

CompTIA

Exam Questions SK0-005

CompTIA Server+ Certification Exam



NEW QUESTION 1

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: D

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 2

A server administrator is connecting a new storage array to a server. The administrator has obtained multiple IP addresses for the array. Which of the following connection types is the server most likely using to connect to the array?

- A. eSATA
- B. USB
- C. FC
- D. iSCSI

Answer: D

Explanation:

iSCSI is a protocol that allows SCSI commands to be transmitted over IP networks, enabling remote access to storage devices. iSCSI uses IP addresses to identify and communicate with the storage array, so having multiple IP addresses for the array indicates that iSCSI is being used. eSATA, USB, and FC are other types of connections that use different protocols and connectors than iSCSI. References: CompTIA Server+ Certification Exam Objectives, Domain 3.0: Storage, Objective 3.1: Given a scenario, install and deploy primary storage devices based on given specifications and interfaces.

NEW QUESTION 3

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

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 4

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

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 5

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

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 6

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

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 7

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

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 8

DRAG DROP

A recent power Outage caused email services to go down. A server administrator also received alerts from the datacenter's UPS. After some investigation, the server administrator learned that each PDU was rated at a maximum Of 12A.

INSTRUCTIONS

Ensure power redundancy is implemented throughout each rack and UPS alarms are resolved. Ensure the maximum potential PDU consumption does not exceed 80% or 9.6A).

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

Data Center Racks 1 and 2

Show Question Reset All Answers

Rack 1 PDU A: 11A MAX PDU B: 6A MAX

Rack Switch 1

VM Host 1

VM Host 2

Mail Relay

SAN

PDU A

Rack 2 PDU A: 8A MAX PDU B: 8A MAX

Rack Switch 2

Domain Controller

?

?

PDU A

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Data Center Racks 1 and 2



NEW QUESTION 9

Which of the following script types would MOST likely be used on a modern Windows server OS?

- A. Batch
- B. VBS
- C. Bash
- D. PowerShell

Answer: D

Explanation:

PowerShell is a scripting language and a command-line shell that is designed for Windows server administration. It can perform various tasks such as configuration, automation, and management of servers and applications. Verified References: [PowerShell], [Scripting language]

NEW QUESTION 10

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
- C. Run the two power cables down the right side of the rack toward the UPS.
- D. Use the longest cables possible to allow for adjustment of the server rail within the rack.
- E. Install an Ethernet patch panel and a PDU to accommodate the network and power cables.

Answer: B

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 10

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

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 14

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

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

Answer: A

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 17

A server administrator needs to configure a server on a network that will have no more than 30 available IP addresses. Which of the following subnet addresses will be the MOST efficient for this network?

- A. 255.255.255.0
- B. 255.255.255.128
- C. 255.255.255.224
- D. 255.255.255.252

Answer: C

Explanation:

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

NEW QUESTION 19

Which of the following concepts refers to prioritizing a connection that had previously worked successfully?

- A. Round robin
- B. SCP
- C. MRU
- D. Link aggregation

Answer: C

Explanation:

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

NEW QUESTION 20

An administrator receives an alert stating a S.M.A.R.T. error has been detected. Which of the following should the administrator run FIRST to determine the issue?

- A. A hard drive test
- B. A RAM test
- C. A power supply swap
- D. A firmware update

Answer: A

Explanation:

A S.M.A.R.T. error is an indication of a potential failure of a hard drive.
S.M.A.R.T. stands for Self-Monitoring, Analysis and Reporting Technology and it is a feature that monitors the health and performance of hard drives. A hard drive test can help diagnose the issue and determine if the drive needs to be replaced. References: <https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives> (Objective 1.1)

NEW QUESTION 23

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

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

D. Failover

Answer: C

Explanation:

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

NEW QUESTION 26

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

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

Answer: B

Explanation:

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

NEW QUESTION 27

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

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

Answer: DF

Explanation:

Port 443 is the default port for HTTPS, which is the protocol used for secure web communication. HTTPS uses SSL/TLS certificates to encrypt the data between the web server and the browser. Port 443 is commonly used for web servers that need to provide secure services, such as online banking, e-commerce, or email. By allowing port 443, the administrator can access the web server's interface and manage its settings¹.

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

NEW QUESTION 32

A server technician is installing a new server OS on legacy server hardware. Which of the following should the technician do FIRST to ensure the OS will work as intended?

- A. Consult the HCL to ensure everything is supported.
- B. Migrate the physical server to a virtual server.
- C. Low-level format the hard drives to ensure there is no old data remaining.
- D. Make sure the case and the fans are free from dust to ensure proper cooling.

Answer: A

Explanation:

The first thing that the technician should do before installing a new server OS on legacy server hardware is to consult the HCL (Hardware Compatibility List) to ensure everything is supported. The HCL is a list of hardware devices and components that are tested and certified to work with a specific OS or software product. The HCL helps to avoid compatibility issues and performance problems that may arise from using unsupported or incompatible hardware. Migrating the physical server to a virtual server may be a good option to improve scalability and flexibility, but it requires additional hardware and software resources and may not be feasible for legacy server hardware. Low-level formatting the hard drives may be a good practice to erase any old data and prepare the drives for a new OS installation, but it does not guarantee that the hardware will work with the new OS. Making sure the case and the fans are free from dust may be a good practice to ensure proper cooling and prevent overheating, but it does not guarantee that the hardware will work with the new OS. References:

<https://www.howtogeek.com/190014/virtualization-basics-understanding-techniques-and-fundamentals/> <https://www.howtogeek.com/173353/how-to-low-level-format-or-write-zeros-to-a-hard-drive/> <https://www.howtogeek.com/303282/how-to-manage-your-pcs-fans-for-optimal-airflow-and-cooling/>

NEW QUESTION 33

An organization recently experienced power outages. The administrator noticed the server did not have enough time to shut down properly. After the outages, the administrator had additional batteries installed in the UPS. Which of the following best describes the solution the administrator implemented?

- A. The solution reduced shutdown time.
- B. The solution improved load balancing.
- C. The solution increased power out.
- D. The solution extended runtime.

Answer: D

Explanation:

The solution the administrator implemented extended runtime. Runtime is the amount of time that a UPS can provide backup power to a server in case of a power outage. By installing additional batteries in the UPS, the administrator increased the capacity and duration of the backup power, allowing the server more time to shut down properly. References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 1, Lesson 1.4, Objective 1.4

NEW QUESTION 35

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

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

Answer: D

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 38

Which of the following commands would MOST likely be used to register a new service on a Windows OS?

- A. set-service
- B. net
- C. sc
- D. services.msc

Answer: C

Explanation:

The sc command is used to create, delete, start, stop, pause, or query services on a Windows OS. It can also be used to register a new service by using the create option. References: <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/sc-create>

NEW QUESTION 43

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

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

Answer: A

Explanation:

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

NEW QUESTION 48

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: C

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 53

Which of the following license types most commonly describes a product that incurs a yearly cost regardless of how much it is used?

- A. Physical
- B. Subscription
- C. Open-source
- D. Per instance
- E. Per concurrent user

Answer: B

Explanation:

A subscription license is a type of license that grants the user the right to use a product or service for a fixed period of time, usually a year. The user pays a recurring fee, regardless of how much they use the product or service. Subscription licenses are common for cloud- based software and services, such as Microsoft 365 or DocuSign2.

References = 1: Compare All Microsoft 365 Plans (Formerly Office 365) - Microsoft Store(<https://www.microsoft.com/en-us/microsoft-365/buy/compare-all-microsoft-365-products>) 2: DocuSign Pricing | eSignature Plans for Personal & Business(<https://ecom.docusign.com/plans-and-pricing/esignature>)

NEW QUESTION 56

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

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 59

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

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

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

- A.
- | Folder name | Share permissions | File permissions |
|-------------|---------------------------|-------------------|
| DATA | Authenticated users: read | Ann: full control |
- B.
- | Folder name | Share permissions | File permissions |
|-------------|-------------------|-------------------|
| DATA | Ann: full control | Ann: full control |
- C.
- | Folder name | Share permissions | File permissions |
|-------------|-----------------------------------|------------------|
| DATA | Authenticated users: full control | Ann: modify |
- D.
- | Folder name | Share permissions | File permissions |
|-------------|----------------------------------------|-------------------|
| DATA | Authenticated users: read
Ann: read | Ann: full control |

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

Explanation:

Option D is the best practice to set up Ann's permissions correctly, exposing only the minimum rights required. Option D shows that the share permissions on the DATA folder grant Ann Change access, which allows her to read, write, and delete files in the shared folder. The file permissions grant Ann Modify access, which

allows her to read, write, execute, and delete files in the folder. This combination of permissions gives Ann the ability to write anything to the DATA folder using the network, as well as to modify and delete existing files. This meets the requirement of giving Ann modify permissions to the shared folder.

NEW QUESTION 61

A security analyst suspects a remote server is running vulnerable network applications. The analyst does not have administrative credentials for the server. Which of the following would MOST likely help the analyst determine if the applications are running?

- A. User account control
- B. Anti-malware
- C. A sniffer
- D. A port scanner

Answer: D

Explanation:

A port scanner is the tool that would most likely help the analyst determine if the applications are running on a remote server. A port scanner is a software tool that scans a network device for open ports. Ports are logical endpoints for network communication that are associated with specific applications or services. By scanning the ports on a remote server, the analyst can identify what applications or services are running on that server and what protocols they are using. A port scanner can also help detect potential vulnerabilities or misconfigurations on a server.

NEW QUESTION 65

A technician has been asked to check on a SAN. Upon arrival, the technician notices the red LED indicator shows a disk has failed. Which of the following should the technician do NEXT, given the disk is hot swappable?

- A. Stop sharing the volume
- B. Replace the disk
- C. Shut down the SAN
- D. Stop all connections to the volume

Answer: B

Explanation:

The next thing that the technician should do, given the disk is hot swappable, is to replace the disk. A hot swappable disk is a disk that can be removed and replaced without shutting down the system or affecting its operation. A hot swappable disk is typically used in a storage array that has RAID (Redundant Array of Independent Disks) configuration that provides fault tolerance and redundancy. If a disk fails in a RAID array, it can be replaced by a new disk without interrupting the service or losing any data. The new disk will automatically rebuild itself using the data from the other disks in the array.

NEW QUESTION 69

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: CD

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-windows/>

NEW QUESTION 72

Which of the following licenses would MOST likely include vendor assistance?

- A. Open-source
- B. Version compatibility
- C. Subscription
- D. Maintenance and support

Answer: D

Explanation:

Maintenance and support is a type of license that would most likely include vendor assistance. Maintenance and support is a contract that defines the level and scope of service and assistance that a vendor provides to a customer for using their software product. Maintenance and support may include technical support, bug fixes, patches, updates, upgrades, documentation, training, and other benefits. Maintenance and support licenses usually have an annual fee based on the number of users or devices covered by the contract. Open-source is a type of license that allows free access to the source code and modification and distribution of the software product, but does not guarantee vendor assistance. Version compatibility is not a type of license, but a feature that ensures software products can work with different versions of operating systems or other software products. Subscription is a type of license that allows access to software products for a limited period of time based on recurring payments, but does not necessarily include vendor assistance. References: <https://www.techopedia.com/definition/1440/software-licensing>
<https://www.techopedia.com/definition/1032/business-impact-analysis-bia>

NEW QUESTION 77

A data center environment currently hosts more than 100 servers that include homegrown and commercial software. The management team has asked the server

administrator to find a way to eliminate all company-owned data centers. Which of the following models will the administrator most likely choose to meet this need?

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

Answer: C

Explanation:

A public cloud model will most likely meet the need of eliminating all company-owned data centers. A public cloud is a type of cloud computing service that is provided by a third-party vendor over the internet. A public cloud offers scalability, flexibility, and cost-effectiveness for hosting servers and applications, as the customers only pay for the resources they use and do not have to maintain their own infrastructure. A public cloud can also provide high availability, security, and performance for the servers and applications, as the vendor manages the underlying hardware and software. A public cloud can support various types of services, such as software as a service (SaaS), platform as a service (PaaS), or infrastructure as a service (IaaS). References: [CompTIA Server+ Certification Exam Objectives], Domain 1.0: Server Administration, Objective 1.2: Given a scenario, compare and contrast server roles and requirements for each.

NEW QUESTION 80

A company uses a hot-site, disaster-recovery model. Which of the following types of data replication is required?

- A. Asynchronous
- B. Incremental
- C. Application consistent
- D. Constant

Answer: D

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 81

A server administrator wants to ensure a storage array can survive the failure of two drives without the loss of data. Which of the following RAID levels should the administrator choose?

- A. 1
- B. 5
- C. 6

Answer: D

Explanation:

RAID 6 is a level of RAID that can survive the failure of two drives without the loss of data. RAID 6 uses block-level striping with two parity blocks distributed across all member disks. RAID 6 can tolerate two simultaneous drive failures and still provide data access and redundancy. RAID 0 is a level of RAID that uses striping without parity or mirroring, and offers no fault tolerance. RAID 0 cannot survive any drive failure without data loss. RAID 1 is a level of RAID that uses mirroring without parity or striping, and offers fault tolerance by duplicating data on two or more disks. RAID 1 can survive one drive failure without data loss, but not two. RAID 5 is a level of RAID that uses block-level striping with one parity block distributed across all member disks. RAID 5 can tolerate one drive failure without data loss, but not two. References:

? https://en.wikipedia.org/wiki/Standard_RAID_levels

NEW QUESTION 83

Which of the following is an example of load balancing?

- A. Round robin
- B. Active-active
- C. Active-passive
- D. Failover

Answer: A

Explanation:

Round robin is an example of load balancing. Load balancing is the method of distributing network traffic equally across a pool of resources that support an application. Load balancing improves application availability, scalability, security, and performance by preventing any single resource from being overloaded or unavailable. Round robin is a simple load balancing algorithm that assigns each incoming request to the next available resource in a circular order. For example, if there are three servers (A, B, C) in a load balancer pool, round robin will send the first request to server A, the second request to server B, the third request to server C, the fourth request to server A again, and so on. Reference: <https://simplicable.com/new/load-balancing>

NEW QUESTION 84

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

- A. A security camera
- B. A mantrap
- C. A security guard
- D. A proximity card

Answer: B

Explanation:

A mantrap is a security device that consists of two interlocking doors that allow only one person to enter at a time. A mantrap would prevent employees from blocking the door in the main data center and force them to enter properly using their credentials. The other options would not enforce proper entry to the data center

NEW QUESTION 85

A server administrator implemented a new backup solution and needs to configure backup methods for remote sites. These remote sites have low bandwidth and backups must not interfere with the network during normal business hours. Which of the following methods can be used to meet these requirements? (Select two).

- A. Open file
- B. Archive
- C. Cloud
- D. Snapshot
- E. Differential
- F. Synthetic full

Answer: BE

Explanation:

Archive is a method of storing historical data that is not frequently accessed or modified. Archive can reduce the amount of data that needs to be backed up and save bandwidth and storage space. Differential is a method of backing up only the data that has changed since the last full backup. Differential can also save bandwidth and storage space, as well as speed up the backup process.

References:

CompTIA Server+ Certification Exam Objectives1, page 12

Server Management: Server Hardware Installation and Management2, Module 2, Lesson 5

NEW QUESTION 86

An analyst is planning a new point-to-point Ethernet connection between a university campus and a newly acquired space downtown that is about 5mi (8km) away. The analyst would like the fastest possible connection speed. Which of the following would best meet the analyst's needs?

- A. 1000BASE-LX 1Gb single-mode plenum fiber connection
- B. 10GBASE-T 10Gb copper plenum Ethernet connection
- C. 1000BASE-T 1Gb copper non-plenum Ethernet connection
- D. 10GBASE-SR 10Gb multimode plenum fiber connection

Answer: A

Explanation:

A 1000BASE-LX 1Gb single-mode plenum fiber connection would best meet the analyst's needs for a new point-to-point Ethernet connection between a university campus and a newly acquired space downtown that is about 5mi (8km) away. A 1000BASE-LX is a type of Ethernet standard that supports data transmission at 1 gigabit per second over single-mode fiber cables using long wavelength lasers. 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 plenum fiber cable is a type of optical fiber cable that has a special coating that prevents the spread of fire or toxic fumes in case of burning. A plenum fiber cable is suitable for installation in plenum spaces, which are areas used for air circulation in buildings, such as above ceilings or below floors. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Networking, Objective 4.2: Given a scenario involving server networking issues (e.g., network interface card failure), troubleshoot using appropriate tools.

NEW QUESTION 91

A server administrator has been asked to implement a password policy that will help mitigate the chance of a successful brute-force attack. Which of the following password policies should the administrator implement first?

- A. Lockout
- B. Length
- C. Complexity
- D. Minimum age

Answer: B

Explanation:

Password length is the first password policy that the administrator should implement to help mitigate the chance of a successful brute-force attack. A brute-force attack is a method of guessing passwords by trying all possible combinations of characters until the correct one is found. The longer the password, the more combinations there are, and the more time and resources it takes to crack it. Therefore, password length is a key factor in password strength and security.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.2, Objective 3.2

NEW QUESTION 95

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

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

Answer: B

Explanation:

The administrator needs to install SSL to make the website trusted. SSL stands for Secure Sockets Layer, which is an encryption-based Internet security protocol that ensures privacy, authentication, and data integrity in web communications. SSL enables HTTPS (Hypertext Transfer Protocol Secure), which is a secure version of HTTP (Hypertext Transfer Protocol) that encrypts the data exchanged between a web browser and a web server. SSL also uses digital certificates to

verify the identity of the web server and establish trust with the web browser. A web server that implements SSL has HTTPS in its URL instead of HTTP and displays a padlock icon or a green bar in the browser's address bar.

NEW QUESTION 97

A technician recently applied a critical OS patch to a working sever. After rebooting, the technician notices the server is unable to connect to a nearby database server. The technician validates a connection can be made to the database from another host. Which of the following is the best NEXT step to restore connectivity?

- A. Enable HIDS.
- B. Change the service account permissions.
- C. Check the host firewall rule.
- D. Roll back the applied patch.

Answer: C

Explanation:

A host firewall is a software that controls the incoming and outgoing network traffic on a server based on predefined rules and filters. It can block or allow certain ports, protocols, or addresses that are used for communication with other servers or devices. If a server is unable to connect to another server after applying a patch, it is possible that the patch changed or added a firewall rule that prevents the connection. The administrator should check the host firewall rule and modify it if necessary to restore connectivity. Verified References: [Host firewall], [Network connection]

NEW QUESTION 99

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

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 101

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

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 file.

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 files.

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 files.

1: CompTIA Server+ Certification Exam Objectives

NEW QUESTION 105

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

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 109

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

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

Answer: D

Explanation:

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 111

A technician has received multiple reports of issues with a server. The server occasionally has a BSOD, powers off unexpectedly, and has fans that run continuously. Which of the following BEST represents what the technician should investigate during troubleshooting?

- A. Firmware incompatibility
- B. CPU overheating
- C. LED indicators
- D. ESD issues

Answer: B

Explanation:

Unexpected shutdowns. If the system is randomly shutting down or rebooting, the most likely cause is a heat problem.
Reference: <https://www.microsoftpressstore.com/articles/article.aspx?p=2224043&seqNum=3>

NEW QUESTION 113

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

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 118

An administrator is alerted to a hardware failure in a mission-critical server. The alert states that two drives have failed. The administrator notes the drives are in different RAID 1 arrays, and both are hot-swappable. Which of the following steps will be the MOST efficient?

- A. Replace one drive, wait for a rebuild, and replace the next drive.
- B. Shut down the server and replace the drives.
- C. Replace both failed drives at the same time.
- D. Replace all the drives in both degraded arrays.

Answer: C

Explanation:

Since both drives are in different RAID 1 arrays and both are hot-swappable, the most efficient step is to replace both failed drives at the same time. This can minimize the downtime and avoid unnecessary reboots. RAID 1 provides mirroring, which means that data is duplicated on both drives in the array. Therefore, replacing one drive will not affect the data on the other drive or the functionality of the array. References: https://en.wikipedia.org/wiki/Standard_RAID_levels#RAID_1

NEW QUESTION 123

Which of the following should an administrator use to transfer log files from a Linux server to a Windows workstation?

- A. Telnet
- B. Robocopy
- C. XCOPY
- D. SCP

Answer: D

Explanation:

The administrator should use SCP to transfer log files from a Linux server to a Windows workstation. SCP (Secure Copy Protocol) is a protocol that allows secure file transfer between two devices using SSH (Secure Shell) encryption. SCP can transfer files between different operating systems, such as Linux and Windows, as long as both devices have an SSH client installed. SCP can also preserve file attributes, such as permissions and timestamps, during the transfer.

NEW QUESTION 127

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

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.

NEW QUESTION 130

A site is considered a warm site when it:
? has basic technical facilities connected to it.
? has faulty air conditioning that is awaiting service.
? is almost ready to take over all operations from the primary site.

A. is fully operational and continuously providing services.

Answer: A

Explanation:

A warm site is a backup site that has some of the necessary hardware, software, and network resources to resume operations, but not all of them. A warm site requires some time and effort to become fully operational. A warm site is different from a cold site, which has minimal or no resources, and a hot site, which has all the resources and is ready to take over immediately. References: CompTIA Server+ Study Guide, Chapter 10: Disaster Recovery, page 403.

NEW QUESTION 134

Which of the following backup types should be chosen for database servers?

- A. Differential
- B. Incremental
- C. Synthetic full
- D. Open file

Answer: C

Explanation:

A synthetic full backup is a type of backup that combines a full backup with one or more incremental backups to create a new full backup without accessing the source data. This type of backup is suitable for database servers, as it reduces the backup window, minimizes the impact on the server performance, and provides faster recovery time. Verified References: [Synthetic Full Backup]

NEW QUESTION 135

A senior administrator instructs a technician to run the following script on a Linux server: for i in {1..65536}; do echo \$i; telnet localhost \$i; done
The script mostly returns the following message: Connection refused. However, there are several entries in the console display that look like this:
80
Connected to localhost 443
Connected to localhost
Which of the following actions should the technician perform NEXT?

- A. Look for an unauthorized HTTP service on this server
- B. Look for a virus infection on this server
- C. Look for an unauthorized Telnet service on this server
- D. Look for an unauthorized port scanning service on this server.

Answer: A

Explanation:

The script that the technician is running is trying to connect to every port on the localhost (the same machine) using telnet, a network protocol that allows remote access to a command-line interface. The script mostly fails because most ports are closed or not listening for connections. However, the script succeeds on ports 80 and 443, which are the default ports for HTTP and HTTPS protocols, respectively. These protocols are used for web services and web browsers. Therefore, the technician should look for an unauthorized HTTP service on this server, as it may indicate a security breach or a misconfiguration. Looking for a virus infection on this server is also possible, but not the most likely source of the issue. Looking for an unauthorized Telnet service on this server is not relevant, as the script is using telnet as a client, not a server. Looking for an unauthorized port scanning service on this server is not relevant, as the script is scanning ports on the localhost, not on other machines. References:

? <https://phoenixnap.com/kb/telnet-windows>
? <https://www.techopedia.com/definition/23337/http-port-80>
? <https://www.techopedia.com/definition/23336/https-port-443>

NEW QUESTION 138

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

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

Answer: C

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 140

A company stores extremely sensitive data on an air-gapped system. Which of the following can be implemented to increase security against a potential insider threat?

- A. Two-person Integrity
- B. SSO
- C. SIEM
- D. Faraday cage
- E. MFA

Answer: A

Explanation:

Two-person integrity is a security measure that can be implemented to increase security against a potential insider threat on an air-gapped system. An air-gapped system is a system that is isolated from any network connection and can only be accessed physically. An insider threat is a malicious actor who has authorized access to an organization's system or data and uses it for unauthorized or harmful purposes. Two-person integrity is a system of storage and handling that requires the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures, for accessing certain sensitive data or material. This way, no single person can compromise the security or integrity of the data or material without being noticed by another person. SSO (Single Sign-On) is a feature that allows users to access multiple applications or systems with one set of credentials, but it does not prevent insider threats. SIEM (Security Information and Event Management) is a tool that collects and analyzes log data from various sources to detect and respond to security incidents, but it does not work on air-gapped systems. A Faraday cage is a structure that blocks electromagnetic signals from entering or leaving, but it does not prevent physical access or insider threats. MFA (Multi-Factor Authentication) is a method that requires users to provide two or more pieces of evidence to verify their identity, such as something they know, something they have, or something they are, but it does not prevent insider threats. References: <https://www.howtogeek.com/169080/air-gap-how-to-isolate-a-computer-to-protect-it-from-hackers/> <https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-it-matter/> <https://www.howtogeek.com/202794/what-is-the-difference-between-127.0.0.1-and-0.0.0.0/> <https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual-files/>

NEW QUESTION 145

An administrator has been asked to increase the storage capacity of a stand-alone file server but no further expansion slots are available. Which of the following would be the FASTEST solution to implement with no downtime?

- A. Configure a RAID array.
- B. Replace the current drives with higher-capacity disks.
- C. Implement FCoE for more storage capacity.
- D. Connect the server to a SAN

Answer: D

Explanation:

A SAN (Storage Area Network) is a network of storage devices that can provide shared storage capacity to multiple servers. By connecting the server to a SAN, the administrator can increase the storage capacity of the server without adding any internal disks or expansion cards. This solution can be implemented quickly and without any downtime. Verified References: [What is a SAN and how does it differ from NAS?]

NEW QUESTION 149

An administrator is setting up a new server and has been asked to install an operating system that does not have a GUI because the server has limited resources. Which of the following installation options should the administrator use?

- A. Bare metal
- B. Headless
- C. Virtualized
- D. Slipstreamed

Answer: B

Explanation:

A headless installation is an installation method that does not require a graphical user interface (GUI) or a monitor, keyboard, and mouse. It can be done remotely through a network connection or a command-line interface. A headless installation is suitable for a server that has limited resources and does not need a GUI.

References:

? CompTIA Server+ Certification Exam Objectives1, page 14

? Server Management: Server Hardware Installation and Management2, Module 2, Lesson 5

NEW QUESTION 153

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

- A. The server has an architecture mismatch
- B. The system time is not synchronized
- C. The technician does not have sufficient privileges
- D. The external firewall is blocking access
- E. The default gateway is incorrect
- F. The local system log file is full

Answer: DE

Explanation:

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

NEW QUESTION 158

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

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 159

A technician is deploying a single server to monitor and record 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

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 160

Which of the following encryption methodologies would MOST likely be used to ensure encrypted data cannot be retrieved if a device is stolen?

- A. End-to-end encryption
- B. Encryption in transit
- C. Encryption at rest
- D. Public key encryption

Answer: C

Explanation:

Encryption at rest is a type of encryption methodology that would most likely be used to ensure encrypted data cannot be retrieved if a device is stolen. Encryption at rest is a process of encrypting stored data on a device such as a hard drive, SSD, USB flash drive, or mobile device. This way, if the device is lost or stolen, the

data cannot be accessed without the encryption key or password. Encryption at rest can be implemented using software tools such as BitLocker on Windows or FileVault on Mac OS, or hardware features such as self-encrypting drives or Trusted Platform Module chips. End-to-end encryption is a type of encryption methodology that ensures encrypted data cannot be intercepted or modified by third parties during transmission over a network. Encryption in transit is a type of encryption methodology that protects encrypted data while it is moving from one location to another over a network. Public key encryption is a type of encryption algorithm that uses a pair of keys: a public key that can be shared with anyone and a private key that is kept secret by the owner. References: <https://www.howtogeek.com/196541/bitlocker-101-what-it-is-how-it-works-and-how-to-use-it/> <https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual-files/> <https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-it-matter/> <https://www.howtogeek.com/195877/what-is-encryption-and-how-does-it-work/>

NEW QUESTION 164

A server administrator has received tickets from users who report the system runs very slowly and various unrelated messages pop up when they try to access an internet-facing web application using default ports. The administrator performs a scan to check for open ports and reviews the following report:

Starting Nmap 7.70 <https://nmap.org>) at 2019-09-19 14:30 UTC Nmap scan report for www.abc.com (172.45.6.85)

Host is up (0.0021s latency)

Other addresses for www.abc.com (not scanned) : 4503 : F7b0 : 4293: 703: : 3209 RDNS record for 172.45.6.85: 1ga45s12-in-f1.2d100.net

Port State Service 21/tcp filtered ftp 22/tcp filtered ssh 23/tcp filtered telnet

69/tcp open @username.com 80/tcp open http

110/tcp filtered pop 143/tcp filtered imap 443/tcp open https

1010/tcp open www.popup.com 3389/tcp filtered ms-abc-server

Which of the following actions should the server administrator perform on the server?

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

Answer: A

Explanation:

Port 69 is used for TFTP (Trivial File Transfer Protocol), which is an insecure and unencrypted protocol for file transfer. Port 1010 is used for a malicious website that generates pop-up ads. Both of these ports are likely to be exploited by hackers or malware to compromise the server or the web application. The server administrator should close these ports and rerun the scan to verify that they are no longer open.

References = 1: Why Are Some Network Ports Risky, And How Do You Secure Them? - How-To Geek(<https://www.howtogeek.com/devops/why-are-some-ports-risky-and-how-do-you-secure-them/>) 2: Switchport Port Security Explained With Examples -

ComputerNetworkingNotes(<https://www.computernetworkingnotes.com/ccna-study-guide/switchport-port-security-explained-with-examples.html>)

NEW QUESTION 165

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: BD

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 168

An administrator is installing a new server and OS. After installing the OS, the administrator logs in and wants to quickly check the network configuration. Which of the following is the best command to use to accomplish this task?

- A. tracer
- B. telnet
- C. ipconfig
- D. ping

Answer: C

NEW QUESTION 170

A server administrator has received calls regarding latency and performance issues with a file server. After reviewing all logs and server features the administrator discovers the server came with four Ethernet ports, but only one port is currently in use. Which of the following features will enable the use of all available ports using a single IP address?

- A. Network address translation
- B. in-band management
- C. Round robin
- D. NIC teaming

Answer: D

Explanation:

NIC teaming is a feature that allows the use of multiple network interface cards (NICs) as a single logical interface with a single IP address. It can improve the network performance, bandwidth, and redundancy of a server. Verified References: [NIC teaming], [Network interface card]

NEW QUESTION 175

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

- A. An ACL
- B. Antivirus
- C. DLP
- D. A firewall

Answer: C

Explanation:

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

NEW QUESTION 177

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

- A. Restore the server from a snapshot.
- B. Restore the server from backup.
- C. Swap the drive and initialize the disk.
- D. Swap the drive and initialize the array.

Answer: C

Explanation:

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

NEW QUESTION 179

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

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 180

Which of the following relates to how much data loss a company agrees to tolerate in the event of a disaster?

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

Answer: A

Explanation:

Reference: <https://www.druva.com/blog/understanding-rpo-and-rto/>

The Recovery Time Objective (RTO) is the maximum amount of time that a company agrees to tolerate in the event of a disaster before restoring its normal operations. The RTO is based on the business impact analysis (BIA) and the criticality of the processes and data involved. The RTO helps determine the backup and recovery strategies and resources needed to minimize downtime and data loss.

Reference: <https://www.ibm.com/cloud/learn/recovery-time-objective>

NEW QUESTION 181

A server administrator is configuring a new server that will hold large amounts of information. The server will need to be accessed by multiple users at the same time. Which of the following server roles will the administrator MOST likely need to install?

- A. Messaging
- B. Application
- C. Print

D. Database

Answer: D

Explanation:

Few people are expected to use the database at the same time and users don't need to customize the design of the database.

Reference: <https://support.microsoft.com/en-us/office/ways-to-share-an-access-desktop-database-03822632-da43-4d8f-ba2a-68da245a0446>

The server role that the administrator will most likely need to install for a server that will hold large amounts of information and will need to be accessed by multiple users at the same time is database. A database is a collection of structured data that can be stored, queried, manipulated, and analyzed using various methods and tools. A database server is a server that hosts one or more databases and provides access to them over a network. A database server can handle large amounts of information and support concurrent requests from multiple users or applications.

NEW QUESTION 186

An administrator has been troubleshooting a server issue. The administrator carefully questioned the users and examined the available logs. Using this information, the administrator was able to rule out several possible causes and develop a theory as to what the issue might be. Through further testing, the administrator's theory proved to be correct. Which of the following should be the next step to troubleshoot the issue?

- A. Document the findings and actions.
- B. Escalate the issue to the management team.
- C. Implement the solution.
- D. Establish an action plan.

Answer: D

Explanation:

The next step to troubleshoot the issue after developing and testing a theory is to establish an action plan. This involves identifying the steps needed to implement the solution, estimating the time and resources required, and evaluating the potential risks and impacts of the solution. Documenting the findings and actions, escalating the issue to the management team, or implementing the solution are steps that should be done after establishing an action plan. References: [CompTIA Server+ Certification Exam Objectives], Domain 6.0: Disaster Recovery, Objective 6.2: Explain troubleshooting theory and methodologies.

NEW QUESTION 188

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: AC

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.

Reference:

<https://www.csoonline.com/article/3191531/securing-risky-network-ports.html>

NEW QUESTION 189

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

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 193

Due to a disaster incident on a primary site, corporate users are redirected to cloud services where they will be required to be authenticated just once in order to use all cloud services.

Which of the following types of authentications is described in this scenario?

- A. MFA
- B. NTLM
- C. Kerberos
- D. SSO

Answer: D

NEW QUESTION 195

A staff member who is monitoring a data center reports one rack is experiencing higher temperatures than the racks next to it, despite the hardware in each rack being the same. Which of the following actions would MOST likely remediate the heat issue?

- A. Installing blanking panels in all the empty rack spaces
- B. Installing an additional POU and spreading out the power cables
- C. Installing servers on the shelves instead of sliding rails
- D. Installing front bezels on all the server's in the rack

Answer: A

Explanation:

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

NEW QUESTION 197

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

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

Answer: A

Explanation:

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

NEW QUESTION 199

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

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

Answer: B

Explanation:

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

Reference: <https://www.getsafeonline.org/business/articles/unnecessary-services/>

NEW QUESTION 203

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

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 208

Which of the following licensing models allows the greatest number of concurrent Windows VMS to run on a host for the lowest cost?

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

Answer: A

Explanation:

The answer to this question may depend on several factors, such as the number and type of Windows VMs, the number and type of host machines, the number and type of users, and the specific licensing terms and conditions of each licensing model. However, based on the information available from the web search results, one possible answer is per user. Per user licensing model is a licensing model that allows a user to access Windows VMs from any device, regardless of the number of devices or VMs. Per user licensing model is available for Windows 10 Enterprise E3/E5, Windows VDA E3/E5, and Microsoft 365 F3/E3/E5. Per user licensing model may offer the greatest number of concurrent Windows VMs to run on a host for the lowest cost if the following conditions are met:

? The user needs to access multiple Windows VMs from different devices, such as desktops, laptops, tablets, or smartphones.

? The user needs to access Windows VMs that run different versions or editions of Windows, such as Windows 10 Enterprise, Windows 10 Pro, or Windows 7 Enterprise.

? The user needs to access Windows VMs that run on different types of host machines, such as physical servers, virtual servers, or cloud servers.

? The user does not need to access Windows VMs that run on dedicated hardware or have specific performance or security requirements.

According to the web search results¹, per user licensing model costs \$84 per user per year for Windows 10 Enterprise E3, \$168 per user per year for Windows 10 Enterprise E5,

\$100.80 per user per year for Windows VDA E3, and \$196.80 per user per year for Windows VDA E5. These prices are based on the Open License Program and may vary depending on the volume and agreement level²

Per core licensing model is a licensing model that requires a license for each core of the processor on the host machine that runs Windows VMs. Per core licensing model is available for Windows Server 2022 Datacenter and Standard editions. Per core licensing model may offer a lower cost than per user licensing model if the following conditions are met:

? The host machine has a low number of cores or a high core density.

? The host machine runs a high number of Windows VMs with low resource consumption.

? The host machine runs only Windows Server VMs with the same edition as the host machine.

According to the web search results², per core licensing model costs \$6,155 for 16 core licenses for Windows Server 2022 Datacenter edition and \$1,069 for 16 core licenses for Windows Server 2022 Standard edition. These prices are suggested retail prices and may vary depending on the reseller²

Per instance licensing model is a licensing model that requires a license for each instance of Windows that runs on a host machine or a VM. Per instance licensing model is available for Windows Server 2022 Essentials edition and some older versions of Windows Server. Per instance licensing model may offer a lower cost than per user or per core licensing model if the following conditions are met:

? The host machine runs only one instance of Windows Server with low resource consumption.

? The host machine does not need to run any other VMs or applications.

? The host machine does not need any advanced features or functions that are available in Datacenter or Standard editions.

According to the web search results², per instance licensing model costs \$501 for one server license for Windows Server 2022 Essentials edition. This price is suggested retail price and may vary depending on the reseller²

Per concurrent user licensing model is a licensing model that allows a certain number of users to access Windows VMs at the same time, regardless of the number of devices or VMs. Per concurrent user licensing model is not available for any current version of Windows or Windows Server. Per concurrent user licensing model was available for some older versions of Windows Server Terminal Services or Remote Desktop Services, but it was discontinued due to complexity and compliance issues. Therefore, per concurrent user licensing model cannot be used for running Windows VMs on a host.

NEW QUESTION 211

A server technician installs a new NIC on a server and configures the NIC for IP connectivity. The technician then tests the connection using the ping command. Given the following partial output of the ping and ipconfig commands:

```
ipconfig /all

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

pinging 192.168.1.1 with 32 bytes of data:

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

Which of the following caused the issue?

- A. Duplicate IP address
- B. Incorrect default gateway
- C. DHCP misconfiguration
- D. Incorrect routing table

Answer: A

Explanation:

? The ping command output shows that the NIC has an IP address of 192.168.1.100 and a default gateway of 192.168.1.1. However, when the technician tries to ping the default gateway, the reply comes from another IP address: 192.168.1.101. This means that there is another device on the network that has the same IP address as the default gateway, and it is responding to the ping request instead of the intended destination.

? A duplicate IP address can cause network connectivity problems, such as packet loss, routing errors, or unreachable hosts. To resolve this issue, the technician should either change the IP address of the default gateway or the device that is conflicting with it, or use DHCP to assign IP addresses automatically and avoid conflicts.

? The other options are not correct because they do not explain the ping output. An incorrect default gateway would cause no reply or a destination unreachable message, not a reply from a different IP address. A DHCP misconfiguration would cause an invalid or no IP address on the NIC, not a duplicate IP address on the network. An incorrect routing table would cause routing errors or unreachable destinations, not a reply from a different IP address.

References:

? https://askleo.com/what_is_ping_and_what_does_its_output_tell_me/

? <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/ping>

NEW QUESTION 214

Hackers recently targeted a company with an attack that resulted in a system breach, which compromised the organization's data. Because of the system breach, the administrator had to bypass normal change management procedures. Which of the following change management activities was necessary?

- A. Cancelled change request
- B. Change request postponement
- C. Emergency change request
- D. Privilege change request
- E. User permission change request

Answer: C

Explanation:

An emergency change request is a type of change request that is initiated in response to an urgent situation, such as a system breach, that requires immediate action to restore normal operations or prevent further damage. An emergency change request may bypass some of the normal change management procedures, such as approval, testing, or documentation, in order to expedite the implementation of the change. However, an emergency change request should still follow the basic steps of change management, such as identification, analysis, planning, execution, and evaluation, and should be reviewed and documented after the change is completed.

References: CompTIA Server+ Study Guide, Chapter 11: Change Management, page 443.

NEW QUESTION 218

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

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

Answer: D

Explanation:

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

NEW QUESTION 221

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

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 224

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

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

Answer: C

Explanation:

A loop is a programming construct that allows a block of code to be executed repeatedly until a certain condition is met. 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 forserverinservers:
```

```
# 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 228

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

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

Answer: C

Explanation:

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

NEW QUESTION 232

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

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

Answer: B

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 234

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

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

The administrator configures the IP address for the new server as follows: IP address: 192.168.1.1/24

Default gateway: 192.168.10.1

A ping sent to the default gateway is not successful. Which of the following IP address/default gateway combinations should the administrator have used for the new server?

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

Answer: A

Explanation:

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

NEW QUESTION 237

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

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 240

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

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.

Reference:

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

NEW QUESTION 245

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: B

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 248

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

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 252

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

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 256

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

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

Answer: C

Explanation:

Bash is a scripting language that is commonly used in Linux systems to automate tasks and manipulate text. Bash scripts can run commands, variables, functions, loops, and conditional statements. PowerShell is a scripting language that is mainly used in Windows systems, while batch command files are simple text files that

contain a series of commands to be executed by the command-line interpreter. Visual Basic is a programming language that is used to create applications, not scripts. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Server Administration, Objective 4.2: Given a scenario, perform proper server maintenance techniques.

NEW QUESTION 261

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

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 265

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

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

Answer: B

Explanation:

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

NEW QUESTION 268

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: D

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]

NEW QUESTION 272

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

- A. 21
- B. 22
- C. 23
- D. 443

Answer: B

Explanation:

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

NEW QUESTION 277

Which of the following licensing concepts is based on the number of logical processors a server has?

- A. Per core
- B. Per socket
- C. Per instance
- D. Per server

Answer: A

Explanation:

Per core licensing is based on the number of logical processors a server has. A logical processor is either a physical core or a virtual core created by hyperthreading. Per core licensing requires purchasing a license for each logical processor on the server. Verified References: [Per core licensing], [Logical processor]

NEW QUESTION 282

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

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 284

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

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 289

An administrator is troubleshooting connectivity to a remote server. The goal is to remotely connect to the server to make configuration changes. To further troubleshoot, a port scan revealed the ports on the server as follows:

Port 22: Closed
Port 23: Open
Port 990: Closed

Which of the following next steps should the administrator take?

Reboot the workstation and then the server.

- A. Open port 990 and close port 23.
- B. Open port 22 and close port 23.
- C. Open all of the ports listed.
- D. Close all of the ports listed.

Answer: B

Explanation:

Port 22 is used for SSH (Secure Shell), which is a secure and encrypted protocol for remote access to a server. Port 23 is used for Telnet, which is an insecure and unencrypted protocol for remote access. Port 990 is used for FTPS (File Transfer Protocol Secure), which is a secure and encrypted protocol for file transfer. The administrator should open port 22 and close port 23 to enable SSH and disable Telnet, as SSH is more secure and reliable than Telnet. The administrator does not need to open port 990, as FTPS is not required for making configuration changes¹²³.

References = 1: Remote Desktop - Allow access to your PC from outside your network(<https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-allow-outside-access>) 2: Test remote network port connection in Windows 10 - Winaero(<https://winaero.com/test-remote-network-port-connection-in-windows-10/>) 3: Windows Command to check if a remote server port is opened?(<https://superuser.com/questions/1035018/windows-command-to-check-if-a-remote-server-port-is-opened>)

NEW QUESTION 292

After the installation of an additional network card into a server, the server will not boot into the OS. A technician tests the network card in a different server with a different OS and verifies the card functions correctly. Which of the following should the technician do NEXT to troubleshoot this issue?

- A. Remove the original network card and attempt to boot using only the new network card.
- B. Check that the BIOS is configured to recognize the second network card.
- C. Ensure the server has enough RAM to run a second network card.
- D. Verify the network card is on the HCL for the OS.

Answer: D

Explanation:

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

NEW QUESTION 295

A technician is trying to determine the reason why a Linux server is not communicating on a network. The returned network configuration is as follows:

```
eth0: flags=4163<UP, BROADCAST,RUNNING,MULTICAST> mtu 1500
```

```
inet 127.0.0.1 network 255.255.0.0 broadcast 127.0.0.1
```

 Which of the following BEST describes what is happening?

- A. The server is configured to use DHCP on a network that has multiple scope options
- B. The server is configured to use DHCP, but the DHCP server is sending an incorrect subnet mask
- C. The server is configured to use DHCP on a network that does not have a DHCP server
- D. The server is configured to use DHCP, but the DHCP server is sending an incorrect MTU setting

Answer: C

Explanation:

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

NEW QUESTION 298

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 301

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

- A. Backup recovery
- B. Simulated
- C. Tabletop
- D. Live failover

Answer: D

Explanation:

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

NEW QUESTION 304

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

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

Answer: B

Explanation:

Dynamic disk is a technology that allows an administrator to build a software RAID on a Windows server. Dynamic disk is a type of disk management that supports creating volumes that span multiple disks, stripe data across disks, mirror data between disks, or use parity for fault tolerance. Dynamic disk can be used to create RAID 0 (striping), RAID 1 (mirroring), RAID 5 (striping with parity), or spanned volumes on Windows servers. Logical volume management is a technology that allows creating and resizing logical volumes on Linux servers. GPT (GUID Partition Table) is a standard for defining the partition structure on a disk. UEFI (Unified Extensible Firmware Interface) is a specification for the interface between the operating system and the firmware. References:

<https://www.howtogeek.com/school/using-windows-admin-tools-like-a-pro/lesson2/> <https://www.howtogeek.com/howto/40702/how-to-manage-and-use-lvm-logical->

volume-management-in-ubuntu/ <https://www.howtogeek.com/193669/whats-the-difference-between-gpt-and-mbr-when-partitioning-a-drive/><https://www.howtogeek.com/56958/htg-explains-how-uefi-will-replace-the-bios/>

NEW QUESTION 307

Which of the following is used for fail over, providing access to all the services currently in use by an organization without having to physically move any servers or employees?

- A. The cloud
- B. A cold site
- C. A warm site
- D. An emergency operations center

Answer: A

Explanation:

The solution that is used for failover, providing access to all the services currently in use by an organization without having to physically move any servers or employees, is the cloud. The cloud is a term that refers to a network of remote servers that are hosted on the Internet and provide various services, such as storage, computing, networking, and applications. The cloud can be used for failover, which is a backup operation that automatically switches to a standby system or service in case of a failure or disruption of the primary system or service. By using the cloud for failover, an organization can ensure continuous availability and accessibility of its services without requiring any physical relocation or intervention.

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

NEW QUESTION 310

Which 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

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-files/>

NEW QUESTION 314

While running a local network security scan an administrator discovers communication between clients and one of the web servers is happening in cleartext. Company policy requires all communication to be encrypted. Which of the following ports should be closed to stop the cleartext communication?

- A. 21
- B. 22
- C. 443
- D. 3389

Answer: A

Explanation:

Port 21 is used for FTP (File Transfer Protocol), which is a protocol that transfers files between servers and clients in cleartext, meaning that anyone can intercept and read the data. To stop this communication, port 21 should be closed on the web server and replaced with a secure protocol, such as SFTP (Secure File Transfer Protocol) or FTPS (File Transfer Protocol Secure), which use encryption to protect the data. Verified References: [FTP vs SFTP vs FTPS]

NEW QUESTION 315

A technician learns users are unable to log in to a Linux server with known-working LDAP credentials. The technician logs in to the server with a local account and confirms the system is functional and can communicate over the network, and is configured correctly. However, the server log has entries regarding Kerberos errors. Which of the following is the MOST likely source of the issue?

- A. A local firewall is blocking authentication requests.
- B. The users have expired passwords
- C. The system clock is off by more than five minutes
- D. The server has no access to the LDAP host

Answer: C

Explanation:

Kerberos is a network authentication protocol that uses tickets to allow clients and servers to prove their identity to each other. Kerberos relies on accurate time synchronization between the parties involved, as the tickets have expiration dates and timestamps. If the system clock of a Linux server is off by more than five minutes from the LDAP server or the domain controller, the Kerberos authentication will fail and generate errors. A local firewall is unlikely to block authentication requests if the server can communicate over the network and is configured correctly. The users' passwords are not relevant if they are known-working LDAP

credentials. The server has access to the LDAP host if it can communicate over the network and is configured correctly. References:
? https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/identity_management_guide/kerberos_errors
? <https://www.ibm.com/docs/en/aix/7.2?topic=authentication-kerberos-time-synchronization>

NEW QUESTION 316

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SK0-005 Practice Exam Features:

- * SK0-005 Questions and Answers Updated Frequently
- * SK0-005 Practice Questions Verified by Expert Senior Certified Staff
- * SK0-005 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SK0-005 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SK0-005 Practice Test Here](#)