# CompTIA

## Exam Questions SK0-005

CompTIA Server+ Certification Exam

**NEW QUESTION 1**
An administrator restores several database files without error while participating in a mock disaster recovery exercise. Later, the administrator reports that the restored databases are
corrupt and cannot be used. Which of the following would best describe what caused this issue?

A. The databases were not backed up to be application consistent.
B. The databases were asynchronously replicated
C. The databases were mirrored
D. The database files were locked during the restoration process.

**Answer:** A

**Explanation:**
Application consistent backup is a method of backing up data that ensures the integrity and consistency of the application state. It involves notifying the application to flush its data from memory to disk and quiescing any write operations before taking a snapshot of the data. If the databases were not backed up to be application consistent, they might contain incomplete or corrupted data that cannot be restored properly. References:
CompTIA Server+ Certification Exam Objectives1, page 12 What is Application Consistent Backup and How to Achieve It2 Application-Consistent Backups3

**NEW QUESTION 2**
A server administrator mounted a new hard disk on a Linux system with a mount point of
/newdisk. It was later determined that users were unable to create directories or files on the new mount point. Which of the following commands would successfully mount the drive with the required parameters?

A. echo /newdisk >> /etc/fstab
B. net use /newdisk
C. mount –o remount, rw /newdisk
D. mount –a

**Answer:** C

**Explanation:**
The administrator should use the command mount –o remount,rw /newdisk to successfully mount the drive with the required parameters. The mount command is used to mount file systems on Linux systems. The –o option specifies options for mounting file systems. The remount option re-mounts an already mounted file system with different options. The rw option mounts a file system with read-write permissions. In this case,
/newdisk is a mount point for a new hard disk that was mounted with read-only permissions by default. To allow users to create directories or files on /newdisk, the administrator needs to re-mount /
Reference:
https://unix.stackexchange.com/QUESTION NO:s/149399/how-to-remount-as-read-write-a- specific-mount-of-device

**NEW QUESTION 3**
A systems administrator needs to create a data volume out of four disks with the MOST redundancy. Which of the following is the BEST solution?

A. RAID 0
B. RAID 1
C. RAID 5
D. RAID 6

**Answer:** D

**Explanation:**
RAID 6 is a type of RAID level that uses two parity blocks to provide fault tolerance and redundancy for data storage. RAID 6 can withstand the failure of up to two disks in the array without losing any data. RAID 6 requires a minimum of four disks to operate, and it distributes the data and parity blocks across all the disks in the array. RAID 6 has a high write penalty, which means that it takes more time and resources to write data to the disks than to read data from them. However, RAID 6 offers a highlevel of data protection and reliability, which makes it suitable for applications that require high availability and durability1.
RAID 1 provides redundancy and fault tolerance by mirroring the data from one disk to another disk. RAID 1 offers high read performance and data security, but it has low capacity and write performance. RAID 1 requires a minimum of two disks to operate, and it can only tolerate the failure of one disk in the array. If more than one disk fails, all the data in the array is lost2.
RAID 5 provides redundancy and fault tolerance by using one parity block to store information that can be used to reconstruct the data in case of a disk failure. RAID 5 requires a minimum of three disks to operate, and it distributesthe data and parity blocks across all the disks in the array. RAID 5 offers a balance between performance, capacity, and data protection, but it can only tolerate the failure of one disk in the array. If more than one disk fails, all the data in the array is lost2. Therefore, among these options, RAID 6 is the best solution for creating a data volume out of four disks with the most redundancy.

**NEW QUESTION 4**
An administrator needs to reconfigure a teamed network connection on a server in a remote data center. Which of the following will offer the most resilient connection while performing this change?

A. Use of an 00B solution
B. Use of a crash cart
C. Use of a VNC console
D. Use of an RDP console

**Answer:** A

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

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

**NEW QUESTION 5**
A server administrator is exporting Windows system files before patching and saving them to the following location:
\\server1\ITDept\
Which of the following is a storage protocol that the administrator is MOST likely using to save this data?

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

**Answer:** C

**Explanation:**
 The storage protocol that the administrator is most likely using to save data to the location \server1\ITDept\ is CIFS. CIFS (Common Internet File System) is a protocol that allows file sharing and remote access over a network. CIFS is based on SMB (Server Message Block), which is a protocol that enables communication between devices on a network. CIFS uses UNC (Universal Naming Convention) paths to identify network resources, such as files or folders. A UNC path has the format \servername\sharename\path\filename. In this case, server1 is the name of the server, ITDept is the name of the shared folder, and \ is the path within the shared folder.

**NEW QUESTION 6**
A server administrator is installing a new server that uses 40G0 network connectivity. The administrator needs to find the proper cables to connect the server to the switch. Which of the following connectors should the administrator use?

A. SFP+
B. GBIC
C. SFP
D. QSFP+

**Answer:** D

**Explanation:**
 QSFP+ is a type of connector that should be used to connect a server to a switch that uses 40G network connectivity. QSFP+ (Quad Small Form-factor Pluggable Plus) is a compact, hot-pluggable transceiver module that supports data rates up to 40 Gbps. QSFP+ modules can be used for various network protocols and media types, such as Ethernet, Fibre Channel, InfiniBand, or optical fiber. QSFP+ modules have a 38-pin edge connector and can be inserted into a QSFP+ port on a switch or a server. SFP+ (Small Form-factor Pluggable Plus) is a type of connector that supports data rates up to 10 Gbps, but not 40 Gbps. SFP+ modules have a 20-pin edge connector and can be inserted into an SFP+ port on a switch or a server. GBIC (Gigabit Interface Converter) is an older type of connector that supports data rates up to 1 Gbps, but not 40 Gbps. GBIC modules have an SC duplex connector and can be inserted into a GBIC port on a switch or a server. SFP (Small Form-factor Pluggable) is another older type of connector that supports data rates up to 1 Gbps or 4 Gbps, but not 40 Gbps. SFP modules have an LC duplex connector and can be inserted into an SFP port on a switch or a server. References: https://www.howtogeek.com/190014/virtualization-basics-understanding-techniques-and- fundamentals/ https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and- why-does-it-matter/ https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual-files/

**NEW QUESTION 7**
A systems administrator is performing maintenance on 12 Windows servers that are in different racks at a large datacenter. Which of the following would allow the administrator to perform maintenance on all 12 servers without having to physically be at each server? (Choose two.)

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

**Answer:** AB

**Explanation:**
 The methods that would allow the administrator to perform maintenance on all 12 servers without having to physically be at each server are remote desktop and IP KVM. Remote desktop is a feature that allows a user to access and control another computer over a network using a graphical user interface (GUI). Remote desktop can enable remote administration, troubleshooting, and maintenance of servers without requiring physical presence at the server location. IP KVM (Internet Protocol Keyboard Video Mouse) is a device that allows a user to access and control multiple servers over a network using a single keyboard, monitor, and mouse. IP KVM can provide remote access to servers regardless of their operating system or power state, and can also support virtual media and serial console functions.
Reference:
https://www.blackbox.be/en-be/page/27559/Resources/Technical-Resources/Black-Box- Explains/kvm/ Benefits-of-using-KVM-over-IP

**NEW QUESTION 8**
An organization purchased six new 4TB drives for a server. An administrator is tasked with creating an efficient RAID given the minimum disk space requirement of 19TBs. Which of the following should the administrator choose to get the most efficient use of space?

A. RAID 1
B. RAID 5
C. RAID 6
D. RAID 10

**Answer:** B

**Explanation:**

RAID 5 is a RAID level that uses disk striping with parity. It requires a minimum of three disks and can handle one disk failure. RAID 5 distributes the parity information across all the disks in the array, which improves the read performance and reduces the write penalty. The capacity of a RAID 5 array is (N-1) times the size of the smallest disk, where N is the number of disks in the array. Therefore, for six 4TB disks, the capacity of a RAID 5 array would be (6-1) x 4TB = 20TB, which meets the minimum disk space requirement of 19TB. RAID 5 also has the leastamount of disk space lost to RAID overhead among the options, as it only uses onedisk's worth of space for parity

## NEW QUESTION 9

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 10

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

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

A. Drive
B. Database
C. Folder
D. File

**Answer:** A

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

## NEW QUESTION 13

Which of the following testing exercises for disaster recovery is primarily used to discuss incident response strategies for critical systems without affecting production data?

A. Tabletcp
B. Backup recovery test
C. Lrverail over
D. Hot-site visit audit

**Answer:** A

**Explanation:**
A tabletop exercise is a type of disaster recovery testing exercise that is primarily used to discuss incident response strategies for critical systems without affecting production data. A tabletop exercise is a discussion-based session where team members meet in an informal, classroom setting to review their roles and responsibilities during an emergency and their responses to a hypothetical scenario. A facilitator guides the participants through the discussion and evaluates the strengths and weaknesses of the preparedness program. A tabletop exercise does not involve any actual deployment of resources oractivation of systems12. A backup recovery test (B) is a type of disaster recovery testing exercise that involves restoring data from backup media to verify its integrity and availability. A backup recovery test may affect production data if it is not performed on a separate environment. A live failover © is a type of disaster recovery testing exercise that involves switching operations from a primary site to a secondary site in case of a failure or disruption. A live failover may affect production data if it is not performed on a simulated environment. A hot-site visit audit (D) is a type of disaster recovery testing exercise that involves inspecting and evaluating a hot site, which is a backup location that has fully operational equipment and resources to resume business operations in case of a disaster. A hot-site visit audit does not involve any discussion of incident response strategies or simulation of scenarios. References: 1 https://www.ready.gov/testing-exercises2 https://www.ready.gov/exercises

**NEW QUESTION 16**
A systems administrator is setting up a server on a LAN that uses an address space that follows the RFC 1918 standard. Which of the following IP addresses should the administrator use to be in compliance with the standard?

A. 11.251.196.241
B. 171.245.198.241
C. 172.16.19.241
D. 193.168.145.241

**Answer:** C

**Explanation:**
The administrator should use 172.16.19.241 as an IP address to be in compliance with RFC 1918 standard. RFC 1918 defines three ranges of IP addresses that are reserved for private internets, meaning they are not globally routable on the public Internet and can be used within an enterprise without any risk of conflict or overlap with other networks. These ranges are:
* 10.0.0.0 - 10.255.255.255 (10/8 prefix) 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
* 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
Out of these ranges, only 172.16.19.241 falls within one of them (172.16/12 prefix). The other options are either public IP addresses that belong to other organizations or networks (11.251.196.241, 171.245.198.241) or invalid IP addresses that do not conform to any standard (193.168.145.241).
Reference: https://whatis.techtarget.com/definition/RFC-1918

**NEW QUESTION 21**
Which of the following actions should a server administrator take once a new backup scheme has been configured?

A. Overwrite the backups
B. Clone the configuration
C. Run a restore test
D. Check the media integrity

**Answer:** C

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

**NEW QUESTION 23**
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 24**
A server administrator is currently working on an incident. Which of the following steps should the administrator perform before resolving the issue?

A. Inform the impacted users.
B. Make the changes to the system.
C. Determine the probable causes.
D. Identify changes to the server.

**Answer:** C

**Explanation:**
The step that the server administrator should perform before resolving the issue is to determine the probable causes. This step is part of the troubleshooting process that follows a logical and systematic approach to identify and solve problems with servers and applications. The troubleshooting process consists of several steps, such as:
? Identify the problem: Gather information from various sources, such as users, logs, or alerts, to understand the symptoms and scope of the problem.
? Establish a theory of probable cause: Analyze the information and formulate one or more possible causes of the problem based on evidence or experience.
? Test the theory to determine cause: Perform tests or experiments to verify or eliminate each possible cause until the root cause is found.
? Establish a plan of action to resolve the problem and implement the solution: Design and execute a plan to fix the problem using appropriate tools and techniques.
? Verify full system functionality and implement preventive measures: Confirm that the problem is resolved and that no other issues arise as a result of the solution. Implement preventive measures to avoid recurrence of the problem or improve performance.
? Document findings, actions, and outcomes: Record the details of the problem, its cause, its solution, and its outcome for future reference or knowledge sharing. References: [CompTIA Server+ Certification Exam Objectives], Domain 6.0: Troubleshooting, Objective 6.1: Given a scenario involving server hardware

issues (e.g., power supply failure), troubleshoot using appropriate tools.

**NEW QUESTION 29**
A server administrator needs to harden a server by only allowing secure traffic and DNS inquiries. A port scan reports the following ports are open:

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

**Answer:** D

**Explanation:**
The administrator should only allow secure traffic and DNS inquiries on the server, which means that only ports 22, 53, and 443 should be open. Port 22 is used for SSH (Secure Shell), which is a protocol that allows secure remote login and command execution over a network connection using a command-line interface (CLI). Port 53 is used for DNS (Domain Name System), which is a service that translates domain names into IP addresses and vice versa. Port 443 is used for HTTPS (Hypertext Transfer Protocol Secure), which is a secure version of HTTP that encrypts the data exchanged between a web browser and a web server. Reference: https://tools.cisco.com/security/center/resources/dns_best_practices

**NEW QUESTION 34**
Following a recent power outage, a server in the datacenter has been constantly going offline and losing its configuration. Users have been experiencing access issues while using the application on the server. The server technician notices the data and time are incorrect when the server is online. All other servers are working. Which of the following would MOST likely cause this issue? (Choose two.)

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

**Answer:** BF

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

**NEW QUESTION 38**
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 management activity that is used to address urgent issues that pose a significant risk to the organization, such as a system breach. An emergency change request requires immediate action and approval, and it may bypass some of the normal change management procedures, such as testing, documentation, or stakeholder communication12.
References = 1: Change Management Plans: A Definitive Guide -Indeed(https://www.indeed.com/career-advice/career-development/change-management-activities) 2: The 10 Best Change Management Activities-Connecteam(https://connecteam.com/top-10-change-management-activities/)

**NEW QUESTION 41**
A server room contains ten physical servers that are running applications and a cluster of three dedicated hypervisors. The hypervisors are new and only have 10% utilization. The Chief Financial Officer has asked that the IT department do what it can to cut back on power consumption and maintenance costs in the data center. Which of the following would address the request with minimal server downtime?

A. Unplug the power cables from the redundant power supplies, leaving just the minimum required.
B. Convert the physical servers to the hypervisors and retire the ten servers.
C. Reimage the physical servers and retire all ten servers after the migration is complete.
D. Convert the ten servers to power-efficient core editions.

**Answer:** B

**Explanation:**
This option would reduce power consumption and maintenance costs by consolidating the physical servers into virtual machines on the hypervisors. This would also free up space and resources in the data center. The other options would either not address the request, increase power consumption, or require more maintenance.

**NEW QUESTION 42**
A technician noted the RAID hard drives were functional while troubleshooting a motherboard failure. The technician installed a spare motherboard with similar specifications and used the original components. Which of the following should the technician do to restore operations with minimal downtime?

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

**Answer:** C

**Explanation:**
RAID (Redundant Array of Independent Disks) is a technology that combines multiple hard drives into a logical unit that provides improved performance, reliability, or capacity. RAID can be implemented by hardware, software, or a combination of both. Hardware RAID uses a dedicated controller to manage the RAID array, while software RAID uses the operating system or a driver to do the same1.
In this scenario, the technician noted that the RAID hard drives were functional while troubleshooting a motherboard failure. This means that the data on the drives was not corrupted or lost. However, the technician installed a spare motherboard with similar specifications and used the original components. This means that the new motherboard may not have the same RAID configuration as the old one, or it may not recognize the existing RAID array at all. Therefore, the technician needs to reconfigure the RAID in order to restore operations with minimal downtime.

**NEW QUESTION 43**
An administrator has been asked to disable CPU hyperthreading on a server to satisfy a licensing issue. Which of the following best describes how the administrator will likely perform this action?

A. Use a RDP/VNC session.
B. Modify the startup configuration.
C. Use a PowerSheII/Bash script.
D. Use the BIOS/UEFI setup.

**Answer:** D

**Explanation:**
The BIOS (Basic Input/Output System) or UEFI (Unified Extensible Firmware Interface) setup is a program that allows users to configure the hardware settings of a computer, such as the CPU, memory, disk, and boot options. The BIOS/UEFI setup can be accessed by pressing aspecific key (such as F2, F10, or Delete) during the boot process, before the operating system loads12.
One of the settings that can be changed in the BIOS/UEFI setup is the CPU hyperthreading option. Hyperthreading is a technology that enables a single physical CPU core to execute two threads or tasks simultaneously, improving the performance and efficiency of multi- threaded applications. However, some software licenses may limit the number of CPU cores or threads that can be used, and therefore require disabling hyperthreading on the server34.
To disable hyperthreading on a server, the administrator will likely need to enter the BIOS/UEFI setup and navigate to the processor options menu. There, the administrator will find a setting for Intel ® Hyperthreading Technology or Hyperthreading Function, which can be enabled or disabled. The administrator will need to disable this setting and save the changes. This will turn off hyperthreading on the server and reduce the number of logical CPUs to match the number of physical cores5.

**NEW QUESTION 48**
An application server cannot communicate with a newly installed database server. The database server, which has static IP information, is reading the following output from ipconf ig:



```
IP: 10.0.10.240
Mask: 255.255.255.128
Gateway: 10.0.10.1
```

The application server is reading the following output from ipconf ig:



```
IP: 10.0.10.25
Mask: 255.255.255.128
Gateway: 10.0.10.1
```

Which of the following most likely contains an error?

A. IP address
B. DHCP
C. Gateway
D. Subnet mask

**Answer:** D

**Explanation:**
The subnet mask is most likely containing an error that prevents the application server from communicating with the newly installed database server. The subnet mask is a binary number that defines how many bits of an IP address are used for the network portion and how many bits are used for the host portion. The subnet mask determines which devices belong to the same network or subnet and can communicate directly with each other without routing or switching devices. The subnet mask of the database server is 255.255.O.O, which means that all 32 bits of its IP address are used for the network portion and none for the host portion, which is invalid and makes it unreachable by any other device on any network or subnet. The subnet mask of the application server is 255.O.O.O, which means

that only 8 bits of its IP address are used for the network portion and 24 bits are used for the host portion, which is also uncommon and makes it incompatible with most networks or subnets. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Networking, Objective 4.1: Given a scenario, configure network settings for servers.

**NEW QUESTION 53**
A technician is checking a server rack. Upon entering the room, the technician notices the tans on a particular server in the rack are running at high speeds. This is the only server in the rack that is experiencing this behavior. The ambient temperature in the room appears to be normal. Which of the following is the MOST likely reason why the fans in that server are operating at full speed?

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

**Answer:** C

**Explanation:**
 This is the most likely reason why the fans in that server are operating at full speed while the ambient temperature in the room is normal and the other servers in the rack are not experiencing this behavior. A fan failure is a situation where one or more fans in a server stop working or malfunction due to wear and tear, dust, or other factors. This can cause overheating and performance issues on the server. To prevent this, most servers have a fan redundancy feature that allows the other fans to increase their speed and airflow to compensate for the failed fan and maintain a safe temperature level. The server is not likely to be in the process of shutting down, as this would not cause the fans to run at high speeds. An incorrect fan size is not likely to be inserted into the server, as most fans are standardized and compatible with the server chassis and motherboard. The server is not likely to be utilizing more memory than the other servers, as this would not cause a significant increase in temperature or fan speed. References: https://www.howtogeek.com/303282/how-to-manage-your-pcs-fans-for-optimal-airflow-and-cooling/https://www.howtogeek.com/174288/how-to-tell-if-your-computer-is-overheating-and-what-to-do-about-it/

**NEW QUESTION 55**
A server is only able to connect to a gigabit switch at 100Mb. Other devices are able to access the network port at full gigabit speeds, and when the server is brought to another location, it is able to connect at full gigabit speed. Which of the following should an administrator check first?

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

**Answer:** C

**Explanation:**
The first thing that the administrator should check is the network cable. The network cable is a physical medium that connects a server to a switch or other network device. The network cable can affect the speed and quality of the network connection, depending on its type, length, and condition. If the network cable is damaged, faulty, or incompatible, it can cause the server to connect at a lower speed than expected. Therefore, the administrator should check the network cable for any signs of wear, tear, or mismatch, and replace it if necessary.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 2, Lesson 2.1, Objective 2.1

**NEW QUESTION 57**
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 60**
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 61**
A security administrator ran a port scanning tool against a virtual server that is hosting a secure website. A list of open ports was provided as documentation. The management team has requested that non-essential ports be disabled on the firewall. Which of the following ports must remain open?

A. 25
B. 443
C. 3389
D. 8080

**Answer:** B

**Explanation:**
The port that must remain open for a secure website is port 443. Port 443 is used by Hypertext Transfer Protocol Secure (HTTPS), which is an extension of HTTP that encrypts and authenticates the communication between a web server and a web browser. HTTPS ensures that the data transmitted over the web is protected from eavesdropping, tampering, or spoofing. Therefore, port 443 must remain open for a secure website to function properly.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 2, Lesson 2.2, Objective 2.2

**NEW QUESTION 65**
An organization is donating its outdated server equipment to a local charity. Which of the following describes what the organization should do BEFORE donating the equipment?

A. Remove all the data from the server drives using the least destructive method.
B. Repurpose and recycle any usable server components.
C. Remove all the components from the server.
D. Review all company polices.

**Answer:** D

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

**NEW QUESTION 70**
An administrator is tasked with building an environment consisting of four servers that can each serve the same website. Which of the following concepts is described?

A. Load balancing
B. Direct access
C. Overprovisioning
D. Network teaming

**Answer:** A

**Explanation:**
Load balancing is a concept that distributes the workload across multiple servers or other resources to optimize performance, availability, and scalability. Load balancing can be implemented at different layers of the network, such as the application layer, the transport layer, or the network layer. Load balancing can use various algorithms or methods to determine how to distribute the traffic, such as round robin, least connections, or weighted distribution.
References: CompTIA Server+ Study Guide, Chapter 6: Networking, page 241.

**NEW QUESTION 73**
A server administrator is deploying a new server that has two hard drives on which to install the OS. Which of the following RAID configurations should be used to provide redundancy for the OS?

A. RAID 0
B. RAID 1
C. RAID 5
D. RAID 6

**Answer:** B

**Explanation:**
RAID 1 (mirroring) is a RAID configuration that should be used to provide redundancy for the OS on a server that has two hard drives on which to install the OS. RAID 1 (mirroring) is a configuration that duplicates data across two or more drives. It provides fault tolerance and improves read performance, but reduces storage capacity by half. If one drive fails in RAID 1, the other drive can continue to operate without data loss or system downtime. RAID 0 (striping) is a configuration that splits data across two or more drives without parity or redundancy. It improves performance but offers no fault tolerance. If one drive fails in RAID 0, all data is lost and the system cannot boot. RAID 5 (striping with parity) is a configuration thatstripes data across three or more drives with parity information. It provides fault tolerance and improves performance, but reduces storage capacity by one drive's worth of space. RAID 5 can tolerate one drive failure without data loss, but not two or more. RAID 6 (striping with double parity) is a configuration that stripes data across four or more drives with double parity information. It provides fault tolerance and improves performance, but reduces storage capacity by two drives' worth of space. RAID 6 can tolerate two drive failures without data loss, but not three or more.References:https://www.howtogeek.com/199068/how-to-upgrade-your-existing-hard-drive-in-under-an-hour/

**NEW QUESTION 74**
The accounting department needs more storage and wants to retain the current data for quick read-write access. The accounting server does not have any internet drive bays available to keep both disks however the server does have USB 3 0 and eSATA ports available. Which of the following is the BEST way to accomplish

the department's goals?

A. Copy the existing data to an external USB 3 0 enclosure.
B. Place the existing data on a DVD and use the internal DVD-ROM drive.
C. Transfer the existing data to an external eSATA enclosure.
D. Move the existing data to a ne
E. larger internal hard drive.

**Answer:** C

**Explanation:**
The best way to accomplish the department's goals is to transfer the existing data to an external eSATA enclosure, which is a device that connects an external hard drive to a computer using an eSATA port. This will allow the accounting department to retain the current data for quick read-write access, as eSATA provides high-speed data transfer rates and supports hot-plugging. Unlike USB 3.0, eSATA does not share bandwidth with other devices, which can improve performance and reliability. Verified References: [eSATA vs USB 3.0]

## NEW QUESTION 75
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 78
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 80
A technician is attempting to log in to a Linux server as root but cannot remember the administrator password. Which of the following is the LEAST destructive method of resetting the administrator password?

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

**Answer:** C

**Explanation:**
This is the least destructive method of resetting the administrator password because it does not require modifying any files or reinstalling the OS. It only requires changing the boot parameters temporarily and running a command to change the password.References:https://wiki.archlinux.org/title/Reset_lost_root_password#Using_GR UB

## NEW QUESTION 81
Users cannot access a new server by name, but the server does respond to a ping request using its IP address. All the user workstations receive their IP information from a DHCP server. Which of the following would be the best step to perform NEXT?

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

**Answer:** B

**Explanation:**
If users cannot access a new server by name, but the server does respond to a ping request using its IP address, it means that there is a problem withname resolution. The DNS (Domain Name System) is a service that maps hostnames to IP addresses and vice versa. Therefore, the best step to perform next is to examine the DNS to see if the new server record exists and matches its IP address. If not, the DNS record needs to be added or updated accordingly. Running the tracert command from a workstation would not help with name resolution, as it only shows the route taken by packets to reach a destination by IP address. Correcting the missing DHCP scope would not help either, as DHCP (Dynamic Host Configuration Protocol) only assigns IP addresses and other network settings to clients, but does not resolve names. Updating the workstation hosts file would be a temporary workaround, but not a permanent solution, as it would require manually editing every workstation's hosts file with the new server's name and IP address. References: https://www.howtogeek.com/164981/how-to-use-nslookup-to-check- domain-name-information-in-microsoft-windows/https://www.howtogeek.com/howto/27350/beginner-geek-how-to-edit-your-hosts- file/

**NEW QUESTION 84**
A server administrator receives the following output when trying to ping a local host:

```
ping imhrh-vc.net
Reply from imhrh-vc.net. Destination host unreachable.
Reply from imhrh-vc.net. Destination host unreachable.
Reply from imhrh-vc.net. Destination host unreachable.
Reply from imhrh-vc.net. Destination host unreachable.
```

Which of the following is MOST likely the issue?

A. Firewall
B. DHCP
C. DNS
D. VLAN

**Answer:** A

**Explanation:**
A firewall is a network device or software that filters and controls the incoming and outgoing traffic based on predefined rules. A firewall can block or allow certain types of packets, ports, protocols, or IP addresses. The output of the ping command shows that the local host is unreachable, which means that there is no network connectivity between the source and the destination. This could be caused by a firewall that is blocking the ICMP (Internet Control Message Protocol) packets that ping uses to test the connectivity.References: https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives (Objective 2.2)

**NEW QUESTION 89**
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 3651 or DocuSign2.
References = 1: Compare All Microsoft 365 Plans (Formerly Office 365) - Microsoft Store(https://www.microsoft.com/en-us/microsoft-365/buy/compare-all-microsoft-365- products) 2: DocuSign Pricing | eSignature Plans for Personal & Business(https://ecom.docusign.com/plans-and-pricing/esignature)

**NEW QUESTION 92**
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 96**
A technician recently replaced a NIC that was not functioning. Since then, no device driver is found when starting the server, and the network card is not

functioning. Which of the following should the technician check first?

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

**Answer:** C

**Explanation:**
 The technician should check the hardware compatibility list (HCL) first to see if the new NIC is supported by the server's operating system. The HCL is a list of hardware devices that have been tested and verified to work with a specific operating system. If the NIC is not on the HCL, it means that there is no device driver available or compatible for it, and the NIC will not function properly.
References: CompTIAServer+ SK0-005 Certification Study Guide, Chapter 5, Lesson 5.2, Objective 5.2

**NEW QUESTION 100**
A systems administrator needs to configure a new server and external storage for a new production application environment. Based on end-user specifications, the new solution needs to adhere to the following basic requirements:
* 1. The OS must be installed in a separate disk partition. In case of hard drive failure, it cannot be affected.
* 2. Application data IOPS performance is a must.
* 3. Data availability is a high priority, even in the case of multiple hard drive failures.
Which of the following are the BEST options to comply with the user requirements? (Choose three.)

A. Install the OS on a RAID 0 array.
B. Install the OS on a RAID 1 array.
C. Configure RAID 1 for the application data.
D. Configure RAID 5 for the application data.
E. Use SSD hard drives for the data application array.
F. Use SATA hard drives for the data application array.
G. Use a single JBOD for OS and application data.

**Answer:** BDE

**Explanation:**
 To comply with the user requirements, the best options are to install the OS on a RAID 1 array, configure RAID 5 for the application data, and use SSD hard drives for the data application array. Here is why:
? RAID 1 is a mirroring technique that creates an exact copy of data on two disks.
This provides redundancy and fault tolerance in case of hard drive failure. RAID 1 also improves read performance since either disk can be read at the same time. Therefore, installing the OS on a RAID 1 array meets the first requirement of separating the OS from the application data and protecting it from hard drive failure.
? RAID 5 is a striping technique with parity that distributes data and parity blocks
across three or more disks. This provides improved performance and storage efficiency compared to RAID 1, as well as fault tolerance in case of a single disk failure. Therefore, configuring RAID 5 for the application data meets the second and third requirements of providing high IOPS performance and data availability.
? SSD hard drives are solid-state drives that use flash memory to store data. They
have no moving parts and offer faster read and write speeds, lower latency, and lower power consumption than traditional HDDs. Therefore, using SSD hard drives for the data application array meets the second requirement of providing high IOPS performance.
References:
? https://phoenixnap.com/kb/raid-levels-and-types
? https://en.wikipedia.org/wiki/Standard_RAID_levels

**NEW QUESTION 102**
A server administrator must respond to tickets within a certain amount of time. The server administrator needs to adhere to the:

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

**Answer:** D

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

**NEW QUESTION 103**
A server administrator just installed a new physical server and needs to harden the applications on the server. Which of the following best describes a method of application hardening?

A. Install the latest patches.
B. Disable unneeded hardware.
C. Set the boot order.
D. Enable a BIOS password.

**Answer:** A

**Explanation:**
A method of application hardening is installing the latest patches. Application hardening is a process of reducing the attack surface and vulnerabilities of an application by applying security measures and best practices. Installing the latest patches is one way to harden an application, as patches are updates that fix bugs, errors, or security issues in an application. By installing the latest patches, an application can be protected from known exploits or threats.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.5, Objective 3.5

**NEW QUESTION 107**
Users ate experiencing issues when trying to access resources on multiple servers. The servers are virtual and run on an ESX server. A systems administrator is investigating but is unable to connect to any of the virtual servers. When the administrator connects to the host, a purple screen with while letters appears. Which of the following troubleshooting steps should the administrator perform FIRST?

A. Check the power supplies
B. Review the log files.
C. Reinstall the ESX server.
D. Reseat the processors.

**Answer:** B

**Explanation:**
 A purple screen with white letters on an ESX server indicates a kernel panic, which is a fatal error that causes the system to crash and stop functioning3. The first troubleshooting step that an administrator should perform is to review the log files, which may contain information about the cause of the error, such as hardware failures, software bugs, or configuration issues4. Checking the power supplies (A) may not be relevant, as the system is still displaying a screen. Reinstalling the ESX server © or reseating the processors (D) are drastic measures that may result in data loss or further damage, and should only be attempted after ruling out other possible causes. References: 3
https://kb.vmware.com/s/article/10145084 https://www.altaro.com/vmware/vmware-esxi-purple-screen-death/

**NEW QUESTION 112**
A systems administrator is setting up a server farm for a new company. The company has a public range of IP addresses and uses the addresses internally. Which of the following IP addresses best fits this scenario?

A. 10.3.7.27
B. 127.0.0.1
C. 192.168.7.1
D. 216,176,128.10

**Answer:** D

**Explanation:**
The IP address that best fits this scenario is 216.176.128.10. This is a public IP address that belongs to a range of addresses that are assigned and registered by an Internet service provider (ISP) and can be accessed from anywhere on the Internet. The company has a public range of IP addresses and uses them internally, which means that they do not use private IP addresses or network address translation (NAT) to communicate within their network.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 2, Lesson 2.2, Objective 2.2

**NEW QUESTION 115**
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 118**
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 RAIDthat 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 122**

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 125**
A technician is attempting to update a server's firmware. After inserting the media for the firmware and restarting the server, the machine starts normally into the OS. Which of the following should the technician do NEXT to install the firmware?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 128**
An application needs 10GB of RAID 1 for log files, 20GB of RAID 5 for data files, and 20GB of RAID 5 for the operating system. All disks will be 10GB in capacity. Which of the following is the MINIMUM number of disks needed for this application?

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

**Answer:** C

**Explanation:**

To calculate the minimum number of disks needed for this application, we need to consider the RAID levels and their disk requirements. RAID 1 requires a minimum of two disks and provides mirroring, which means that data is duplicated on both disks. RAID 5 requires a minimum of three disks and provides striping with parity, which means that data is distributed across all disks with one disk storing parity information for error correction. RAID 5 can tolerate one disk failure without losing data. To create a 10GB RAID 1 array for log files, we need two 10GB disks. To create a 20GB RAID 5 array for data files, we need four 10GB disks (three for data and one for parity). To create a 20GB RAID 5 array for the operating system, we need another four 10GB disks (three for data and one for parity). Therefore, the total number of disks needed is 2 + 4 + 4 = 10. However, since we can use different RAID levels for different partitions on the same disk, we can optimize the disk usage by using only eight disks as follows: Disk 1: 10GB RAID 1 (log files) + 10GB RAID 5 (data files) Disk 2: 10GB RAID 1 (log files) + 10GB RAID 5 (data files) Disk 3: 10GB RAID 5 (data files) + 10GB RAID 5 (OS) Disk 4: 10GB RAID 5 (data files) + 10GB RAID 5 (OS) Disk 5: 10GB RAID 5 (parity for data files) + 10GB RAID 5 (OS) Disk 6: 10GB RAID 5 (OS) + unused space Disk 7: 10GB RAID 5 (parity for OS) + unused space Disk 8: unused space References:https://en.wikipedia.org/wiki/Standard_RAID_levels

**NEW QUESTION 132**
Which of the following physical security concepts would most likely be used to limit personnel access to a restricted area within a data center?

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

**Answer:** A

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

**NEW QUESTION 136**
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 137**
A server administrator needs to create a new folder on a file server that only specific users can access. Which of the following BEST describes how the server administrator can accomplish this task?

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

**Answer:** C

**Explanation:**
The top portion of the dialog box lists the users and/or groups that have access to the file or folder.
Reference:https://www.uwec.edu/kb/article/drives-establishing-windows-file-and-folder- level-permissions/

**NEW QUESTION 138**
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 142**
Which of the following BEST describes overprovisioning in a virtual server environment?

A. Committing more virtual resources to virtual machines than there are physical resources present
B. Installing more physical hardware than is necessary to run the virtual environment toallow for future expansion
C. Allowing a virtual machine to utilize more resources than are allocated to it based on the server load
D. Ensuring there are enough physical resources to sustain the complete virtual environment in the event of a host failure

**Answer:** A

**Explanation:**
This is the best definition of overprovisioning in a virtual server environment because it means allocating more CPU, memory, disk, or network resources to the virtual machines than what is actually available on the physical host. This can lead to performance issues and resource contention. References:https://www.hpe.com/us/en/insights/articles/10-virtualization-mistakes-everyone-makes-1808.html

**NEW QUESTION 146**
A technician has moved a data drive from a new Windows server to an older Windows server. The hardware recognizes the drive, but the data is not visible to the OS. Which of the following is the most likely cause of the issue?

A. The disk uses GPT.
B. The partition is formatted with ext4.
C. The partition is formatted with FAT32.
D. The disk uses MBR.

**Answer:** A

**Explanation:**
The most likely cause of the issue is that the disk uses GPT.GPT stands for GUID Partition Table, which is a newer standard for disk partitioning that supports larger disks and more partitions than theolder MBR (Master Boot Record) standard1.However, GPT is not compatible with some older operating systems, such as Windows XP or Windows Server 20032. Therefore, if the data drive was formatted with GPT on a new Windows server and then moved to an older Windows server, the older server may not be able to recognize the GPT partitions and access the data on the drive.
The partition being formatted with ext4, FAT32, or MBR are not likely causes of the issue.Ext4 is a file system that is commonly used on Linux-based systems, but it can also be read by Windows with some third-party software3.FAT32 is a file system that is widely compatible with most operating systems and devices, but it

has some limitations such as a maximum file size of 4 GB and a maximum partition size of 8 TB4.MBR is not a file system, but a partitioning scheme that can support various file systems such as NTFS, FAT32, or exFAT5.However, MBR has some disadvantages compared to GPT, such as a maximum disk size of 2 TB and a maximum number of primary partitions of four1.

**NEW QUESTION 148**
A technician set up a new multifunction printer. After adding the printer to the print server, the technician configured the printer on each user's machine. Several days later, users reported that they were no longer able to print, but scanning to email worked. Which of the following is most likely causing this issue?

A. The gateway is no longer being reached.
B. The network firewall was enabled.
C. The printer's network interface failed.
D. The printer had DHCP enabled.

**Answer:** D

**Explanation:**
The most likely cause of this issue is that the printer had DHCP enabled, which changed its IP address after adding it to the print server and configuring it on each user's machine. DHCP (Dynamic Host Configuration Protocol) is a network protocol that assigns IP addresses and other network configuration parameters to devices automatically, without manual intervention. DHCP can simplify network management and avoid IP conflicts, but it can also cause problems if the devices are not configured to use static or reserved IP addresses. If the printer had DHCP enabled, it might have received a different IP address from the DHCP server after rebooting or reconnecting to the network, which would make it unreachable by the print server and the users' machines that were configured with the previous IP address. Scanning to email would still work, as it does not depend on the print server or the users' machines, but on the printer's SMTP settings and internet connection. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Networking, Objective 4.l: Given a scenario, configure network settings for servers.

**NEW QUESTION 150**
An administrator notices nigh traffic on a certain subnetand wouldlike 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 153**
Which of the following BEST measures now much downtime an organization can tolerate Curing an unplanned outage?

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

**Answer:** C

**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- biahttps://www.techopedia.com/definition/8239/mean-time-to-repair-mttr

**NEW QUESTION 154**
A technician is connecting a server's secondary NIC to a separate network. The technician connects the cable to the switch but then does not see any link lights on the NIC. The technician confirms there is nothing wrong on the network or with the physical connection. Which of the following should the technician perform NEXT?

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

**Answer:** C

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

**NEW QUESTION 159**

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 163**
A server administrator needs to keep a copy of an important fileshare that can be used to restore the share as quickly as possible. Which of the following is the BEST solution?

A. Copy the fileshare to an LTO-4 tape drive
B. Configure a new incremental backup job for the fileshare
C. Create an additional partition and move a copy of the fileshare
D. Create a snapshot of the fileshare

**Answer:** D

**Explanation:**
The best solution to keep a copy of an important fileshare that can be used to restore the share as quickly as possible is to create a snapshot of the fileshare. A snapshot is a point-in-time copy of a file system or a volume that captures the state and data of the fileshare at a specific moment. A snapshot can be created instantly and with minimal overhead, as it only stores the changes made to the fileshare after the snapshot was taken. A snapshot can be used to restore the fileshare to its previous state in case of data loss or corruption.

**NEW QUESTION 167**
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 172**
A server administrator noticesthe/var/log/audit/audit.logfileon a Linux server is rotating loo frequently. The administrator would like to decrease the number of times the leg rotates without losing any of the information in the logs. Which of the following should the administrator configure?

A. increase theaudi
B. log file size in the appropriate confutation file.
C. Decrease the duration of the log rotate cycle tor theaudi
D. log file.
E. Remove the tog rotate directive from the audit .log We configuration.
F. Move the audi
G. leg files to a remote syslog server.

**Answer:** A

**Explanation:**
The audit.log file is a file that records security-related events on a Linux server, such as user login, file access, and system commands. The logrotate utility is a tool that rotates, compresses, and deletes old log files based on certain criteria, such as size, time, or frequency. To decrease the number of times the log rotates without losing any information, the administrator should increase the audit.log file size in the appropriate configuration file, such as /etc/logrotate.conf or /etc/logrotate.d/auditd. Verified References: [audit.log], [logrotate]

**NEW QUESTION 174**
An administrator discovers a Bash script file has the following permissions set in octal notation;
777
Which of the following is the MOST appropriate command to ensure only the root user can modify and execute the script?

A. chmod go-rw>:
B. chmod u=rwx
C. chmod u+wx
D. chmod g-rwx

**Answer:** A

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

## NEW QUESTION 177
A company stores extremely sensitive data on an alt-gapped system. Which of the following can Be Implemented to increase security against a potential insider threat?

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

**Answer:** A

**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 179
Which of the following commands should a systems administrator use to create a batch script to map multiple shares'?

A. nbtstat
B. netuse
C. tracert
D. netstst

**Answer:** B

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

## NEW QUESTION 182
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 185**
A junior administrator needs to configure a single RAID 5 volume out of four 200GB drives attached to the server using the maximum possible capacity. Upon completion, the server reports that all drives were used, and the approximate volume size is 400GB. Which of the following BEST describes the result of this configuration?

A. RAID 0 was configured by mistake.
B. RAID 5 was configured properly.
C. JBOD was configured by mistake.
D. RAID 10 was configured by mistake.

**Answer:** B

**Explanation:**
The output of the configuration shows that RAID 5 was configured properly using four 200GB drives. The approximate volume size of 400GB is correct, since RAID 5 uses one disk for parity and the rest for data. Therefore, the usable storage capacity is three-fourths of the total capacity, which is 600GB out of 800GB. The other RAID levels given would result in different volume sizes: RAID 0 would result in 800GB, RAID 1 would result in 200GB, and JBOD would result in an error since it does not support multiple drives in a single volume.References:https://en.wikipedia.org/wiki/Standard_RAID_levels#RAID_5

**NEW QUESTION 189**
A company recently implemented VoIP across a multicampus environment with ten locations. The company uses many network technologies, including fiber, copper, and wireless. Users calling between three of the locations have reported that voices sound strange. Which of the following should be monitored to narrow down the issue?

A. Disk IOPS
B. CPU utilization
C. RAM utilization
D. Network latency

**Answer:** D

**Explanation:**
Network latency is the measure of delay in data transmission over a network. It can affect the quality of voice over IP (VoIP) calls by causing echo, jitter, or distortion.
Network latencycan be caused by various factors such as network congestion, distance, routing, or bandwidth. To monitor network latency, you can use tools such as ping, traceroute, or network analyzers.
References: CompTIA Server+ Study Guide, Chapter 6: Networking, page 237.

**NEW QUESTION 194**
An administrate is helping to replicate a large amount of data between two Windows servers. The administrator is unsure how much data has already been transferred. Which of the following will BEST ensure all the data is copied consistently?

A. rsync
B. copy
C. scp
D. robocopy

**Answer:** D

**Explanation:**
Robocopy (Robust File Copy) is a command-line tool that can copy files and folders between Windows servers or computers. It has many features and options that can ensure all the data is copied consistently, such as retrying failed copies, resuming interrupted copies, copying permissions and attributes, mirroring source and destination directories, and logging the copy progress and results. Verified References: [Robocopy], [File copy]

**NEW QUESTION 196**
Hosting data in different regional locations but not moving it for long periods of time describes:

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

**Answer:** B

**Explanation:**
Data at rest refers to data that is stored in a persistent state on any device or media, such as hard drives, tapes, or cloud storage. Data at rest does not move for long periods of time unless it is accessed or modified by authorized users or applications. A cold site (A) is a backup location that has minimal or no equipment and resources to resume business operations in case of a disaster. On-site retention © is a policy of keeping backup data on premises for a certain period of time before transferring it to an off-site location.
Off-site storage (D) is a method of storing backup data in a remote location that is physically or logically separated from the primary site. References: https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest https://www.techopedia.com/definition/144/cold-site https://www.enterprisestorageforum.com/backup/onsite-offsite- backup.htmlhttps://www.techopedia.com/definition/24195/offsite-storage

**NEW QUESTION 201**
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 204
Which of the following security risks provides unauthorized access to an application?

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

**Answer:** A

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

## NEW QUESTION 206
A data center has 4U rack servers that needto be replaced using VMsbutwithout losingany data. Whichofthefollowingmethodswill MOST likelybe used to replace these servers?

A. Unattended scripted OS installation
B. P2V
C. VM cloning

**Answer:** C

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

## NEW QUESTION 209
A technician has received tickets responding a server is responding slowly during business hours. Which of the following should the technician implement so the team will be informed of this behavior in real time?

A. Log rotation
B. Alerts
C. Reports
D. Log stopping

**Answer:** B

**Explanation:**
Alerts are notifications that inform the technician or the team of any issues or events that occur on a server or a network. Alerts can be configured to trigger based on certain thresholds, such as CPU usage, disk space, memory utilization, or response time. Alerts can help the technician monitor and troubleshoot the server performance in real time. Verified References: [Alerts], [Server performance]

## NEW QUESTION 213
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. tracert
B. telnet
C. ipconfig
D. ping

**Answer:** C

**NEW QUESTION 216**
Which of the following would MOST likely be part of the user authentication process when implementing SAML across multiple applications?

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

**Answer:** A

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

**NEW QUESTION 217**
An administrator is only able to log on to a server with a local account. The server has been successfully joined to the domain and can ping other servers by IP address. Which of the following locally defined settings is MOST likely misconfigured?

A. DHCP
B. WINS
C. DNS
D. TCP

**Answer:** C

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

**NEW QUESTION 221**
A technicianretailed a new4TBharddrive inaWindows server. Which of the following should the technician perform FIRST to provision the newdrive?

A. Configure the drive as a base disk.
B. Configure the drive as a dynamic disk.
C. Partition the drive using MBR.
D. Partition the drive using OPT.

**Answer:** D

**Explanation:**
GPT (GUID Partition Table) is a partitioning scheme that allows creating partitions on large hard drives (more than 2 TB). It supports up to 128 partitions per drive and uses 64-bit addresses to locate them. MBR (Master Boot Record) is an older partitioning scheme that has limitations on the size and number of partitions (up to 4 primary partitions or 3 primary and 1 extended partition per drive). To provision a new 4 TB drive, the technician should partition it using GPT. Verified References: [GPT], [MBR]

**NEW QUESTION 222**
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 rebuild ing. 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 223**
Which of the following attacks is the most difficult to mitigate with technology?

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

**Answer:** D

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

**NEW QUESTION 224**
An administrator needs to disable root login over SSH. Which of the following tiles should be edited to complete this task?

A. /root.ssh/sshd/config
B. /etc.ssh/sshd_config
C. /root/.ssh/ssh_config
D. /etc.sshs_shd_config

**Answer:** B

**Explanation:**
To disable root login over SSH, the server administrator needs to edit the SSH configuration file located at /etc/ssh/sshd_config. This file contains various settings for the SSH daemon that runs on the server and accepts incoming SSH connections. The administrator needs to find the line that says PermitRootLogin and change it to no or comment it out with a # symbol. Then, the administrator needs to restart the SSH service for the changes to take effect.
References:https://www.howtogeek.com/828538/how-and- why-to-disable-root-login-over-ssh-on-linux/

**NEW QUESTION 225**
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 230**
A newly installed server is accessible to local users, but remote users are unable to connect. Which of the following is MOST likely misconfigured?

A. The IP address
B. The default gateway
C. The VLAN
D. The subnet mask

**Answer:** B

**Explanation:**
This is the most likely misconfigured setting because the default gateway is the router that connects the local network to other networks. If the default gateway is incorrect, the server will not be able to communicate with remote users or devices outside its own subnet.
References:https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig

**NEW QUESTION 234**
A company is reviewing options for its current disaster recovery plan and potential changes to it. The security team will not allow customer data to egress to non-company equipment, and the company has requested recovery in the shortest possible time. Which of the following will BEST meet these goals?

A. A warm site
B. A hot site
C. Cloud recovery
D. A cold site

**Answer:** B

**Explanation:**
A hot site is a type of disaster recovery site that has all the equipment and data ready to resume operations as soon as possible after a disaster. A hot site is usually located in a different geographic area than the primary site and has redundant power, cooling, network, and security systems. A hot site is best for the company that wants to recover in the shortest possible time and does not want customer data to egress to non- company equipment. A warm site is a type of disaster recovery site that has some equipment and data ready, but requires some configuration and restoration before resuming operations. A cold site is a type of disaster recovery site that has only basic infrastructure and space available, but requires significant setup and installation before resuming operations. Cloud recovery is a type of disaster recovery service that uses cloud- based resources and platforms to store backups and restore data and applications after a disaster.
References: https://www.techopedia.com/definition/11172/hot-site https://www.techopedia.com/definition/11173/warm-site
https://www.techopedia.com/definition/11174/cold- sitehttps://www.techopedia.com/definition/29836/cloud-recovery

**NEW QUESTION 236**
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 241**
A server administrator deployed a new product that uses a non-standard port for web access on port 8443. However, users are unable to access the new application. The server administrator checks firewall rules and determines 8443 is allowed. Which of the following is most likely the cause of the issue?

A. Intrusion detection is blocking the port.
B. The new application's DNS entry is incorrect.
C. The application should be changed to use port 443.
D. The core switch has a network issue.

**Answer:** B

**Explanation:**
A DNS entry is a record that maps a domain name to an IP address. If the DNS entry for the new application is incorrect, users will not be able to resolve the domain name to the correct IP address and port number. This will prevent them from accessing the application, even if the firewall rules allow port 8443. To fix this issue, the server administrator should verify and update the DNS entry for the new application.
References: CompTIA Server+ Study Guide, Chapter 6: Networking, page 230.

**NEW QUESTION 243**
A large number of connections to port 80 is discovered while reviewing the log files on a server. The server is not functioning as a web server. Which of the following represent the BEST immediate actions to prevent unauthorized server access? (Choose two.)

A. Audit all group privileges and permissions
B. Run a checksum tool against all the files on the server
C. Stop all unneeded services and block the ports on the firewall
D. Initialize a port scan on the server to identify open ports
E. Enable port forwarding on port 80
F. Install a NIDS on the server to prevent network intrusions

**Answer:** CF

**Explanation:**
The best immediate actions to prevent unauthorized server access are to stop all unneeded services and block the ports on the firewall. Stopping unneeded services reduces the attack surface of the server by eliminating potential entry points for attackers. For example, if the server is not functioning as a web server, there is no need to run a web service on port 80. Blocking ports on the firewall prevents unauthorized network traffic from reaching the server. For example, if port 80 is not needed for any legitimate purpose, it can be blocked on the firewall to deny any connection attempts on that port.

**NEW QUESTION 247**
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 249**
Which of the following documents would be useful when trying to restore IT infrastructure operations after a non-planned interruption?

A. Service-level agreement
B. Disaster recovery plan
C. Business impact analysis

D. Business continuity plan

**Answer:** B

**Explanation:**
A disaster recovery plan would be useful when trying to restore IT infrastructure operations after a non-planned interruption. A disaster recovery plan is a document that outlines the steps and procedures to recover from a major disruption of IT services caused by natural or man-made disasters, such as fire, flood, earthquake, cyberattack, etc. A disaster recovery plan typically includes:
? A list of critical IT assets and resources that need to be protected and restored
? A list of roles and responsibilities of IT staff and stakeholders involved in the recovery process
? A list of backup and recovery strategies and tools for data, applications, servers, networks, etc.
? A list of communication channels and methods for notifying users, customers, vendors, etc.
? A list of testing and validation methods for ensuring the functionality and integrity of restored systems
? A list of metrics and criteria for measuring the effectiveness and efficiency of the recovery process
A disaster recovery plan helps IT organizations to minimize downtime, data loss, and financial impact of a disaster, as well as to resume normal operations as quickly as possible.

**NEW QUESTION 254**
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 255**
Following a recent power outage, a server in the data center has been constantly going offline and losing its configuration. Users have been experiencing access issues while using the application on the server. The server technician notices the date and time are incorrect when the server is online. All other servers are working. Which of the following would most likely cause this issue? (Select two).

A. The server has a faulty power supply.
B. The server has a CMOS battery failure.
C. The server requires OS updates.
D. The server has a malfunctioning LED panel.
E. The servers have NTP configured.
F. CPU frequency scaling is set too high.

**Answer:** BE

**Explanation:**
A CMOS battery failure can cause the server to lose its BIOS settings, including the date and time, which can affect the server's functionality and connectivity. The servers have NTP (Network Time Protocol) configured to synchronize their clocks with a reliable time source, which can prevent time drift and ensure consistent timestamps. If one server has a wrong date and time, it can cause conflicts and errors with the other servers that have NTP configured.
References:
? CompTIA Server+ Certification Exam Objectives1, page 9
? Signs or symptoms of a CMOS battery failure2
? NTP: Network Time Protocol

**NEW QUESTION 256**
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 258**
Which of the following steps in the troubleshooting theory should be performed after a solution has been implemented? (Choose two.)

A. Perform a root cause analysis
B. Develop a plan of action
C. Document the findings
D. Escalate the issue
E. Scope the issue
F. Notify the users

**Answer:** CF

**Explanation:**
 The steps in the troubleshooting theory that should be performed after a solution has been implemented are document the findings and notify the users. The troubleshooting theory is a systematic process of identifying and resolving problems or issues with a system or device. The troubleshooting theory consists of several steps that can be summarized as follows:
? Identify the problem: Gather information, scope the issue, establish a theory of probable cause.
? Establish a plan of action: Test the theory, determine next steps, escalate if necessary.
? Implement the solution: Execute the plan, verify functionality, prevent recurrence.
? Document the findings: Record actions taken, outcomes achieved, lessons learned.
? Notify the users: Communicate resolution status, confirm satisfaction, provide follow-up.
Documenting the findings is an important step that helps create a record of what was done and why, what worked and what didn't, and what can be improved or avoided in the future. Documenting the findings can also help with reporting, auditing, compliance, or training purposes. Notifying the users is another important step that helps inform the affected parties of what was done and how it was resolved, confirm that the problem is fixed and that they are satisfied with the outcome, and provide any follow-up instructions or recommendations.

**NEW QUESTION 260**
A server administrator receives a report that Ann, a new user, is unable to save a file to her home directory on a server. The administrator checks Ann's home directory permissions and discovers the following:
dr-xr-xr-- /home/Ann
Which of the following commands should the administrator use to resolve the issue without granting unnecessary permissions?

A. chmod777/home/Ann
B. chmod666/home/Ann
C. chmod711/home/Ann
D. chmod754/home/Ann

**Answer:** D

**Explanation:**
The administrator should use the command chmod 754 /home/Ann to resolve the issue without granting unnecessary permissions. The chmod command is used to change the permissions of files and directories on a Linux server. The permissions are represented by three numbers, each ranging from 0 to 7, that correspond to the read ®, write (w), and execute (x) permissions for the owner, group, and others respectively. The numbers are calculated by adding up the values of each permission: r = 4, w = 2, x = 1. For example, 7 means rwx (4 + 2 + 1), 6 means rw- (4 + 2), 5 means r-x (4 + 1), etc. In this case, Ann's home directory has the permissions dr-xr-xr–, which means that only the owner (d) can read ® and execute (x) the directory, and the group and others can only read ® and execute (x) but not write (w) to it. This prevents Ann from saving files to her home directory. To fix this issue, the administrator should grant write permission to the owner by using chmod 754 /home/Ann, which means that the owner can read ®, write (w), and execute (x) the directory, the group can read ® and execute (x) but not write (w) to it, and others can only read ® but not write (w) or execute (x) it. This way, Ann can save files to her home directory without giving unnecessary permissions to others.
Reference:
https://linuxize.com/post/what-does-chmod-777-mean/

**NEW QUESTION 263**
A server administrator is building a pair of new storage servers. The servers will replicate; therefore, no redundancy is required, but usable capacity must be maximized. Which of the following RAID levels should the server administrator implement?

A. 1
B. 5
C. 6
D. 10

**Answer:** A

**Explanation:**
The RAID level that should be implemented to maximize usable capacity without requiring redundancy is RAID 0. RAID (Redundant Array of Independent Disks) is a technology that combines multiple physical disks into a logical unit that provides improved performance, reliability, or both. RAID 0 is a RAID level that splits data evenly across two or more disks without parity or mirroring. RAID 0 does not provide any redundancy or fault tolerance, but it increases usable capacity and performance by allowing parallel read and write operations.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 1, Lesson 1.2, Objective 1.2

**NEW QUESTION 266**
A server administrator encounters some issues with the server OS after applying monthly patches. Which of the following troubleshooting steps should the administrator perform?

A. Implement rollback procedures.
B. Upgrade the drivers.
C. Reinstall the OS.
D. Reboot the server.

**Answer:** A

**Explanation:**
 This option would restore the server OS to a previous state before applying the monthly patches. This would help troubleshoot the issues caused by the patches

and determine if they are compatible with the server OS. The other options would either not address the issues, cause data loss, or require more time and resources

**NEW QUESTION 270**
A new 40GB NIC has just been installed in a server but is not detected within the Windows server OS. Which of the following would most likely fix the issue?

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

**Answer:** A

**Explanation:**
Updating the firmware on the NIC is the most likely solution to fix the issue of a new 40GB NIC not being detected within the Windows server OS. Firmware is a softwareprogram that controls the functionality of a hardware device, such as a NIC (network interface card). A NIC is a device that enables network communication for a server by providing an interface between the server and the network cable or wireless connection. Updating the firmware on the NIC can improve its performance, compatibility, and stability with the server OS and network protocols. References: CompTIAServer+ Certification Exam Objectives, Domain 4.0: Networking, Objective 4.1: Given a scenario, configure network settings for servers.

**NEW QUESTION 273**
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 275**
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: 192.168.10.2/24Default gateway: 192.168.10.1
B. IP address: 192.168.1.2/24 Default gateway: 192.168.10.1
C. IP address: 192.168.10.3/24Default gateway: 192.168.20.1
D. IP address: 192.168.10.24/24Default 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 279**
A server technician arrives at a data center to troubleshoot a physical server that is not responding to remote management software. The technician discovers the servers in the data center are not connected to a KVM switch, and their out-of-band management cards have not been configured. Which of the following should the technician do to access the server for troubleshooting purposes?

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

**Answer:** C

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

**NEW QUESTION 280**
A technician has beer tasked to install a new CPU. Prior to the retaliation 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 283**
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 286**
......

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons 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](https://www.certshared.com/exam/SK0-005/)