Number: SK0-005
Passing Score: 800
Time Limit: 120
File Version: 14.0

Exam Code: SK0-005
Exam Name: CompTIA Server+ Certification Exam

Exam A

QUESTION 1
A server technician is deploying a server with eight hard drives. The server specifications call for a RAID configuration that can handle up to two drive failures but also allow for the least amount of drive space lost to RAID overhead. Which of the following RAID levels should the technician configure for this drive array?

A. RAID 0
B. RAID 5
C. RAID 6
D. RAID 10

Correct Answer: C
Section:
Explanation:
The technician should configure RAID 6 for this drive array to meet the server specifications. RAID 6 is a type of RAID level that provides fault tolerance and performance enhancement by using striping and dual parity. Striping means dividing data into blocks and distributing them across multiple disks to increase speed and capacity. Parity means calculating and storing extra information that can be used to reconstruct data in case of disk failure. RAID 6 uses two sets of parity information for each stripe, which are stored on different disks. This way, RAID 6 can handle up to two disk failures without losing any data or functionality. RAID 6 also allows for the least amount of drive space lost to RAID overhead compared to other RAID levels that can handle two disk failures, such as RAID 1+0 or RAID 0+1.
Reference:
https://www.booleanworld.com/raid-levels-explained/

QUESTION 2
Which of the following should an administrator use to transfer log files from a Linux server to a Windows workstation?

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

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

QUESTION 3
Users in an office lost access to a file server following a short power outage. The server administrator noticed the server was powered off. Which of the following should the administrator do to prevent this situation in the future?

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

Correct Answer: D
Section:
Explanation:
The administrator should connect the server to a UPS to prevent this situation in the future. A UPS (Uninterruptible Power Supply) is a device that provides backup power to a server or other device in case of a power outage or surge. A UPS typically consists of one or more batteries and an inverter that converts the battery power into AC power that the server can use. A UPS can also protect the server from power fluctuations that can damage its components or cause data corruption. By connecting the server to a UPS, the administrator can ensure that the server will continue to run or shut down gracefully during a power failure.

QUESTION 4
Which of the following would be BEST to help protect an organization against social engineering?

A. More complex passwords
B. Recurring training and support
C. Single sign-on
D. An updated code of conduct to enforce social media

Correct Answer: B
Section:
Explanation:
The best way to protect an organization against social engineering is to provide recurring training and support. Social engineering is a type of attack that exploits human psychology and behavior to manipulate people into divulging confidential information or performing malicious actions. Social engineering can take various forms, such as phishing emails, phone calls, impersonation, baiting, or quid pro quo. The best defense against social engineering is to educate and empower the employees to recognize and avoid common social engineering techniques and report any suspicious activities or incidents. Recurring training and support can help raise awareness and reinforce best practices among the employees.

QUESTION 5
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

Correct Answer: C
Section:
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.

QUESTION 6
A server administrator is installing an OS on a new server. Company policy states no one is to log in directly to the server. Which of the following Installation methods is BEST suited to meet the company policy?

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

Correct Answer: B
Section:
Explanation:
A core installation is a type of installation method that is best suited to meet the company policy that states no one is to log in directly to the server. A core installation is a minimal installation option that is available when deploying some editions of Windows Server. A core installation includes most but not all server roles and features, but does not include a graphical user interface (GUI). A core installation can only be managed remotely using command-line tools such as PowerShell or Windows Admin Center, or using graphical tools such as Server Manager or Remote Desktop from another computer. This reduces the attack surface, resource consumption, and maintenance requirements of the server. A GUI installation is a type of installation method that includes a graphical user interface (GUI) and allows local or remote management using graphical tools or command-line tools. A virtualized installation is a type of installation method that involves creating and running one or more virtual machines on a physical host using a hypervisor such as Hyper-V or VMware. A clone installation is a type of installation method that involves creating an exact copy of an existing server's configuration and data on another server using tools such as Sysprep or Clonezilla. Reference: https://www.howtogeek.com/67469/the-beginners-guide-to-shell-scriptingthe- basics/ https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-driveremovable- devices-and-individual-files/ https://www.howtogeek.com/199068/how-to-upgradeyour- existing-hard-drive-in-under-an-hour/

QUESTION 7
A technician has several possible solutions to a reported server issue. Which of the following BEST represents how the technician should proceed with troubleshooting?

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

Correct Answer: C
Section:
Explanation:
This is the best way to proceed with troubleshooting when the technician has several possible solutions to a reported server issue. Making one change at a time and testing allows the technician to isolate the cause and effect of each solution and determine which one works best. It also helps to avoid introducing new problems or complicating existing ones by making multiple changes at once. Determining whether there is a common element in the symptoms causing multiple problems is a good step to perform before identifying possible solutions, but not after. Performing a root cause analysis is a good step to perform after resolving the issue, but not during. Documenting the findings, actions, and outcomes throughout the process is a good practice to follow at every step of troubleshooting, but not a specific way to proceed with testing possible solutions. Reference: https://www.howtogeek.com/174288/how-to-tell-if-your-computer-is-overheating-and-what-to-doabout- it/ https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-itmatter/

QUESTION 8
Winch of the following is a type of replication in which all files are replicated, all the time?

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

Correct Answer: A
Section:
Explanation:
Constant replication is a type of replication in which all files are replicated, all the time. Replication is a process of copying data from one location to another for backup, recovery, or distribution purposes. Constant replication is also known as real-time replication or synchronous replication. It ensures that any changes made to the source data are immediately reflected on the target data without any delay or lag. Constant replication provides high availability and consistency, but it requires high bandwidth and low latency. Application consistent replication is a type of replication that ensures that the replicated data is consistent with the state of the application that uses it. It involves quiescing or pausing the application before taking a snapshot of the data and resuming the application after the snapshot is taken. Application consistent replication provides better recovery point objectives than crash consistent replication, which does not quiesce the application before taking a snapshot. Synthetic full replication is a type of replication that involves creating a new full backup by using the previous full backup and related incremental backups. It reduces the backup window and network bandwidth consumption by transferring only changed data from the source to the target. Full replication is a type of replication that involves copying all data from the source to the target regardless of whether it has changed or not. It provides a complete backup of the data, but it requires more storage space and network bandwidth than incremental or differential replication.
Reference: https://www.howtogeek.com/199068/how-to-upgrade-your-existing-hard-drive-inunder- an-hour/ https://www.howtogeek.com/202794/what-is-the-difference-between-127.0.0.1- and-0.0.0.0/

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

QUESTION 9
A technician is deploying a single server to monitor and record me security cameras at a remote site, which of the following architecture types should be used to minimize cost?

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

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

QUESTION 10
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+

Correct Answer: D
Section:
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. Reference: https://www.howtogeek.com/190014/virtualization-basics-understandingtechniques- and-fundamentals/ https://www.howtogeek.com/428483/what-is-end-to-endencryption- and-why-does-it-matter/ https://www.howtogeek.com/443611/how-to-encrypt-yourmacs- system-drive-removable-devices-and-individual-files/

QUESTION 11
Due to a recent application migration, a company's current storage solution does not meet the necessary requirements tor hosting data without impacting performance when the data is accessed in real time by multiple users. Which of the following is the BEST solution for this Issue?

A. Install local external hard drives for affected users.
B. Add extra memory to the server where data is stored.

C. Compress the data to increase available space.
D. Deploy a new Fibre Channel SAN solution.

Correct Answer: D
Section:
Explanation:
A Fibre Channel SAN solution is a type of storage area network (SAN) that uses high-speed optical fiber cables to connect servers and storage devices. A SAN allows for hosting data without impacting performance when the data is accessed in real time by multiple users, as it provides fast data transfer rates, low latency, high availability, and scalability12. A local external hard drive (A) would not be suitable for multiple users, as it would limit the accessibility and security of the data. Adding extra memory to the server (B) would not solve the problem of data access performance, as it would not increase the bandwidth or reduce the congestion of the network. Compressing the data © would not improve the performance either, as it would add extra overhead and complexity to the data processing and retrieval. Reference: 1 https://www.techradar.com/best/best-cloudstorage 2 https://solutionsreview.com/data-storage/the-best-enterprise-data-storage-solutions/

QUESTION 12
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.

Correct Answer: B
Section:
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. Reference: 3 https://kb.vmware.com/s/article/1014508 4 https://www.altaro.com/vmware/vmwareesxi- purple-screen-death/

QUESTION 13
Hosting data in different regional locations but not moving it for long periods of time describes:

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

Correct Answer: B
Section:
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. Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest https://www.techopedia.com/definition/144/cold-site
https://www.enterprisestorageforum.com/backup/onsite-offsite-backup.html
https://www.techopedia.com/definition/24195/offsite-storage

QUESTION 14

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

Correct Answer: A
Section:
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

QUESTION 15
A server administrator is completing an OS installation for a new server. The administrator patches the server with the latest vendor-suggested software, configures DHCP, and verifies all network cables are properly connected in the IDF, but there is no network connectivity. Which of the following is the MOST likely reason for the lack of connectivity?

A. The VLAN Is improperly configured.
B. The DNS configuration Is invalid.
C. The OS version is not compatible with the network switch vendor.
D. The HIDS is preventing the connection.

Correct Answer: A
Section:
Explanation:
If the server administrator patches the server with the latest vendor-suggested software, configures DHCP, and verifies all network cables are properly connected in the IDF, but there is no network connectivity, then the most likely reason for the lack of connectivity is that the VLAN is improperly configured. A VLAN (Virtual Local Area Network) is a logical grouping of network devices that share the same broadcast domain and can communicate with each other without routing. If the server is assigned to a different VLAN than the DHCP server or the default gateway, it will not be able to obtain an IP address or reach other network devices. The DNS configuration is not relevant for network connectivity, as DNS only resolves names to IP addresses. The OS version is not likely to be incompatible with the network switch vendor, as most network switches use standard protocols and interfaces. The HIDS (Host-based Intrusion Detection System) is not likely to prevent the connection, as HIDS only monitors and alerts on suspicious activities on the host. Reference:
https://www.howtogeek.com/190014/virtualization-basics-understanding-techniques-andfundamentals/ https://www.howtogeek.com/164981/how-to-use-nslookup-to-check-domain-nameinformation- in-microsoft-windows/
https://www.howtogeek.com/202794/what-is-an-intrusiondetection- system-ids-and-how-does-it-work/

QUESTION 16
A datacenter in a remote location lost power. The power has since been restored, but one ol the servers has not come back online. After some investigation, the server is found to still be powered off. Which of the following is the BEST method to power on the server remotely?

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

Correct Answer: B
Section:

Explanation:
Out-of-band console is a tool that can be used to command a remote shutdown of a physical Linux server. Out-of-band console is a method of accessing a server's console through a dedicated management port or device that does not rely on the server's operating system or network connection. Out-of-band console can be used to power cycle, reboot, update firmware, monitor performance, and perform other tasks remotely even if the server is unresponsive or offline. Crash cart is a mobile unit that contains a keyboard, monitor, mouse, and other tools that can be used to troubleshoot a server on-site, but it requires physical access to the server. IP KVM (Internet Protocol Keyboard Video Mouse) switch is a hardware device that allows remote access to multiple servers using a web browser or a client software, but it requires network connectivity and may not work if the SSH connection is lost. RDP (Remote Desktop Protocol) is a protocol that allows remote access to a Windows server's graphical user interface, but it does not work on Linux servers and requires network connectivity. Reference: https://www.techopedia.com/definition/13623/crash-cart https://www.techopedia.com/definition/13624/kvm-switch
https://www.techopedia.com/definition/3422/remote-desktop-protocol-rdp

QUESTION 17
Which of the following encryption methodologies would MOST likely be used to ensure encrypted data cannot be retrieved if a device is stolen?

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

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

QUESTION 18
A backup application is copying only changed files each line it runs. During a restore, however, only a single file is used. Which of the following backup methods does this describe?

A. Open file
B. Synthetic full
C. Full Incremental
D. Full differential

Correct Answer: B
Section:
Explanation:
A synthetic full backup is a backup method that describes copying only changed files each time it runs and using only a single file during a restore. A synthetic full backup is a backup approach that involves creating a new full backup by using the previous full backup and related incremental backups. This means that a backup solution does not have to transfer the full amount of data from the source machine and can synthetize the latest incremental backups with the last full backup to create a new full backup. This reduces the backup window and network bandwidth consumption. During a restore, only the latest synthetic full backup file is needed to recover the data. Open file backup is a backup method that allows backing up files that are in use or locked by applications. Full incremental backup is a backup method that involves performing a full backup first and then backing up only the changed files since the last backup. Full differential backup is a backup method that involves performing a full backup first and then backing up only the changed files since the last full backup. Reference: https://www.nakivo.com/blog/what-is-synthetic-backup/ https://www.howtogeek.com/192115/what-you-need-to-know-about-creating-system-imagebackups/

QUESTION 19
Which of the following describes the installation of an OS contained entirely within another OS installation?

A. Host
B. Bridge
C. Hypervisor
D. Guest

Correct Answer: D
Section:
Explanation:
The installation of an OS contained entirely within another OS installation is described as a guest. A guest is a term that refers to a virtual machine (VM) that runs on top of a host operating system (OS) using a hypervisor or a virtualization software. A guest can have a different OS than the host, and can run multiple applications or services independently from the host. A guest can also be isolated from the host and other guests for security or testing purposes.

QUESTION 20
A server technician is installing a Windows server OS on a physical server. The specifications for the installation call for a 4TB data volume. To ensure the partition is available to the OS, the technician must verify the:

A. hardware is UEFI compliant
B. volume is formatted as GPT
C. volume is formatted as MBR
D. volume is spanned across multiple physical disk drives

Correct Answer: B
Section:
Explanation:
To ensure the partition is available to the OS, the technician must verify that the volume is formatted as GPT. GPT (GUID Partition Table) is a partitioning scheme that defines how data is organized on a hard disk drive (HDD) or a solid state drive (SSD). GPT uses globally unique identifiers (GUIDs) to identify partitions and supports up to 128 primary partitions per disk. GPT also supports disks larger than 2 TB and has a backup copy of the partition table at the end of the disk for data recovery. GPT is required for installing Windows on UEFI-based PCs, which offer faster boot time and better security than legacy BIOS-based PCs.

QUESTION 21
An administrator is configuring a server that will host a high-performance financial application. Which of the following disk types will serve this purpose?

A. SAS SSD
B. SATA SSD
C. SAS drive with 10000rpm
D. SATA drive with 15000rpm

Correct Answer: A
Section:
Explanation:
The best disk type for a high-performance financial application is a SAS SSD. A SAS SSD (Serial Attached SCSI Solid State Drive) is a type of storage device that uses flash memory chips to store data and has a SAS interface to connect to a server or a storage array. A SAS SSD offers high speed, low latency, high reliability, and high durability compared to other types of disks, such as SATA SSDs, SAS HDDs, or SATA HDDs. A SAS SSD can handle high I/O workloads and deliver consistent performance for applications that require fast data access and processing.
Reference:
https://www.hp.com/us-en/shop/tech-takes/sas-vs-sata

QUESTION 22
Which of the following DR testing scenarios is described as verbally walking through each step of the DR plan in the context of a meeting?

A. Live failover

B. Simulated failover
C. Asynchronous
D. Tabletop

Correct Answer: D
Section:
Explanation:
The DR testing scenario that is described as verbally walking through each step of the DR plan in the context of a meeting is tabletop. A tabletop test is a type of disaster recovery (DR) test that involves discussing and reviewing the DR plan with key stakeholders and participants in a simulated scenario. A tabletop test does not involve any actual execution of the DR plan or any disruption of the normal operations. A tabletop test can help identify gaps, issues, or inconsistencies in the DR plan and improve communication and coordination among the DR team members.

QUESTION 23
An administrator needs to perform bare-metal maintenance on a server in a remote datacenter. Which of the following should the administrator use to access the server's console?

A. IP KVM
B. VNC
C. A crash cart
D. RDP
E. SSH

Correct Answer: A
Section:
Explanation:
The administrator should use an IP KVM to access the server's console remotely for bare-metal maintenance. An IP KVM stands for Internet Protocol Keyboard Video Mouse, which is a device that allows remote control of a server's keyboard, video, and mouse over a network connection, such as LAN or Internet. An IP KVM enables an administrator to perform tasks such as BIOS configuration, boot sequence selection, operating system installation, etc., without being physically present at the server location.
The other options are not suitable for bare-metal maintenance because they require either physical access to the server (a crash cart) or an operating system running on the server (VNC, RDP, SSH). A crash cart is a mobile unit that contains a monitor, keyboard, mouse, and cables that can be plugged into a server for direct access to its console. VNC stands for Virtual Network Computing, which is a software that allows remote desktop sharing and control over a network connection using a graphical user interface (GUI). RDP stands for Remote Desktop Protocol, which is a protocol that allows remote desktop access and control over a network connection using a GUI or command-line interface (CLI). SSH stands for Secure Shell, which is a protocol that allows secure remote login and command execution over a network connection using a CLI.

QUESTION 24
A technician needs to provide a VM with high availability. Which of the following actions should the technician take to complete this task as efficiently as possible?

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

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

QUESTION 25
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. chmod 777 /home/Ann
B. chmod 666 /home/Ann
C. chmod 711 /home/Ann
D. chmod 754 /home/Ann

Correct Answer: D
Section:
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/

QUESTION 26
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

Correct Answer: B
Section:
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.

QUESTION 27
A systems administrator is setting up a new server that will be used as a DHCP server. The administrator installs the OS but is then unable to log on using Active Directory credentials. The administrator logs on using the local administrator account and verifies the server has the correct IP address, subnet mask, and default gateway. The administrator then gets on another server and can ping the new server. Which of the following is causing the issue?

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

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

QUESTION 28
A systems administrator is preparing to install two servers in a single rack. The administrator is concerned that having both servers in one rack will increase the chance of power issues due to the increased load. Which of the following should the administrator implement FIRST to address the issue?

A. Separate circuits
B. An uninterruptible power supply
C. Increased PDU capacity
D. Redundant power supplies

Correct Answer: A
Section:
Explanation:
The administrator should implement separate circuits first to address the issue of power issues due to the increased load. Separate circuits are electrical wiring systems that provide independent power sources for different devices or groups of devices. By using separate circuits, the administrator can avoid overloading a single circuit with too many servers and reduce the risk of power outages, surges, or fires. Separate circuits also provide redundancy and fault tolerance, as a failure in one circuit will not affect the other circuit.

QUESTION 29
Which of the following is a method that is used to prevent motor vehicles from getting too close to building entrances and exits?

A. Bollards
B. Reflective glass
C. Security guards
D. Security cameras

Correct Answer: A
Section:
Explanation:
Bollards are an example of a method that is used to prevent motor vehicles from getting too close to building entrances and exits. Bollards are short, sturdy posts that are installed on sidewalks, parking lots, or roads to create physical barriers and control traffic flow. Bollards can be used to protect pedestrians, buildings, or other structures from vehicle collisions or attacks. Bollards can be made of various materials, such as metal, concrete, or plastic, and can be fixed, removable, or retractable.
Reference: https://en.wikipedia.org/wiki/Bollard

QUESTION 30
A technician is installing a variety of servers in a rack. Which of the following is the BEST course of action for the technician to take while loading the rack?

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

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

QUESTION 31
A technician is configuring a server that requires secure remote access. Which of the following ports should the technician use?

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

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

QUESTION 32
A server administrator is using remote access to update a server. The administrator notices numerous error messages when using YUM to update the applications on a server. Which of the following should the administrator check FIRST?

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

Correct Answer: C
Section:
Explanation:
The administrator should check disk space in the /var directory first when using YUM to update applications on a server. YUM stands for Yellowdog Updater Modified, which is a software package manager for Linux systems that use RPM (Red Hat Package Manager) packages. YUM downloads and installs packages from online repositories and resolves dependencies automatically. YUM stores its cache files in the /var/cache/yum directory by default. These cache files include metadata and package data for each repository that YUM uses. If there is not enough disk space in the /var directory, YUM may fail to update applications and generate error messages.

QUESTION 33
Which of the following is an example of load balancing?

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

Correct Answer: A
Section:

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

QUESTION 34
Which of the following is the MOST appropriate scripting language to use for a logon script for a Linux box?

A. VBS
B. Shell
C. Java
D. PowerShell
E. Batch

Correct Answer: B
Section:
Explanation:
Shell is the most appropriate scripting language to use for a logon script for a Linux box. Shell is a generic term for a command-line interpreter that allows users to interact with the operating system by typing commands and executing scripts. Shell scripts are files that contain a series of commands and instructions that can be executed by a shell. Shell scripts are commonly used for automating tasks, such as logon scripts that run when a user logs on to a system. There are different types of shells available for Linux systems, such as Bash, Ksh, Zsh, etc., but they all share a similar syntax and functionality.

QUESTION 35
Which of the following tools will analyze network logs in real time to report on suspicious log events?

A. Syslog
B. DLP
C. SIEM
D. HIPS

Correct Answer: C
Section:
Explanation:
SIEM is the tool that will analyze network logs in real time to report on suspicious log events. SIEM stands for Security Information and Event Management, which is a software solution that collects, analyzes, and correlates log data from various sources, such as servers, firewalls, routers, antivirus software, etc. SIEM can detect anomalies, patterns, trends, and threats in the log data and generate alerts or reports for security monitoring and incident response. SIEM can also provide historical analysis and compliance reporting for audit purposes.
Reference:
https://www.manageengine.com/products/eventlog/syslog-server.html

QUESTION 36
Which of the following will correctly map a script to a home directory for a user based on username?

A. \\server\users$\username
B. \\server\%username%
C. \\server\FirstInitialLastName
D. \\server\$username$

Correct Answer: B
Section:
Explanation:
The administrator should use \server%username% to correctly map a script to a home directory for a user based on username. %username% is an environment variable that represents the current user's name on a Windows system. By using this variable in the path of the script, the administrator can dynamically map the script to the user's home directory on the server. For example, if the user's name is John, the script will be mapped to \server\John.
Reference:
https://social.technet.microsoft.com/Forums/windows/en-US/07cfcb73-796d-48aa-96a9- 08280a1ef25a/ mapping-home-directory-with-username-variable?forum=w7itprogeneral

QUESTION 37
A server that recently received hardware upgrades has begun to experience random BSOD conditions. Which of the following are likely causes of the issue? (Choose two.)

A. Faulty memory
B. Data partition error
C. Incorrectly seated memory
D. Incompatible disk speed
E. Uninitialized disk
F. Overallocated memory

Correct Answer: A, C
Section:
Explanation:
Faulty memory and incorrectly seated memory are likely causes of the random BSOD conditions on the server. Memory is one of the most common hardware components that can cause BSOD (Blue Screen of Death) errors on Windows systems. BSOD errors occur when the system encounters a fatal error that prevents it from continuing to operate normally. Memory errors can be caused by faulty or incompatible memory modules that have physical defects or manufacturing flaws. Memory errors can also be caused by incorrectly seated memory modules that are not properly inserted or locked into the memory slots on the motherboard. This can result in loose or poor connections between the memory modules and the motherboard.

QUESTION 38
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

Correct Answer: B
Section:
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.

QUESTION 39
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

Correct Answer: B
Section:
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 CDROM, 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.

QUESTION 40
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

Correct Answer: C
Section:
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 readwrite 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 41
Which of the following must a server administrator do to ensure data on the SAN is not compromised if it is leaked?

A. Encrypt the data that is leaving the SAN
B. Encrypt the data at rest
C. Encrypt the host servers
D. Encrypt all the network traffic

Correct Answer: B
Section:

QUESTION 42
Which of the following BEST describes the concept of right to downgrade?

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

D. It allows a previous version of an OS to be installed and covered by the same license as the newer version

Correct Answer: D
Section:
Explanation:
The concept of right to downgrade allows a previous version of an OS to be installed and covered by the same license as the newer version. For example, if a customer has a license for Windows 10 Pro, they can choose to install Windows 8.1 Pro or Windows 7 Professional instead and still be compliant with the license terms. Downgrade rights are granted by Microsoft for certain products and programs, such as Windows and Windows Server software acquired through Commercial Licensing, OEM, or retail channels. Downgrade rights are intended to provide customers with flexibility and compatibility when using Microsoft software.

QUESTION 43
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

Correct Answer: D
Section:
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

QUESTION 44
Which of the following open ports should be closed to secure the server properly? (Choose two.)

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

Correct Answer: A, C
Section:
Explanation:
The administrator should close ports 21 and 23 to secure the server properly. Port 21 is used for FTP (File Transfer Protocol), which is an unsecure protocol that allows file transfer between a client and a server over a network connection. FTP does not encrypt the data or the credentials that are transmitted, making them vulnerable to interception or modification by attackers. Port 23 is used for Telnet, which is an unsecure protocol that allows remote login and command execution over a network connection using a CLI. Telnet does not encrypt the data or the credentials that are transmitted, making them vulnerable to interception or modification by attackers.
Reference:
https://www.csoonline.com/article/3191531/securing-risky-network-ports.html

QUESTION 45
Which of the following must a server administrator do to ensure data on the SAN is not compromised if it is leaked?

A. Encrypt the data that is leaving the SAN
B. Encrypt the data at rest
C. Encrypt the host servers
D. Encrypt all the network traffic

Correct Answer: B
Section:
Explanation:
The administrator must encrypt the data at rest to ensure data on the SAN is not compromised if it is leaked. Data at rest refers to data that is stored on a device or a medium, such as a hard drive, a flash drive, or a SAN (Storage Area Network). Data at rest can be leaked if the device or the medium is lost, stolen, or accessed by unauthorized parties. Encrypting data at rest means applying an algorithm that transforms the data into an unreadable format that can only be decrypted with a key. Encryption protects data at rest from being exposed or misused by attackers who may obtain the device or the medium.

QUESTION 46
A server technician has been asked to upload a few files from the internal web server to the internal FTP server. The technician logs in to the web server using PuTTY, but the connection to the FTP server fails. However, the FTP connection from the technician's workstation is su?cessful. To troubleshoot the issue, the technician executes the following command on both the web server and the workstation:
ping ftp.acme.local
The IP address in the command output is different on each machine. Which of the following is the MOST likely reason for the connection failure?

A. A misconfigured firewall
B. A misconfigured hosts.deny file
C. A misconfigured hosts file
D. A misconfigured hosts.allow file

Correct Answer: D
Section:
Explanation:
A misconfigured hosts file can cause name resolution issues on a server. A hosts file is a text file that maps hostnames to IP addresses on a local system. It can be used to override DNS settings or provide custom name resolution for testing purposes. However, if the hosts file contains incorrect or outdated entries, it can prevent the system from resolving hostnames properly and cause connectivity problems. To fix this issue, the administrator should check and edit the hosts file accordingly.

QUESTION 47
A company deploys antivirus, anti-malware, and firewalls that can be assumed to be functioning properly. Which of the following is the MOST likely system vulnerability?

A. Insider threat
B. Worms
C. Ransomware
D. Open ports
E. Two-person integrity

Correct Answer: A
Section:
Explanation:
Insider threat is the most likely system vulnerability in a company that deploys antivirus, antimalware, and firewalls that can be assumed to be functioning properly. An insider threat is a malicious or negligent act by an authorized user of a system or network that compromises the security or integrity of the system or network. An insider threat can include data theft, sabotage, espionage, fraud, or other types of attacks. Antivirus, anti-malware, and firewalls are security tools that can protect a system or network from external threats, such as viruses, worms, ransomware, or open ports. However, these tools cannot prevent an insider threat from exploiting their access privileges or credentials to harm the system or network.

QUESTION 48
A security analyst suspects a remote server is running vulnerable network applications. The analyst does not have administrative credentials for the server. Which of the following would MOST likely help the analyst determine if the applications are running?

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

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

QUESTION 49
A server is performing slowly, and users are reporting issues connecting to the application on that server. Upon investigation, the server administrator notices several unauthorized services running on that server that are successfully communicating to an external site. Which of the following are MOST likely causing the issue?
(Choose two.)

A. Adware is installed on the users' devices
B. The firewall rule for the server is misconfigured
C. The server is infected with a virus
D. Intrusion detection is enabled on the network
E. Unnecessary services are disabled on the server
F. SELinux is enabled on the server

Correct Answer: C, F
Section:
Explanation:
The server is infected with a virus and SELinux is enabled on the server are most likely causing the issue of unauthorized services running on the server. A virus is a type of malicious software that infects a system and performs unwanted or harmful actions, such as creating, modifying, deleting, or executing files. A virus can also create backdoors or open ports on a system to allow remote access or communication with external sites. SELinux (Security-Enhanced Linux) is a security module for Linux systems that enforces mandatory access control policies on processes and files. SELinux can prevent unauthorized services from running on a server by restricting their access to resources based on their security context. However, SELinux can also cause problems if it is not configured properly or if it conflicts with other security tools.

QUESTION 50
A server technician is configuring the IP address on a newly installed server. The documented configuration specifies using an IP address of 10.20.10.15 and a default gateway of 10.20.10.254. Which of the following subnet masks would be appropriate for this setup?

A. 255.255.255.0
B. 255.255.255.128
C. 255.255.255.240
D. 255.255.255.254

Correct Answer: A
Section:

Explanation:
The administrator should use a subnet mask of 255.255.255.0 for this setup. A 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 network portion identifies the specific network that the IP address belongs to, while the host portion identifies the specific device within that network. The subnet mask is usually written in dotted decimal notation, where each octet represents eight bits of the binary number. A 1 in the binary number means that the corresponding bit in the IP address is part of the network portion, while a 0 means that it is part of the host portion. For example, a subnet mask of 255.255.255.0 means that the first 24 bits (three octets) of the IP address are used for the network portion and the last 8 bits (one octet) are used for the host portion. This subnet mask allows up to 254 hosts per network (2^8 - 2). In this case, the IP address of 10.20.10.15 and the default gateway of 10.20.10.254 belong to the same network of 10.20.10.0/24 (where /24 indicates the number of bits used for the network portion), which can be defined by using a subnet mask of 255.255.255.0.

QUESTION 51
A storage administrator is investigating an issue with a failed hard drive. A technician replaced the drive in the storage array; however, there is still an issue with the logical volume. Which of the following best describes the NEXT step that should be completed to restore the volume?

A. Initialize the volume
B. Format the volume
C. Replace the volume
D. Rebuild the volume

Correct Answer: D
Section:
Explanation:
The administrator should rebuild the volume to restore it after replacing the failed hard drive. A volume is a logical unit of storage that can span across multiple physical disks. A volume can be configured with different levels of RAID (Redundant Array of Independent Disks) to provide fault tolerance and performance enhancement. When a hard drive in a RAID volume fails, the data on that drive can be reconstructed from the remaining drives using parity or mirroring techniques. However, this process requires a new hard drive to replace the failed one and a rebuild operation to copy the data from the existing drives to the new one. Rebuilding a volume can take a long time depending on the size and speed of the drives and the RAID level.

QUESTION 52
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

Correct Answer: C, F
Section:
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.

QUESTION 53
A company is running an application on a file server. A security scan reports the application has a known vulnerability. Which of the following would be the company's BEST course of action?

A. Upgrade the application package
B. Tighten the rules on the firewall

C. Install antivirus software
D. Patch the server OS

Correct Answer: A
Section:
Explanation:
The best course of action for the company is to upgrade the application package to fix the known vulnerability. A vulnerability is a weakness or flaw in an application that can be exploited by an attacker to compromise the security or functionality of the system. Upgrading the application package means installing a newer version of the application that has patched or resolved the vulnerability. This way, the company can prevent potential attacks that may exploit the vulnerability and cause damage or loss.

QUESTION 54
A technician runs top on a dual-core server and notes the following conditions:
top –- 14:32:27, 364 days, 14 users load average 60.5 12.4 13.6 Which of the following actions should the administrator take?

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

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

QUESTION 55
A technician needs to set up a server backup method for some systems. The company's management team wants to have quick restores but minimize the amount of backup media required. Which of the following are the BEST backup methods to use to support the management's priorities? (Choose two.)

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

Correct Answer: A, E
Section:
Explanation:
The best backup methods to use to support the management's priorities are differential and incremental. A backup is a process of copying data from a source to a destination for the purpose of restoring it in case of data loss or corruption. There are different types of backup methods that vary in terms of speed, efficiency, and storage requirements. Differential and incremental backups are two types of partial backups that only copy the data that has changed since the last full backup. A full backup is a type of backup that copies all the data from the source to the destination. A full backup provides the most complete and reliable restore option, but it also takes the longest time and requires the most storage space. A differential backup copies only the data that has changed since the last full backup. A differential backup provides a faster restore option than an incremental backup, but it also takes more time and requires more storage space than an incremental backup. An incremental backup copies only the data that has changed since the last backup, whether it was a full or an incremental backup. An incremental backup provides the fastest and most efficient backup option, but it also requires multiple backups to restore the data completely.

QUESTION 56
Ann, an administrator, is configuring a two-node cluster that will be deployed. To check the cluster's functionality, she shuts down the active node. Cluster behavior is as expected, and the passive node is now active. Ann powers on the server again and wants to return to the original configuration. Which of the following cluster features will allow Ann to complete this task?

A. Heartbeat
B. Failback
C. Redundancy
D. Load balancing

Correct Answer: B
Section:
Explanation:
The cluster feature that will allow Ann to complete her task is failback. A cluster is a group of servers that work together to provide high availability, scalability, and load balancing for applications or services. A cluster can have different nodes or members that have different roles or states. An active node is a node that is currently running an application or service and serving requests from clients. A passive node is a node that is on standby and ready to take over if the active node fails. A failover is a process of switching from a failed or unavailable node to another node in a cluster. A failback is a process of switching back from a failover node to the original node after it becomes available again. Failback can be automatic or manual depending on the cluster configuration.

QUESTION 57
Which of the following policies would be BEST to deter a brute-force login attack?

A. Password complexity
B. Password reuse
C. Account age threshold
D. Account lockout threshold

Correct Answer: D
Section:
Explanation:
The best policy to deter a brute-force login attack is account lockout threshold. A brute-force login attack is a type of attack that tries to guess a user's password by trying different combinations of characters until it finds the correct one. This attack can be performed manually or with automated tools that use dictionaries, wordlists, or algorithms. An account lockout threshold is a policy that specifies how many failed login attempts are allowed before an account is locked out temporarily or permanently. This policy prevents an attacker from trying unlimited password guesses and reduces the chances of finding the correct password.

QUESTION 58
A technician needs to install a Type 1 hypervisor on a server. The server has SD card slots, a SAS controller, and a SATA controller, and it is attached to a NAS. On which of the following drive types should the technician install the hypervisor?

A. SD card
B. NAS drive
C. SATA drive
D. SAS drive

Correct Answer: D
Section:
Explanation:
The technician should install the Type 1 hypervisor on a SAS drive. A Type 1 hypervisor is a layer of software that runs directly on top of the physical hardware and creates virtual machines that share the hardware resources. A Type 1 hypervisor requires fast and reliable storage for optimal performance and stability. A SAS drive is a type of hard disk drive that uses Serial Attached SCSI (SAS) as its interface protocol. SAS drives offer high speed, low latency, and high reliability compared to other types of drives, such as SD cards, NAS drives, or SATA drives. SD cards are flash memory cards that offer low cost and portability but have low speed, low capacity, and low durability. NAS drives are network-attached storage devices that offer high capacity and easy access but have high latency and low reliability due to network dependency. SATA drives are hard disk drives that use Serial ATA

(SATA) as their interface protocol. SATA drives offer moderate speed, moderate cost, and moderate reliability but have lower performance and durability than SAS drives.

QUESTION 59
A technician is trying to determine the reason why a Linux server is not communicating on a network. The returned network configuration is as follows:
eth0: flags=4163<UP, BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 127.0.0.1 network 255.255.0.0 broadcast 127.0.0.1
Which of the following BEST describes what is happening?

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

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

QUESTION 60
When configuring networking on a VM, which of the following methods would allow multiple VMs to share the same host IP address?

A. Bridged
B. NAT
C. Host only
D. vSwitch

Correct Answer: B
Section:
Explanation:
The method that would allow multiple VMs to share the same host IP address is NAT. NAT (Network Address Translation) is a technique that allows multiple devices to use a single public IP address by mapping their private IP addresses to different port numbers. NAT can be used for VM networking to enable multiple VMs on the same host to access the internet or other networks using the host's IP address. NAT can also provide security benefits by hiding the VMs' private IP addresses from external networks.
Reference: https://www.virtualbox.org/manual/ch06.html

QUESTION 61
A technician recently upgraded several pieces of firmware on a server. Ever since the technician rebooted the server, it no longer communicates with the network. Which of the following should the technician do FIRST to return the server to service as soon as possible?

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

Correct Answer: D
Section:

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

QUESTION 62
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

Correct Answer: C
Section:
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.

QUESTION 63
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

Correct Answer: D
Section:
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.

QUESTION 64
Which of the following can be BEST described as the amount of time a company can afford to be down during recovery from an outage?

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

Correct Answer: C
Section:
Explanation:

The term that best describes the amount of time a company can afford to be down during recovery from an outage is RTO. RTO (Recovery Time Objective) is a metric that defines the maximum acceptable downtime for an application, system, or process after a disaster or disruption. RTO helps determine the level of urgency and resources required for restoring normal business operations. RTO is usually measured in minutes, hours, or days, depending on the criticality and impact of the service.
Reference:
https://whatis.techtarget.com/definition/recovery-time-objective-RTO

QUESTION 65
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

Correct Answer: C
Section:
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.

QUESTION 66
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

Correct Answer: A, B
Section:
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

QUESTION 67
A server administrator is experiencing difficulty configuring MySQL on a Linux server. The administrator issues the getenforce command and receives the following output:
># Enforcing
Which of the following commands should the administrator issue to configure MySQL successfully?

A. setenforce 0

B. setenforce permissive
C. setenforce 1
D. setenforce disabled

Correct Answer: A
Section:
Explanation:
The command that the administrator should issue to configure MySQL successfully is setenforce 0. This command sets the SELinux (Security-Enhanced Linux) mode to permissive, which means that SELinux will not enforce its security policies and will only log any violations. SELinux is a feature that provides mandatory access control (MAC) for Linux systems, which can enhance the security and prevent unauthorized access or modification of files and processes. However, SELinux can also interfere with some applications or services that require specific permissions or ports that are not allowed by SELinux by default. In this case, MySQL may not be able to run properly due to SELinux restrictions. To resolve this issue, the administrator can either disable SELinux temporarily by using setenforce 0, or permanently by editing the /etc/selinux/config file and setting SELINUX=disabled. Alternatively, the administrator can configure SELinux to allow MySQL to run by using commands such as semanage or setsebool.
Reference:
https://blogs.oracle.com/mysql/selinux-and-mysql-v2

QUESTION 68
Which of the following backup types only records changes to the data blocks on a virtual machine?

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

Correct Answer: B
Section:
Explanation:
The backup type that only records changes to the data blocks on a virtual machine is snapshot. A snapshot is a point-in-time copy of a virtual machine (VM) that captures the state and data of the VM at a specific moment. A snapshot can be created instantly and with minimal overhead, as it only stores the changes made to the VM after the snapshot was taken. A snapshot can be used to restore the VM to its previous state in case of data loss or corruption.

QUESTION 69
Which of the following server types would benefit MOST from the use of a load balancer?

A. DNS server
B. File server
C. DHCP server
D. Web server

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

QUESTION 70

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

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

Correct Answer: D
Section:
Explanation:
The type of data replication that is required for a hot-site disaster recovery model is constant. A hot site is a type of disaster recovery site that has fully operational IT infrastructure and equipment that can take over the primary site's functions immediately in case of a disaster or disruption. A hot site requires constant data replication between the primary site and the hot site to ensure that the data is up-to-date and consistent. Constant data replication means that any changes made to the data at the primary site are immediately copied to the hot site without any delay or lag.

QUESTION 71
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

Correct Answer: D, E
Section:
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.

QUESTION 72
A server administrator was asked to build a storage array with the highest possible capacity. Which of the following RAID levels should the administrator choose?

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

Correct Answer: A
Section:
Explanation:
The RAID level that provides the highest possible capacity for a storage array is RAID 0. RAID 0 is a type of RAID level that provides performance enhancement by using striping. Striping means dividing data into blocks and distributing them across multiple disks to increase speed and capacity. RAID 0 does not provide any fault tolerance or redundancy, as it does not use any parity or mirroring techniques. RAID 0 uses all of the available disk

space for data storage, without losing any space for overhead. Therefore, RAID 0 provides the highest possible capacity for a storage array, but also has the highest risk of data loss.
Reference: https://www.thinkmate.com/inside/articles/what-is-raid

QUESTION 73
A server administrator was asked to build a storage array with the highest possible capacity. Which of the following RAID levels should the administrator choose?

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

Correct Answer: A
Section:
Explanation:
The RAID level that provides the highest possible capacity for a storage array is RAID 0. RAID 0 is a type of RAID level that provides performance enhancement by using striping. Striping means dividing data into blocks and distributing them across multiple disks to increase speed and capacity. RAID 0 does not provide any fault tolerance or redundancy, as it does not use any parity or mirroring techniques. RAID 0 uses all of the available disk space for data storage, without losing any space for overhead. Therefore, RAID 0 provides the highest possible capacity for a storage array, but also has the highest risk of data loss.
Reference: https://www.thinkmate.com/inside/articles/what-is-raid

QUESTION 74
A technician needs to deploy an operating system that would optimize server resources. Which of the following server installation methods would BEST meet this requirement?

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

Correct Answer: C
Section:
Explanation:
The server installation method that would optimize server resources is core. Core is a minimal installation option that is available for some operating systems, such as Windows Server and Linux. Core installs only the essential components and features of the operating system, without any graphical user interface (GUI) or other unnecessary services or applications. Core reduces the disk footprint, memory usage, CPU consumption, and attack surface of the server, making it more efficient and secure. Core can be managed remotely using command-line tools, PowerShell, or GUI tools.
Reference:
https://docs.microsoft.com/en-us/windows-server/administration/performance-tuning/hardware/

QUESTION 75
A company's IDS has identified outbound traffic from one of the web servers coming over port 389 to an outside address. This server only hosts websites. The company's SOC administrator has asked a technician to harden this server. Which of the following would be the BEST way to complete this request?

A. Disable port 389 on the server
B. Move traffic from port 389 to port 443
C. Move traffic from port 389 to port 637
D. Enable port 389 for web traffic

Correct Answer: A
Section:
Explanation:

The best way to complete the request to harden the server is to disable port 389 on the server. Port 389 is the default port used by LDAP (Lightweight Directory Access Protocol), which is a protocol that allows access and modification of directory services over a network. LDAP can be used for authentication, authorization, or information retrieval purposes. However, LDAP does not encrypt its data by default, which can expose sensitive information or credentials to attackers who can intercept or modify the network traffic. Therefore, port 389 should be disabled on a web server that only hosts websites and does not need LDAP functionality. Alternatively, port 636 can be used instead of port 389 to enable LDAPS (LDAP over SSL/TLS), which encrypts the data using SSL/TLS certificates.

QUESTION 76
Which of the following licenses would MOST likely include vendor assistance?

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

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

QUESTION 77
Alter rack mounting a server, a technician must install four network cables and two power cables for the server. Which of the following is the MOST appropriate way to complete this task?

A. Wire the four network cables and the two power cables through the cable management arm using appropriate-length cables.
B. Run the tour network cables up the left side of the rack to the top of the rack switch. Run the two power cables down the right side of the rack toward the UPS.
C. Use the longest cables possible to allow for adjustment of the server rail within the rack.
D. Install an Ethernet patch panel and a PDU to accommodate the network and power cables.

Correct Answer: B
Section:
Explanation:
This is the most appropriate way to complete the task because it follows the best practices of cable management. Cable management is a process of organizing and securing cables in a rack or a server room to improve airflow, accessibility, safety, and aesthetics. Running the network cables up the left side and the power cables down the right side of the rack helps to avoid cable clutter, interference, and confusion. It also makes it easier to trace and troubleshoot cables if needed. Using appropriatelength cables also helps to reduce cable slack and excess. Wiring the cables through the cable management arm may cause stress and damage to the cables when moving the server in or out of the rack. Using the longest cables possible may create cable loops and tangles that can block airflow and increase fire hazards. Installing an Ethernet patch panel and a PDU (Power Distribution Unit) may be useful for accommodating more network and power cables, but not necessary for a single server.
Reference: https://www.howtogeek.com/303282/how-to-manage-your-pcs-fans-for-optimal-airflowand- cooling/ https://www.howtogeek.com/303290/how-to-properly-manage-your-cables/

QUESTION 78
An administrator is configuring a host-based firewall tor a server. The server needs to allow SSH, FTP, and LDAP traffic. Which of the following ports must be configured so this traffic will be allowed? (Select THREE).

A. 21
B. 22
C. 53
D. 67

E. 69
F. 110
G. 123
H. 389

Correct Answer: A, B, H
Section:
Explanation:
These are the port numbers that must be configured on a host-based firewall for a server that needs to allow SSH, FTP, and LDAP traffic. A port number is a numerical identifier that specifies a communication endpoint for a network protocol or an application. A host-based firewall is a software tool that monitors and controls incoming and outgoing network traffic on a single host based on predefined rules. SSH (Secure Shell) is a protocol that allows secure remote access and file transfer over an encrypted connection. The default port number for SSH is 22. FTP (File Transfer Protocol) is a protocol that allows transferring files between hosts over a network connection. The default port number for FTP is 21. LDAP (Lightweight Directory Access Protocol) is a protocol that allows accessing and managing directory services over a network connection. The default port number for LDAP is 389. Reference: https://www.howtogeek.com/190014/virtualization-basics-understandingtechniques- and-fundamentals/ https://www.howtogeek.com/220152/what-is-the-differencebetween- 127.0.0.1-and-0.0.0.0/ https://www.howtogeek.com/428483/what-is-end-to-endencryption- and-why-does-it-matter/

QUESTION 79
Which of the following, if properly configured, would prevent a user from installing an OS on a server? (Select TWO).

A. Administrator password
B. Group Policy Object
C. Root password
D. SELInux
E. Bootloader password
F. BIOS/UEFI password

Correct Answer: E, F
Section:
Explanation:
These are two methods that can prevent a user from installing an OS on a server if properly configured. A bootloader password is a password that protects the bootloader from unauthorized access or modification. The bootloader is a program that loads the operating system into memory when the system boots up. If a user does not know the bootloader password, they cannot change the boot order or boot from another device such as a CD-ROM or USB drive that contains an OS installation media. A BIOS/UEFI password is a password that protects the BIOS (Basic Input Output System) or UEFI (Unified Extensible Firmware Interface) from unauthorized access or modification. The BIOS or UEFI is a firmware that initializes and configures the hardware components of the system before loading

QUESTION 80
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.

Correct Answer: A
Section:
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.
Reference: https://www.howtogeek.com/190014/virtualization-basics-understanding-techniquesand- fundamentals/ https://www.howtogeek.com/173353/how-to-low-level-format-or-write-zerosto- a-hard-drive/
https://www.howtogeek.com/303282/how-to-manage-your-pcs-fans-for-optimalairflow- and-cooling/

QUESTION 81
Which of me following BEST describes a disaster recovery site with a target storage array that receives replication traffic and servers that are only powered on In the event of a disaster?

A. Cloud
B. Cold
C. Hot
D. Warm

Correct Answer: D
Section:
Explanation:
A warm site is a type of disaster recovery site that has a target storage array that receives replication traffic and servers that are only powered on in the event of a disaster. A warm site is a compromise between a hot site and a cold site. A warm site has some equipment and data ready, but requires some configuration and restoration before resuming operations. A warm site is usually located in a different geographic area than the primary site and has redundant power, cooling, network, and security systems. A warm site is suitable for organizations that can tolerate some downtime and data loss in case of a disaster. A cloud site is a type of disaster recovery site that uses cloud-based resources and platforms to store backups and restore data and applications after a disaster. 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. 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. Reference:
https://www.techopedia.com/definition/11172/hot-site https://www.techopedia.com/definition/11173/warm-site
https://www.techopedia.com/definition/11174/cold-site
https://www.techopedia.com/definition/29836/cloud-recovery

QUESTION 82
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

Correct Answer: B
Section:
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 that stripes data across three or more drives with parity information. It provides fault tolerance and improves performance, but reduces storage capacity by one drive's worth of space. RAID 5 can tolerate one drive failure without data loss, but not two or more. 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. Reference:
https://www.howtogeek.com/199068/how-toupgrade- your-existing-hard-drive-in-under-an-hour/

QUESTION 83
Which of me following should be placed at the top of a Bash script to ensure it can be executed?

A. bash
B. !execute

C. #!
D. @eacho off

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

QUESTION 84
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

Correct Answer: A
Section:
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. Reference:
https://www.howtogeek.com/169080/air-gap-how-to-isolate-a-computer-to-protect-it-fromhackers/ https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-itmatter/
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-removabledevices- and-individual-files/

QUESTION 85
A Linux administrator created a script that will run at startup. After successfully writing the script, the administrator received me following output when trying to execute the script:
Bash ./startup,sh:Permission denied
Which of the following commands would BEST resolve the error message?

A. Chmod +w startup.sh
B. Chmod 444 startup.sh
C. Chmod+x startup.sh
D. Chmod 466 startUp,sh

Correct Answer: C
Section:

Explanation:
This is the command that would best resolve the error message “Bash ./startup.sh: Permission denied” when trying to execute a script on Linux. Chmod is a command that changes the permissions of files or directories on Linux. +x is an option that adds the execute permission to the file or directory for the owner, group, and others. startup.sh is the name of the script file that needs to be executed. By running chmod +x startup.sh, the technician grants execute permission to the script file and allows it to be run by any user. Chmod +w startup.sh would add write permission to the file, but not execute permission. Chmod 444 startup.sh would set read-only permission for all users, but not execute permission. Chmod 466 startup.sh would set read and write permission for the owner and write-only permission for group and others, but not execute permission. Reference: https://www.howtogeek.com/437958/how-to-use-the-chmod-command-on-linux

QUESTION 86
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.

Correct Answer: C
Section:
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. Reference: https://www.howtogeek.com/303282/how-to-manage-your-pcs-fans-for-optimal-airflow-andcooling/ https://www.howtogeek.com/174288/how-to-tell-if-your-computer-is-overheating-andwhat- to-do-about-it/

QUESTION 87
Which of me following is the BEST action to perform before applying patches to one of the hosts in a high availability cluster?

A. Disable the heartbeat network.
B. Fallback cluster services.
C. Set the cluster to active-active.
D. Failover all VMs.

Correct Answer: D
Section:
Explanation:
This is the best action to perform before applying patches to one of the hosts in a high availability cluster. A high availability cluster is a group of hosts that act like a single system and provide continuous uptime. A high availability cluster is often used for load balancing, backup, and failover purposes. Failover is a process of transferring workloads from one host to another in case of a failure or maintenance. By failing over all VMs (Virtual Machines) from the host that needs to be patched to another host in the cluster, the technician can ensure that there is no downtime or data loss during the patching process. Disabling the heartbeat network is not a good action to perform, as this would disrupt the communication and synchronization between the hosts in the cluster. Fallback cluster services is not a valid term, but it may refer to restoring cluster services after a failover, which is not relevant before applying patches. Setting the cluster to active-active is not a good action to perform, as this would increase the load on both hosts and reduce redundancy. Reference: https://www.howtogeek.com/190014/virtualization-basics-understanding-techniques-andfundamentals/ https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-doesit- matter/

QUESTION 88
A technician is working on a Linux server. The customer has reported that files in the home directory are missing. The /etc/ f stab file has the following entry:
nfsserver:/home /home nfs defaults 0 0
However, a df -h /home command returns the following information:
/dev/sda2 10G 1G 9G 10% /home

Which of the following should the technician attempt FIRST to resolve the issue?

A. mkdir /home
B. umount nfsserver:/home
C. rmdir nfsserver:/home/dev/sda2
D. mount /home

Correct Answer: B
Section:
Explanation:
The /etc/fstab file contains the information about the file systems that are mounted automatically at boot time or on demand. The entry nfsserver:/home /home nfs defaults 0 0 indicates that the /home directory on the local server is mounted from the /home directory on a remote server called nfsserver using the NFS protocol. However, the df -h /home command shows that the /home directory is actually mounted from a local partition /dev/sda2, which may not contain the user's files. This means that the NFS mount failed or was overridden by another mount. To resolve the issue, the technician should attempt to unmount the local partition using umount nfsserver:/home, which will detach the /home directory from /dev/sda2. Then, the technician should try to mount the NFS share again using mount /home, which will attach the /home directory to nfsserver:/home according to the /etc/fstab entry12. Creating a new directory (A) or removing an existing one © would not help, as they would not affect the mount point. Mounting /home (D) without unmounting it first would not work, as it would result in an error that the mount point is busy3.
Reference: 1 https://askubuntu.com/questions/374870/home-directory-not-beingcreated 2 https://www.techrepublic.com/article/how-to-properly-automount-a-drive-in-ubuntulinux/ 3 https://serverfault.com/questions/587855/cannot-find-home-directory-on-linux-server

QUESTION 89
A server room with many racks of servers is managed remotely with occasional on-site support. Which of the following would be the MOST cost-effective option to administer and troubleshoot network problems locally on the servers?

A. Management port
B. Crash cart
C. IP KVM
D. KVM

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

QUESTION 90
A systems administrator is investigating a server with a RAID array that will not boot into the OS. The administrator notices all the hard drives are reporting to be offline. The administrator checks the RAID controller and verifies the configuration is correct. The administrator then replaces one of the drives with a known-good drive, but it appears to be unavailable as well. Next, the administrator takes a drive out of the server and places it in a spare server, and the drive is available and functional. Which of the following is MOST likely causing the issue?

A. The kernel is corrupt.
B. Resources are misallocated.
C. The backplane has failed.
D. The drives need to be reseated.

Correct Answer: C
Section:
Explanation:
The backplane is a circuit board that connects multiple hard drives to a RAID controller and provides power and data transfer between them. If the backplane has failed, it may cause all the hard drives to be offline and prevent the server from booting into the OS. The fact that replacing one of the drives with a known-good drive did not work, and that taking a drive out of the server and placing it in a spare server made it functional, suggests that the problem is not with the drives themselves but with the backplane. A corrupt kernel (A) would not affect the status of the hard drives, as it is a software component of the OS. Resource misallocation (B) would not cause all the hard drives to be offline, as it is a configuration issue that affects how resources are assigned to processes or applications. Reseating the drives (D) would not help, as it would not fix a faulty backplane.
Reference: https://www.dell.com/support/kbdoc/en-us/000130114/how-to-troubleshoot-a-faultybackplane

QUESTION 91
Which of the following can be used to map a network drive to a user profile?

A. System service
B. Network service
C. Login script
D. Kickstart script

Correct Answer: C
Section:
Explanation:
A login script is a file that contains commands or instructions that are executed when a user logs into a system or network. A login script can be used to map a network drive to a user profile, which means that the user will have access to a shared folder or resource on another computer or server. A login script can be written in various languages, such as batch, PowerShell, or VBScript, and can be assigned to a user or a group using tools such as Group Policy or Active Directory . A system service (A) is a program that runs in the background and performs tasks that are essential for the operation of the system, such as security, networking, or hardware management. A system service does not map a network drive to a user profile. A network service (B) is a program that provides functionality or resources to other programs or devices over a network, such as file sharing, printing, or web hosting. A network service does not map a network drive to a user profile. A kickstart script (D) is a file that contains configuration settings and commands for automated installation of Linux operating systems. A kickstart script does not map a network drive to a user profile. Reference:
https://www.howtogeek.com/118452/how-to-map-network-drives-from-the-command-prompt-inwindows/ https://docs.microsoft.com/en-us/windows-server/administration/windowscommands/ logon

QUESTION 92
Which of the following are measures that should be taken when a data breach occurs? (Select TWO).

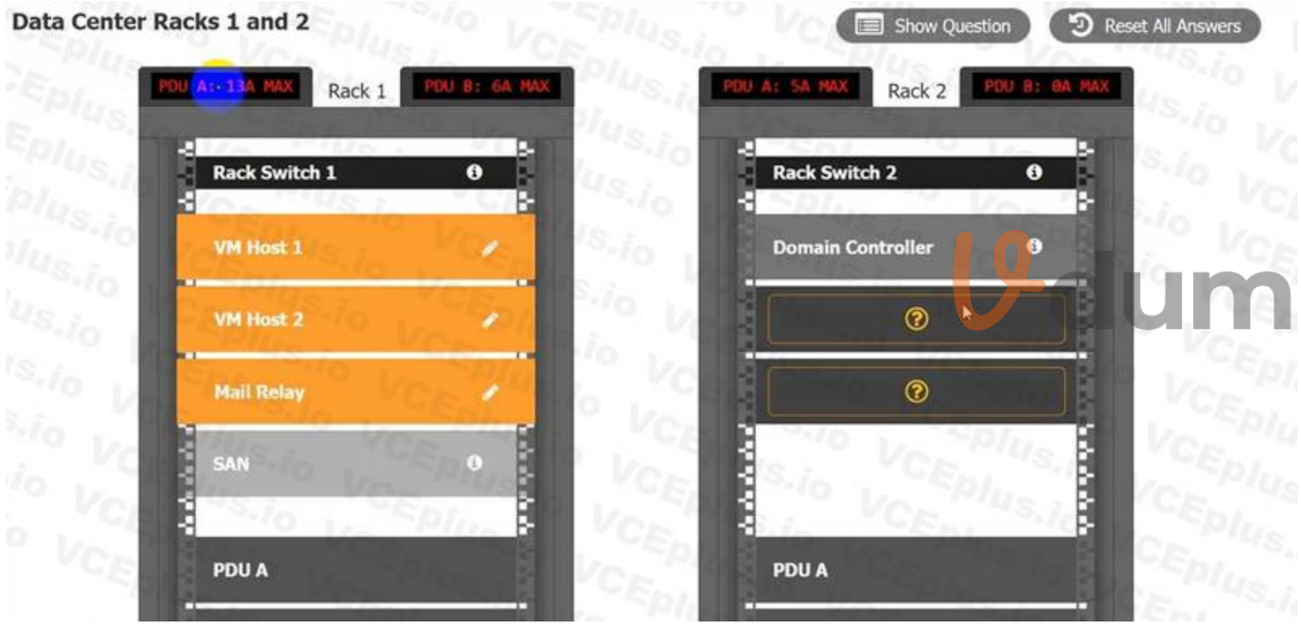
A. Restore the data from backup.
B. Disclose the incident.
C. Disable unnecessary ports.
D. Run an antivirus scan.
E. Identify the exploited vulnerability.
F. Move the data to a different location.

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

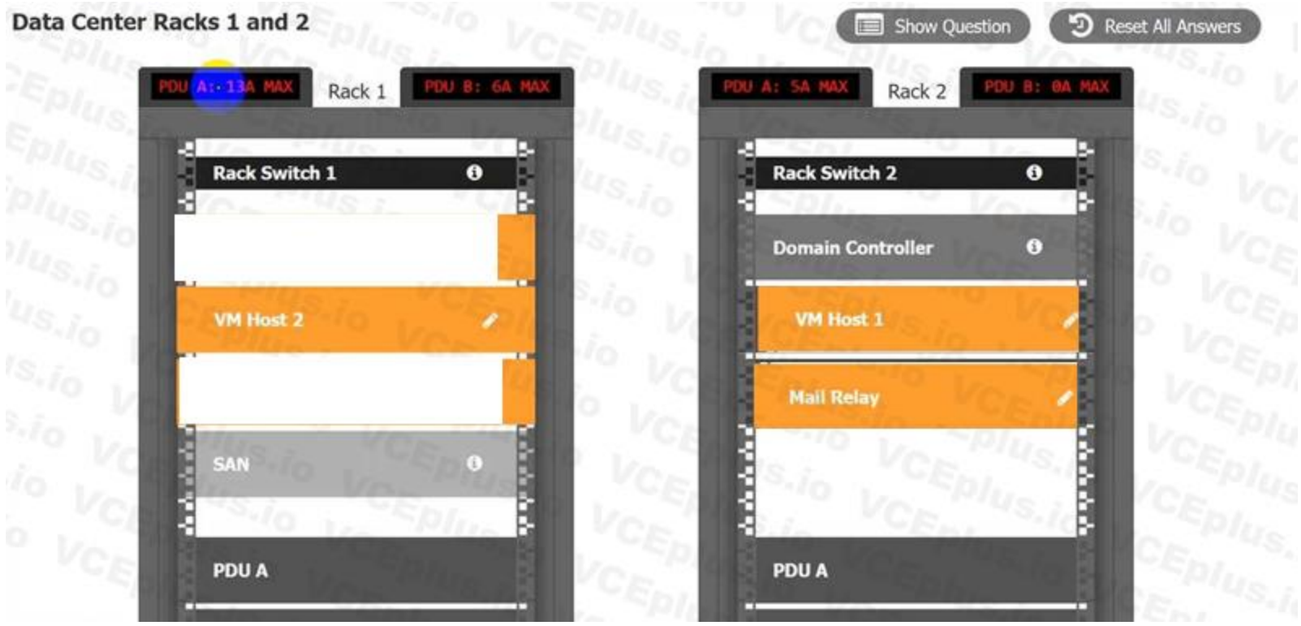
detecting and removing malicious software from a system or network. However, this does not address how the data breach occurred or what vulnerability was exploited. Moving the data to a different location is a measure that involves transferring the data to another storage device or location that may be more secure or less accessible. However, this does not address how the data breach occurred or what vulnerability was exploited.
Reference: https://www.howtogeek.com/428483/what-is-end-to-endencryption- and-why-does-it-matter/ https://www.howtogeek.com/202794/what-is-the-differencebetween- 127.0.0.1-and-0.0.0.0/
https://www.howtogeek.com/443611/how-to-encrypt-your-macssystem- drive-removable-devices-and-individual-files/

QUESTION 93
DRAG DROP
A recent power Outage caused email services to go down. A sever administrator also received alerts from the datacenter's UPS.
After some investigation, the server administrator learned that each POU was rated at a maximum Of 12A.
INSTRUCTIONS
Ensure power redundancy is implemented throughout each rack and UPS alarms are resolved. Ensure the maximum potential PDU consumption does not exceed 80% or 9.6A).
a. PDU selections must be changed using the pencil icon.
b. VM Hosts 1 and 2 and Mail Relay can be moved between racks.
c. Certain devices contain additional details

Select and Place:



Correct Answer:



Section:
Explanation:

QUESTION 94
An organization implements split encryption keys for sensitive files. Which of the following types of risks does this mitigate?

A. Hardware failure
B. Marware
C. Data corruption
D. Insider threat

Correct Answer: D
Section:
Explanation:
An insider threat is a type of risk that can be mitigated by implementing split encryption keys for sensitive files. An insider threat is a malicious actor who has authorized access to an organization's system or data and uses it for unauthorized or harmful purposes. An insider threat can cause data breaches, sabotage, fraud, theft, espionage, or other damages to the organization. Split encryption keys are a method of encrypting data using multiple keys that are stored separately and require collaboration to decrypt. Split encryption keys can prevent an insider threat from accessing or compromising sensitive data without being detected by another authorized party who holds another key. Hardware failure is a type of risk that involves physical damage or malfunction of hardware components such as hard drives, memory modules, power supplies, or fans. Hardware failure can cause data loss, system downtime, performance issues, or other problems for the organization. Hardware failure cannot be mitigated by split encryption keys, but by backup, redundancy, monitoring, and maintenance measures.

QUESTION 95
A data center employee shows a driver's license to enter the facility Once the employee enters, the door immediately doses and locks, triggering a scale that then weighs the employee before granting access to another locked door. This is an example of.

A. mantrap.
B. a bollard
C. geofencing
D. RFID.

Correct Answer: A
Section:
Explanation:
A mantrap is a security device that consists of a small space with two sets of interlocking doors, such that the first set of doors must close before the second one opens. A mantrap can be used to control access to a data center by verifying the identity and weight of the person entering. A bollard is a sturdy post that prevents vehicles from entering a restricted area. Geofencing is a technology that uses GPS or RFID to create a virtual boundary around a location and trigger an action when a device crosses it. RFID is a technology that uses radio waves to identify and track objects or people.
Reference:
https://www.techopedia.com/definition/16293/mantrap
https://www.techopedia.com/definition/1437/bollard
https://www.techopedia.com/definition/23961/geofencing
https://www.techopedia.com/definition/506/radio-frequency-identification-rfid

QUESTION 96
A technician learns users are unable to tog in to a Linux server with known-working LDAP credentials. The technician logs in to the server with a local account and confirms the system is functional can communicate over the network, and is configured correctly However, the server log has entries regarding Kerberos errors. Which of the following is the MOST likely source of the issue?

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

Correct Answer: C
Section:
Explanation:
Kerberos is a network authentication protocol that uses tickets to allow clients and servers to prove their identity to each other. Kerberos relies on accurate time synchronization between the parties involved, as the tickets have expiration dates and timestamps. If the system clock of a Linux server is off by more than five minutes from the LDAP server or the domain controller, the Kerberos authentication will fail and generate errors. A local firewall is unlikely to block authentication requests if the server can communicate over the network and is configured correctly. The users' passwords are not relevant if they are known-working LDAP credentials. The server has access to the LDAP host if it can communicate over the network and is configured correctly. Reference:
https://access.redhat.com/documentation/enus/red_hat_enterprise_linux/6/html/identity_management_guide/kerberos_errors https://www.ibm.com/docs/en/aix/7.2?topic=authentication-kerberos-time-synchronization

QUESTION 97
Which of the following BEST describes a warm site?
The site has all infrastructure and live data.

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

Correct Answer: D
Section:
Explanation:
A warm site is a type of disaster recovery site that has some pre-installed hardware, software, and network connections, but not as much as a hot site. A warm site also has some backup data, but not as current as a hot site. A warm site requires some time and effort to become fully operational in the event of a disaster. A hot site is a disaster recovery site that has all infrastructure and live data, and can take over the primary site's operations immediately. A cold site is a disaster recovery site that has no infrastructure or data, and requires significant time and resources to set up. Reference:
https://www.enterprisestorageforum.com/management/disaster-recovery-site/ https://www.techopedia.com/definition/3780/warm-site

QUESTION 98
An administrator is configuring a new server for use as a database server. It will have two mirrored drives to hold the operating system, and there will be three drive bays remaining for storage Which of the following RAID levels will yield the BEST combination of available space and redundancy?

A. RAID
B. RAID 1
C. RAIDS
D. RAID 10

Correct Answer: D
Section:
Explanation:
RAID 10 is the RAID level that will yield the best combination of available space and redundancy when configuring a new server for use as a database server with two mirrored drives for the operating system and three drive bays remaining for storage. RAID 10, also known as RAID 1+0, is a RAID configuration that combines disk mirroring and disk striping to protect data. It requires a minimum of four disks and stripes data across mirrored pairs. As long as one disk in each mirrored pair is functional, data can be retrieved. RAID 10 provides high performance, fault tolerance, and fast recovery, but it reduces storage capacity by half. RAID 0 is a RAID configuration that splits data across two or more drives without parity or redundancy. It improves performance but offers no fault tolerance. If one drive fails in RAID 0, all data is lost and the system cannot boot. RAID 1 is a RAID configuration that duplicates data across two or more drives. It provides fault tolerance and improves read performance, but reduces storage capacity by half. If one drive fails in RAID 1, the other drive can continue to operate without data loss or system downtime. RAID 5 is a RAID configuration that stripes data across three or more drives with parity information. It provides fault tolerance and improves performance, but reduces storage capacity by one drive's worth of space. RAID 5 can tolerate one drive failure without data loss, but not two or more. Reference:
https://www.howtogeek.com/199068/how-to-upgrade-your-existing-hard-drive-in-under-an-hour/ https://www.howtogeek.com/202794/what-is-the-difference-between-127.0.0.1-and-0.0.0.0/

QUESTION 99
The management team at a healthcare organization is concerned about being able to access the dairy vital records if there is an IT disaster that causes both servers and the network lo be offline. Which of the following backup types can the organization use to mitigate this risk?

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

Correct Answer: D
Section:
Explanation:
A print backup is a type of backup that can be used to mitigate the risk of being unable to access the daily vital records if there is an IT disaster that causes both servers and the network to be offline. A print backup is a backup that involves printing out the data on paper and storing it in a secure location. A print backup can provide offline access to the data without relying on any hardware or software components that may be affected by the disaster. However, a print backup has some drawbacks such as high cost, low efficiency, low security, and environmental impact. A tape backup is a type of backup that involves storing the data on magnetic tape cartridges that can be accessed using a tape drive or a tape library. A tape backup can provide offline access to the data with high capacity, low cost, and long durability, but it requires special equipment and software that may not be available during a disaster. A cloud backup is a type of backup that involves storing the data on remote servers or platforms that can be accessed over the internet using a web browser or an application. A cloud backup can provide online access to the data with high scalability, flexibility, and security, but it requires network connectivity and bandwidth that may not be available during a disaster. A disk backup is a type of backup that involves storing the data on hard disk drives or solid state drives that can be accessed using a computer or a device. A disk backup can provide online or offline access to the data with high performance, reliability, and portability, but it requires compatible hardware and software that may not be available during a disaster. Reference:
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-devicesand- individual-files/
https://www.howtogeek.com/199068/how-to-upgrade-your-existing-harddrive- in-under-an-hour/ https://www.howtogeek.com/202794/what-is-the-difference-between-127

QUESTION 100
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

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

QUESTION 101
A server technician downloaded new firmware from the manufacturer's website. The technician then attempted to install the firmware on the server, but the installation failed, stating the file is potentially corrupt. Which of the following should the technician have checked prior to installing the firmware?

A. DLF configuration
B. MBR failure
C. ECC support
D. MD5 checksum

Correct Answer: D
Section:
Explanation:
A MD5 checksum is a value that is calculated from a file using a cryptographic hash function. A MD5 checksum is used to verify the integrity of a file by comparing it with the original value provided by the manufacturer or the source. If the MD5 checksums match, it means that the file is authentic and has not been corrupted or tampered with. If the MD5 checksums do not match, it means that the file is potentially corrupt or malicious and should not be installed12. A DLF configuration (A) is a setting that determines how a dynamic link library (DLL) is loaded into memory and executed by an application. A DLF configuration does not check the integrity of a file. A MBR failure (B) is a problem that occurs when the master boot record (MBR) of a disk is damaged or corrupted, preventing the system from booting. A MBR failure does not check the integrity of a file. ECC support © is a feature that enables error-correcting code (ECC) memory to detect and correct data errors in RAM. ECC support does not check the integrity of a file. Reference: 1 https://www.comparitech.com/netadmin/ file-integrity-monitoring-tools/ 2 https://csrc.nist.gov/CSRC/media/Presentations/Firmware- Integrity-Verification-Monitoring-and-Re/images-media/day2_demonstration_330-420.pdf

QUESTION 102
A technician needs to install a Type 1 hypervisor on a server. The server has SD card slots, a SAS controller, and a SATA controller, and it is attached to a NAS. On which of the following drive types should the technician install the hypervisor?

A. SD card
B. NAS drive
C. SATA drive
D. SAS drive

Correct Answer: A
Section:
Explanation:
A SD card is a type of flash memory card that can be used to store data and run applications. A SD card can be used to install a Type 1 hypervisor on a server, as it provides fast boot time, low power consumption, and high reliability. A Type 1 hypervisor runs directly on the underlying computer’s physical hardware, interacting directly with its CPU, memory, and physical storage. For this reason, Type 1 hypervisors are also referred to as bare-metal hypervisors. A Type 1 hypervisor takes the place of a host operating system and VM resources are scheduled directly to the hardware by the hypervisor123. A NAS drive (B) is a type of network-attached storage (NAS) device that provides shared access to files and data over a network. A NAS drive cannot be used to install a Type 1 hypervisor on a server, as it requires a network connection and a host operating system to function. A SATA drive © is a type of hard disk drive (HDD) or solid state drive (SSD) that uses the Serial ATA (SATA) interface to connect to a computer. A SATA drive can be used to install a Type 1 hypervisor on a server, but it may have some disadvantages compared to a SD card, such as slower boot time, higher power consumption, and lower reliability. A SAS drive (D) is a type of hard disk drive (HDD) or solid state drive (SSD) that uses the Serial Attached SCSI

(SAS) interface to connect to a computer. A SAS drive can also be used to install a Type 1 hypervisor on a server, but it may have similar disadvantages as a SATA drive, and it may also be more expensive and less compatible than a SD card. Reference: 1 https://phoenixnap.com/kb/what-is-hypervisor-type-1- 2 2 https://www.ibm.com/topics/hypervisors 3 https://www.redhat.com/en/topics/virtualization/w hat-is-a-hypervisor

QUESTION 103
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

Correct Answer: B
Section:
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.
Reference: 1 https://docs.microsoft.com/en-us/windows-server/administration/windowscommands/ net-use 2 https://www.watchingthenet.com/create-a-batch-file-to-map-drivesfolders. html

QUESTION 104
In which of the following media rotation schemes are daily, weekly, and monthly backup media utilized in a first-in, first-out method?

A. Waterfall
B. Synthetic full
C. Tower of Hanoi
D. Grandfather-father-son

Correct Answer: D
Section:
Explanation:
Grandfather-father-son (GFS) is a common backup rotation scheme that uses daily, weekly, and monthly backup media in a first-in, first-out (FIFO) method. The daily backups are rotated on a 3- months basis using a FIFO system as above. The weekly backups are similarly rotated on a bi-yearly basis, and the monthly backups are rotated on an annual basis. The oldest backup media in each cycle are overwritten by the newest ones. This scheme provides multiple versions of backup data at different intervals, allowing for flexible restoration options. Waterfall is another name for GFS. Synthetic full is a backup method that combines an initial full backup with subsequent incremental backups to create a new full backup without transferring all data again. Tower of Hanoi is another backup rotation scheme that uses an algorithm based on moving disks between three pegs.
Reference:
https://en.wikipedia.org/wiki/Backup_rotation_scheme

QUESTION 105
The HIDS logs on a server indicate a significant number of unauthorized access attempts via USB devices at startup. Which of the following steps should a server administrator take to BEST secure the server without limiting functionality?

A. Set a BIOS/UEFI password on the server.
B. Change the boot order on the server and restrict console access. C Configure the host OS to deny login attempts via USB.
C. Disable all the USB ports on the server.

Correct Answer: B
Section:
Explanation:
Changing the boot order on the server and restricting console access would prevent unauthorized access attempts via USB devices at startup, as the server would not boot from any external media and only authorized users could access the console. Setting a BIOS/UEFI password on the server would also help, but it could be bypassed by resetting the CMOS battery or using a backdoor password. Configuring the host OS to deny login attempts via USB would not prevent booting from a malicious USB device that could compromise the system before the OS loads. Disabling all the USB ports on the server would limit functionality, as some peripherals or devices may need to use them.
Reference:
https://www.pcmag.com/how-to/dont-plug-it-in-how-to-prevent-a-usb-attack https://www.techopedia.com/definition/10362/boot-order
https://www.techopedia.com/definition/10361/console-access
https://www.techopedia.com/definition/102/bios-password
https://www.techopedia.com/definition/10363/cmos-battery

QUESTION 106
A server administrator wants to ensure a storage array can survive the failure of two drives without the loss of dat

A. Which of the following RAID levels should the administrator choose?
B. 0
C. 1
D. 5
E. 6

Correct Answer: D
Section:
Explanation:
RAID 6 is a level of RAID that can survive the failure of two drives without the loss of data. RAID 6 uses block-level striping with two parity blocks distributed across all member disks. RAID 6 can tolerate two simultaneous drive failures and still provide data access and redundancy. RAID 0 is a level of RAID that uses striping without parity or mirroring, and offers no fault tolerance. RAID 0 cannot survive any drive failure without data loss. RAID 1 is a level of RAID that uses mirroring without parity or striping, and offers fault tolerance by duplicating data on two or more disks. RAID 1 can survive one drive failure without data loss, but not two. RAID 5 is a level of RAID that uses blocklevel striping with one parity block distributed across all member disks. RAID 5 can tolerate one drive failure without data loss, but not two. Reference:
https://en.wikipedia.org/wiki/Standard_RAID_levels

QUESTION 107
A senior administrator instructs a technician to run the following script on a Linux server:
for i in {1..65536); do echo Si; telnet localhost $i; done
The script mostly returns the following message: Connection refused. However, there are several entries in the console display that look like this:
80
Connected to localhost
443
Connected to localhost
Which of the following actions should the technician perform NEXT?

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

D. Look for an unauthorized port scanning service on this server.

Correct Answer: A
Section:
Explanation:
The script that the technician is running is trying to connect to every port on the localhost (the same machine) using telnet, a network protocol that allows remote access to a command-line interface. The script mostly fails because most ports are closed or not listening for connections. However, the script succeeds on ports 80 and 443, which are the default ports for HTTP and HTTPS protocols, respectively. These protocols are used for web services and web browsers. Therefore, the technician should look for an unauthorized HTTP service on this server, as it may indicate a security breach or a misconfiguration. Looking for a virus infection on this server is also possible, but not the most likely source of the issue. Looking for an unauthorized Telnet service on this server is not relevant, as the script is using telnet as a client, not a server. Looking for an unauthorized port scanning service on this server is not relevant, as the script is scanning ports on the localhost, not on other machines.
Reference:
https://phoenixnap.com/kb/telnet-windows
https://www.techopedia.com/definition/23337/http-port-80
https://www.techopedia.com/definition/23336/https-port-443

QUESTION 108
An administrator is troubleshooting connectivity to a remote server. The goal is to remotely connect to the server to make configuration changes. To further troubleshoot, a port scan revealed the ports on the server as follows:
Port 22: Closed
Port 23: Open
Port 990: Closed
Which of the following next steps should the administrator take?
Reboot the workstation and then the server.

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

Correct Answer: B
Section:
Explanation:
Port 22 is used for SSH (Secure Shell), which is a secure and encrypted protocol for remote access to a server. Port 23 is used for Telnet, which is an insecure and unencrypted protocol for remote access. Port 990 is used for FTPS (File Transfer Protocol Secure), which is a secure and encrypted protocol for file transfer. The administrator should open port 22 and close port 23 to enable SSH and disable Telnet, as SSH is more secure and reliable than Telnet. The administrator does not need to open port 990, as FTPS is not required for making configuration changes123.
References = 1: Remote Desktop - Allow access to your PC from outside your network(https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-allow-outside-access) 2: Test remote network port connection in Windows 10 - Winaero(https://winaero.com/test-remote-network-port-connection-in-windows-10/) 3: Windows Command to check if a remote server port is opened?(https://superuser.com/questions/1035018/windows-command-to-check-if-a-remote-server-port-is-opened)

QUESTION 109
A server administrator has received tickets from users who report the system runs very slowly and various unrelated messages pop up when they try to access an internet-facing web application using default ports. The administrator performs a scan to check for open ports and reviews the following report:
Starting Nmap 7.70 https://nmap.org) at 2019-09-19 14:30 UTC
Nmap scan report for www.abc.com (172.45.6.85)
Host is up (0.0021s latency)
Other addresses for www.abc.com (not scanned) : 4503 : F7b0 : 4293: 703: : 3209
RDNS record for 172.45.6.85: 1ga45s12-in-f1.2d100.net
Port State Service
21/tcp filtered ftp

22/tcp filtered ssh
23/tcp filtered telnet
69/tcp open @username.com
80/tcp open http
110/tcp filtered pop
143/tcp filtered imap
443/tcp open https
1010/tcp open www.popup.com
3389/tcp filtered ms-abc-server
Which of the following actions should the server administrator perform on the server?

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

Correct Answer: A
Section:
Explanation:
Port 69 is used for TFTP (Trivial File Transfer Protocol), which is an insecure and unencrypted protocol for file transfer. Port 1010 is used for a malicious website that generates pop-up ads. Both of these ports are likely to be exploited by hackers or malware to compromise the server or the web application. The server administrator should close these ports and rerun the scan to verify that they are no longer open12.
References = 1: Why Are Some Network Ports Risky, And How Do You Secure Them? - How-To Geek(https://www.howtogeek.com/devops/why-are-some-ports-risky-and-how-do-you-secure-them/) 2: Switchport Port Security Explained With Examples - ComputerNetworkingNotes(https://www.computernetworkingnotes.com/ccna-study-guide/switchport-port-security-explained-with-examples.html)

QUESTION 110
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

Correct Answer: B
Section:
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)

QUESTION 111
An administrator is troubleshooting a server that is rebooting and crashing. The administrator notices that the server is making sounds that are louder than usual. Upon closer inspection, the administrator discovers that the noises are coming from the front of the chassis. Which of the following is the most likely reason for this behavior?

A. One of the fans has failed.
B. The power supply has failed.
C. The RAM is malfunctioning.

D. The CPU is overheating.

Correct Answer: A
Section:
Explanation:
A server has multiple fans inside the chassis to cool down the components and prevent overheating. If one of the fans fails, it can cause the server to reboot and crash due to thermal issues. A failed fan can also make loud noises due to friction or vibration.The administrator should check the fans and clean them from dust and debris, or replace them if they are damaged12.
References=1: It's Too Loud!3 Solutions to Remedy Server Noise - Computerware Blog | DC Metro | Computerware Blog(https://www.cwit.com/blog/it-s-too-loud-3-solutions-to-remedy-server-noise)2: What factors affect the noise level of a server? - Server Fault(https://serverfault.com/questions/430550/what-factors-affect-the-noise-level-of-a-server)

QUESTION 112
A server administrator is tasked with upgrading the network on a server to 40Gbps. After installing the card, which of the following connectors should the administrator use?

A. QSFP+
B. 10 GigE
C. SFP
D. SFP+

Correct Answer: A
Section:
Explanation:
QSFP+ (Quad Small Form-Factor Pluggable Plus):This transceiver type is designed specifically to handle 40Gbps network speeds. QSFP+ connectors are hot-swappable and support various cable types, including fiber optic and copper (DAC).
10GigE:While a valid network technology, 10GigE only supports up to 10Gbps, not the required 40Gbps.
SFP (Small Form-factor Pluggable):A common transceiver type, but the standard SFP only supports a maximum of 1Gbps.
SFP+ (Enhanced Small Form-factor Pluggable):Supports up to 10Gbps, not sufficient for 40Gbps in this scenario.
References:
CompTIA Server+ Objectives(Exam codes SK0-004 or SK0-005): Search for sections on networking standards and transceiver types.

QUESTION 113
Which of the following describes the concept of allocating more resources than what is available on a hypervisor?

A. Direct access
B. Overprovisioning
C. Link aggregation
D. Component redundancy
E. Scalability

Correct Answer: B
Section:
Explanation:
Overprovisioning:Involves allocating more virtual resources (e.g., CPU, RAM, storage) to virtual machines than the total physical resources available on a hypervisor. The idea is for resources to be dynamically shared, assuming not all VMs will demand their maximum allocation simultaneously.
Direct Access:This usually refers to technologies like RDMA (Remote Direct Memory Access) that allow for very low-latency, direct access to the memory of another computer over a network.
Link Aggregation:The practice of combining multiple physical network links to create a single logical link with increased bandwidth.
Component Redundancy:Refers to having multiple hardware components (e.g., power supplies, hard drives) to provide fault tolerance.
Scalability:The ability of a system to adapt and handle increased workloads by adding resources.
References:

CompTIA Server+ Objectives(Exam codes SK0-004 or SK0-005): Review the sections on virtualization concepts.
Virtualization Technology Documentation:Refer to documentation for popular hypervisors like VMware vSphere, Microsoft Hyper-V, or open-source solutions.