompTIA.

NEW QUESTION: 50
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. Bridged networking
B. Round robin
C. Network address translation
D. Link aggregation
Answer: B (LEAVE A REPLY)
Explanation

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

NEW QUESTION: 51
Which of the following backup types resets the archive bit each time it is run?
A. Differential
B. Snapshot
C. Incremental
D. Synthic full
Answer: (SHOW ANSWER)
Incremental backup is a type of backup that only backs up the files that have changed since the last backup, whether it was a full or an incremental backup. Incremental backup resets the archive bit each time it is run, which means it clears the flag that indicates whether or not the file has been backed up. Incremental backup can save time and space compared to full backup, but it requires more time and resources to restore data from multiple backups. Reference: https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives (Objective 3.1)

NEW QUESTION: 52
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.

NEW QUESTION: 53
A datacenter in a remote location lost power. The power has since been restored, but one ol the servers has not come back online. After some investigation, the server is found to still be powered off. Which of the following is the BEST method to power on the server remotely?
A. Crash cart
B. Out-of-band console
C. IP KVM
D. RDP
Answer: (SHOW ANSWER)
Out-of-band console is a tool that can be used to command a remote shutdown of a physical Linux server. Out-of-band console is a method of accessing a server's console through a dedicated management port or device that does not rely on the server's operating system or network connection. Out-of-band console can be used to power cycle, reboot, update firmware, monitor performance, and perform other tasks remotely even if the server is unresponsive or offline. Crash cart is a mobile unit that contains a keyboard, monitor, mouse, and other tools that can be used to troubleshoot a server on-site, but it requires physical access to the server. IP KVM (Internet Protocol Keyboard Video Mouse) switch is a hardware device that allows remote access to multiple servers using a web browser or a client software, but it

requires network connectivity and may not work if the SSH connection is lost. RDP (Remote Desktop Protocol) is a protocol that allows remote access to a Windows server's graphical user interface, but it does not work on Linux servers and requires network connectivity. Reference: https://www.techopedia.com/definition/13623/crash-cart https://www.techopedia.com/definition/13624/kvm-switch https://www.techopedia.com/definition/3422/remote-desktop-protocol-rdp

NEW QUESTION: 54
A company wants to deploy software to all users, Out very few of men will be using the software at any one point in time. Which of the following licensing models would be BEST lot the company?
A. Per instance
B. Per concurrent user
C. Per site
D. Per core
Answer: B (LEAVE A REPLY)

NEW QUESTION: 55
A server administrator receives a report that Ann, a new user, is unable to save a file to her home directory on a server. The administrator checks Ann's home directory permissions and discovers the following:
dr-xr-xr-- /home/Ann
Which of the following commands should the administrator use to resolve the issue without granting unnecessary permissions?
A. chmod777/home/Ann
B. chmod666/home/Ann
C. chmod711/home/Ann
D. chmod754/home/Ann
Answer: D (LEAVE A REPLY)
Explanation
The administrator should use the command chmod 754 /home/Ann to resolve the issue without granting unnecessary permissions. The chmod command is used to change the permissions of files and directories on a Linux server. The permissions are represented by three numbers, each ranging from 0 to 7, that correspond to the read , write (w), and execute (x) permissions for the owner, group, and others respectively. The numbers are calculated by adding up the values of each permission: r = 4, w = 2, x = 1. For example, 7 means rwx (4 + 2 + 1), 6 means rw- (4 + 2), 5 means r-x (4 + 1), etc. In this case, Ann's home directory has the permissions dr-xr-xr-, which means that only the owner (d) can read and execute (x) the directory, and the group and others can only read and execute (x) but not write (w) to it. This prevents Ann from saving files to her home directory. To fix this issue, the administrator should grant write permission to the owner by using chmod 754
/home/Ann, which means that the owner can read , write (w), and execute (x) the directory, the group can read and execute (x) but not write (w) to it, and others can only read but not write (w) or execute (x) it.
This way, Ann can save files to her home directory without giving unnecessary permissions to others.

NEW QUESTION: 56
A server technician is installing a new server OS on legacy server hardware. Which of the following should the technician do FIRST to ensure the OS will work as intended?
A. Consult the HCL to ensure everything is supported.

B. Migrate the physical server to a virtual server.
C. Low-level format the hard drives to ensure there is no old data remaining.
D. Make sure the case and the fans are free from dust to ensure proper cooling.
Answer: A (LEAVE A REPLY)
Since this is legacy server hardware it would be important to make sure that it can handle/support a particular O/S before attempting an install. The rest of the answers have little to nothing to do with an install an O/S on legacy hardware.

NEW QUESTION: 57
A server room with many racks of servers is managed remotely with occasional on-site support. Which of the following would be the MOST cost-effective option to administer and troubleshoot network problems locally on the servers?
A. Management port
B. Crash cart
C. IP KVM
D. KVM
Answer: C (LEAVE A REPLY)
An IP KVM (keyboard, video, mouse) is a device that allows remote access and control of multiple servers over a network using a web browser or a client software. An IP KVM is a cost-effective option to administer and troubleshoot network problems locally on the servers, as it eliminates the need for physical presence or dedicated hardware for each server. A management port (A) is a network interface that is used for out-of-band management of network devices, such as routers or switches. A management port does not provide local access to servers. A crash cart (B) is a mobile unit that contains a monitor, keyboard, mouse, and other tools for troubleshooting servers in a data center. A crash cart requires physical access to each server and may not be cost-effective for many racks of servers. A KVM (D) is a device that allows switching between multiple servers using a single keyboard, video, and mouse. A KVM does not provide remote access over a network and requires physical connection to each server. Reference: https://www.enterprisestorageforum.com/management/best-data-storage-solutions-and-software-2021/ https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/cloud-storage-vs-on-premises-servers

NEW QUESTION: 58
A Linux administrator created a script that will run at startup. After successfully writing the script, the administrator received me following output when trying to execute the script:
Bash ./startup,sh:Permission denied
Which of the following commands would BEST resolve the error message?
A. Chmod+x startup.sh
B. Chmod +w startup.sh
C. Chmod 466 startUp,sh
D. Chmod 444 startup.sh
Answer: A (LEAVE A REPLY)

NEW QUESTION: 59
Which of me following should be placed at the top of a Bash script to ensure it can be executed?
A. bash
B. !execute

C. #!
D. @eacho off
Answer: C (LEAVE A REPLY)
#! is the symbol that should be placed at the top of a Bash script to ensure it can be executed. #! is also known as shebang or hashbang. It is a special notation that tells the operating system which interpreter to use to run the script. The shebang is followed by the path to the interpreter, such as /bin/bash for Bash, /bin/python for Python, or /bin/perl for Perl. For example, a Bash script that prints "Hello World" would start with:
#!/bin/bash echo "Hello World"
The shebang must be the first line of the script and must not have any spaces between the # and ! symbols. bash is not a valid shebang by itself, as it does not specify the path to the interpreter. !execute is not a valid shebang at all, as it does not start with #. @echo off is a command that disables the echoing of commands in a batch file on Windows, but it has nothing to do with Bash scripts on Linux.
Reference: https://www.howtogeek.com/67469/the-beginners-guide-to-shell-scripting-the-basics/ https://www.howtogeek.com/435903/what-is-a-shebang-line/

NEW QUESTION: 60
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)
Explanation
A snapshot is a feature that can be used in hypervisors to restore to a previous version. A snapshot is a point-in-time copy of a virtual machine (VM) that captures the state and data of the VM at a specific moment.
A snapshot can be created instantly and with minimal overhead, as it only stores the changes made to the VM after the snapshot was taken. A snapshot can be used to restore the VM to its previous state in case of data loss or corruption.

NEW QUESTION: 61
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)
Explanation
Blanking panels are metal or plastic plates that are installed in the empty spaces of a rack to prevent hot air from recirculating back to the front of the rack. This can improve the airflow and cooling efficiency of the rack and reduce the heat generated by the servers. Verified References: [Blanking panel], [Rack cooling]

NEW QUESTION: 62
A server technician is installing a new server OS on legacy server hardware. Which of the following should the technician do FIRST to ensure the OS will work as intended?
A. Consult the HCL to ensure everything is supported.
B. Low-level format the hard drives to ensure there is no old data remaining.
C. Migrate the physical server to a virtual server.
D. Make sure the case and the fans are free from dust to ensure proper cooling.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 63
An administrator is asked to harden a Linux server after installing the OS. Which of the following should the administrator do FIRST?
A. Set up a personal firewall.
B. Install the latest OS patches.
C. Disable the HIDS.
D. Enable WOL.
Answer: (SHOW ANSWER)

NEW QUESTION: 64
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)
Explanation
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.

NEW QUESTION: 65
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)
Explanation
SIEM is the tool that will analyze network logs in real time to report on suspicious log events. SIEM stands for Security Information and Event Management, which is a software solution that collects, analyzes, and correlates log data from various sources, such as servers, firewalls, routers, antivirus software, etc. SIEM can detect anomalies, patterns, trends, and threats in the log data and generate alerts or reports for security monitoring and incident response. SIEM can also provide historical analysis and compliance reporting for audit purposes.

NEW QUESTION: 66
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. SFTP
B. NFS
C. CIFS
D. FTP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 67
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.

NEW QUESTION: 68
SIMULATION
A recent power outage caused email services to go down. A server administrator also received averts from the datacenter's UPS.
After some investigation, the server administrator learned that each PDU was rated at a maximum of 12A.
Instructions
Ensure power redundancy is implemented throughout each rack and UPS alarms are resolved.
Ensure the maximum potential PDU consumption does not exceed
80% (or 9.6A).
a. PDU selections must be changed using the penal icon.
b. VM Hosts 1 and 2 and Mall Relay can be moved between racks.
c. Certain devices contain additional details.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Rack 1
Rack Switch 1
Mail Relay
SAN
PDU A
PDU B
UPS R1
Rack 2
Rack Switch 2
Domain Controller
VM Host 2
VM Host 1
PDU A
PDU B
UPS R2


PDU A: 13A MAX
Rack 1
PDU B: 6A MAX
PDU A: 5A MAX
Rack 2
PDU B: 0A MAX
Rack Switch 1
Rack Switch 2
VM Host 1
VM Host 2
Mail Relay
SAN
UPS-R1
Shutdown Time (min)
70 min
PDU A
PDU B
UPS R1
PDU B
UPS R2
dumpsfiles.com
CompTIA


PDU A: 13A MAX
Rack 1
PDU B: 6A MAX
PDU A: 5A MAX
Rack 2
PDU B: 0A MAX
Rack Switch 1
Rack Switch 2
VM Host 1
VM Host 2
Mail Relay
SAN
PDU A
PDU B
UPS R1
UPS R2
VM Host 2
Max Amps Consumed Per Power Supply
6
Shutdown Time (min)
20 min
Primary Power Supply
PDU B
Failover Power Supply
PDU B
PDU A
PDU B
Available
Apply
Reset
dumpsfiles.com
CompTIA

Answer:

1. Mailrelay - Keep the mail relay on the existing Rack1 and change the primary power supply to PDU-B and Failover powersupply as PDU B.
2. Move the VM Host 1 and VM Host2 to Rack2.

Assign primary power supply PDU A to VM host1
Assign Failover power supply PDU B to VM host1
Assign primary power supply PDU B to VM host2
Assign Failover power supply PDU A to VM host2

NEW QUESTION: 69

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: C,F (LEAVE A REPLY)
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: 70
An administrator is configuring a new server for use as a database server. It will have two mirrored drives to hold the operating system, and there will be three drive bays remaining for storage Which of the following RAID levels will yield the BEST combination of available space and redundancy?
A. RAID
B. RAID 1
C. RAIDS
D. RAID 10
Answer: D (LEAVE A REPLY)
RAID 10 is the RAID level that will yield the best combination of available space and redundancy when configuring a new server for use as a database server with two mirrored drives for the operating system and three drive bays remaining for storage. RAID 10, also known as RAID 1+0, is a RAID configuration that combines disk mirroring and disk striping to protect data. It requires a minimum of four disks and stripes data across mirrored pairs. As long as one disk in each mirrored pair is functional, data can be retrieved. RAID 10 provides high performance, fault tolerance, and fast recovery, but it reduces storage capacity by half. RAID 0 is a RAID 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 1 is a RAID 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 5 is a RAID 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 or more. Reference: https://www.howtogeek.com/199068/how-to-upgrade-your-existing-hard-drive-in-under-an-hour/ https://www.howtogeek.com/202794/what-is-the-difference-between-127.0.0.1-and-0.0.0.0/

NEW QUESTION: 71
Which of the following describes a configuration i winch both nodes of a redundant system respond to service requests whenever possible?
A. Active-passive
B. Failover
C. Active-active
D. Fallback
Answer: C (LEAVE A REPLY)
Explanation
Active-active is a configuration in which both nodes of a redundant system respond to service requests whenever possible. It can improve the performance, availability, and load balancing of the system by distributing the workload among the nodes. However, it also requires more synchronization and coordination between the nodes to avoid conflicts or errors. Verified References: [Active-active], [Redundant system]

NEW QUESTION: 72
Which of the following licenses would MOST likely include vendor assistance?
A. Version compatibility
B. Subscription
C. Open-source
D. Maintenance and support
Answer: (SHOW ANSWER)

NEW QUESTION: 73
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. Reference:
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: 74
A technician runs top on a dual-core server and notes the following conditions:
top -- 14:32:27, 364 days, 14 users load 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: (SHOW ANSWER)
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: 75
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)
Constant Replication
The primary system replicates data changed data blocks continually. Constant replication is also referred to as "continuous replication." The replication process occurs in the background, permitting users to access the data without interruption.
Constant replication is different than regular backups, where files must be closed to be duplicated.

NEW QUESTION: 76
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: D (LEAVE A REPLY)
Explanation
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: 77
A newly installed server is accessible to local users, but remote users are unable to connect. Which of the following is MOST likely misconfigured?
A. The IP address
B. The default gateway
C. The VLAN
D. The subnet mask
Answer: B (LEAVE A REPLY)
Explanation
This is the most likely misconfigured setting because the default gateway is the router that connects the local network to other networks. If the default gateway is incorrect, the server will not be able to communicate with remote users or devices outside its own subnet.
References:
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig

NEW QUESTION: 78
A company is reviewing options for its current disaster recovery plan and potential changes to it. The security team will not allow customer data to egress to non-company equipment, and the company has requested recovery in the shortest possible time. Which of the following will BEST meet these goals?
A. A warm site
B. A hot site
C. Cloud recovery
D. A cold site
Answer: B (LEAVE A REPLY)
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. Reference: https://www.techopedia.com/definition/11172/hot-site https://www.techopedia.com/definition/11173/warm-site https://www.techopedia.com/definition/11174/cold-site https://www.techopedia.com/definition/29836/cloud-recovery

NEW QUESTION: 79
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)

Explanation
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: 80
Which of the following backup types resets the archive bit each time it is run?
A. Differential
B. Snapshot
C. Incremental
D. Synthic full
Answer: (SHOW ANSWER)
Explanation
Incremental backup is a type of backup that only backs up the files that have changed since the last backup, whether it was a full or an incremental backup. Incremental backup resets the archive bit each time it is run, which means it clears the flag that indicates whether or not the file has been backed up. Incremental backup can save time and space compared to full backup, but it requires more time and resources to restore data from multiple backups. References:
https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives (Objective 3.1)

NEW QUESTION: 81
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)
Explanation
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: 82
An administrator is troubleshooting a failure in the datacenter in which a server shut down/powered 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. Redundant power supplies require 220V power

B. The power supplies were not cross-connected
C. Both power supplies were connected to the same power feed
D. The UPS batteries were overcharged
Answer: (SHOW ANSWER)

NEW QUESTION: 83
Which of the following BEST describes the metric that is used to measure server downtime?
A. RPO
B. SLA
C. BIA
D. MTTR
Answer: (SHOW ANSWER)

NEW QUESTION: 84
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)
SSH port 22 for secure remote access and 443 is https for encrypted website browsing.

NEW QUESTION: 85
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)
Explanation
The most efficient subnet address for a network that will have no more than 30 available IP addresses is 255.255.255.224. This subnet mask corresponds to a /27 prefix length, which means that 27 bits are used for the network portion and 5 bits are used for the host portion of an IP address. With 5 bits for hosts, there are 2^5 - 2 = 30 possible host addresses per subnet, which meets the requirement. The other options are either too large or too small for the network size. Reference: https://www.ibm.com/cloud/learn/subnet-mask

NEW QUESTION: 86
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: (SHOW ANSWER)
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. Reference: https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives (Objective 1.2)

NEW QUESTION: 87
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)
Explanation
JBOD (Just a Bunch Of Disks) is a storage configuration that combines different types and sizes of hard drives into one logical unit without any RAID level or redundancy. It allows users to see all the drives within the unit as one large storage space. JBOD can utilize all the available capacity of the drives but does not provide any performance or fault tolerance benefits. Verified References: [JBOD], [RAID]

NEW QUESTION: 88
Which of the following testing exercises for disaster recovery is primarily used to discuss incident response strategies for critical systems without affecting production data?
A. Tabletcp
B. Backup recovery test
C. Lrverail over
D. Hot-site visit audit
Answer: A (LEAVE A REPLY)
A tabletop exercise is a type of disaster recovery testing exercise that is primarily used to discuss incident response strategies for critical systems without affecting production data. A tabletop exercise is a discussion-based session where team members meet in an informal, classroom setting to review their roles and responsibilities during an emergency and their responses to a hypothetical scenario. A facilitator guides the participants through the discussion and evaluates the strengths and weaknesses of the preparedness program. A tabletop exercise does not involve any actual deployment of resources or activation of systems12. A backup recovery test (B) is a type of disaster recovery testing exercise that involves restoring data from backup media to verify its integrity and availability. A backup recovery test may affect production data if it is not performed on a separate environment. A live failover is a type of disaster recovery testing exercise that involves switching operations from a primary site to a secondary site in case of a failure or disruption. A live failover may affect production data if it is not performed on a simulated environment. A hot-site visit audit (D) is a type of disaster recovery testing exercise that involves inspecting and evaluating a hot site, which is a backup location that has fully operational equipment and resources to resume business operations in case of a disaster. A hot-site visit audit does not involve any discussion of incident response strategies or simulation of scenarios. Reference: 1 https://www.ready.gov/testing-exercises 2 https://www.ready.gov/exercises

NEW QUESTION: 89
Which of the following should be configured in pairs on a server to provide network redundancy?
A. MRU
B. SCP
C. DLP
D. CPU
E. NIC
Answer: (SHOW ANSWER)
Explanation
NIC stands for network interface card, which is a hardware component that allows a server to connect to a network. Configuring NICs in pairs on a server would provide network redundancy, meaning that if one NIC fails, the other one can take over and maintain network connectivity. The other options are not related to network redundancy.

NEW QUESTION: 90
Which of the following is a method that is used to prevent motor vehicles from getting too close to building entrances and exits?
A. Bollards
B. Reflective glass
C. Security guards
D. Security cameras
Answer: A (LEAVE A REPLY)
Explanation
Bollards are an example of a method that is used to prevent motor vehicles from getting too close to building entrances and exits. Bollards are short, sturdy posts that are installed on sidewalks, parking lots, or roads to create physical barriers and control traffic flow. Bollards can be used to protect pedestrians, buildings, or other structures from vehicle collisions or attacks. Bollards can be made of various materials, such as metal, concrete, or plastic, and can be fixed, removable, or retractable.

NEW QUESTION: 91
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: (SHOW ANSWER)

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: 92

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

A. Biometrics

B. Push notifications

C. Smart carts

D. Physical tokens

Answer: (SHOW ANSWER)

Explanation

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

NEW QUESTION: 93

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)
Explanation
This is the most likely misconfigured setting because DNS is the service that resolves hostnames to IP addresses and vice versa. If the DNS server is incorrect or unreachable, the administrator will not be able to log on to the server with a domain account because the server will not be able to authenticate with the domain controller. References:
https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/dns-troubleshooting

NEW QUESTION: 94
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: 95
A technician is laying out a filesystem on a new Linux server. Which of the following tools would work BEST to allow the technician to increase a partition's size in the future without reformatting it?
A. LVM
B. DiskPart
C. fdisk
D. Format
Answer: A (LEAVE A REPLY)
Explanation
LVM (Logical Volume Manager) is a tool that allows the technician to increase a partition's size in the future without reformatting it on a Linux server. LVM creates logical volumes that can span across multiple physical disks or partitions and can be resized dynamically without

losing data. LVM also provides other features such as snapshots, encryption, and RAID. DiskPart, fdisk, and Format are tools that can be used to partition and format disks, but they do not allow increasing a partition's size without reformatting it. References:
https://www.howtogeek.com/howto/40702/how-to-manage-and-use-lvm-logical-volume-management-in-ubuntu
https://www.howtogeek.com/school/using-windows-admin-tools-like-a-pro/lesson2/
https://www.howtogeek.com/howto/17001/how-to-format-a-usb-drive-in-ubuntu-using-gparted/

NEW QUESTION: 96
Which of the following BEST measures now much downtime an organization can tolerate Curing an unplanned outage?
A. BIA
B. RTO
C. MTTR
D. SLA
Answer: D (LEAVE A REPLY)

NEW QUESTION: 97
A server administrator wants to run a performance monitor for optimal system utilization. Which of the following metrics can the administrator use for monitoring? (Choose two.)
A. Memory
B. Page file
C. Services
D. Application
E. CPU
F. Heartbeat
Answer: (SHOW ANSWER)
Explanation
Memory and CPU are two metrics that can be used for monitoring system utilization. Memory refers to the amount of RAM that is available and used by the system and its processes. CPU refers to the percentage of processor time that is consumed by the system and its processes. Both memory and CPU can affect the performance and responsiveness of the system and its applications. Monitoring memory and CPU can help identify bottlenecks, resource contention, memory leaks, high load, etc.

NEW QUESTION: 98
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: (SHOW ANSWER)
Reference:
https://unix.stackexchange.com/QUESTION NO:s/149399/how-to-remount-as-read-write-a-specific-mount-of-device

NEW QUESTION: 99
A server administrator has configured a web server. Which of the following does the administrator need to install to make the website trusted?
A. PKI
B. SSL
C. LDAP
D. DNS
Answer: (SHOW ANSWER)
Explanation
The administrator needs to install SSL to make the website trusted. SSL stands for Secure Sockets Layer, which is an encryption-based Internet security protocol that ensures privacy, authentication, and data integrity in web communications. SSL enables HTTPS (Hypertext Transfer Protocol Secure), which is a secure version of HTTP (Hypertext Transfer Protocol) that encrypts the data exchanged between a web browser and a web server. SSL also uses digital certificates to verify the identity of the web server and establish trust with the web browser. A web server that implements SSL has HTTPS in its URL instead of HTTP and displays a padlock icon or a green bar in the browser's address bar.

NEW QUESTION: 100
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)
Explanation
Dynamic disk is a technology that allows an administrator to build a software RAID on a Windows server.
Dynamic disk is a type of disk management that supports creating volumes that span multiple disks, stripe data across disks, mirror data between disks, or use parity for fault tolerance. Dynamic disk can be used to create RAID 0 (striping), RAID 1 (mirroring), RAID 5 (striping with parity), or spanned volumes on Windows servers. Logical volume management is a technology that allows creating and resizing logical volumes on Linux servers. GPT (GUID Partition Table) is a standard for defining the partition structure on a disk. UEFI (Unified Extensible Firmware Interface) is a specification for the interface between the operating system and the firmware. References:
https://www.howtogeek.com/school/using-windows-admin-tools-like-a-pro/lesson2/
https://www.howtogeek.com/howto/40702/how-to-manage-and-use-lvm-logical-volume-management-in-ubuntu
https://www.howtogeek.com/193669/whats-the-difference-between-gpt-and-mbr-when-partitioning-a-drive/
https://www.howtogeek.com/56958/htg-explains-how-uefi-will-replace-the-bios/

NEW QUESTION: 101
A server administrator is testing a disaster recovery plan. The test involves creating a downtime scenario and taking the necessary steps. Which of the following testing methods is the administrator MOST likely performing?
A. Backup recovery
B. Simulated

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

NEW QUESTION: 102
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: (SHOW ANSWER)
Reference:
https://www.redhat.com/en/topics/data-storage/network-attached-storage

NEW QUESTION: 103
A junior administrator needs to configure a single RAID 5 volume out of four 200GB drives attached to the server using the maximum possible capacity. Upon completion, the server reports that all drives were used, and the approximate volume size is 400GB. Which of the following BEST describes the result of this configuration?
A. RAID 0 was configured by mistake.
B. RAID 5 was configured properly.
C. JBOD was configured by mistake.
D. RAID 10 was configured by mistake.
Answer: (SHOW ANSWER)
The output of the configuration shows that RAID 5 was configured properly using four 200GB drives. The approximate volume size of 400GB is correct, since RAID 5 uses one disk for parity and the rest for data. Therefore, the usable storage capacity is three-fourths of the total capacity, which is 600GB out of 800GB. The other RAID levels given would result in different volume sizes: RAID 0 would result in 800GB, RAID 1 would result in 200GB, and JBOD would result in an error since it does not support multiple drives in a single volume.
Reference: https://en.wikipedia.org/wiki/Standard_RAID_levels#RAID_5

NEW QUESTION: 104
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.
D. Assign ownership on the folder for each user.
Answer: (SHOW ANSWER)
The top portion of the dialog box lists the users and/or groups that have access to the file or folder.

NEW QUESTION: 105
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: (SHOW ANSWER)
Explanation
If the server administrator patches the server with the latest vendor-suggested software, configures DHCP, and verifies all network cables are properly connected in the IDF, but there is no network connectivity, then the most likely reason for the lack of connectivity is that the VLAN is improperly configured. A VLAN (Virtual Local Area Network) is a logical grouping of network devices that share the same broadcast domain and can communicate with each other without routing. If the server is assigned to a different VLAN than the DHCP server or the default gateway, it will 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-win
https://www.howtogeek.com/202794/what-is-an-intrusion-detection-system-ids-and-how-does-it-work/

NEW QUESTION: 106
An administrator is adding NAS-based storage to a server. Which of the following strategies will allow users to see BEST performance with this new NAS storage?
A. Connect server to NAS storage using two redundant SCSI controllers.
B. Connect server to NAS storage using two teamed 1 Gb NICs.
C. Connect server to NAS storage using two redundant fabric switches.
D. Connect server to NAS storage using two redundant HBAs.
Answer: (SHOW ANSWER)

NEW QUESTION: 107
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: 108
A company deploys antivirus, anti-malware, and firewalls that can be assumed to be functioning properly.
Which of the following is the MOST likely system vulnerability?
A. Insider threat
B. Worms
C. Ransomware
D. Open ports
E. Two-person integrity
Answer: (SHOW ANSWER)
Explanation
Insider threat is the most likely system vulnerability in a company that deploys antivirus, anti-malware, and firewalls that can be assumed to be functioning properly. An insider threat is a malicious or negligent act by an authorized user of a system or network that compromises the security or integrity of the system or network. An insider threat can include data theft, sabotage, espionage, fraud, or other types of attacks. Antivirus, anti-malware, and firewalls are security tools that can protect a system or network from external threats, such as viruses, worms, ransomware, or open ports. However, these tools cannot prevent an insider threat from exploiting their access privileges or credentials to harm the system or network.

NEW QUESTION: 109
A technician is trying to determine the reason why a Linux server is not communicating on a network. The returned network configuration is as follows:
eth0: flags=4163<UP, BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 127.0.0.1 network 255.255.0.0 broadcast 127.0.0.1
Which of the following BEST describes what is happening?
A. The server is configured to use DHCP on a network that has multiple scope options
B. The server is configured to use DHCP, but the DHCP server is sending an incorrect subnet mask
C. The server is configured to use DHCP on a network that does not have a DHCP server

D. The server is configured to use DHCP, but the DHCP server is sending an incorrect MTU setting
Answer: C (LEAVE A REPLY)
Explanation
The reason why the Linux server is not communicating on a network is that it is configured to use DHCP on a network that does not have a DHCP server. DHCP (Dynamic Host Configuration Protocol) is a protocol that allows a client device to obtain an IP address and other network configuration parameters from a DHCP server automatically. However, if there is no DHCP server on the network, the client device will not be able to obtain a valid IP address and will assign itself a link-local address instead. A link-local address is an IP address that is only valid within a local network segment and cannot be used for communication outside of it. A link-local address has a prefix of 169.254/16 in IPv4 or fe80::/10 in IPv6. In this case, the Linux server has assigned itself a link-local address of 127.0.0.1, which is also known as the loopback address. The loopback address is used for testing and troubleshooting purposes and refers to the device itself. It cannot be used for communication with other devices on the network.

NEW QUESTION: 110
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)
Explanation
This is the most appropriate way to complete the task because it follows the best practices of cable management. Cable management is a process of organizing and securing cables in a rack or a server room to improve airflow, accessibility, safety, and aesthetics. Running the network cables up the left side and the power cables down the right side of the rack helps to avoid cable clutter, interference, and confusion. It also makes it easier to trace and troubleshoot cables if needed. Using appropriate-length cables also helps to reduce cable slack and excess. Wiring the cables through the cable management arm may cause stress and damage to the cables when moving the server in or out of the rack. Using the longest 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: 111
Which of the following server types would benefit MOST from the use of a load balancer?
A. DNS server
B. File server
C. DHCP server
D. Web server
Answer: (SHOW ANSWER)
Reference:

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

NEW QUESTION: 112
A server administrator was asked to implement a site backup solution. The backup window during regular business days is from midnight to 6:00 a.m. because end-of-cycle payroll processing will occur for the next three months. Which of the following backup methodologies would satisfy this restriction in performing short backups?
A. Perform daily incremental backups.
B. Perform daily normal backups.
C. Perform daily full backups.
D. Perform daily differential backups.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 113
A server room contains ten physical servers that are running applications and a cluster of three dedicated hypervisors. The hypervisors are new and only have 10% utilization. The Chief Financial Officer has asked that the IT department do what it can to cut back on power consumption and maintenance costs in the data center. Which of the following would address the request with minimal server downtime?
A. Unplug the power cables from the redundant power supplies, leaving just the minimum required.
B. Convert the physical servers to the hypervisors and retire the ten servers.
C. Reimage the physical servers and retire all ten servers after the migration is complete.
D. Convert the ten servers to power-efficient core editions.
Answer: B (LEAVE A REPLY)
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: 114
Which of the following steps in the troubleshooting theory should be performed after a solution has been implemented? (Choose two.)
A. Scope the issue
B. Develop a plan of action
C. Notify the users
D. Document the findings
E. Escalate the issue
F. Perform a root cause analysis
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 115
A server administrator needs to validate the integrity of all system files. Which of the following methods should the administrator use?
A. Run an encryption program to generate a checksum for all files on the system and compare it to an original report.
B. Run a sniffer program to generate a checksum for all files on the system and compare it to an original report.
C. Run a hash program to generate a checksum for all files on the system and compare it to an original report.
D. Run an antivirus program to generate a checksum for all files on the system and compare it to an original report.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 116
A server administrator wants to check the open ports on a server. Which of the following commands should the administrator use to complete the task?
A. nslookup
B. nbtstat
C. telnet
D. netstat -a
Answer: D (LEAVE A REPLY)
https://linuxhint.com/netstat-a/

NEW QUESTION: 117
An administrator is configuring a server that will host a high-performance financial application.
Which of the following disk types will serve this purpose?
A. SAS SSD
B. SATA SSD
C. SAS drive with 10000rpm
D. SATA drive with 15000rpm
Answer: A (LEAVE A REPLY)

1. The bytes that make up your document are saved in storage.
2. The computer signals to storage that it needs the bytes.
3. The bytes leave storage via the SAS and SATA cables and travel to the CPU at the motherboard - it's the CPU that runs Microsoft Word.
4. When you've finished writing for the day, you save the file.
5. The bytes travel back along the SAS or SATA cables and reenter storage.

https://www.hp.com/us-en/shop/tech-takes/sas-vs-sata