

CompTIA.SK0-005.v2024-01-13.q159

Exam Code:	SK0-005
Exam Name:	CompTIA Server+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	159
Version:	v2024-01-13
# of views:	950
# of Questions views:	1590
https://www.freepdfdumps.com/CompTIA.SK0-005.v2024-01-13.q159.html	

NEW QUESTION: 1

A systems administrator is performing maintenance on 12 Windows servers that are in different racks at a large datacenter. Which of the following would allow the administrator to perform maintenance on all 12 servers without having to physically be at each server? (Choose two.)

- A. Remote desktop
- B. IP KVM
- C. A console connection
- D. A virtual administration console
- E. Remote drive access
- F. A crash cart

Answer: A,B ([LEAVE A REPLY](#))

Explanation

The methods that would allow the administrator to perform maintenance on all 12 servers without having to physically be at each server are remote desktop and IP KVM. Remote desktop is a feature that allows a user to access and control another computer over a network using a graphical user interface (GUI). Remote desktop can enable remote administration, troubleshooting, and maintenance of servers without requiring physical presence at the server location. IP KVM (Internet Protocol Keyboard Video Mouse) is a device that allows a user to access and control multiple servers over a network using a single keyboard, monitor, and mouse. IP KVM can provide remote access to servers regardless of their operating system or power state, and can also support virtual media and serial console functions.

NEW QUESTION: 2

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

- A. Restore the data from backup.
- B. Disclose the incident.

- C. Disable unnecessary ports.
- D. Run an antivirus scan.
- E. Identify the exploited vulnerability.
- F. Move the data to a different location.

Answer: B,E (LEAVE A REPLY)

Explanation

These are two measures that should be taken when a data breach occurs. A data breach is an unauthorized or illegal access to confidential or sensitive data by an internal or external actor. A data breach can result in financial losses, reputational damage, legal liabilities, and regulatory penalties for the affected organization.

Disclosing the incident is a measure that involves informing the relevant stakeholders, such as customers, employees, partners, regulators, and law enforcement, about the nature, scope, and impact of the data breach.

Disclosing the incident can help to mitigate the negative consequences of the data breach, comply with legal obligations, and restore trust and confidence. Identifying the exploited vulnerability is a measure that involves investigating and analyzing the root cause and source of the data breach. Identifying the exploited vulnerability can help to prevent further data loss, remediate the security gaps, and improve the security posture of the organization. Restoring the data from backup is a measure that involves recovering the lost or corrupted data from a secondary storage device or location. However, this does not address the underlying issue of how the data breach occurred or prevent future breaches. Disabling unnecessary ports is a measure that involves closing or blocking network communication endpoints that are not required for legitimate purposes. However, this does not address how the data breach occurred or what vulnerability was exploited.

Running an antivirus scan is a measure that involves detecting and removing malicious software from a system or network. However, this does not address how the data breach occurred or what vulnerability was exploited.

Moving the data to a different location is a measure that involves transferring the data to another storage device or location that may be more secure or less accessible. However, this does not address how the data breach occurred or what vulnerability was exploited. References:

<https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-it-matter/>

<https://www.howtogeek.com/202794/what-is-the-difference-between-127.0.0.1-and-0.0.0.0/>

<https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual>

NEW QUESTION: 3

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: 4

A technician is attempting to log in to a Linux server as root but cannot remember the administrator password.

Which of the following is the LEAST destructive method of resetting the administrator password?

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

Answer: ([SHOW ANSWER](#))

Explanation

This is the least destructive method of resetting the administrator password because it does not require modifying any files or reinstalling the OS. It only requires changing the boot parameters temporarily and running a command to change the password. References:

https://wiki.archlinux.org/title/Reset_lost_root_password#Using_GRUB

NEW QUESTION: 5

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

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

Answer: C ([LEAVE A REPLY](#))

Explanation

Link aggregation is the best option to implement on the new server to ensure the least amount of network downtime but a good amount of network speed. Link aggregation is a technique of combining multiple physical network interfaces into one logical interface to increase bandwidth, redundancy, and load balancing.

Link aggregation can improve the performance and availability of the server by allowing it to use more than one network path for data transmission and failover in case of link failure. Link aggregation can be implemented using various protocols, such as IEEE 802.3ad (LACP), Cisco EtherChannel, or Linux bonding. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Networking, Objective

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

NEW QUESTION: 6

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: 7

A server administrator is racking new servers in a cabinet with multiple connections from the servers to power supplies and the network. Which of the following should the administrator recommend to the organization to best address this situation?

- A. Rack balancing
- B. Cable management
- C. Blade enclosure
- D. Rail kits

Answer: B ([LEAVE A REPLY](#))

Explanation

Cable management is the process of organizing, securing, and labeling cables in a server rack or cabinet. Cable management can help improve airflow and cooling, reduce clutter and confusion, prevent damage and interference, and enhance safety and aesthetics¹²³. Cable management can be achieved by using various tools and accessories, such as cable trays, ties, hooks, clips, labels, ducts, and organizers¹².

NEW QUESTION: 8

Which of the following physical security concepts would most likely be used to limit personnel access to a restricted area within a data center?

- A. An access control vestibule
- B. Video surveillance
- C. Bollards
- D. Data center camouflage

Answer: A ([LEAVE A REPLY](#))

Explanation

An access control vestibule is a physical security concept that limits personnel access to a restricted area within a data center. It is a small room or hallway that has two doors: one that leads to the outside and one that leads to the restricted area. The doors are controlled by an electronic lock that requires authentication, such as a card reader, biometric scanner, or keypad. Only authorized personnel can enter the vestibule and access the restricted area. References: CompTIA Server+ Certification Exam Objectives, Domain 5.0: Security, Objective 5.1: Given a scenario, apply physical security methods to a server.

NEW QUESTION: 9

Joe, a user in the IT department cannot save changes to a sensitive file on a Linux server. An ls -l& shows the following listing;

```
-rw-r--r 1 Ann IT 6780 12 June 2019 filename
```

Which of the following commands would BEST enable the server technician to allow Joe to have access without granting excessive access to others?

- A. `chmod 777 filename`
- B. `chown Joe filename`
- C. `Chmod g+w filename`
- D. `chgrp IT filename`

Answer: C ([LEAVE A REPLY](#))

Explanation

The `chmod` command is used to change the permissions of files and directories. The `g+w` option means to grant write permission to the group owner of the file. Since Joe is a member of the IT group, which is also the group owner of the file, this command will allow him to save changes to the file without affecting the permissions of other users. Verified References: [Linux `chmod` command]

NEW QUESTION: 10

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](#)**)**

Explanation

The output of the configuration shows that RAID 5 was configured properly using four 200GB drives. The approximate volume size of 400GB is correct, since RAID 5 uses one disk for parity and the rest for data.

Therefore, the usable storage capacity is three-fourths of the total capacity, which is 600GB out of 800GB.

The other RAID levels given would result in different volume sizes: RAID 0 would result in 800GB, RAID 1 would result in 200GB, and JBOD would result in an error since it does not support multiple drives in a single volume. References:

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

NEW QUESTION: 11

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

- A. Constant
- B. Application consistent
- C. Synthetic full
- D. Full

Answer: A ([LEAVE A REPLY](#))

Explanation

Constant replication is a type of replication in which all files are replicated, all the time. Replication is a process of copying data from one location to another for backup, recovery, or distribution purposes. Constant replication is also known as real-time replication or synchronous replication. It ensures that any changes made to the source data are immediately reflected on the target data without any delay or lag. Constant replication provides high availability and consistency, but it requires high bandwidth and low latency. Application consistent replication is a type of replication that ensures that the replicated data is consistent with the state of the application that uses it. It involves quiescing or pausing the application before taking a snapshot of the data and resuming the application after the snapshot is taken. Application consistent replication provides better recovery point objectives than crash consistent replication, which does not quiesce the application before taking a snapshot. Synthetic full replication is a type of replication that involves creating a new full backup by using the previous full backup and related incremental backups. It reduces the backup window and network bandwidth consumption by transferring only changed data from the source to the target. Full replication is a type of replication that involves copying all data from the source to the target regardless of whether it has changed or not. It provides a complete backup of the data, but it requires more storage space and network bandwidth than incremental or differential replication. References:

<https://www.howtogeek.com/199068/how-to-upgrade-your-existing-hard-drive-in-under-an-hour/>

<https://www.howtogeek.com/202794/what-is-the-difference-between-127.0.0.1-and-0.0.0.0/>

<https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual>

NEW QUESTION: 12

Which of the following BEST describes a guarantee of the amount of time it will take to restore a downed service?

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

Answer: A ([LEAVE A REPLY](#))

Explanation

RTO stands for Recovery Time Objective and it is a metric that defines the maximum acceptable amount of time that a system or service can be unavailable after a disaster or disruption. RTO is part of the business continuity planning and disaster recovery planning processes. RTO ensures a guarantee of the amount of time it will take to restore a downed service by setting a target or goal for recovery. RTO can vary depending on the criticality and priority of the service.

References:

<https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives> (Objective 3.3)

NEW QUESTION: 13

Which of the following BEST measures how much downtime an organization can tolerate during an unplanned outage?

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

Answer: C ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 14

An administrator has been asked to deploy a database server that provides the highest performance with fault tolerance. Which of the following RAID levels will fulfill this request?

- A. RAID0
- B. RAID1
- C. RAID 5
- D. RAID 6
- E. RAID 10

Answer: E ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 15

Network connectivity to a server was lost when it was pulled from the rack during maintenance. Which of the following should the server administrator use to prevent this situation in the future?

- A. Cable management
- B. Rail kits

- C. A wireless connection
- D. A power distribution unit

Answer: A ([LEAVE A REPLY](#))

Explanation

The server administrator should use cable management to prevent network connectivity loss when pulling a server from the rack during maintenance. Cable management is a practice of organizing and securing the cables that connect various devices and components in a system. Cable management can help improve airflow, reduce clutter, prevent tangling, and avoid accidental disconnection or damage of cables. Cable management can be done using various tools and techniques, such as cable ties, cable trays, cable labels, cable organizers, or cable ducts.

NEW QUESTION: 16

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

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

Answer: ([SHOW ANSWER](#)**)**

Explanation

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

References: <https://www.geeksforgeeks.org/what-is-hot-swapping/>

<https://www.howtogeek.com/268249/what-is-hot-swapping-and-what-devices-support-it/>

Valid SK0-005 Dumps shared by Actual4test.com for Helping Passing SK0-005 Exam!

Actual4test.com now offer the **newest SK0-005 exam dumps**, the Actual4test.com SK0-005 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SK0-005 dumps with Test Engine here:

Special Discount: [Freepdfdumps](#))

NEW QUESTION: 17

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

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

Answer: D ([LEAVE A REPLY](#))

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: 18

A technician is creating a network share that will be used across both Unix and Windows clients at the same time. Users need read and write access to the files. Which of the following would be BEST for the technician to deploy?

- A. iSCSI
- B. CIFS
- C. HTTPS
- D. DAS

Answer: ([SHOW ANSWER](#)**)**

Explanation

CIFS (Common Internet File System) is a protocol that allows file sharing across different operating systems, such as Unix and Windows. It supports read and write access to files and folders on a network share. It is also known as SMB (Server Message Block). Verified References: [CIFS], [File sharing]

NEW QUESTION: 19

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

- A. The server has a faulty power supply

- B. The server has a CMOS battery failure
- C. The server requires OS updates
- D. The server has a malfunctioning LED panel
- E. The servers do not have NTP configured
- F. The time synchronization service is disabled on the servers

Answer: B,F ([LEAVE A REPLY](#))

Explanation

The server has a CMOS battery failure and the time synchronization service is disabled on the servers. The CMOS battery is a small battery on the motherboard that powers the BIOS settings and keeps track of the date and time when the server is powered off. If the CMOS battery fails, the server will lose its configuration and display an incorrect date and time when it is powered on. This can cause access issues for users and applications that rely on accurate time stamps. The time synchronization service is a service that synchronizes the system clock with a reliable external time source, such as a network time protocol (NTP) server. If the time synchronization service is disabled on the servers, they will not be able to update their clocks automatically and may drift out of sync with each other and with the network. This can also cause access issues for users and applications that require consistent and accurate time across the network.

NEW QUESTION: 20

Which of the following BEST measures how much downtime an organization can tolerate during an unplanned outage?

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

Answer: C ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 21

A server administrator is building a pair of new storage servers. The servers will replicate; therefore, no redundancy is required, but usable capacity must be maximized. Which of the following RAID levels should the server administrator implement?

- A. 0
- B. 1
- C. 5
- D. 6
- E. 10

Answer: ([SHOW ANSWER](#))

Explanation

The RAID level that should be implemented to maximize usable capacity without requiring redundancy is RAID 0. RAID (Redundant Array of Independent Disks) is a technology that combines multiple physical disks into a logical unit that provides improved performance, reliability, or both. RAID 0 is a RAID level that splits data evenly across two or more disks without parity or mirroring. RAID 0 does not provide any redundancy or fault tolerance, but it increases usable capacity and performance by allowing parallel read and write operations.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 1, Lesson 1.2, Objective 1.2

NEW QUESTION: 22

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

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

Answer: ([SHOW ANSWER](#))

Explanation

The write cache is a feature of some RAID controllers that allows them to temporarily store data in a fast memory buffer before writing it to the disk drives. This improves the performance and efficiency of write operations, especially for random and small writes. However, if the battery on the controller goes bad, the controller may disable the write cache to prevent data loss in case of a power failure. This can degrade the disk drive performance significantly, as every write operation will have to wait for the disk drives to complete.

References:

<https://www.dell.com/support/kbdoc/en-us/000131486/understanding-raid-controller-battery-learn-cycle>

<https://www.techrepublic.com/article/understanding-raid-controller-write-cache/>

NEW QUESTION: 23

A technician needs to provide a VM with high availability. Which of the following actions should the technician take to complete this task as efficiently as possible?

- A. Take a snapshot of the original VM
- B. Clone the original VM
- C. Convert the original VM to use dynamic disks
- D. Perform a P2V of the original VM

Answer: B ([LEAVE A REPLY](#))

Explanation

Cloning the original VM is the most efficient way to provide a VM with high availability. Cloning is the process of creating an exact copy of a VM, including its configuration, operating system, applications, and data. A cloned VM can be used as a backup or a replica of the original VM, and can be powered on and run independently. Cloning can be done quickly and easily using vSphere tools or other third-party software. By cloning the original VM and placing it on a different host server or availability zone, the technician can ensure that if the original VM fails, the cloned VM can take over its role and provide uninterrupted service to the users and applications.

NEW QUESTION: 24

A company wants to deploy software to all users, but very few of them will be using the software at any one point in time. Which of the following licensing models would be BEST for the company?

- A. Per site
- B. Per concurrent user
- C. Per core
- D. Per instance

Answer: B ([LEAVE A REPLY](#))

Explanation

Per concurrent user licensing is a model that allows a fixed number of users to access the software at any one point in time. This model is best for the company that wants to deploy software to all users, but very few of them will be using the software at any one point in time. This way, the company can save money by paying only for the number of simultaneous users, rather than for every user who has access to the software. Per site licensing is a model that allows unlimited users within a specific location to use the software. Per core licensing is a model that charges based on the number of processor cores on the server where the software is installed. Per instance licensing is a model that charges based on the number of copies of the software running on different servers or virtual machines. References:

<https://www.pcmag.com/encyclopedia/term/concurrent-use-license>

<https://www.techopedia.com/definition/1440/software-licensing>

NEW QUESTION: 25

A datacenter in a remote location lost power. The power has since been restored, but one of the servers has not come back online. After some investigation, the server is found to still be powered off. Which of the following is the BEST method to power on the server remotely?

- A. Crash cart
- B. Out-of-band console
- C. IP KVM
- D. RDP

Answer: B ([LEAVE A REPLY](#))

Explanation

Out-of-band console is a tool that can be used to command a remote shutdown of a physical Linux server.

Out-of-band console is a method of accessing a server's console through a dedicated management port or device that does not rely on the server's operating system or network connection. Out-of-band console can be used to power cycle, reboot, update firmware, monitor performance, and perform other tasks remotely even if the server is unresponsive or offline.

Crash cart is a mobile unit that contains a keyboard, monitor, mouse, and other tools that can be used to troubleshoot a server on-site, but it requires physical access to the server. IP KVM (Internet Protocol Keyboard Video Mouse) switch is a hardware device that allows remote access to multiple servers using a web browser or a client software, but it requires network connectivity and may not work if the SSH connection is lost. RDP (Remote Desktop Protocol) is a protocol that allows remote access to a Windows server's graphical user interface, but it does not work on Linux servers and requires network connectivity. References:

<https://www.techopedia.com/definition/13623/crash-cart>

<https://www.techopedia.com/definition/13624/kvm-switch>

<https://www.techopedia.com/definition/3422/remote-desktop-protocol-rdp>

NEW QUESTION: 26

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

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

Answer: (SHOW ANSWER)

Explanation

Port 443 is the default port for HTTPS, which is the protocol used for secure web communication. HTTPS uses SSL/TLS certificates to encrypt the data between the web server and the browser. Port 443 is commonly used for web servers that need to provide secure services, such as online

banking, e-commerce, or email. By allowing port 443, the administrator can access the web server's interface and manage its settings¹.

Port 3389 is the default port for RDP, which is the protocol used for remote desktop connection. RDP allows a user to remotely access and control another computer over a network. Port 3389 is commonly used for remote administration, technical support, or remote work. By allowing port 3389, the administrator can connect to the web server's desktop and perform tasks that require graphical user interface².

NEW QUESTION: 27

An organization stores backup tapes of its servers at cold sites. The organization wants to ensure the tapes are properly maintained and usable during a DR scenario. Which of the following actions should the organization perform?

- A.** Have the facility inspect and inventory the tapes on a regular basis.
- B.** Have duplicate equipment available at the cold site.
- C.** Retrieve the tapes from the cold site and test them.
- D.** Use the test equipment at the cold site to read the tapes.

Answer: C ([LEAVE A REPLY](#))

Explanation

The organization should retrieve the tapes from the cold site and test them to ensure they are properly maintained and usable during a DR scenario. A cold site is a location that has space and power for backup equipment, but no actual equipment installed or configured. The organization stores backup tapes of its servers at cold sites as a precaution in case of a disaster that affects its primary site. However, backup tapes can degrade over time due to environmental factors such as temperature, humidity, dust, or magnetic fields.

Therefore, the organization should periodically retrieve the tapes from the cold site and test them on compatible equipment to verify their integrity and readability.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 6, Lesson 6.4, Objective 6.4

NEW QUESTION: 28

An administrator is troubleshooting an application performance issue on a virtual server with two vCPUs. The application performance logs indicate CPU contention. The administrator adds more vCPU cores to the VM, yet the issue persists. Which of the following is the most likely reason for this issue?

- A.** The server has high page utilization.
- B.** The server has high disk latency.
- C.** The application is single-threaded.
- D.** The application cannot be virtualized.

Answer: C ([LEAVE A REPLY](#))

Explanation

A single-threaded application is an application that can only execute one task or process at a time. A single-threaded application can only utilize one CPU core, regardless of how many cores are available or assigned to the virtual machine. Therefore, adding more vCPU cores to the VM will not improve the performance of the application, as it will still be limited by the speed and capacity of one core¹².

To troubleshoot this issue, the administrator should check if the application is single-threaded or multi-threaded. This can be done by using tools such as Task Manager, Performance Monitor, or Process Explorer on Windows, or `top`, `htop`, or `ps` on Linux³⁴. If the application is single-threaded, the administrator should consider the following options:

Reduce the number of vCPU cores on the VM to match the number of threads that the application can use. This can help avoid CPU contention and co-stop issues that may arise from having too many vCPUs relative to the number of physical cores on the host⁵.

Upgrade the physical CPU on the host to a faster or newer model that can provide higher clock speed and performance for the single core that the application uses.

Optimize the application code or configuration to make it more efficient or multi-threaded, if possible.

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

NEW QUESTION: 29

A technician is sizing a new server and, for service reasons, needs as many hot-swappable components as possible. Which of the following server components can most commonly be replaced without downtime?

(Select three).

- A. Drives
- B. Fans
- C. CMOSIC
- D. Processor
- E. Power supplies
- F. Motherboard
- G. Memory
- H. BIOS

Answer: A,B,E ([LEAVE A REPLY](#))

Explanation

Drives, fans, and power supplies are server components that can most commonly be replaced without downtime if they are hot-swappable. Hot-swappable components can be removed and inserted while the server is running, without affecting its operation or performance. Drives store data and applications, fans cool down the server components, and power supplies provide electricity to the server. Replacing these components can prevent data loss, overheating, or power failure. References: CompTIA Server+ Certification Exam Objectives, Domain 2.0: Hardware, Objective 2.2: Given a scenario, install, configure and maintain server components.

NEW QUESTION: 30

A Linux server was recently updated. Now, the server stops during the boot process with a blank screen and an f prompt. Which of the following is the most likely cause of this issue?

- A. The system is booting to a USB flash drive.
- B. The UEFI boot was interrupted by a missing Linux boot file.
- C. The BIOS could not find a bootable hard disk.
- D. The BIOS firmware needs to be upgraded.

Answer: B ([LEAVE A REPLY](#))

Explanation

The most likely cause of this issue is that the UEFI boot was interrupted by a missing Linux boot file. UEFI (Unified Extensible Firmware Interface) is a standard that defines the interface and functionality of the firmware that initializes the hardware and software components of a system before loading the operating system. UEFI boot is a process that uses UEFI firmware to load and execute a boot loader, which is a program that loads the operating system kernel and other essential files. A Linux boot file is a file that contains information and instructions for the boot loader, such as the location of the kernel, the root file system, and the boot parameters. If a Linux boot file is missing or corrupted, the boot loader cannot find or load the kernel, and the system stops during the boot process with a blank screen and an f prompt.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 4, Lesson 4.1, Objective 4.1

NEW QUESTION: 31

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

- A. Differential
- B. Synthetic full
- C. Archive
- D. Full
- E. Incremental
- F. Open file

Answer: A,E ([LEAVE A REPLY](#))

Explanation

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

the longest time and requires the most storage space. A differential backup copies only the data that has changed since the last full backup. A differential backup provides a faster restore option than an incremental backup, but it also takes more time and requires more storage space than an incremental backup. An incremental backup copies only the data that has changed since the last backup, whether it was a full or an incremental backup. An incremental backup provides the fastest and most efficient backup option, but it also requires multiple backups to restore the data completely.

Valid SK0-005 Dumps shared by Actual4test.com for Helping Passing SK0-005 Exam! Actual4test.com now offer the **newest SK0-005 exam dumps**, the Actual4test.com SK0-005 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SK0-005 dumps with Test Engine here:

https://www.actual4test.com/SK0-005_examcollection.html (492 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 32

Which of the following symbols is used to write a text description per line within a PowerShell script?

- A. %
- B. @
- C. &
- D. #

Answer: D ([LEAVE A REPLY](#))

Explanation

The # symbol is used to write a text description per line within a PowerShell script. A text description is also known as a comment, which is a line of code that is ignored by the PowerShell interpreter and serves as documentation or explanation for human readers. The # symbol indicates that everything following it on the same line is a comment and not part of the script commands or expressions. For example:

This is a comment in PowerShellWrite-Host "Hello World" # This command prints Hello World to the console References: CompTIA Server+ Certification Exam Objectives, Domain 6.0:

Troubleshooting, Objective 6.3:

Given a scenario, troubleshoot scripting errors using PowerShell commands.

NEW QUESTION: 33

An administrator is investigating a physical server that will not Boot into the OS. The server has three hard drives configured in a RAID 5 array. The server passes POST, but the OS does not load. The administrator verifies the CPU and RAM are both seated correctly and checks the dual power supplies. The administrator then verifies all the BIOS settings are correct and connects a

bootable USB drive in the server, and the OS loads correctly. Which of the following is causing the issue?

- A. The page file is too small.
- B. The CPU has failed.
- C. There are multiple failed hard drives.
- D. There are mismatched RAM modules.
- E. RAID 5 requires four drives

Answer: (SHOW ANSWER)

Explanation

If a server has three hard drives configured in a RAID 5 array, it means that the data is striped across all three drives with parity information. RAID 5 can tolerate one drive failure without losing data, but not two or more.

If there are multiple failed hard drives, the RAID 5 array will become corrupted and the OS will not load. The other options are not likely to cause the issue, as the server passes POST, the CPU and RAM are seated correctly, the BIOS settings are correct, and the OS loads from a bootable USB drive. RAID 5 does not require four drives, it can work with three or more. References: <https://www.technewstoday.com/what-is-a-raid-5/>

NEW QUESTION: 34

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

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

Answer: C,D (LEAVE A REPLY)

Explanation

Signal blocking is a technique that prevents or reduces the transmission of electromagnetic signals from a building to the outside. Signal blocking can be achieved by using materials that absorb, reflect, or scatter the signals, such as metal, concrete, or mesh. Signal blocking can protect the data center from eavesdropping, interference, or jamming by unauthorized parties¹.

Camouflage is a technique that disguises or conceals the appearance of a building to make it less noticeable or identifiable from the outside. Camouflage can be achieved by using colors, patterns, shapes, or vegetation that blend in with the surrounding environment. Camouflage can protect the data center from detection, reconnaissance, or targeting by hostile parties

NEW QUESTION: 35

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

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

Answer: A ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 36

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

- A. Bollards
- B. Signal blocking
- C. Reflective glass
- D. Data center camouflage

Answer: (SHOW ANSWER)

Explanation

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

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

NEW QUESTION: 37

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

- A. Copy the fileshare to an LTO-4 tape drive
- B. Configure a new incremental backup job for the fileshare

- C. Create an additional partition and move a copy of the fileshare
- D. Create a snapshot of the fileshare

Answer: D ([LEAVE A REPLY](#))

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: 38

An administrator is working on improving the security of a new domain controller. A report indicates several open ports on the server. Which of the following ports should the administrator disable?

- A. 135
- B. 636
- C. 3268
- D. 3389

Answer: D ([LEAVE A REPLY](#))

Explanation

The port that should be disabled on the firewall is port 3389. Port 3389 is used by Remote Desktop Protocol (RDP), which is a protocol that allows remote access and control of a Windows system through a graphical user interface. RDP can pose a security risk if it is not properly configured or secured, as it can expose the system to unauthorized or malicious access from external sources. Therefore, port 3389 should be disabled on the firewall unless it is needed for legitimate purposes.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.3, Objective 3.3

NEW QUESTION: 39

An administrator is configuring a host-based firewall for 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)

Explanation

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. References:

<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: 40

A company has implemented a requirement to encrypt all the hard drives on its servers as part of a data loss prevention strategy. Which of the following should the company also perform as a data loss prevention method?

- A. Encrypt all network traffic
- B. Implement MFA on all the servers with encrypted data
- C. Block the servers from using an encrypted USB
- D. Implement port security on the switches

Answer: (SHOW ANSWER)

Explanation

The company should also implement MFA on all the servers with encrypted data as a data loss prevention method. MFA stands for multi-factor authentication, which is a method of verifying a user's identity by requiring two or more pieces of evidence, such as something they know (e.g., a password), something they have (e.g., a token), or something they are (e.g., a fingerprint). MFA adds an extra layer of security to prevent unauthorized access to sensitive data, even if the user's password is compromised or stolen. Encrypting the hard drives on the servers protects the data from being read or copied if the drives are physically removed or stolen, but it does not prevent unauthorized access to the data if the user's credentials are valid.

NEW QUESTION: 41

An administrator is troubleshooting performance issues on a server that was recently upgraded. The administrator met with users/stakeholders and documented recent changes in an effort to

determine whether the server is better or worse since the changes. Which of the following would BEST help answer the server performance question?

- A. Server performance thresholds
- B. A server baseline
- C. A hardware compatibility list
- D. An application service-level agreement

Answer: B ([LEAVE A REPLY](#))

Explanation

A server baseline is a set of metrics that represents the normal performance and behavior of a server under a specific workload and configuration. A server baseline can help answer the server performance question by comparing the current performance with the previous performance before the upgrade. This can help identify any changes or issues that may have affected the server performance. References:

<https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives> (Objective 4.2)

NEW QUESTION: 42

Which of the following BEST describes a warm site?

- A. The site has all infrastructure and live data.
- B. The site has all infrastructure and some data
- C. The site has partially redundant infrastructure and no network connectivity
- D. The site has partial infrastructure and some data.

Answer: D ([LEAVE A REPLY](#))

Explanation

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

<https://www.enterprisestorageforum.com/management/disaster-recovery-site/>

<https://www.techopedia.com/definition/3780/warm-site>

NEW QUESTION: 43

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](#))

Explanation

Maintenance and support is a type of license that would most likely include vendor assistance. Maintenance and support is a contract that defines the level and scope of service and assistance that a vendor provides to a customer for using their software product. Maintenance and support may include technical support, bug fixes, patches, updates, upgrades, documentation, training, and other benefits. Maintenance and support licenses usually have an annual fee based on the number of users or devices covered by the contract. Open-source is a type of license that allows free access to the source code and modification and distribution of the software product, but does not guarantee vendor assistance. Version compatibility is not a type of license, but a feature that ensures software products can work with different versions of operating systems or other software products. Subscription is a type of license that allows access to software products for a limited period of time based on recurring payments, but does not necessarily include vendor assistance.

References:

<https://www.techopedia.com/definition/1440/software-licensing>

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

NEW QUESTION: 44

A server administrator has been creating new VMs one by one. The administrator notices the system requirements are very similar, even with different applications. Which of the following would help the administrator accomplish this task in the SHORTEST amount of time and meet the system requirements?

- A. Snapshot
- B. Deduplication
- C. System Restore
- D. Template

Answer: (SHOW ANSWER)

Explanation

The method that would help the administrator accomplish the task of creating new VMs in the shortest amount of time and meet the system requirements is template. A template is a preconfigured virtual machine image that contains an operating system, applications, settings, and other components. A template can be used to create multiple identical or customized VMs quickly and easily, without having to install and configure each VM from scratch. A template can save time and ensure consistency across VMs.

NEW QUESTION: 45

A user logs in to a Linux server and attempts to run the following command:

```
sudo emacs /root/file
```

However the user gets the following message:

User userid is not allowed to execute Temacs' on this server. Which of the following would BEST allow the user to find out which commands can be used?

- A. visudo | grep userid

- B. `sudo -l -U userid`
- C. `cat /etc/passwd`
- D. `userlist | grep userid`

Answer: B ([LEAVE A REPLY](#))

Explanation

This is the best command to find out which commands can be used by a user with sudo privileges because it lists the allowed and forbidden commands for a given user or role. The -l option stands for list, and the -U option specifies the user name. The output of this command will show what commands can be executed with sudo by that user on that server. References:

<https://www.sudo.ws/man/1.8.13/sudo.man.html>

NEW QUESTION: 46

A technician is attempting to update a server's firmware. After inserting the media for the firmware and restarting the server, the machine starts normally into the OS. Which of the following should the technician do NEXT to install the firmware?

- A. Press F8 to enter safe mode
- B. Boot from the media
- C. Enable HIDS on the server
- D. Log in with an administrative account

Answer: B ([LEAVE A REPLY](#))

Explanation

The technician should boot from the media to install the firmware on the server. Firmware is a type of software that controls the low-level functions of hardware devices, such as BIOS (Basic Input/Output System), RAID controllers, network cards, etc. Firmware updates are often provided by hardware manufacturers to fix bugs, improve performance, or add new features to their devices. To install firmware updates on a server, the technician needs to boot from a media device (such as a CD-ROM, DVD-ROM, USB flash drive, etc.) that contains the firmware files and installation program. The technician cannot install firmware updates from within the operating system because firmware updates often require restarting or resetting the hardware devices.

Valid SK0-005 Dumps shared by Actual4test.com for Helping Passing SK0-005 Exam!

Actual4test.com now offer the **newest SK0-005 exam dumps**, the Actual4test.com SK0-005 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SK0-005 dumps with Test Engine here:

https://www.actual4test.com/SK0-005_examcollection.html (**492** Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 47

An administrator is working locally in a data center with multiple server racks. Which of the following is the best low-cost option to connect to any server while on site?

- A. Crash cart
- B. IPKVM
- C. Remote console access
- D. IPMI

Answer: A ([LEAVE A REPLY](#))

Explanation

A crash cart is the best low-cost option to connect to any server while on site in a data center with multiple server racks. A crash cart is a mobile unit that contains a monitor, a keyboard, a mouse, and cables that can be plugged into any server for direct access and control. A crash cart can be used for troubleshooting, maintenance, or configuration of servers without requiring remote access or network connectivity. A crash cart is also easy to move around and store in a data center. References: [CompTIA Server+ Certification Exam Objectives], Domain 2.0: Hardware, Objective 2.4: Given a scenario involving server management issues (e.g., remote access), troubleshoot using appropriate tools.

NEW QUESTION: 48

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

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

Answer: C ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 49

A server administrator is installing an OS on a new server. Company policy states no one is to log in directly to the server. Which of the following Installation methods is BEST suited to meet the company policy?

- A. GUI
- B. Core
- C. Virtualized
- D. Clone

Answer: (SHOW ANSWER)**Explanation**

A core installation is a type of installation method that is best suited to meet the company policy that states no one is to log in directly to the server. A core installation is a minimal installation option that is available when deploying some editions of Windows Server. A core installation includes most but not all server roles and features, but does not include a graphical user interface (GUI). A core installation can only be managed remotely using command-line tools such as PowerShell or Windows Admin Center, or using graphical tools such as Server Manager or Remote Desktop from another computer. This reduces the attack surface, resource consumption, and maintenance requirements of the server. A GUI installation is a type of installation method that includes a graphical user interface (GUI) and allows local or remote management using graphical tools or command-line tools. A virtualized installation is a type of installation method that involves creating and running one or more virtual machines on a physical host using a hypervisor such as Hyper-V or VMware. A clone installation is a type of installation method that involves creating an exact copy of an existing server's configuration and data on another server using tools such as Sysprep or Clonezilla. References:

<https://www.howtogeek.com/67469/the-beginners-guide-to-shell-scripting-the-basics/>

<https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual>

<https://www.howtogeek.com/199068/how-to-upgrade-your-existing-hard-drive-in-under-an-hour/>

NEW QUESTION: 50

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

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

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

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

Answer: A (LEAVE A REPLY)**Explanation**

The IP address configuration that the technician should assign to the new server so the members of the accounting group can access the server is 172.16.25.90/24 for the IP address and

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

NEW QUESTION: 51

Users at a company work with highly sensitive data. The security department implemented an administrative and technical control to enforce least-privilege access assigned to files. However, the security department has discovered unauthorized data exfiltration. Which of the following is the BEST way to protect the data from leaking?

- A. Utilize privacy screens.
- B. Implement disk quotas.
- C. Install a DLP solution.
- D. Enforce the lock-screen feature.

Answer: ([SHOW ANSWER](#))

Explanation

Components of a Data Loss Solution

NEW QUESTION: 52

A human resources analyst is attempting to email the records for new employees to an outside payroll company. Each time the analyst sends an email containing employee records, the email is rejected with an error message. Other emails outside the company are sent correctly. Which of the following is MOST likely generating the error?

- A. DHCP configuration
- B. Firewall rules
- C. DLP software
- D. Intrusion detection system

Answer: C ([LEAVE A REPLY](#))

Explanation

DLP (Data Loss Prevention) software is a type of security software that monitors and controls the transfer of sensitive or confidential data outside the organization. DLP software can prevent data breaches, data leaks, or data theft by blocking, encrypting, or alerting on unauthorized data transfers. DLP software can be applied to various channels, such as email, web, cloud, or removable devices.

In this scenario, the human resources analyst is attempting to email the records for new employees to an outside payroll company. The records for new employees may contain sensitive

or confidential data, such as personal information, tax information, or bank account information. The DLP software may detect this data and block the email from being sent outside the company, as it may violate the company's data protection policy or regulations. The DLP software may also generate an error message to inform the analyst of the reason for the rejection.

NEW QUESTION: 53

Users are 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 white 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](#))

Explanation

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

References: 3 <https://kb.vmware.com/s/article/1014508> 4

<https://www.altaro.com/vmware/vmware-esxi-purple-screen-death/>

NEW QUESTION: 54

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

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

Answer: ([SHOW ANSWER](#))

Explanation

The top portion of the dialog box lists the users and/or groups that have access to the file or folder.

NEW QUESTION: 55

Hosting data in different regional locations but not moving it for long periods of time describes:

- A. a cold site.
- B. data at rest.
- C. on-site retention.
- D. off-site storage.

Answer: ([SHOW ANSWER](#))

Explanation

Data at rest refers to data that is stored in a persistent state on any device or media, such as hard drives, tapes, or cloud storage. Data at rest does not move for long periods of time unless it is accessed or modified by authorized users or applications. A cold site (A) is a backup location that has minimal or no equipment and resources to resume business operations in case of a disaster. On-site retention is a policy of keeping backup data on premises for a certain period of time before transferring it to an off-site location. Off-site storage (D) is a method of storing backup data in a remote location that is physically or logically separated from the primary site. References:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest>

<https://www.techopedia.com/definition/144/cold-site>

<https://www.enterprisestorageforum.com/backup/onsite-offsite-backup.html>

<https://www.techopedia.com/definition/24195/offsite-storage>

NEW QUESTION: 56

An application needs 10GB of RAID 1 for log files, 20GB of RAID 5 for data files, and 20GB of RAID 5 for the operating system. All disks will be 10GB in capacity. Which of the following is the MINIMUM number of disks needed for this application?

- A. 6
- B. 7
- C. 8
- D. 9

Answer: C ([LEAVE A REPLY](#))

Explanation

To calculate the minimum number of disks needed for this application, we need to consider the RAID levels and their disk requirements. RAID 1 requires a minimum of two disks and provides mirroring, which means that data is duplicated on both disks. RAID 5 requires a minimum of three disks and provides striping with parity, which means that data is distributed across all disks with one disk storing parity information for error correction. RAID 5 can tolerate one disk failure without losing data. To create a 10GB RAID 1 array for log files, we need two 10GB disks. To create a 20GB RAID 5 array for data files, we need four 10GB disks (three for data and one for parity). To create a 20GB RAID 5 array for the operating system, we need another four 10GB disks (three for data and one for parity). Therefore, the total number of disks needed is $2 + 4 + 4 = 10$.

However, since we can use different RAID levels for different partitions on the same disk, we can optimize the disk usage by using only eight disks as follows: Disk 1: 10GB RAID 1 (log files) +

10GB RAID 5 (data files) Disk 2: 10GB RAID 1 (log files) + 10GB RAID 5 (data files) Disk 3: 10GB RAID 5 (data files) + 10GB RAID 5 (OS) Disk 4: 10GB RAID 5 (data files) + 10GB RAID 5 (OS) Disk 5: 10GB RAID 5 (parity for data files) + 10GB RAID 5 (OS) Disk 6: 10GB RAID 5 (OS) + unused space Disk 7: 10GB RAID 5 (parity for OS) + unused space Disk 8: unused space References: https://en.wikipedia.org/wiki/Standard_RAID_levels

NEW QUESTION: 57

Which of the following describes a configuration in which both nodes of a redundant system respond to service requests whenever possible?

- A. Active-passive
- B. Failover
- C. Active-active
- D. Fallback

Answer: (SHOW ANSWER)

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: 58

A technician noted the RAID hard drives were functional while troubleshooting a motherboard failure. The technician installed a spare motherboard with similar specifications and used the original components. Which of the following should the technician do to restore operations with minimal downtime?

- A. Reinstall the OS and programs.
- B. Configure old drives to RAID.
- C. Reconfigure the RAID.
- D. Install from backup.

Answer: C (LEAVE A REPLY)

Explanation

RAID (Redundant Array of Independent Disks) is a technology that combines multiple hard drives into a logical unit that provides improved performance, reliability, or capacity. RAID can be implemented by hardware, software, or a combination of both. Hardware RAID uses a dedicated controller to manage the RAID array, while software RAID uses the operating system or a driver to do the same¹.

In this scenario, the technician noted that the RAID hard drives were functional while troubleshooting a motherboard failure. This means that the data on the drives was not corrupted or lost. However, the technician installed a spare motherboard with similar specifications and

used the original components. This means that the new motherboard may not have the same RAID configuration as the old one, or it may not recognize the existing RAID array at all. Therefore, the technician needs to reconfigure the RAID in order to restore operations with minimal downtime.

NEW QUESTION: 59

Which of the following backup types only records changes to the data blocks on a virtual machine?

- A. Differential
- B. Snapshot
- C. Incremental
- D. Synthetic full

Answer: ([SHOW ANSWER](#))

Explanation

The backup type that only records changes to the data blocks on a virtual machine is snapshot. 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: 60

A server administrator is setting up a new payroll application. Compliance regulations require that all financial systems logs be stored in a central location. Which of the following should the administrator configure to ensure this requirement is met?

- A. Alerting
- B. Retention
- C. Shipping
- D. Rotation

Answer: C ([LEAVE A REPLY](#))

Explanation

Shipping is a process of sending logs from one system to another system for centralized storage and analysis.

Shipping can help ensure compliance with regulations that require financial systems logs to be stored in a central location. Shipping can also help improve security, performance, and scalability of log management.

References:

<https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives> (Objective 3.4)

NEW QUESTION: 61

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

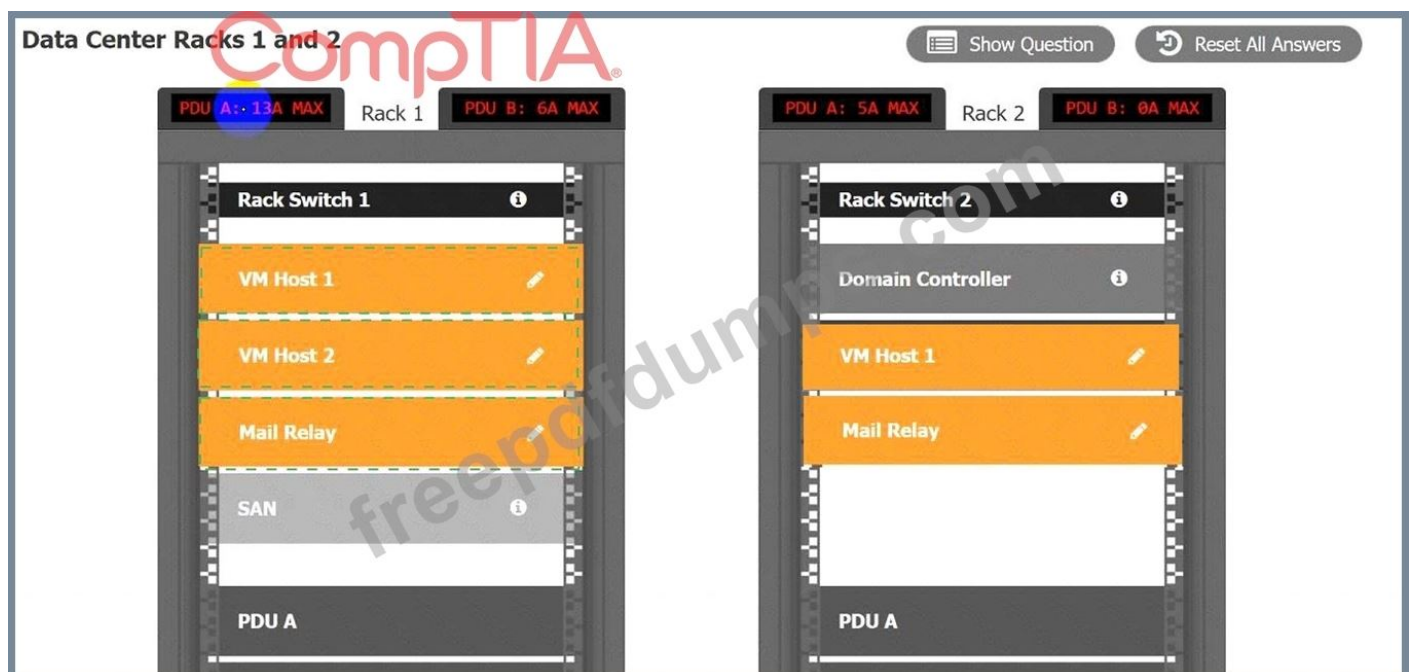
Ensure power redundancy is implemented throughout each rack and UPS alarms are resolved.

Ensure the maximum potential PDU consumption does not exceed 80% or 9.6A).

- PDU selections must be changed using the pencil icon.
- VM Hosts 1 and 2 and Mail Relay can be moved between racks.
- Certain devices contain additional details



Answer:



Explanation

Graphical user interface, application Description automatically generated



Valid SK0-005 Dumps shared by Actual4test.com for Helping Passing SK0-005 Exam!
Actual4test.com now offer the **newest SK0-005 exam dumps**, the Actual4test.com SK0-005 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SK0-005 dumps with Test Engine here:
https://www.actual4test.com/SK0-005_examcollection.html (492 Q&As Dumps, **30%OFF**
Special Discount: **Freepdfdumps**)

NEW QUESTION: 62

A systems administrator recently installed a new virtual server. After completing the installation, the administrator was only able to reach a few of the servers on the network. While testing, the administrator discovered only servers that had similar IP addresses were reachable. Which of the following is the most likely cause of the issue?

- A. The jumbo frames are not enabled.
- B. The subnet mask is incorrect.
- C. There is an IP address conflict.
- D. There is an improper DNS configuration.

Answer: B ([LEAVE A REPLY](#))

Explanation

A subnet mask is a number that distinguishes the network address and the host address within an IP address¹.

A subnet mask allows network traffic to understand IP addresses by splitting them into the network and host addresses. If the subnet mask is incorrect, the network traffic may not be able to determine the correct destination for the packets, and only reach some of the servers that have similar IP addresses. For example, if the new virtual server has an IP address of 192.168.1.100 and a subnet mask of 255.255.0.0, it can only communicate with servers that have IP addresses in the range of 192.168.0.0 to 192.168.255.255. To fix this issue, the systems administrator needs to check and correct the subnet mask of the new virtual server according to the network configuration.

NEW QUESTION: 63

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 successful. 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: 64

A datacenter technician is attempting to troubleshoot a server that keeps crashing. The server runs normally for approximately five minutes, but then it crashes. After restoring the server to operation, the same cycle repeats.

The technician confirms none of the configurations have changed, and the load on the server is steady from power-on until the crash. Which of the following will MOST likely resolve the issue?

- A.** Reseating any expansion cards in the server
- B.** Replacing the failing hard drive
- C.** Reinstalling the heat sink with new thermal paste
- D.** Restoring the server from the latest full backup

Answer: C ([LEAVE A REPLY](#))

Explanation

The most likely solution to resolve the issue of the server crashing after running normally for approximately five minutes is to reinstall the heat sink with new thermal paste. A heat sink is a device that dissipates heat from a component, such as a processor or a graphics card, by transferring it to a cooling medium, such as air or liquid. A heat sink is usually attached to the component using thermal paste, which is a substance that fills the gaps between the heat sink and the component and improves thermal conductivity. Thermal paste can degrade over time and lose its effectiveness, resulting in overheating and performance issues. If a server crashes after running for a short period of time, it may indicate that the processor is overheating due to insufficient cooling.

To resolve this issue, the technician should remove the heat sink, clean the old thermal paste, apply new thermal paste, and reinstall the heat sink.

NEW QUESTION: 65

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

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

Answer: C,D ([LEAVE A REPLY](#))

Explanation: If the server is not reachable by name but can be accessed by IP address, it means that there is a problem with name resolution. The hosts file and the DNS server are both responsible for mapping hostnames to IP addresses. Therefore, the server administrator should

check these two files for any errors or inconsistencies that might prevent the server from being resolved by name. References:

<https://www.howtogeek.com/662249/how-to-edit-the-hosts-file-on-linux/>

<https://www.howtogeek.com/164981/how-to-use-nslookup-to-check-domain-name-information-in-microsoft-win>

NEW QUESTION: 66

Which of the following licensing models was created by software companies in response to the increasing density of processors?

- A. Per-instance
- B. Per-server
- C. per-user
- D. per-core

Answer: D ([LEAVE A REPLY](#))

Explanation

The correct answer is D. per-core.

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

NEW QUESTION: 67

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: 68

Which of the following attacks is the most difficult to mitigate with technology?

- A. Ransomware
- B. Backdoor
- C. SQL injection
- D. Phishing

Answer: (SHOW ANSWER)

Explanation

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

NEW QUESTION: 69

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

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

Answer: (SHOW ANSWER)

Explanation

The administrator should connect the server to a UPS to prevent this situation in the future. A UPS (Uninterruptible Power Supply) is a device that provides backup power to a server or other device in case of a power outage or surge. A UPS typically consists of one or more batteries and an inverter that converts the battery power into AC power that the server can use. A UPS can also protect the server from power fluctuations that can damage its components or cause data

corruption. By connecting the server to a UPS, the administrator can ensure that the server will continue to run or shut down gracefully during a power failure.

NEW QUESTION: 70

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

- A. Security guards
- B. Security cameras
- C. Bollards
- D. An access control vestibule

Answer: D ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 71

Which of the following often-overlooked parts of the asset life cycle can cause the greatest number of issues in relation to PII exposure?

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

Answer: D ([LEAVE A REPLY](#))

Explanation

Disposal is the part of the asset life cycle that can cause the greatest number of issues in relation to PII exposure. PII stands for personally identifiable information, which is any data that can be used to identify a specific individual, such as name, address, phone number, email, social security number, etc. PII exposure is the unauthorized access or disclosure of PII, which can result in identity theft, fraud, or other harms to the individuals whose data is compromised. Disposal is the process of getting rid of an asset that is no longer needed or useful, such as a server, a hard drive, or a mobile device. If the disposal is not done properly, the PII stored on the asset may still be accessible or recoverable by unauthorized parties, such as hackers, thieves, or competitors. Therefore, it is important to follow best practices for secure disposal of assets that

contain PII, such as wiping, encrypting, shredding, or physically destroying the data storage media

NEW QUESTION: 72

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: 73

An administrator needs to increase the size of an existing RAID 6 array that is running out of available space.

Which of the following is the best way the administrator can perform this task?

- A. Replace all the array drives at once and then expand the array.
- B. Expand the array by changing the RAID level to 6.
- C. Expand the array by changing the RAID level to 10.
- D. Replace the array drives one at a time and then expand the array.

Answer: ([SHOW ANSWER](#)**)**

Explanation

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

NEW QUESTION: 74

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](#))

Explanation

netstat is a command-line tool that displays network connections, routing tables, interface statistics, and more.

The -a option shows all listening and non-listening sockets on the server. This can help check the open ports on a server and identify any unwanted or malicious connections. References:

<https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat>

NEW QUESTION: 75

A security technician generated a public/private key pair on a server. The technician needs to copy the key pair to another server on a different subnet. Which of the following is the most secure method to copy the keys?

HTTP

- A. FTP
- B. SCP
- C. USB

Answer: C ([LEAVE A REPLY](#))

Explanation

SCP (Secure Copy Protocol) is a protocol that allows users to securely transfer files between servers using SSH (Secure Shell) encryption. SCP encrypts both the data and the authentication information, preventing unauthorized access, interception, or modification of the files¹. SCP also preserves the file attributes, such as permissions, timestamps, and ownership².

NEW QUESTION: 76

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

- A. Connect the diagnostic card to the PCIe connector.
- B. Connect a console cable to the server NIC.
- C. Connect to the server from a crash cart.
- D. Connect the virtual administration console.

Answer: C ([LEAVE A REPLY](#))

Explanation

A crash cart is a mobile device that consists of a monitor, a keyboard, a mouse, and a network connection. It can be used to access a physical server that is not responding to remote management software or does not have out-of-band management cards configured. The

technician can connect the crash cart to the server using a VGA or HDMI cable and troubleshoot the server locally. Verified References: [Crash cart], [Out-of-band management]

Valid SK0-005 Dumps shared by Actual4test.com for Helping Passing SK0-005 Exam! Actual4test.com now offer the **newest SK0-005 exam dumps**, the Actual4test.com SK0-005 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SK0-005 dumps with Test Engine here:

https://www.actual4test.com/SK0-005_examcollection.html (492 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 77

A VLAN needs to be configured within a virtual environment for a new VM. Which of the following will ensure the VM receives a correct IP address?

- A. A virtual router
- B. A host NIC
- C. A VPN
- D. A virtual switch
- E. A vNIC

Answer: D ([LEAVE A REPLY](#))

Explanation

The correct answer is D. A virtual switch.

A virtual switch is a software-based network device that connects the virtual machines (VMs) in a virtual environment and allows them to communicate with each other and with the physical network. A virtual switch can also create and manage virtual LANs (VLANs), which are logical segments of a network that separate the traffic of different VMs or groups of VMs. A VLAN needs a DHCP server to assign IP addresses to the VMs that belong to it. A virtual switch can act as a DHCP relay agent and forward the DHCP requests from the VMs to the DHCP server on the physical network. This way, the VMs can receive correct IP addresses for their VLANs. A virtual router is a software-based network device that routes packets between different networks or subnets.

A virtual router can also create and manage VLANs, but it is not necessary for a VM to receive a correct IP address. A virtual router can be used to provide additional security, redundancy, or load balancing for the VMs. A host NIC is a physical network interface card that connects the host machine to the physical network. A host NIC can also support VLAN tagging, which allows the host machine to communicate with different VLANs on the network. However, a host NIC alone cannot ensure that a VM receives a correct IP address for its VLAN. The host NIC needs to be connected to a virtual switch that can relay the DHCP requests from the VMs to the DHCP server. A VPN is a virtual private network that creates a secure tunnel between two or more devices over the internet.

A VPN can be used to encrypt and protect the data traffic of the VMs, but it is not related to the configuration of VLANs or IP addresses. A VPN does not affect how a VM receives a correct IP address for its VLAN. A vNIC is a virtual network interface card that connects a VM to a virtual switch or a virtual router. A vNIC can also support VLAN tagging, which allows the VM to communicate with different VLANs on the network.

However, a vNIC alone cannot ensure that a VM receives a correct IP address for its VLAN. The vNIC needs to be connected to a virtual switch or a virtual router that can relay the DHCP requests from the VMs to the DHCP server¹²

NEW QUESTION: 78

A server administrator is using remote access to update a server. The administrator notices numerous error messages when using YUM to update the applications on a server. Which of the following should the administrator check FIRST?

- A.** Network connectivity on the server
- B.** LVM status on the server
- C.** Disk space in the /var directory
- D.** YUM dependencies

Answer: C ([LEAVE A REPLY](#))

Explanation

The administrator should check disk space in the /var directory first when using YUM to update applications on a server. YUM stands for Yellowdog Updater Modified, which is a software package manager for Linux systems that use RPM (Red Hat Package Manager) packages. YUM downloads and installs packages from online repositories and resolves dependencies automatically. YUM stores its cache files in the /var/cache/yum directory by default. These cache files include metadata and package data for each repository that YUM uses.

If there is not enough disk space in the /var directory, YUM may fail to update applications and generate error messages.

NEW QUESTION: 79

A company wants to find an affordable way to simulate a fail over of a critical application. The company does not currently have a solution for it. The application consists of 15 servers, and the company would like to simulate on production configurations and IP address schemes. Which of the following would be the most cost-effective solution?

- A.** Build a warm site and perform a fail over of the application.
- B.** Build a cloud IaaS and perform a fail over of the application.
- C.** Build a hot site and perform a fail over of the application.
- D.** Build a cold site and perform a fail over of the application.
- E.** Perform a tabletop fail over of the application.

Answer: B ([LEAVE A REPLY](#))

Explanation

Cloud IaaS (Infrastructure as a Service) is a service model that allows users to rent virtualized computing resources over the internet, such as servers, storage, network, and software. Cloud IaaS can provide several benefits for disaster recovery and failover scenarios, such as:

Lower cost: Cloud IaaS can reduce the capital and operational expenses of building and maintaining a physical disaster recovery site, as users only pay for the resources they use on demand¹².

Scalability: Cloud IaaS can offer flexible and elastic scalability of resources, as users can easily provision or deprovision resources according to their needs and workload¹².

Availability: Cloud IaaS can ensure high availability and reliability of the application, as users can leverage the cloud provider's redundant and geographically distributed infrastructure¹².

Simplicity: Cloud IaaS can simplify the failover process, as users can use the cloud provider's tools and services to automate and orchestrate the failover operations¹².

Therefore, building a cloud IaaS and performing a failover of the application would be the most cost-effective solution for the company, as it would allow them to simulate a failover of a critical application on production configurations and IP address schemes without investing in a physical disaster recovery site.

NEW QUESTION: 80

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

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

Answer: A ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 81

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 four 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: 82

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: 83

Which of the following security risks provides unauthorized access to an application?

- A. Backdoor
- B. Data corruption
- C. Insider threat
- D. Social engineering

Answer: [\(SHOW ANSWER\)](#)

Explanation

A backdoor is a security risk that provides unauthorized access to an application. A backdoor is a hidden or undocumented way of bypassing the normal authentication or encryption mechanisms of an application, allowing an attacker to gain remote access, execute commands, or steal data. A backdoor can be created intentionally by the developer, maliciously by an attacker, or unintentionally by a programming error. References: CompTIA Server+ Certification Exam Objectives, Domain 5.0: Security, Objective 5.2:

Given a scenario, apply logical access control methods.

NEW QUESTION: 84

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

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

Answer: [C \(LEAVE A REPLY\)](#)

Explanation

An action that the administrator should take to harden the hardware of a new server is to set a BIOS password.

BIOS (Basic Input/Output System) is a firmware that initializes the hardware components and settings of a system before loading the operating system. BIOS password is a security feature that requires a user to enter a password before accessing or modifying the BIOS settings or booting up the system. By setting a BIOS password, the administrator can prevent unauthorized or malicious users from changing the hardware configuration or boot order of the server.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 5, Lesson 5.1, Objective 5.1

NEW QUESTION: 85

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

- A. Variable

- B. Loop
- C. Comparator
- D. Conditional

Answer: B ([LEAVE A REPLY](#))

Explanation

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

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

Copy

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

1: CompTIA Server+ Certification Exam Objectives

NEW QUESTION: 86

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

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

Answer: D ([LEAVE A REPLY](#))

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: 87

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

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

Answer: C ([LEAVE A REPLY](#))

Explanation

Camouflage is an architectural reinforcement that is used to attempt to conceal the exterior of an organization.

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

NEW QUESTION: 88

A server administrator has noticed that the storage utilization on a file server is growing faster than planned.

The administrator wants to ensure that, in the future, there is a more direct relationship between the number of users using the server and the amount of space that might be used. Which of the following would BEST enable this correlation?

- A. Partitioning
- B. Deduplication
- C. Disk quotas
- D. Compression

Answer: C ([LEAVE A REPLY](#))

Explanation

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

Disk quotas can also provide reports and alerts on disk space usage and quota status.

NEW QUESTION: 89

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

- A.** A firewall blocking the ICMP echo reply.
- B.** The DHCP scope option is incorrect
- C.** The DNS entries for the print server are incorrect.
- D.** The hosts file misconfigured.

Answer: D ([LEAVE A REPLY](#))

Explanation

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

References: [Hosts file], [DNS]

NEW QUESTION: 90

A technician is attempting to reboot a remote physical Linux server. However, attempts to command a shutdown -----now result in the loss of the SSH connection. The server still responds to pings. Which of the following should the technician use to command a remote shutdown?

- A.** virtual serial console
- B.** A KVM
- C.** An IDRAC
- D.** A crash cart

Answer: ([SHOW ANSWER](#)**)**

Explanation

An IDRAC (Integrated Dell Remote Access Controller) is a tool that can be used to command a remote shutdown of a physical Linux server. An IDRAC is a hardware device that provides out-of-band management for Dell servers. It allows the technician to access the server's console, power cycle, reboot, or shut down the server remotely using a web interface or a command-line interface. An IDRAC does not depend on the operating system or network connectivity of the server. A virtual serial console is a tool that can be used to access a remote virtual machine's console using a serial port connection. A KVM (Keyboard, Video, Mouse) switch is a device that allows the technician to switch between different computer sources using the same keyboard, monitor, and mouse. A crash cart is a mobile unit that contains a keyboard, monitor, mouse, and other tools that can be connected to a physical server for troubleshooting purposes. References: <https://www.dell.com/support/kbdoc/en-us/000131486/understanding-the-idrac>

<https://www.howtogeek.com/799968/what-is-a-kvm-switch/>

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

NEW QUESTION: 91

The network's IDS is giving multiple alerts that unauthorized traffic from a critical application server is being sent to a known-bad public IP address.

One of the alerts contains the following information:

Exploit Alert

Attempted User Privilege Gain

2/2/07-3: 09:09 10.1.200.32

--> 208.206.12.9:80

This server application is part of a cluster in which two other servers are also servicing clients.

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

- A. Disable all services on the affected application server.
- B. Perform a vulnerability scan on all the servers within the cluster and patch accordingly.
- C. Block access to 208.206.12.9 from all servers on the network.
- D. Change the IP address of all the servers in the cluster to the 208.206.12.0/26 subnet.
- E. Enable GPO to install an antivirus on all the servers and perform a weekly reboot.
- F. Perform an antivirus scan on all servers within the cluster and reboot each server.

Answer: ([SHOW ANSWER](#))

Explanation

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

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

Valid SK0-005 Dumps shared by Actual4test.com for Helping Passing SK0-005 Exam!
Actual4test.com now offer the **newest SK0-005 exam dumps**, the Actual4test.com SK0-005 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SK0-005 dumps with Test Engine here:

Special Discount: [Freepdfdumps](#))

NEW QUESTION: 92

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

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

Answer: D ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 93

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

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

Answer: ([SHOW ANSWER](#)**)**

Explanation

User activity reports were used to identify the security breach in the human resources department. User activity reports are records of the actions and events performed by users on a system or network, such as login/logout times, files accessed or modified, commands executed, or websites visited. User activity reports can help monitor and audit user behavior, detect and investigate security incidents, and enforce policies and compliance. User activity reports can be generated by various tools, such as log management software, security information and event management (SIEM) systems, or user and entity behavior analytics (UEBA) solutions.

References: [CompTIA Server+ Certification Exam Objectives], Domain 5.0: Security, Objective

5.2: Given a scenario, apply logical access control methods.

NEW QUESTION: 94

Users cannot access a new server by name, but the server does respond to a ping request using its IP address.

All the user workstations receive their IP information from a DHCP server. Which of the following would be the best step to perform NEXT?

- A. Run the tracert command from a workstation.
- B. Examine the DNS to see if the new server record exists.
- C. Correct the missing DHCP scope.
- D. Update the workstation hosts file.

Answer: B ([LEAVE A REPLY](#))

Explanation

If users cannot access a new server by name, but the server does respond to a ping request using its IP address, it means that there is a problem with name resolution. The DNS (Domain Name System) is a service that maps hostnames to IP addresses and vice versa. Therefore, the best step to perform next is to examine the DNS to see if the new server record exists and matches its IP address. If not, the DNS record needs to be added or updated accordingly.

Running the tracert command from a workstation would not help with name resolution, as it only shows the route taken by packets to reach a destination by IP address. Correcting the missing DHCP scope would not help either, as DHCP (Dynamic Host Configuration Protocol) only assigns IP addresses and other network settings to clients, but does not resolve names. Updating the workstation hosts file would be a temporary workaround, but not a permanent solution, as it would require manually editing every workstation's hosts file with the new server's name and IP address.

References:

<https://www.howtogeek.com/164981/how-to-use-nslookup-to-check-domain-name-information-in-microsoft-win>

<https://www.howtogeek.com/howto/27350/beginner-geek-how-to-edit-your-hosts-file/>

NEW QUESTION: 95

A server technician notices a server is very low on disk space. Upon inspecting the disk utilization, the technician discovers server logs are taxing up a large amount of space. There is no central log server. Which of the following would help free up disk space?

- A. Log rotation
- B. Log shipping
- C. Log alerting
- D. Log analysis

Answer: B ([LEAVE A REPLY](#))

Explanation

Log rotation is a process that periodically renames, compresses, and deletes old log files to free up disk space and keep log files manageable. Log rotation can be configured using tools such as

logrotate or cron on Linux systems, or using Windows Task Scheduler or PowerShell scripts on Windows systems. Log rotation can also help with log analysis and troubleshooting by making it easier to find relevant information in smaller and more recent log files. References:

<https://www.mezmo.com/learn-log-management/what-is-log-rotation-how-does-it-work>

<https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/logman>

NEW QUESTION: 96

Which of the following licensing models is MOST appropriate for a data center that has a variable daily equipment count?

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

Answer: D ([LEAVE A REPLY](#))

Explanation

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

Verified References: [Per Core Licensing and Basic Definitions]

NEW QUESTION: 97

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 cards
- D. Physical tokens

Answer: B ([LEAVE A REPLY](#))

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: 98

Which of the following actions should a server administrator take once a new backup scheme has been configured?

- A. Overwrite the backups

- B. Clone the configuration
- C. Run a restore test
- D. Check the media integrity

Answer: ([SHOW ANSWER](#))

Explanation

The action that the server administrator should take once a new backup scheme has been configured is to run a restore test. A restore test is a process of verifying that the backup data can be successfully recovered and restored to its original location or a different location. A restore test can help ensure that the backup scheme is working properly, that the backup data is valid and consistent, and that there are no errors or issues during the recovery process. A restore test should be performed periodically and after any changes to the backup configuration or environment.

NEW QUESTION: 99

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: ([SHOW ANSWER](#))

Explanation

The type of data replication that is required for a hot-site disaster recovery model is constant. A hot site is a type of disaster recovery site that has fully operational IT infrastructure and equipment that can take over the primary site's functions immediately in case of a disaster or disruption. A hot site requires constant data replication between the primary site and the hot site to ensure that the data is up-to-date and consistent.

Constant data replication means that any changes made to the data at the primary site are immediately copied to the hot site without any delay or lag.

NEW QUESTION: 100

A server administrator has a system requirement to install the virtual OS on bare metal hardware. Which of the following hypervisor virtualization technologies should the administrator use to BEST meet the system requirements? (Select TWO)

- A. Host
- B. Template
- C. Clone
- D. Type1
- E. Type2
- F. Guest

Answer: ([SHOW ANSWER](#))

Explanation

A template is a preconfigured virtual machine image that can be used to create new virtual machines quickly and easily. A template can include the operating system, applications, settings, and data that are required for a specific purpose or role. A type 1 hypervisor is a virtualization technology that runs directly on bare metal hardware, without requiring an underlying operating system. A type 1 hypervisor can provide better performance, security, and isolation for virtual machines than a type 2 hypervisor, which runs on top of an operating system. Verified

References: [Template], [Type 1 hypervisor]

NEW QUESTION: 101

A server administrator is instating a new server in a data center. The administrator connects the server to a midplane but does not connect any cables Which of the following types of servers is the administrator MOST likely installing?

- A. Rack
- B. Virtual
- C. Tower
- D. Blade

Answer: ([SHOW ANSWER](#))

Explanation

A blade server is a type of server that is installed in a chassis or an enclosure that provides power, cooling, networking, and management features. The blade server does not have any cables attached to it, as it connects to the chassis through a midplane or a backplane. A blade server can save space, energy, and cost compared to other types of servers. Verified

References: [Blade server], [Chassis]

NEW QUESTION: 102

The management team has mandated the use of data-at-rest encryption on all corporate servers. Using this encryption paradigm will ensure:

- A. website traffic is protected while traversing the internet.
- B. files stored on the server are protected against physical theft.
- C. attachments that are emailed from this server cannot be intercepted.
- D. databases in use are protected from remote hackers.

Answer: B ([LEAVE A REPLY](#))

Explanation

Data-at-rest encryption is a method of encrypting data while it is stored on a storage device, such as a hard drive, an SSD, or a tape library. This ensures that if the data is stolen or lost, it will be unreadable without the encryption key. Data-at-rest encryption does not protect data while it is in transit over the network, in use by the CPU or memory, or attached to an email.

NEW QUESTION: 103

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

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

Answer: A,C ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 104

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

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

Answer: ([SHOW ANSWER](#)**)**

Explanation

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

NEW QUESTION: 105

A technician needs maximum power redundancy while configuring a new server rack. Which of the following should be specified? (Select two).

- A. Separate circuits
- B. Rack balancing
- C. Blanking panels

- D. High-voltage PDUs
- E. KVM placement
- F. Multiple UPSs

Answer: A,F ([LEAVE A REPLY](#))

Explanation

Separate circuits and multiple UPSs can provide fail-safe power redundancy for a server rack. Separate circuits mean that the server rack is connected to two or more independent power sources, such as different utility lines or generators. This can prevent a single point of failure in the power supply, as if one circuit goes down, the other circuit can still provide power to the server rack¹. Multiple UPSs mean that the server rack has two or more uninterruptible power supplies, which are devices that provide backup power and surge protection in case of a power outage or fluctuation. Multiple UPSs can be connected to separate circuits, or to different outlets on the same circuit, to increase the reliability and availability of power for the server rack²³.

NEW QUESTION: 106

Several new components have been added to a mission-critical server, and corporate policy states all new components must meet server hardening requirements. Which of the following should be applied?

- A. Definition updates
- B. Driver updates
- C. OS security updates
- D. Application updates

Answer: B ([LEAVE A REPLY](#))

Explanation

Driver updates should be applied to the new components that have been added to a mission-critical server, as part of the server hardening requirements. Drivers are software programs that enable the communication and functionality of hardware devices, such as network cards, storage controllers, or graphics cards. Updating drivers can improve the performance, compatibility, and stability of the new components with the server operating system and applications. References: CompTIA Server+ Certification Exam Objectives, Domain 2.0: Hardware, Objective 2.2: Given a scenario, install, configure and maintain server components.

Valid SK0-005 Dumps shared by Actual4test.com for Helping Passing SK0-005 Exam!
Actual4test.com now offer the **newest SK0-005 exam dumps**, the Actual4test.com SK0-005 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SK0-005 dumps with Test Engine here:

Special Discount: Freepdfdumps)

NEW QUESTION: 107

A software developer is unable to reach an internal website. The developer's attempt to ping the FQDN returns the following IP address: 104.18.17.32. Which of the following is the most likely reason for this result?

- A.** The NIC is set to DHCP.
- B.** The default gateway is misconfigured.
- C.** The primary DNS server is 8.8.8.8.
- D.** There is a manual entry in the hosts file.

Answer: D ([LEAVE A REPLY](#))

Explanation

The most likely reason for this result is that there is a manual entry in the hosts file that maps the FQDN to an incorrect IP address (104.18.17.32). The hosts file is a text file that contains mappings of hostnames or domain names to IP addresses, which are used by the operating system to resolve names before querying DNS servers on the network or internet. The hosts file can be used to override DNS settings or block access to certain websites by redirecting them to different IP addresses, such as localhost (127.0.0.1) or invalid addresses (0.0.0.0). If there is a manual entry in the hosts file that conflicts with DNS records, it can cause name resolution errors or connectivity issues. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Networking, Objective 4.1: Given a scenario, configure network settings for servers.

NEW QUESTION: 108

A technician has moved a data drive from a new Windows server to an older Windows server. The hardware recognizes the drive, but the data is not visible to the OS. Which of the following is the MOST Likely cause of the issue?

- A.** The disk uses GPT.
- B.** The partition is formatted with ext4.
- C.** The -partition is formatted with FAT32.
- D.** The disk uses MBn.

Answer: (SHOW ANSWER)

Explanation

GPT (GUID Partition Table) is a partitioning scheme that allows creating partitions on large hard drives (more than 2 TB). It supports up to 128 partitions per drive and uses 64-bit addresses to locate them. However, GPT is not compatible with older versions of Windows, such as Windows XP or Windows Server 2003, which use MBR (Master Boot Record) as the partitioning scheme. If a disk uses GPT, it may not be recognized or accessible by an older Windows server. Verified References: [GPT], [MBR]

NEW QUESTION: 109

A new 40GB NIC has just been installed in a server but is not detected within the Windows server OS. Which of the following would most likely fix the issue?

- A. Update the firmware on the NIC.
- B. Update the server OS.
- C. Update the remote management console.
- D. Update the switch firmware.

Answer: A ([LEAVE A REPLY](#))

Explanation

Updating the firmware on the NIC is the most likely solution to fix the issue of a new 40GB NIC not being detected within the Windows server OS. Firmware is a software program that controls the functionality of a hardware device, such as a NIC (network interface card). A NIC is a device that enables network communication for a server by providing an interface between the server and the network cable or wireless connection. Updating the firmware on the NIC can improve its performance, compatibility, and stability with the server OS and network protocols. References:

CompTIA Server+ Certification Exam Objectives, Domain

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

NEW QUESTION: 110

A technician has been tasked to install a new CPU. Prior to the installation the server must be configured.

Which of the following should the technician update?

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

Answer: B ([LEAVE A REPLY](#))

Explanation

The BIOS (Basic Input/Output System) is a firmware that controls the initialization and booting of a server. It also provides settings for the CPU, such as speed, voltage, and temperature.

Updating the BIOS can improve the performance and compatibility of the CPU and other hardware components. Verified References: [BIOS],

[CPU]

NEW QUESTION: 111

Which of the following backup types resets the archive bit each time it is run?

- A. Differential
- B. Snapshot
- C. Incremental
- D. Synthetic 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: 112

A security manager is concerned that a rogue employee could boot a server from an outside USB drive. Which of the following actions can be taken to reduce this risk? (Select TWO).

- A. Close unneeded ports.
- B. Disable unneeded physical ports.
- C. Set a BIOS password.
- D. Install a SIEM.
- E. Disable unneeded services.
- F. Install a HIDS.

Answer: ([SHOW ANSWER](#))

Explanation

Disabling unneeded physical ports would prevent unauthorized devices from being connected to the server, such as an outside USB drive. Setting a BIOS password would restrict access to the boot settings and prevent unauthorized changes to the boot order. The other options would not address the risk of booting from an outside USB drive

NEW QUESTION: 113

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

- A. SSH
- B. VPN
- C. SELinux
- D. FTPS

Answer: A ([LEAVE A REPLY](#))

Explanation

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

References:

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

NEW QUESTION: 114

An administrator discovers a misconfiguration that impacts all servers but can be easily corrected. The administrator has a list of affected servers and a script to correct the issue. Which of the following scripting principles should the administrator use to cycle through the list of servers to deliver the needed change?

- A. Linked list
- B. String
- C. Loop
- D. Constant

Answer: ([**SHOW ANSWER**](#)**)**

Explanation

A loop is a programming construct that allows a block of code to be executed repeatedly until a certain condition is met¹. A loop can be used to cycle through a list of servers and run a script on each one of them.

For example, in Python, a loop can be written as:

Python

This code is AI-generated. Review and use carefully. Visit our FAQ for more information.

Copy

```
# Assume servers is a list of server names
for server in servers:
    # Run the script on the server
    run_script(server)
```

A loop can help automate the task of correcting the misconfiguration on all servers, saving time and effort.

NEW QUESTION: 115

A server administrator is taking advantage of all the available bandwidth of the four NICs on the server.

Which of the following NIC-teaming technologies should the server administrator utilize?

- A. Fail over
- B. Fault tolerance
- C. Load balancing
- D. Link aggregation

Answer: ([**SHOW ANSWER**](#)**)**

Explanation

Link aggregation is a technique that combines multiple physical network links into one logical link with higher bandwidth and redundancy. It can take advantage of all the available bandwidth of the NICs (Network Interface Cards) on the server and provide load balancing and failover capabilities for network traffic. Verified References: [Link aggregation], [NIC]

NEW QUESTION: 116

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

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

Answer: B ([LEAVE A REPLY](#))

Explanation

The most effective way to mitigate risks associated with privacy-related data leaks when sharing with a third party is customer data encryption and masking. Encryption is a process of transforming data into an unreadable format that can only be decrypted with a key or password. Masking is a process of hiding or replacing sensitive data with fake or meaningless data. By encrypting and masking customer data, the organization can protect the confidentiality and integrity of the data and prevent unauthorized access or disclosure by the third party.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.3, Objective 3.3

NEW QUESTION: 117

A technician has several possible solutions to a reported server issue. Which of the following BEST represents how the technician should proceed with troubleshooting?

- A. Determine whether there is a common element in the symptoms causing multiple problems.
- B. Perform a root cause analysis.
- C. Make one change at a time and test.
- D. Document the findings, actions, and outcomes throughout the process.

Answer: C ([LEAVE A REPLY](#))

Explanation

This is the best way to proceed with troubleshooting when the technician has several possible solutions to a reported server issue. Making one change at a time and testing allows the technician to isolate the cause and effect of each solution and determine which one works best. It also helps to avoid introducing new problems or complicating existing ones by making multiple changes at once. Determining whether there is a common element in the symptoms causing multiple problems is a good step to perform before identifying possible solutions, but not after. Performing a root cause analysis is a good step to perform after resolving the issue, but not during. Documenting the findings, actions, and outcomes throughout the process is a good practice to follow at every step of troubleshooting, but not a specific way to proceed with testing possible solutions.

References:

<https://www.howtogeek.com/174288/how-to-tell-if-your-computer-is-overheating-and-what-to-do-about-it/>

<https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-it-matter/>

NEW QUESTION: 118

A technician is connecting a server's secondary NIC to a separate network. The technician connects the cable to the switch but then does not see any link lights on the NIC. The technician confirms there is nothing wrong on the network or with the physical connection. Which of the following should the technician perform NEXT?

- A. Restart the server
- B. Configure the network on the server
- C. Enable the port on the server
- D. Check the DHCP configuration

Answer: C ([LEAVE A REPLY](#))

Explanation

The next thing that the technician should perform is to enable the port on the server. A port is a logical endpoint that identifies a specific service or application on a network device. A port can be enabled or disabled depending on whether the service or application is running or not. If a port is disabled on a server, it means that the server cannot send or receive any network traffic on that port, which can prevent communication with other devices or services that use that port. In this case, if port 389 is disabled on the server, it means that the server cannot use LDAP to access or modify directory services over a network. To resolve this issue, the technician should enable port 389 on the server using commands such as netsh or iptables.

NEW QUESTION: 119

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

- A. Hardware failure
- B. Malware
- C. Data corruption
- D. Insider threat

Answer: D ([LEAVE A REPLY](#))

Explanation

An insider threat is a type of risk that can be mitigated by implementing split encryption keys for sensitive files. An insider threat is a malicious actor who has authorized access to an organization's system or data and uses it for unauthorized or harmful purposes. An insider threat can cause data breaches, sabotage, fraud, theft, espionage, or other damages to the organization. Split encryption keys are a method of encrypting data using multiple keys that are stored separately and require collaboration to decrypt. Split encryption keys can prevent an insider threat from accessing or compromising sensitive data without being detected by another authorized party who holds another key. Hardware failure is a type of risk that involves physical damage or malfunction of hardware components such as hard drives, memory modules, power supplies, or fans. Hardware failure can cause data loss, system downtime, performance issues,

or other problems for the organization. Hardware failure cannot be mitigated by split encryption keys, but by backup, redundancy, monitoring, and maintenance measures.

NEW QUESTION: 120

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: ([SHOW ANSWER](#))

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: 121

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

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

Answer: ([SHOW ANSWER](#))

Explanation

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

Valid SK0-005 Dumps shared by Actual4test.com for Helping Passing SK0-005 Exam!

Actual4test.com now offer the **newest SK0-005 exam dumps**, the Actual4test.com SK0-005 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SK0-005 dumps with Test Engine here:

Special Discount: Freepdfdumps)

NEW QUESTION: 122

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

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

Answer: A ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 123

A technician recently replaced a NIC that was not functioning. Since then, no device driver is found when starting the server, and the network card is not functioning. Which of the following should the technician check first?

- A.** The boot log
- B.** The BIOS
- C.** The HCL
- D.** The event log

Answer: C ([LEAVE A REPLY](#))

Explanation

The technician should check the hardware compatibility list (HCL) first to see if the new NIC is supported by the server's operating system. The HCL is a list of hardware devices that have been tested and verified to work with a specific operating system. If the NIC is not on the HCL, it means that there is no device driver available or compatible for it, and the NIC will not function properly.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 5, Lesson 5.2, Objective 5.2

NEW QUESTION: 124

A technician is configuring a point-to-point heartbeat connection between two servers using IP addressing.

Which of the following is the most efficient subnet mask for this connection?

- A. /28
- B. /29
- C. /30
- D. /32

Answer: C ([LEAVE A REPLY](#))

Explanation

The most efficient subnet mask for a point-to-point heartbeat connection between two servers using IP addressing is /30. A /30 subnet mask has 255.255.255.252 as its decimal representation and

11111111.11111111.11111111.11111100 as its binary representation. This means that there are only two bits available for the host portion of the IP address, which allows for four possible combinations: 00, 01, 10, and

11. However, the first and the last combinations are reserved for the network address and the broadcast address, respectively. Therefore, only two IP addresses are usable for the point-to-point connection, which is the minimum required for such a link. A /30 subnet mask is also known as a point-to-point prefix because it is commonly used for point-to-point links between routers or servers¹.

A /28 subnet mask has 255.255.255.240 as its decimal representation and

11111111.11111111.11111111.11110000 as its binary representation. This means that there are four bits available for the host portion of the IP address, which allows for 16 possible combinations. However, two of them are reserved for the network address and the broadcast address, respectively. Therefore, 14 IP addresses are usable for the subnet, which is more than needed for a point-to-point connection and would result in wasted addresses.

A /29 subnet mask has 255.255.255.248 as its decimal representation and

11111111.11111111.11111111.11111000 as its binary representation. This means that there are three bits available for the host portion of the IP address, which allows for eight possible combinations. However, two of them are reserved for the network address and the broadcast address, respectively. Therefore, six IP addresses are usable for the subnet, which is still more than needed for a point-to-point connection and would result in wasted addresses.

A /32 subnet mask has 255.255.255.255 as its decimal representation and

11111111.11111111.11111111.11111111 as its binary representation. This means that there are no bits available for the host portion of the IP address, which allows for only one possible combination: all ones.

Therefore, only one IP address is usable for the subnet, which is not enough for a point-to-point connection and would result in an invalid configuration.

Therefore, a /30 subnet mask is the most efficient choice for a point-to-point heartbeat connection between two servers using IP addressing because it provides exactly two usable IP addresses without wasting any addresses or creating any conflicts¹.

NEW QUESTION: 125

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

- A.** A drive failed in the OS array.
- B.** A drive failed and then recovered in the data array.
- C.** A drive failed in both of the arrays.
- D.** A drive failed in the data array.

Answer: A ([LEAVE A REPLY](#))

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

<https://www.technewstoday.com/what-is-a-raid-0/> <https://www.technewstoday.com/what-is-a-raid-10/>

NEW QUESTION: 126

A server administrator is exporting Windows system files before patching and saving them to the following location:

\\server1\ITDept\

Which of the following is a storage protocol that the administrator is MOST likely using to save this data?

- A.** eSATA
- B.** FCoE
- C.** CIFS
- D.** SAS

Answer: ([SHOW ANSWER](#)**)**

Explanation

The storage protocol that the administrator is most likely using to save data to the location \\server1\ITDept\ is CIFS. CIFS (Common Internet File System) is a protocol that allows file

sharing and remote access over a network. CIFS is based on SMB (Server Message Block), which is a protocol that enables communication between devices on a network. CIFS uses UNC (Universal Naming Convention) paths to identify network resources, such as files or folders. A UNC path has the format \servername\sharename\path\filename. In this case, server1 is the name of the server, ITDept is the name of the shared folder, and \ is the path within the shared folder.

NEW QUESTION: 127

A technician needs to deploy an operating system that would optimize server resources. Which of the following server installation methods would BEST meet this requirement?

- A.** Full
- B.** Bare metal
- C.** Core
- D.** GUI

Answer: C ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 128

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

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

Answer: C ([LEAVE A REPLY](#))

Explanation

Bash is a scripting language that is commonly used in Linux systems to automate tasks and manipulate text.

Bash scripts can run commands, variables, functions, loops, and conditional statements. PowerShell is a scripting language that is mainly used in Windows systems, while batch command files are simple text files that contain a series of commands to be executed by the command-line interpreter. Visual Basic is a programming language that is used to create applications, not scripts. References: [CompTIA Server+ Certification Exam Objectives], Domain

4.0: Server Administration, Objective 4.2: Given a scenario, perform proper server maintenance techniques.

NEW QUESTION: 129

A Linux server was recently updated. Now, the server stops during the boot process with a blank screen and an

prompt. When of the following is the MOST likely cause of this issue?

- A. The system is booting to a USB flash drive
- B. The UEFI boot was interrupted by a missing Linux boot file
- C. The BIOS could not find a bootable hard disk
- D. The BIOS firmware needs to be upgraded

Answer: B ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 130

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](#))

Explanation: 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. References:

<https://www.dell.com/support/kbdoc/en-us/000130114/how-to-troubleshoot-a-faulty-backplane>

NEW QUESTION: 131

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

- A. The server has not been joined to the domain.
- B. An IP address has not been assigned to the server.
- C. The server requires a reboot to complete the deployment process.
- D. The domain credentials are invalid.

Answer: A ([LEAVE A REPLY](#))

Explanation

The most likely cause of the issue is that the server has not been joined to the domain. A domain is a logical group of computers and devices that share a common directory service and security policy. A domain controller is a server that manages the domain and authenticates users and computers that want to access domain resources. To log on with domain credentials, a server must be joined to the domain and registered in the directory service. If a server has not been joined to the domain, it will not be recognized or authorized by the domain controller.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 4, Lesson 4.3, Objective 4.3

NEW QUESTION: 132

A server technician has received reports of database update errors. The technician checks the server logs and determines the database is experiencing synchronization errors. To attempt to correct the errors, the technician should FIRST ensure:

- A. the correct firewall zone is active
- B. the latest firmware was applied
- C. NTP is running on the database system
- D. the correct dependencies are installed

Answer: ([SHOW ANSWER](#)**)**

Explanation

The first thing that the technician should ensure to correct the database synchronization errors is that NTP is running on the database system. NTP (Network Time Protocol) is a protocol that synchronizes the clocks of network devices with a reference time source, such as an atomic clock or a GPS receiver. NTP ensures that all devices on a network have accurate and consistent time settings, which can affect various functions and applications. Database synchronization is a process of maintaining data consistency and integrity across multiple database servers or instances. Database synchronization can depend on accurate time settings, as time stamps are often used to determine which data is newer or older, and which data should be updated or

overwritten. If NTP is not running on the database system, it may cause time drift or discrepancy between different database servers or instances, which can result in synchronization errors or data conflicts.

NEW QUESTION: 133

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

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

Answer: A ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 134

A company created a new DR plan. The management team would like to begin performing a review of this plan without endangering company data and with a minimal time commitment. Which of the following testing methods would best allow for this type of review?

- A. Simulated
- B. Tabletop
- C. Live
- D. Non-production

Answer: B ([LEAVE A REPLY](#))

Explanation

Tabletop testing is a method of reviewing a DR plan without endangering company data and with a minimal time commitment. Tabletop testing involves a simulated scenario where the participants discuss their roles and responsibilities, identify potential issues, and evaluate the effectiveness of the plan. Simulated, live, and non-production testing are methods that involve more time and resources, and may pose some risks to company data. References: [CompTIA Server+ Certification Exam Objectives], Domain 6.0: Disaster Recovery, Objective 6.3: Compare and contrast various backup techniques.

NEW QUESTION: 135

A technician is deploying a single server to monitor and record the 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](#))

Explanation

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

NEW QUESTION: 136

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

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

Answer: D ([LEAVE A REPLY](#))

Explanation

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

<https://www.ibm.com/cloud/learn/service-level-agreements>

Valid SK0-005 Dumps shared by Actual4test.com for Helping Passing SK0-005 Exam!
Actual4test.com now offer the **newest SK0-005 exam dumps**, the Actual4test.com SK0-005 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SK0-005 dumps with Test Engine here:
https://www.actual4test.com/SK0-005_examcollection.html (492 Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 137

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: 138

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

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

Answer: A ([LEAVE A REPLY](#))

Explanation

Open-source software is software that is freely available and can be modified and distributed by anyone. It usually requires very little technical support and has no licensing fees. Therefore, it would be the lowest cost solution for an application that does not need much support.

References:

<https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives> (Objective 2.3)

NEW QUESTION: 139

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

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

Answer: ([SHOW ANSWER](#))

Explanation

Retention policies are the guidelines that dictate when to delete data backups based on operational or compliance needs. They specify how long, how, where, and in what format the data backups are stored, and who has authority over them. The other options are not directly related to the deletion of data backups.

<https://backup.ninja/news/Database-Backups-101-Backup-Retention-Policy-Considerations>

NEW QUESTION: 140

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. Tabletop
- B. Backup recovery test
- C. Live failover
- D. Hot-site visit audit

Answer: ([SHOW ANSWER](#))

Explanation

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.

References: 1 <https://www.ready.gov/testing-exercises> 2 <https://www.ready.gov/exercises>

NEW QUESTION: 141

A systems administrator recently upgraded the memory in a server, and now the server does not turn on, and nothing is displayed on the screen.

Which of the following is the next step the administrator should take to diagnose the error without opening the machine?

- A. Perform a cold reboot.
- B. Listen for POST code beeps.
- C. Call technical support.
- D. Check the monitor connection.

Answer: B ([LEAVE A REPLY](#))

Explanation

A power-on self-test (POST) is a diagnostic process that runs when a server is turned on to check the basic functionality of the hardware components and report any errors or faults. A POST code is a series of beeps or flashes that indicate the status of the POST process and identify any problems that prevent the server from booting up. A POST code can be heard through a speaker or seen on a display attached to the server motherboard. A POST code is useful for diagnosing errors without opening the machine or using any software tools.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 5, Lesson 5.1, Objective 5.1

NEW QUESTION: 142

The management team at a healthcare organization is concerned about being able to access the dairy vital records if there is an IT disaster that causes both servers and the network to be offline.

Which of the following backup types can the organization use to mitigate this risk?

- A. Tape
- B. Cloud
- C. Disk
- D. Print

Answer: (SHOW ANSWER)

Explanation

A print backup is a type of backup that can be used to mitigate the risk of being unable to access the daily vital records if there is an IT disaster that causes both servers and the network to be offline. A print backup is a backup that involves printing out the data on paper and storing it in a secure location. A print backup can provide offline access to the data without relying on any hardware or software components that may be affected by the disaster. However, a print backup has some drawbacks such as high cost, low efficiency, low security, and environmental impact. A tape backup is a type of backup that involves storing the data on magnetic tape cartridges that can be accessed using a tape drive or a tape library. A tape backup can provide offline access to

the data with high capacity, low cost, and long durability, but it requires special equipment and software that may not be available during a disaster. A cloud backup is a type of backup that involves storing the data on remote servers or platforms that can be accessed over the internet using a web browser or an application. A cloud backup can provide online access to the data with high scalability, flexibility, and security, but it requires network connectivity and bandwidth that may not be available during a disaster. A disk backup is a type of backup that involves storing the data on hard disk drives or solid state drives that can be accessed using a computer or a device. A disk backup can provide online or offline access to the data with high performance, reliability, and portability, but it requires compatible hardware and software that may not be available during a disaster. References:

<https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-it-matter/>

<https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual-files/>

<https://www.howtogeek.com/199068/how-to-upgrade-your-existing-hard-drive-in-under-an-hour/>

<https://www.howtogeek.com/202794/what-is-the-difference-between-127>

NEW QUESTION: 143

A server administrator just installed a new physical server and needs to harden the OS. Which of the following best describes the OS hardening method?

- A. Apply security updates.
- B. Disable unneeded hardware.
- C. Set a BIOS password.
- D. Configure the boot order.

Answer: A ([LEAVE A REPLY](#))

Explanation

Applying security updates is one of the common operating system hardening methods that can help protect the OS from cyberattacks and vulnerabilities. Security updates are released by the OS developer to fix bugs, patch security holes, and improve performance. By installing the latest updates, the server administrator can ensure that the OS is up to date and secure.

NEW QUESTION: 144

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

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

Answer: B ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 145

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

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

Answer: C ([LEAVE A REPLY](#))

Explanation

The first thing that the administrator should check is the network cable. The network cable is a physical medium that connects a server to a switch or other network device. The network cable can affect the speed and quality of the network connection, depending on its type, length, and condition. If the network cable is damaged, faulty, or incompatible, it can cause the server to connect at a lower speed than expected. Therefore, the administrator should check the network cable for any signs of wear, tear, or mismatch, and replace it if necessary.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 2, Lesson 2.1, Objective 2.1

NEW QUESTION: 146

Which of the following BEST describes the concept of right to downgrade?

- A.** It allows for the return of a new OS license if the newer OS is not compatible with the currently installed software and is returning to the previously used OS
- B.** It allows a server to run on fewer resources than what is outlined in the minimum requirements document without purchasing a license
- C.** It allows for a previous version of an OS to be deployed in a test environment for each current license that is purchased
- D.** It allows a previous version of an OS to be installed and covered by the same license as the newer version

Answer: D ([LEAVE A REPLY](#))

Explanation

The concept of right to downgrade allows a previous version of an OS to be installed and covered by the same license as the newer version. For example, if a customer has a license for Windows

10 Pro, they can choose to install Windows 8.1 Pro or Windows 7 Professional instead and still be compliant with the license terms.

Downgrade rights are granted by Microsoft for certain products and programs, such as Windows and Windows Server software acquired through Commercial Licensing, OEM, or retail channels. Downgrade rights are intended to provide customers with flexibility and compatibility when using Microsoft software.

NEW QUESTION: 147

An administrator notices high traffic on a certain subnet and would like to identify the source of the traffic.

Which of the following tools should the administrator utilize?

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

Answer: ([SHOW ANSWER](#))

Explanation

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

NEW QUESTION: 148

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

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

Answer: ([SHOW ANSWER](#))

Explanation

An out-of-band (OOB) solution is a method of accessing and managing a server remotely without using the network connection or the operating system of the server. An OOB solution can use a dedicated management port, a serial console, or a KVM switch to provide a resilient connection while performing changes to the network configuration of the server. An OOB solution is more reliable than a VNC or RDP console, which depend on the network and the operating system, and more convenient than a crash cart, which requires physical access to the server.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 2, Lesson 2.3, Objective 2.3

NEW QUESTION: 149

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

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

Answer: B ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 150

A technician is checking a server rack. Upon entering the room, the technician notices the fans on a particular server in the rack are running at high speeds. This is the only server in the rack that is experiencing this behavior. The ambient temperature in the room appears to be normal. Which of the following is the MOST likely reason why the fans in that server are operating at full speed?

- A. The server is in the process of shutting down, so fan speed operations have been defaulted to high.
- B. An incorrect fan size was inserted into the server, and the server has had to increase the fan speed to compensate.
- C. A fan failure has occurred, and the other fans have increased speed to compensate.
- D. The server is utilizing more memory than the other servers, so it has increased the fans to compensate.

Answer: C ([LEAVE A REPLY](#))

Explanation

This is the most likely reason why the fans in that server are operating at full speed while the ambient temperature in the room is normal and the other servers in the rack are not experiencing this behavior. A fan failure is a situation where one or more fans in a server stop working or malfunction due to wear and tear, dust, or other factors. This can cause overheating and performance issues on the server. To prevent this, most servers have a fan redundancy feature that allows the other fans to increase their speed and airflow to compensate for the failed fan and maintain a safe temperature level. The server is not likely to be in the process of shutting down, as this would not cause the fans to run at high speeds. An incorrect fan size is not likely to be inserted into the server, as most fans are standardized and compatible with the server chassis and motherboard. The server is not likely to be utilizing more memory than the other servers, as this would not cause a significant increase in temperature or fan speed. References:

<https://www.howtogeek.com/303282/how-to-manage-your-pcs-fans-for-optimal-airflow-and-cooling/>

<https://www.howtogeek.com/174288/how-to-tell-if-your-computer-is-overheating-and-what-to-do-about-it/>

NEW QUESTION: 151

An application server's power cord was accidentally unplugged. After plugging the cord back in the server administrator notices some transactions were not written to the disk array. Which of the following is the MOST likely cause of the issue?

- A. Backplane failure
- B. CMOS failure
- C. Misconfigured RAID
- D. Cache battery failure

Answer: ([SHOW ANSWER](#))

Explanation

A cache battery is a battery that provides backup power to the cache memory of a disk array controller. The cache memory stores data that is waiting to be written to the disk array. If the cache battery fails, the data in the cache memory may be lost or corrupted when the power is interrupted. Verified References: [Cache battery], [Disk array controller]

Valid SK0-005 Dumps shared by Actual4test.com for Helping Passing SK0-005 Exam! Actual4test.com now offer the **newest SK0-005 exam dumps**, the Actual4test.com SK0-005 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SK0-005 dumps with Test Engine here:

https://www.actual4test.com/SK0-005_examcollection.html (**492** Q&As Dumps, **30%OFF**

Special Discount: [Freepdfdumps](#))

NEW QUESTION: 152

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: 153

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: 154

A user cannot save large files to a directory on a Linux server that was accepting smaller files a few minutes ago. Which of the following commands should a technician use to identify the issue?

- A. pvdisplay
- B. mount
- C. df -h
- D. fdisk -l

Answer: C ([LEAVE A REPLY](#))

Explanation

The df -h command should be used to identify the issue of not being able to save large files to a directory on a Linux server. The df -h command displays disk space usage in human-readable format for all mounted file systems on the server. It shows the total size, used space, available space, percentage of use, and mount point of each file system. By using this command, a technician can check if there is enough free space on the file system where the directory is located or if it has reached its capacity limit.

NEW QUESTION: 155

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](#))

Explanation

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: 156

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: 157

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

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

Answer: D ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 158

Which of the following server types would benefit MOST from the use of a load balancer?

- A. DNS server
- B. File server

C. DHCP server

D. Web server

Answer: D ([LEAVE A REPLY](#))

Explanation

The server type that would benefit most from the use of a load balancer is web server. A web server is a server that hosts web applications or websites and responds to requests from web browsers or clients. A load balancer is a device or software that distributes network traffic across multiple servers based on various criteria, such as availability, capacity, or performance. A load balancer can improve the scalability, reliability, and performance of web servers by balancing the workload and preventing any single server from being overloaded or unavailable.

NEW QUESTION: 159

Which of the following is typical of software licensing in the cloud?

A. Per socket

B. Perpetual

C. Subscription-based

D. Site-based

Answer: (SHOW ANSWER)

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

Valid SK0-005 Dumps shared by Actual4test.com for Helping Passing SK0-005 Exam!

Actual4test.com now offer the **newest SK0-005 exam dumps**, the Actual4test.com SK0-005 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SK0-005 dumps with Test Engine here:

https://www.actual4test.com/SK0-005_examcollection.html (**492** Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)