Vendor: CompTIA

Exam Code:SK0-005

Exam Name: CompTIA Server+ Certification Exam

Version: Demo

QUESTION 1

A new virtual server was deployed in a perimeter network. Users have reported the time on the server has been incorrect. The engineer has verified the configuration, and the internal time servers are configured properly. Which of the following should the engineer do to resolve this issue?

A. Check the firewall rules.

B. Replace the CMOS battery in the server.

C. Restart the time servers.

D. Manually correct the time.

Correct Answer: A

QUESTION 2

A storage engineer responds to an alarm on a storage array and finds the battery on the RAID controller needs to be replaced. However, the replacement part will not be available for 14 days. The engineer needs to identify the impact of the failed battery on the system. Which of the following best describes the impact?

A. The read and write performance will be impacted.

B. The read performance will be impacted.

C. The performance will not be impacted.

D. The write performance will be impacted.

Correct Answer: D

QUESTION 3

After installing a new file server, a technician notices the read times for accessing the same file are slower than the read times for other file servers. Which of the following is the first step the technician should take?

A. Add more memory.

B. Check if the cache is turned on.

C. Install faster hard drives.

D. Enable link aggregation.

Correct Answer: B

QUESTION 4

A hardware technician is installing 19 1U servers in a 42-unit rack. The technician needs to allocate enough space per server for optimal air flow.

Which of the following unit sizes should be allocated per server?

A. 1U

B. 2U

C. 3U

D. 4U

Correct Answer: A

This unit size would be sufficient to allocate per server for optimal airflow, as rack mount servers and racks are designed for airflow with all panels and bezels on and all U\\'s filled. Leaving gaps between servers or removing panels and covers may disrupt the airflow and cause overheating. The technician should also ensure that the airflow is front to back, as vertical airflow is likely to be ineffective. Additionally, the technician should use blanking panels, fan trays, or other devices to manage hot spots and improve circulation.

QUESTION 5

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

A. a cold site.

B. data at rest.

C. on-site retention.

D. off-site storage.

Correct Answer: B

The term that describes hosting data in different regional locations but not moving it for long periods of time is "data at rest".

Data at rest refers to data that is not actively being used or transmitted, but is instead stored in a particular location or on a particular device. This can include data that is stored on hard drives, flash drives, or other storage media, as well as

data that is stored in the cloud or on remote servers.

Option A, a cold site, refers to a backup facility that is not operational until a disaster occurs and is typically used for disaster recovery purposes.

Option C, on-site retention, refers to the practice of storing data on site, typically for regulatory or compliance purposes.

Option D, off-site storage, refers to the practice of storing data in a location other than the primary data center, typically for backup or disaster recovery purposes.

QUESTION 6

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

A. Fibre Channel

B. FCoE

C. iSCSI

D. eSATA

Correct Answer: A

The connectivity option that would best meet this requirement is Fibre Channel.

Fibre Channel is a high-speed network technology commonly used for storage area networks (SANs). It provides high-bandwidth, low-latency connectivity for storage devices over an optical connection. Fibre Channel supports speeds up to

16Gbps and is therefore the best option for meeting the requirement of transmitting at 16Gb over an optical connection.

FCoE (Fibre Channel over Ethernet) is a technology that encapsulates Fibre Channel frames within Ethernet frames for transmission over Ethernet networks, but it requires special hardware and is not widely adopted.

iSCSI (Internet Small Computer System Interface) is a storage networking standard that carries SCSI commands over IP networks. It is commonly used in smaller SAN environments, but it may not provide the same performance and reliability

as Fibre Channel.

eSATA (External Serial Advanced Technology Attachment) is an external interface used to connect storage devices to computers, but it is not a networking technology and does not provide the same capabilities as Fibre Channel.

QUESTION 7

A server administrator is taking advantage of all the available bandwidth of the four NICs on the server. Which of the following NIC-teaming technologies should the server administrator utilize?

A. Fail over

B. Fault tolerance

C. Load balancing

D. Link aggregation

Correct Answer: D

QUESTION 8

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

A. pvdisplay

B. mount

C. df -h

D. fdisk -l

Correct Answer: C

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

QUESTION 9

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

A. Restore the data from backup.

B. Disclose the incident.

C. Disable unnecessary ports.

D. Run an antivirus scan.

E. Identify the exploited vulnerability.

F. Move the data to a different location.

Correct Answer: BE

These are two measures that should be taken when a data breach occurs. A data breach is an unauthorized or illegal access to confidential or sensitive data by an internal or external actor. A data breach can result in financial losses, reputational damage, legal liabilities, and regulatory penalties for the affected organization. Disclosing the incident is a measure that involves informing the relevant stakeholders, such as customers, employees, partners, regulators, and law enforcement, about the nature, scope, and impact of the data breach. Disclosing the incident can help to mitigate the negative consequences of the data breach, comply with legal obligations, and restore trust and confidence. Identifying the exploited vulnerability is a measure that involves investigating and analyzing the root cause and source of the data breach. Identifying the exploited vulnerability can help to prevent further data loss, remediate the security gaps, and improve the security posture of the organization. Restoring the data from backup is a measure that involves recovering the lost or corrupted data from a secondary storage device or location. However, this does not address the underlying issue of how the data breach occurred or prevent future breaches. Disabling unnecessary ports is a measure that involves closing or blocking network communication endpoints that are not required for legitimate purposes. However, this does not address how the data breach occurred or what vulnerability was exploited. Running an antivirus scan is a measure that involves detecting and removing malicious software from a system or network. However, this does not address how the data breach occurred or what vulnerability was exploited. Moving the data to a different location is a measure that involves transferring the data to another storage device or location that may be more secure or less accessible. However, this does

not address how the data breach occurred or what vulnerability was exploited.

References:

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

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

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

QUESTION 10

A developer is creating a web application that will contain ve web nodes. The developer\\'s main goal is to ensure the application is always available to the end users. Which of the following should the developer use when designing the web application?

A. Round robin

B. Link aggregation

C. Network address translation

D. Bridged networking

Correct Answer: A

QUESTION 11

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

A. Management port

B. Crash cart

C. IP KVM

D. KVM

Correct Answer: D

Management port - irrelevant choice.

Crash cart - if you on-site support occasionally, not worth to have crash cart.

IP KVM - this connection type use for remote drive access, remote console access, OOB and but more cost.

KVM - local access, less cost

QUESTION 12

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

A. Biometrics

B. Push notifications

C. Smart cards

D. Physical tokens

Correct Answer: B

Option B, push notifications, would be the most cost-effective solution to implement MFA on all servers. With push notifications, the user receives a notification on their mobile device or computer prompting them to approve or deny access to

the server. This method does not require any additional hardware or tokens and can be implemented easily.

Option A, biometrics, may provide a high level of security, but it would require additional hardware such as fingerprint scanners or facial recognition cameras, which can be expensive.

Option C, smart cards, require the purchase and distribution of smart cards to all users, which can be costly and time-consuming to manage.

Option D, physical tokens, such as key fobs or USB tokens, are also costly to purchase and distribute to all users. Additionally, if a user loses their token, it may cause a delay in access to the server until a new token can be distributed.