Number: SK0-005
Passing Score: 800
Time Limit: 120
File Version: 13.0

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

Exam A

QUESTION 1
After the installation of an additional network card into a server, the server will not boot into the OS. A technician tests the network card in a different server with a different OS and verifies the card functions correctly. Which of the following should the technician do NEXT to troubleshoot this issue?

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

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

QUESTION 2
An administrator is troubleshooting performance issues on a server that was recently upgraded. The administrator met with users/stakeholders and documented recent changes in an effort to determine whether the server is better or worse since the changes. Which of the following would BEST help answer the server performance question9

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

Correct Answer: B
Section:
Explanation:
A server baseline is a set of metrics that represents the normal performance and behavior of a server under a specific workload and configuration. A server baseline can help answer the server performance question by comparing the current performance with the previous performance before the upgrade. This can help identify any changes or issues that may have affected the server performance. Reference: https://www.comptia.org/training/resources/exam-objectives/comptiaserver- sk0-005-exam-objectives (Objective 4.2)

QUESTION 3
An application needs 10GB of RAID 1 for log files, 20GB of RAID 5 for data files, and 20GB of RAID 5 for the operating system. All disks will be 10GB in capacity. Which of the following is the MINIMUM number of disks needed for this application?

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

Correct Answer: C
Section:

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

QUESTION 4
The management team has mandated the use of data-at-rest encryption for all data. Which of the following forms of encryption best achieves this goal?

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

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

QUESTION 5
A company recently implemented VoIP across a multicampus environment with ten locations. The company uses many network technologies, including fiber, copper, and wireless. Users calling between three of the locations have reported that voices sound strange. Which of the following should be monitored to narrow down the issue?

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

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

QUESTION 6
Which of the following distributes a load across all interfaces?

A. Link aggregation group
B. Most recently used algorithm
C. Active-passive configuration
D. Failover

Correct Answer: A
Section:
Explanation:
A link aggregation group (LAG) is a technique that combines multiple physical network interfaces into a single logical interface. This allows for the distribution of traffic across all the interfaces in the group, increasing bandwidth and redundancy. A LAG can use different modes to balance the load, such as address hashing, dynamic, or most recently used algorithm.
References:CompTIA Server+ Study Guide, Chapter 6: Networking, page 239.

QUESTION 7
Hackers recently targeted a company with an attack that resulted in a system breach, which compromised the organization's data. Because of the system breach, the administrator had to bypass normal change management procedures. Which of the following change management activities was necessary?

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

Correct Answer: C
Section:
Explanation:
An emergency change request is a type of change request that is initiated in response to an urgent situation, such as a system breach, that requires immediate action to restore normal operations or prevent further damage. An emergency change request may bypass some of the normal change management procedures, such as approval, testing, or documentation, in order to expedite the implementation of the change. However, an emergency change request should still follow the basic steps of change management, such as identification, analysis, planning, execution, and evaluation, and should be reviewed and documented after the change is completed.
References:CompTIA Server+ Study Guide, Chapter 11: Change Management, page 443.

QUESTION 8
An administrator is tasked with building an environment consisting of four servers that can each serve the same website. Which of the following concepts is described?

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

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

QUESTION 9
A company has a data center that is located at its headquarters, and it has a warm site that is located 20mi (32km) away, which serves as a DR location. Which of the following should the company design and implement to ensure its DR site is adequate?

A. Set up the warm site as a DR cold site.
B. Set up a DR site that is in the cloud and in the same region.
C. Set up the warm site as a DR hot site.

D. Set up a DR site that is geographically located in another region.

Correct Answer: D
Section:
Explanation:
A DR site is a backup site that can be used to restore business operations in case of a disaster that affects the primary site. A warm site is a DR site that has some equipment and data ready to be activated quickly, but not as fast as a hot site that has fully operational systems and data. A cold site is a DR site that has only basic infrastructure and no equipment or data. The location of a DR site is an important factor to consider when designing and implementing a DR plan. A DR site that is too close to the primary site may be affected by the same disaster, such as a power outage, a flood, or an earthquake. A DR site that is too far away from the primary site may incur higher costs and latency issues. Therefore, a good practice is to set up a DR site that is geographically located in another region that has different risk factors and environmental conditions than the primary site. This can help ensure that the DR site is available and accessible when needed. Reference:
https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-examobjectives (Objective 3.3)

QUESTION 10
A server administrator is setting up a new payroll application. Compliance regulations require that all financial systems logs be stored in a central location. Which of the following should the administrator configure to ensure this requirement is met?

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

Correct Answer: C
Section:
Explanation:
Shipping is a process of sending logs from one system to another system for centralized storage and analysis. Shipping can help ensure compliance with regulations that require financial systems logs to be stored in a central location. Shipping can also help improve security, performance, and scalability of log management. Reference: https://www.comptia.org/training/resources/examobjectives/ comptia-server-sk0-005-exam-objectives (Objective 3.4)

QUESTION 11
Which of the following is a system that scans outgoing email for account numbers, sensitive phrases, and other forms of PII?

A. SIEM
B. DLP
C. HIDS
D. IPS

Correct Answer: B
Section:
Explanation:
DLP stands for Data Loss Prevention and it is a system that scans outgoing email for account numbers, sensitive phrases, and other forms of PII (Personally Identifiable Information). DLP can help prevent data breaches, comply with regulations, and protect the privacy of customers and employees. DLP can also block, encrypt, or quarantine emails that contain sensitive data. Reference:
https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-examobjectives (Objective 3.2)

QUESTION 12
A systems administrator is setting up a server on a LAN that uses an address space that follows the RFC 1918 standard. Which of the following IP addresses should the administrator use to be in compliance with the standard?

A. 11.251.196.241
B. 171.245.198.241

C. 172.16.19.241
D. 193.168.145.241

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

QUESTION 13
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 14
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 15
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 16
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 17
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 18
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 19
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 20
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 21
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 22
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 23
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 24
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 25
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 26
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 27
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 28
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 29
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 30
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 31
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 32
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 33
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 34
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 35
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 36
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 37
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 38
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 39
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 40
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 41
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 42
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 43

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 44
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 45
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 46
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 47
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 48
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 49
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 50
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 51
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 52
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 53
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 54
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 55
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 56
A storage administrator needs to implement SAN-based shared storage that can transmit at 16Gb over an optical connection. Which of the following connectivity options would BEST meet this requirement?

A. Fibre Channel
B. FCoE
C. iSCSI
D. eSATA

Correct Answer: A
Section:
Explanation:
Fibre Channel is a connectivity option that can transmit at 16Gb over an optical connection for SANbased shared storage. Fibre Channel is a high-speed network technology that provides reliable and secure data transfer between servers and storage devices. Fibre Channel uses optical fiber cables to connect devices and supports various topologies and protocols. FCoE is another connectivity option that uses Fibre Channel over Ethernet, which encapsulates Fibre Channel frames into Ethernet packets. FCoE can also transmit at 16Gb over an optical connection, but it requires a converged network adapter (CNA) and a lossless Ethernet network. iSCSI is another connectivity option that uses SCSI commands over IP networks, which can use either copper or optical cables. iSCSI can transmit at 10Gb or 40Gb over an optical connection, but it has higher latency and lower performance than Fibre Channel. eSATA is another connectivity option that uses SATA commands over external cables, which are usually copper. eSATA can transmit at 6Gb over a copper connection, but it has limited cable length and device support compared to Fibre Channel. Reference:
https://www.ibm.com/topics/storage-area-network
https://www.techopedia.com/definition/1369/fibre-channel-fc https://www.techopedia.com/definition/1368/fibre-channel-over-ethernet-fcoe https://www.techopedia.com/definition/1367/internet-small-computer-system-interface-iscsi
https://www.techopedia.com/definition/1366/external-serial-advanced-technology-attachmentesata

QUESTION 57
Which of the following commands would MOST likely be used to register a new service on a Windows OS?

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

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

QUESTION 58
An administrator receives an alert stating a S.MAR.T. error has been detected. Which of the following should the administrator run FIRST to determine the issue?

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

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

QUESTION 59
An administrator is researching the upcoming licensing software requirements for an application that usually requires very little technical support. Which of the following licensing models would be the LOWEST cost solution?

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

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

QUESTION 60
A server administrator wants to check the open ports on a server. Which of the following commands should the administrator use to complete the task?

A. nslookup

B. nbtstat
C. telnet
D. netstat -a

Correct Answer: D
Section:
Explanation:
netstat is a command-line tool that displays network connections, routing tables, interface statistics, and more. The -a option shows all listening and non-listening sockets on the server. This can help check the open ports on a server and identify any unwanted or malicious connections. Reference:
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat

QUESTION 61
A hardware technician is installing 19 1U servers in a 42 the following unit sizes should be allocated per server?

A. 1U
B. 2U
C. 3U
D. 4U

Correct Answer: A
Section:
Explanation:
1U stands for one unit and it is a standard unit of measurement for rack-mounted servers. It is equal to 1.75 inches (4.45 cm) in height. A 42U rack can accommodate 42 1U servers or a combination of servers with different unit sizes. Therefore, the unit size per server should be 1U if there are 19 1U servers in a 42U rack. Reference: https://www.comptia.org/training/resources/examobjectives/ comptia-server-sk0-005-exam-objectives (Objective 1.2)

QUESTION 62
An administrator is alerted to a hardware failure in a mission-critical server. The alert states that two drives have failed. The administrator notes the drives are in different RAID 1 arrays, and both are hotswappable. Which of the following steps will be the MOST efficient?

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

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

QUESTION 63
A server administrator made a change in a server's BIOS in an attempt to fix an issue with the OS not turning on. However, the change did not successfully correct the issue. Which of the following should the server administrator do NEXT?

A. Reinstall the server OS in repair mode while maintaining the data.
B. Flash the BIOS with the most recent version.
C. Reverse the latest change made to the server and reboot.

D. Restart the server into safe mode and roll back changes.

Correct Answer: C
Section:
Explanation:
The best practice for troubleshooting is to follow a logical and systematic process that involves identifying the problem, establishing a theory of probable cause, testing the theory, establishing a plan of action, implementing the solution, verifying functionality, and documenting findings. Since the problem occurred after a change in the server's BIOS, the most likely cause is that the change was incompatible or incorrect for the OS. Therefore, the next step should be to reverse the latest change made to the server and reboot to see if that fixes the issue. Reference:
https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-examobjectives (Objective 4.3)

QUESTION 64
A technician is decommissioning a server from a production environment. The technician removes the server from the rack but then decides to repurpose the system as a lab server instead of decommissioning it. Which of the following is the most appropriate NEXT step to recycle and reuse the system drives?

A. Reinstall the OS.
B. Wipe the drives.
C. Degauss the drives.
D. Update the IP schema.

Correct Answer: B
Section:
Explanation:
Wiping the drives is the most appropriate step to recycle and reuse the system drives. Wiping the drives means erasing all the data on the drives and overwriting them with random or meaningless data. This can help prevent data leakage, comply with regulations, and prepare the drives for a new installation or configuration. Wiping the drives is different from deleting or formatting the drives, which only remove the references to the data but not the data itself. Reference:
https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-examobjectives (Objective 1.3)

QUESTION 65
A technician is setting up a small office that consists of five Windows 10 computers. The technician has been asked to use a simple IP configuration without manually adding any IP addresses. Which of the following will the technician MOST likely use for the IP address assignment?

A. Static
B. Router-assigned
C. APIPA
D. DHCP

Correct Answer: D
Section:
Explanation:
DHCP stands for Dynamic Host Configuration Protocol and it is a network protocol that automatically assigns IP addresses and other network configuration parameters to devices on a network. DHCP can help simplify IP configuration without manually adding any IP addresses. DHCP works by using a DHCP server that maintains a pool of available IP addresses and leases them to devices that request them. The devices can renew or release their IP addresses as needed. Reference:
https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-examobjectives (Objective 2.1)

QUESTION 66
Which of the following ensures a secondary network path is available if the primary connection fails?

A. Link aggregation

B. Most recently used
C. Heartbeat
D. Fault tolerance

Correct Answer: D
Section:
Explanation:
Fault tolerance is the ability of a system to continue functioning in the event of a failure of one or more of its components. Fault tolerance can ensure a secondary network path is available if the primary connection fails. Fault tolerance can be achieved by using redundant components, such as network cards, cables, switches, routers, etc., that can take over the function of the failed component without interrupting the service. Reference: https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-examobjectives (Objective 2.2)

QUESTION 67
Which of the following backup types resets the archive bit each time it is run?

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

Correct Answer: C
Section:
Explanation:
Incremental backup is a type of backup that only backs up the files that have changed since the last backup, whether it was a full or an incremental backup. Incremental backup resets the archive bit each time it is run, which means it clears the flag that indicates whether or not the file has been backed up. Incremental backup can save time and space compared to full backup, but it requires more time and resources to restore data from multiple backups. Reference:
https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-examobjectives (Objective 3.1)

QUESTION 68
An administrator discovers a Bash script file has the following permissions set in octal notation; 777
Which of the following is the MOST appropriate command to ensure only the root user can modify and execute the script?

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

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

QUESTION 69
A server administrator receives the following output when trying to ping a local host:

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

Which of the following is MOST likely the issue?

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

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

QUESTION 70
The management team has mandated the encryption of all server administration traffic. Which of the following should MOST likely be implemented?

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

Correct Answer: A
Section:
Explanation:
SSH stands for Secure Shell and it is a network protocol that provides encrypted and authenticated communication between two hosts. SSH can be used to remotely access and administer a server using a command-line interface or a graphical user interface. SSH can ensure the encryption of all server administration traffic, which can prevent eavesdropping, tampering, or spoofing by unauthorized parties. Reference: https://www.comptia.org/training/resources/examobjectives/ comptia-server-sk0-005-exam-objectives (Objective 2.4)

QUESTION 71
An administrator is installing a new file server that has four drive bays available. Which of the following RAID types would provide the MOST storage as well as disk redundancy?

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

Correct Answer: C
Section:
Explanation:
RAID 5 is a RAID level that provides striping with parity, which means that data is distributed across all disks with one disk storing parity information for error correction. RAID 5 can tolerate one disk failure without losing data.

RAID 5 provides the most storage as well as disk redundancy out of the four RAID levels given, since it only uses one disk for parity and the rest for data. For example, if four 200GB drives are used in a RAID 5 array, the total storage capacity would be 600GB (200GB x 3), while in RAID 0 it would be 800GB (200GB x 4), in RAID 1 it would be 200GB (200GB x 1), and in RAID 10 it would be 400GB (200GB x 2). Reference: https://en.wikipedia.org/wiki/Standard_RAID_levels#RAID_5

QUESTION 72
A junior administrator needs to configure a single RAID 5 volume out of four 200GB drives attached to the server using the maximum possible capacity. Upon completion, the server reports that all drives were used, and the approximate volume size is 400GB. Which of the following BEST describes the result of this configuration?

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

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

QUESTION 73
Which of the following BEST describes a guarantee of the amount of time it will take to restore a downed service?

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

Correct Answer: A
Section:
Explanation:
RTO stands for Recovery Time Objective and it is a metric that defines the maximum acceptable amount of time that a system or service can be unavailable after a disaster or disruption. RTO is part of the business continuity planning and disaster recovery planning processes. RTO ensures a guarantee of the amount of time it will take to restore a downed service by setting a target or goal for recovery. RTO can vary depending on the criticality and priority of the service. Reference: https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-examobjectives (Objective 3.3)

QUESTION 74
A technician is attempting to log in to a Linux server as root but cannot remember the administrator password. Which of the following is the LEAST destructive method of resetting the administrator password?

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

Correct Answer: C
Section:
Explanation:

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

QUESTION 75
A server shut down after an extended power outage. When power was restored, the system failed to start. A few seconds into booting, the Num Lock, Scroll Lock, and Caps Lock LEDs flashed several times, and the system stopped. Which of the following is the MOST likely cause of the issue?

A. The keyboard is defective and needs to be replaced.
B. The system failed before the display card initialized.
C. The power supply is faulty and is shutting down the system.
D. The NIC has failed, and the system cannot make a network connection.

Correct Answer: B
Section:
Explanation:
This is the most likely cause of the issue because the keyboard LED flash indicates a POST error code. If the display card is not initialized, the system cannot show any error messages on the screen and will stop booting.
Reference: https://www.computerhope.com/beep.htm#04

QUESTION 76
Which of the following BEST describes overprovisioning in a virtual server environment?

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

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

QUESTION 77
A newly installed server is accessible to local users, but remote users are unable to connect. Which of the following is MOST likely misconfigured?

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

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

QUESTION 78
A systems administrator is trying to determine why users in the human resources department cannot access an application server. The systems administrator reviews the application logs but does not see any attempts by the users to access the application. Which of the following is preventing the users from accessing the application server?

A. NAT
B. ICMP
C. VLAN
D. NIDS

Correct Answer: C
Section:
Explanation:
This is the most likely cause of preventing the users from accessing the application server because a VLAN is a logical segmentation of a network that isolates traffic based on certain criteria. If the human resources department and the application server are on different VLANs, they will not be able to communicate with each other unless there is a router or a switch that can route between VLANs.
Reference: https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860- howto-L3-intervlanrouting.html

QUESTION 79
An administrator is only able to log on to a server with a local account. The server has been successfully joined to the domain and can ping other servers by IP address. Which of the following locally defined settings is MOST likely misconfigured?

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

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

QUESTION 80
An administrator is investigating several unexpected documents and video files that recently appeared in a network share. The administrator checks the properties of the files and sees the author's name on the documents is not a company employee. The administrator questions the other users, but no one knows anything about the files. The administrator then checks the log files and discovers the FTP protocol was used to copy the files to the server. Which of the following needs to be done to prevent this from happening again?

A. Implement data loss prevention.
B. Configure intrusion detection.
C. Turn on User Account Control.
D. Disable anonymous access.

Correct Answer: D
Section:
Explanation:
This is the best solution to prevent unauthorized files from being copied to the server via FTP because anonymous access allows anyone to log in to the FTP server without providing a username or password. Disabling anonymous access will require users to authenticate with valid credentials before accessing the FTP server. Reference: https://docs.microsoft.com/enus/
iis/configuration/system.applicationhost/sites/site/ftpserver/security/authentication/anonymous authentication

QUESTION 81
A server administrator purchased a single license key to use for all the new servers that will be imaged this year. Which of the following MOST likely refers to the licensing type that will be used?

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

Correct Answer: D
Section:
Explanation:
This is the most likely licensing type that will be used because volume licensing allows a single license key to be used for multiple installations of a software product. Volume licensing is typically used by organizations that need to deploy software to a large number of devices or users. Reference:
https://www.microsoft.com/en-us/licensing/licensing-programs/volume-licensing-programs

QUESTION 82
Which of the following cloud models is BEST described as running workloads on resources that are owned by the company and hosted in a company-owned data center, as well as on rented servers in another company's data center?

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

Correct Answer: B
Section:
Explanation:
This is the best description of a hybrid cloud model because it combines both private and public cloud resources. A private cloud is a cloud environment that is owned and operated by a single organization and hosted in its own data center. A public cloud is a cloud environment that is owned and operated by a third-party provider and hosted in its data center. A hybrid cloud allows an organization to leverage both types of cloud resources depending on its needs and preferences.
Reference: https://azure.microsoft.com/en-us/overview/what-is-hybrid-cloud-computing/

QUESTION 83
A backup application is copying only changed files each time 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:
This is the best description of a synthetic full backup method because it creates a full backup by combining previous incremental backups with the latest backup. An incremental backup copies only the files that have changed since the last backup, while a full backup copies all the files. A synthetic full backup reduces the storage space and network bandwidth required for backups, while also simplifying the restore process by using a single file.
Reference:
https://www.veritas.com/support/en_US/doc/129705091-129705095-0/br731_wxrttot_ v131910378-129705095

QUESTION 84
A server room contains ten physical servers that are running applications and a cluster of three dedicated hypervisors. The hypervisors are new and only have 10% utilization. The Chief Financial Officer has asked that the IT department do what it can to cut back on power consumption and maintenance costs in the data center. Which of the following would address the request with minimal server downtime?

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

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

QUESTION 85
A server administrator encounters some issues with the server OS after applying monthly patches. Which of the following troubleshooting steps should the administrator perform?

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

Correct Answer: A
Section:
Explanation:
This option would restore the server OS to a previous state before applying the monthly patches. This would help troubleshoot the issues caused by the patches and determine if they are compatible with the server OS. The other options would either not address the issues, cause data loss, or require more time and resources

QUESTION 86
A new application server has been configured in the cloud to provide access to all clients within the network. On-site users are able to access all resources, but remote users are reporting issues connecting to the new application. The server administrator verifies that all users are configured with the appropriate group memberships. Which of the following is MOST likely causing the issue?

A. Telnet connections are disabled on the server.
B. Role-based access control is misconfigured.
C. There are misconfigured firewall rules.
D. Group policies have not been applied.

Correct Answer: C
Section:
Explanation:
This is the most likely cause of the issue because firewall rules can block or allow traffic based on source, destination, port, protocol, or other criteria. If the firewall rules are not configured properly, they can prevent remote users from accessing the cloud application server, while allowing on-site users to access it. Reference: https://docs.microsoft.com/en-us/azure/virtual-network/securityoverview

QUESTION 87
A technician is monitoring a server and notices there is only one NIC plugged in. but the server has two. The NIC is oversaturated, and the technician would like to increase the available bandwidth. Which of the following solutions would be the BEST option to increase the speed of this NIC?

A. Link aggregation
B. Heartbeat
C. Most recently used
D. Active-active

Correct Answer: A
Section:
Explanation:
This is the best solution to increase the speed of the NIC because link aggregation is a technique that combines multiple physical network interfaces into a single logical interface. This can increase the bandwidth, redundancy, and load balancing of network traffic. Link aggregation requires both the server and the switch to support it and be configured accordingly. Reference:
https://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html

QUESTION 88
A user logs in to a Linux server and attempts to run the following command:
sudo emacs /root/file
However the user gets the following message:
User userid is not allowed to execute Temacs' on this server. Which of the following would BEST allow the user to find out which commands can be used?

A. visudo I grep userid
B. sudo -1 -U userid
C. cat /etc/passwd
D. userlist I grep userid

Correct Answer: B
Section:
Explanation:
This is the best command to find out which commands can be used by a user with sudo privileges because it lists the allowed and forbidden commands for a given user or role. The -l option stands for list, and the -U option specifies the user name. The output of this command will show what commands can be executed with sudo by that user on that server. Reference:
https://www.sudo.ws/man/1.8.13/sudo.man.html

QUESTION 89
Which of the following is the MOST secure method to access servers located in remote branch offices?

A. Use an MFAout-of-band solution.
B. Use a Telnet connection.
C. Use a password complexity policy.
D. Use a role-based access policy.

Correct Answer: A
Section:
Explanation:
This is the most secure method to access servers located in remote branch offices because MFA stands for multi-factor authentication, which requires users to provide more than one piece of evidence to prove their identity. An out-of-band solution means that one of the factors is delivered through a separate channel, such as a phone call, a text message, or an email. This adds an extra layer of security and prevents unauthorized access even if a password is compromised. Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

QUESTION 90
Which of the following refers to the requirements that dictate when to delete data backups?

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

Correct Answer: A
Section:
Explanation:
Retention policies are the guidelines that dictate when to delete data backups based on operational or compliance needs. They specify how long, how, where, and in what format the data backups are stored, and who has authority over them. The other options are not directly related to the deletion of data backups.
https://backup.ninja/news/Database-Backups-101-Backup-Retention-Policy-Considerations

QUESTION 91
A security manager is concerned that a rogue employee could boot a server from an outside USB drive. Which of the following actions can be taken to reduce this risk? (Select TWO).

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

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

QUESTION 92
Which of the following should be configured in pairs on a server to provide network redundancy?

A. MRU
B. SCP
C. DLP
D. CPU
E. NIC

Correct Answer: E
Section:
Explanation:
NIC stands for network interface card, which is a hardware component that allows a server to connect to a network. Configuring NICs in pairs on a server would provide network redundancy, meaning that if one NIC fails, the other one can take over and maintain network connectivity. The other options are not related to network redundancy.

QUESTION 93
A company's security team has noticed employees seem to be blocking the door in the main data center when they are working on equipment to avoid having to gain access each time. Which of the following should be implemented to force the employees to enter the data center properly?

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

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

QUESTION 94
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 95
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 96
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 97
A technician re working on a Linux server and re trying to access another server over the network. The technician gets server not found message when trying to execute ping servername but no error messages when using ping servername. Domain.com. Which of the following should the technician do to resolve the error?

A. Configure the domain search variable
B. Change the permissions on resolv. conf
C. Configure the DNS address
D. Modify nsswitch. Conf.

Correct Answer: A
Section:
Explanation:
The domain search variable is used to specify a list of domains that are appended to a hostname when resolving it. If the servername is not fully qualified, the resolver will try each domain in the list until it finds a match or fails. By configuring the domain search variable, the technician can avoid typing the full domain name every time they want to ping a server. Verified
Reference: [How to configure DNS suffixes on Linux systems]

QUESTION 98
Joe. a user m the IT department cannot save changes to a sensitive file on a Linux server. An 1s -1& snows the following listing;

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

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

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

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

QUESTION 99
An administrator has been asked to increase the storage capacity of a stand-alone file server but no further expansion slots are available. Which of the following would be the FASTEST solution to implement with no downtime?

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

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

QUESTION 100
Which of the following licensing models is MOST appropriate tor a data center that has a variable daily equipment count?

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

Correct Answer: D
Section:
Explanation:
A per core licensing model is based on the number of processor cores in a server. This model is suitable for a data center that has a variable daily equipment count, as it allows for scaling up or down the number of cores as needed. A per core licensing model also provides better performance and efficiency than other models. Verified
Reference: [Per Core Licensing and Basic Definitions]

QUESTION 101
A server administrator recently installed a kernel update to test functionality Upon reboot, the administrator determined the new kernel was not compatible with certain server hardware and was unable to uninstall the update. Which of the following should the administrator do to mitigate further issues with the newly instated kernel version?

A. Edit the bootloader configuration file and change the first Kernel stanza to reflect the file location for the last known-good kernel files.
B. Perform a complete OS reinstall on the server using the same media that was used during the initial install.
C. Edit the bootloader configuration file and move the newest kernel update stanza lo the end of the file.
D. Set a BIOS password to prevent server technicians from making any changes to the system.

Correct Answer: A
Section:
Explanation:
The bootloader configuration file is used to specify which kernel version and options to use when booting the system. The first kernel stanza in the file is the default one that is loaded automatically. By editing this stanza and changing it to point to the last known-good kernel files, the administrator can boot the system with a working kernel and avoid any compatibility issues with the new kernel update. Verified
Reference: [How To Change The Linux Kernel Version]

QUESTION 102

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

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

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

QUESTION 103
Users report they ate unable to access an application after a recent third-party patch update. The physical server that is hosting the application keeps crashing on reboot. Although the update was installed directly from the manufacturer's support website as recommended it has now been recalled and removed from the website as the update unintentionally installed unauthorized software after a reboot. Which of the following steps should the administrator perform to restore access to the application while minimizing downtime? (Select TWO)

A. Uninstall recent updates.
B. Reimage the server with a different OS.
C. Run a port scan to verify open ports.
D. Enable a GPO to uninstall the update.
E. Scan and remove any malware.
F. Reformat the server and restore the image from the latest backup.

Correct Answer: E, F
Section:
Explanation:
The most likely cause of the server crashing and the application being inaccessible is that the unauthorized software installed by the update is malware that corrupted the system files or compromised the security of the server. To restore access to the application while minimizing downtime, the administrator should scan and remove any malware from the server, and then reformat the server and restore the image from the latest back-up. This will ensure that the server is clean and has a working configuration of the application. Verified
Reference: [How to Remove Malware from a Server]

QUESTION 104
Which of the following backup types should be chosen for database servers?

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

Correct Answer: C
Section:
Explanation:

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

QUESTION 105
An administrator is troubleshooting a failure in the data center in which a server shut down/turned off when utility power was lost The server had redundant power supplies. Which of the following is the MOST likely cause of this failure?

A. The UPS batteries were overcharged.
B. Redundant power supplies require 220V power
C. Both power supplies were connected to the same power feed
D. The power supplies were not cross-connected

Correct Answer: C
Section:
Explanation:
The most likely cause of this failure is that both power supplies were connected to the same power feed, which means that they both lost power when utility power was lost. To prevent this from happening, redundant power supplies should be connected to different power feeds, preferably from different sources, such as a UPS or a generator. Verified
Reference: [Redundant Power Supply Best Practices]

QUESTION 106
A data center has 4U rack servers that need to be replaced using VMs but without losing any dat

A. Which of the following methods will MOST likely be used to replace these servers?
B. VMFS
C. Unattended scripted OS installation
D. P2V
E. VM cloning

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

QUESTION 107
While running a local network security scan an administrator discovers communication between clients and one of the web servers is happening in cleartext. Company policy requires all communication lo be encrypted.
Which of the following ports should be closed to stop the deartext communication?

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

Correct Answer: A
Section:
Explanation:

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

QUESTION 108
The accounting department needs more storage and wants to retain the current data for quick read-write access. The accounting server does not have any internet drive bays available to keep both disks however the server does have USB 3 0 and eSATA ports available. Which of the following is the BEST way to accomplish the department's goals?

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

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

QUESTION 109
Which of the following should a technician verify FIRST before decommissioning and wiping a file server?

A. The media destruction method
B. The recycling poke?
C. Asset management documentation
D. Non-utilization

Correct Answer: D
Section:
Explanation:
The first thing that a technician should verify before decommissioning and wiping a file server is non-utilization, which means that no one is using or accessing the server or its data. This can be done by checking logs, monitoring network traffic, or contacting users or stakeholders. Non-utilization ensures that decommissioning and wiping will not cause any data loss or disruption to business operations. Verified
Reference: [Server Decommissioning Checklist]

QUESTION 110
A Linux server was recently updated. Now, the server stops during the boot process with a blank screen and an s> prompt. When of the following is the MOST likely cause of this issue?

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

Correct Answer: B
Section:
Explanation:
The most likely cause of this issue is that the UEFI boot was interrupted by a missing Linux boot file, such as grub.cfg or vmlinuz, which are essential for loading the Linux kernel and booting the system. The s> prompt

indicates that the system entered into UEFI Shell mode, which is a command-line interface for troubleshooting UEFI boot issues. The administrator can use UEFI Shell commands to locate and restore the missing boot file or change the boot order. Verified
Reference: [UEFI Shell Guide]

QUESTION 111
Which of the following BEST measures how much downtime an organization can tolerate during an unplanned outage?

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

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

QUESTION 112
A server administrator is creating a new server that will be used to house customer sales records. Which of the following roles will MOST likely be Installed on the server?

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

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

QUESTION 113
An administrator has been asked to verify that all traffic egressing from a company is secured. The administrator confirms all the information that is sent over the network is encrypted. Which of the following describes the type of traffic being encrypted?

A. Network encapsulation
B. Off-site data
C. Secure FTP
D. Data in transit

Correct Answer: D
Section:
Explanation:

Data in transit is data that is being transferred over a network, such as the internet. It can be encrypted to protect it from unauthorized access or tampering. Verified
Reference: [Data in transit], [Encryption]

QUESTION 114
Which of the following script types would MOST likely be used on a modern Windows server OS?

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

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

QUESTION 115
A technician has beer tasked to install a new CPU. Prior to the retaliation the server must be configured. Which of the following should the technician update?

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

Correct Answer: B
Section:
Explanation:
The BIOS (Basic Input/Output System) is a firmware that controls the initialization and booting of a server. It also provides settings for the CPU, such as speed, voltage, and temperature. Updating the BIOS can improve the performance and compatibility of the CPU and other hardware components. Verified
Reference: [BIOS], [CPU]

QUESTION 116
An organization is donating its outdated server equipment to a local charity. Which of the following describes what the organization should do BEFORE donating the equipment?

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

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

QUESTION 117
A staff member who a monitoring a data center reports one rack is experiencing higher temperatures than the racks next to it, despite the hardware in each rack being the same. Which of the following actions would MOST likely remediate the heal issue?

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

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

QUESTION 118
Which of the following asset management documents is used to identify the location of a serves within a data center?

A. Infrastructure diagram
B. Workflow diagram
C. Rack layout
D. Service manual

Correct Answer: C
Section:
Explanation:
A rack layout is a document that shows the physical location and arrangement of servers and other devices within a rack. It can include information such as server names, IP addresses, power consumption, and cable connections. A rack layout can help identify and locate servers easily and efficiently in a data center. Verified
Reference: [Rack layout], [Data center]

QUESTION 119
Which of the following script types uses commands That start with sec-?

A. Batch
B. Bash
C. PowerShell
D. JavaScript

Correct Answer: C
Section:
Explanation:
PowerShell is a scripting language and a command-line shell that uses commands that start with sec- to perform security-related tasks. For example, sec-edit is a command that edits security policies, sec-logon is a command that manages logon sessions, and sec-policy is a command that applies security templates. Verified
Reference: [PowerShell security commands], [Security policy]

QUESTION 120
A developer is creating a web application that will contain five web nodes. The developer's main goal is to ensure the application is always available to the end users. Which of the following should the developer use when

designing the web application?

A. Round robin
B. Link aggregation
C. Network address translation
D. Bridged networking

Correct Answer: A
Section:
Explanation:
Round robin is a load balancing technique that distributes requests among multiple web nodes in a circular order. It ensures that each web node receives an equal amount of requests and improves the availability and performance of the web application. Verified
Reference: [Round robin], [Load balancing]

QUESTION 121
An administrator notices nigh traffic on a certain subnet and would like to identify the source of the traffic. Which of the following tools should the administrator utilize?

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

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

QUESTION 122
Which of the following licensing concepts is based on the number of logical processors a server has?

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

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

QUESTION 123
An application server's power cord was accidentally unplugged. After plugging the cord back in the server administrator notices some transactions were not written to the disk array. Which of the following is the MOST likely cause of the issue?

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

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

QUESTION 124
A server administrator has received calls regarding latency and performance issues with a file server. After reviewing all logs and server features the administrator discovers the server came with four Ethernet ports, out only one port is currently in use. Which of the following features will enable the use of all available ports using a single IP address?

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

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

QUESTION 125
A server administrator notices the /var/log/audit/audit.log file on a Linux server is rotating loo frequently. The administrator would like to decrease the number of times the leg rotates without losing any of the information in the logs. Which of the following should the administrator configure?

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

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

QUESTION 126
A technician is able to copy a Me to a temporary folder on another partition but is unable to copy it to a network share or a USB flash drive. Which of the following is MOST likely preventing the file from being copied to certain locations?

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

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

QUESTION 127
A technician is creating a network snare that will be used across both Unix and Windows clients at the same time. Users need read and write access to the files. Which of the following would be BEST for the technician to deploy?

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

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

QUESTION 128
A technician recently applied a critical OS patch to a working sever. After rebooting, the technician notices the server Is unable to connect to a nearby database server. The technician validates a connection can be made to the database from another host. Which of the following is the best NEXT step to restore connectivity?

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

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

QUESTION 129
A server administrator is instating a new server in a data center. The administrator connects the server to a midplane but does not connect any cables Which of the following types of servers is the administrator MOST likely

installing?

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

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

QUESTION 130
A technician retailed a new 4TB hard drive in a Windows server. Which of the following should the technician perform FIRST to provision the new drive?

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

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

QUESTION 131
A systems administrator has several different types of hard drives. The administrator is setting up a MAS that will allow end users to see all the drives within the NAS. Which of the following storage types should the administrator use?

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

Correct Answer: D
Section:
Explanation:
JBOD (Just a Bunch Of Disks) is a storage configuration that combines different types and sizes of hard drives into one logical unit without any RAID level or redundancy. It allows users to see all the drives within the unit as one large storage space. JBOD can utilize all the available capacity of the drives but does not provide any performance or fault tolerance benefits. Verified
Reference: [JBOD], [RAID]

QUESTION 132
Due to a disaster incident on a primary site, corporate users are redirected to cloud services where they will be required to be authenticated just once in order to use all cloud services.

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

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

Correct Answer: D
Section:

QUESTION 133
An administrator restores several database files without error while participating in a mock disaster recovery exercise. Later, the administrator reports that the restored databases are corrupt and cannot be used. Which of the following would best describe what caused this issue?

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

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

QUESTION 134
An administrator notices high traffic on a certain subnet and would like to identify the source of the traffic. Which of the following tools should the administrator utilize?

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

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

QUESTION 135

A. A site is considered a warm site when it:
B. has basic technical facilities connected to it.
C. has faulty air conditioning that is awaiting service.
D. is almost ready to take over all operations from the primary site.
E. is fully operational and continuously providing services.

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

QUESTION 136
After a technician upgrades the firmware on a database server that is connected to two external storage arrays, the server prompts the technician to configure RAID. The technician knows the server had several configured RAID sets and thinks the firmware upgrade cleared the RAID configurations. Which of the following should the technician do to troubleshoot this issue?

A. Power cycle the storage arrays and rescan RAID on the server.
B. Boot the OS into recovery mode and rescan the disks.
C. Restore the default RAID configuration and reboot.
D. Perform a rescan on the server's RAID controller.

Correct Answer: D
Section:
Explanation:
A rescan on the server's RAID controller is a possible troubleshooting step to detect the existing RAID configurations on the connected storage arrays. A firmware upgrade may cause the RAID controller to lose the RAID metadata or settings, and a rescan may restore them. A rescan is preferable to restoring the default RAID configuration, as the latter may erase the existing data on the arrays. Power cycling the storage arrays or booting the OS into recovery mode may not help if the RAID controller does not recognize the RAID sets.
References:CompTIA Server+ Study Guide, Chapter 7: Storage, page 287.

QUESTION 137
A server administrator deployed a new product that uses a non-standard port for web access on port 8443. However, users are unable to access the new application. The server administrator checks firewall rules and determines 8443 is allowed. Which of the following is most likely the cause of the issue?

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

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

QUESTION 138

A startup company needs to set up an initial disaster recovery site. The site must be cost-effective and deployed quickly. Which of the following sites should the company set up?

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

Correct Answer: B
Section:
Explanation:
A cold site is a backup facility with little or no hardware equipment installed. A cold site is the most cost-effective option among the three disaster recovery sites. However, due to the fact that a cold site doesn't have any pre-installed equipment, it takes a lot of time to properly set it up so as to fully resume business operations1.
References = 1: Disaster Recovery Sites Comparison: Which one to Choose? - NAKIVO(https://www.nakivo.com/blog/overview-disaster-recovery-sites/)

QUESTION 139
A technician is tasked with upgrading 24 hosts simultaneously with a Type 1 hypervisor. Which of the following protocols should the technician use for this upgrade?

A. VPN
B. TFTP
C. SSH
D. HTTP

Correct Answer: B
Section:
Explanation:
TFTP (Trivial File Transfer Protocol) is a simple and lightweight protocol that can be used to transfer files over a network. TFTP is often used to upgrade firmware or software on network devices, such as routers, switches, or servers. TFTP can also be used to install a Type 1 hypervisor, such as VMware ESXi, on multiple hosts simultaneously12.
References = 1: How to Install VMware ESXi Type 1 Hypervisor - MatthewEaton.net(https://mattheweaton.net/posts/how-to-install-vmware-esxi-type-1-hypervisor/) 2: Explore Type 1 Hypervisors - Set Up Virtual Machines Using VirtualBox and vSphere - OpenClassrooms(https://openclassrooms.com/en/courses/7163136-set-up-virtual-machines-using-virtualbox-and-vsphere/7358546-explore-type-1-hypervisors)

QUESTION 140
An administrator is installing a new server and OS. After installing the OS, the administrator logs in and wants to quickly check the network configuration. Which of the following is the best command to use to accomplish this task?

A. tracert
B. telnet
C. ipconfig
D. ping

Correct Answer: C
Section:

QUESTION 141
Hackers recently targeted a company with an attack that resulted in a system breach, which compromised the organization's data. Because of the system breach, the administrator had to bypass normal change management procedures. Which of the following change management activities was necessary?

A. Cancelled change request

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

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

QUESTION 142
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 143
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 144
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 145
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 146
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 147
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.

QUESTION 148
Which of the following distributes a load across all interfaces?

A. Link aggregation group
B. Most recently used algorithm
C. Active-passive configuration
D. Failover

Correct Answer: A
Section:
Explanation:
Link Aggregation:Involves combining multiple physical network interfaces into a single logical interface. This creates increased bandwidth, improved fault tolerance, and load balancing, where traffic can be distributed across all links in the group. (CompTIA Server+ Objectives SK0-004: 2.4)
Why other options are incorrect:
Most recently used algorithm:A concept used in memory management, not network traffic distribution.
Active-passive configuration:Used for failover with only one interface active at a time.
Failover:Ensures service continuity if an interface fails but does not inherently distribute load across multiple links.

QUESTION 149
A technician is installing an OS on ten servers. Which of the following media installation types would allow for the fastest installation time?

A. Network
B. Embedded
C. Optical
D. USB

Correct Answer: A
Section:
Explanation:
Network Installation:Allows the OS image to be deployed from a central server, streamlining deployment across multiple systems simultaneously. This is significantly faster than individual installations from other media. (CompTIA Server+ Objectives SK0-004: 3.1)
Why other options are less optimal:
Embedded:Refers to OSes pre-installed on hardware and not intended for mass deployment.
Optical (CDs/DVDs):Requires physical media insertion on each server, slower than network distribution.
USBSimilar to optical, requires individual installations and can be time-consuming for multiple servers.

QUESTION 150
A web server that is being deployed in the perimeter network needs to be shielded from malicious traffic. Which of the following could help identify these threats?

A. Applying OS updates
B. Disabling unused services
C. Implementing HIDS
D. Installing anti-malware

Correct Answer: C
Section:
Explanation:
HIDS (Host Intrusion Detection System):Continuously monitors a system for suspicious activity and logs or raises alerts when potential threats are identified. This proactive approach is crucial for identifying and mitigating

threats on a web server exposed to the external network.
Applying OS updates:While essential for maintaining system security, updates address vulnerabilities and may not necessarily identify ongoing threats.
Disabling unused services:Reduces the attack surface by minimizing potential entry points for malicious actors, but doesn't actively identify threats.
Installing anti-malware:Primarily designed to detect and remove malware after infection, not for ongoing threat identification.
References:
CompTIA Server+ Objectives(Exam codes SK0-004 or SK0-005): Search for sections on intrusion detection and prevention.

QUESTION 151
A technician is setting up a repurposed server. The minimum requirements are 2TB while ensuring the highest performance and providing support for one drive failure. The technician has the following six drives available:

1	500GB	10,000rpm
2	600GB	10,000rpm
3	500GB	7,200rpm
4	500GB	10,000rpm
5	600GB	15,000rpm
6	600GB	10,000rpm

Which of the following drive selections should the technician utilize to best accomplish this goal?

A. 1,2, 4, and 6
B. 1, 2, 3, 5, and 6
C. 1, 2, 4, 5, and 6
D. 1, 2, 3, 4, and 6

Correct Answer: C
Section:
Explanation:
RAID 5 configuration:Using five of the available drives in a RAID 5 configuration meets the requirements for:
Storage capacity:Four 600GB drives (2, 5, and 6) provide a total usable capacity of 2.4TB (4 * 600 * 0.8), exceeding the minimum requirement of 2TB. RAID 5 introduces parity data for fault tolerance, sacrificing some usable space (one drive's worth).
Performance:The combination of multiple drives in a RAID 5 array improves read performance compared to a single drive setup.
Fault tolerance:Even with a single drive failure (any of the five drives used in the RAID 5), the remaining drives can reconstruct the lost data, allowing the server to continue operating.

QUESTION 152
A security administrator ran a port scanning tool against a virtual server that is hosting a secure website. A list of open ports was provided as documentation. The management team has requested that non-essential ports be disabled on the firewall. Which of the following ports must remain open?

A. 25
B. 53
C. 443
D. 3389
E. 8080

Correct Answer: C
Section:
Explanation:
HTTPS (Secure Web Traffic):Port 443 is the standard port for HTTPS, which is essential for encrypting communication between web browsers and a secure website. (CompTIA Server+ Objectives SK0-004: 4.1)

Why other options are not essential:
25 (SMTP):Used for email transmission
53 (DNS):Used for domain name resolution
**3389 (RDP): ** Used for remote desktop connections
**8080 (Alternate HTTP): ** Sometimes used for web servers, but not the standard secure port

QUESTION 153
A systems administrator is provisioning a large number of virtual Linux machines that will be configured identically. The administrator would like to configure the machines quickly and easily but does not have access to an automation/orchestration platform. Additionally, the administrator would like to set up a system that can be used in the future, even on newer versions of the OS. Which of the following will best meet the administrator's requirements?

A. Deploying each server from a VM template
B. Using a kickstart file during installation
C. Configuring each server manually one at a time
D. Copying/pasting configuration commands into each server through SSH sessions
E. Configuring a single server and then creating clones of it

Correct Answer: B
Section:
Explanation:
Kickstart Files (Linux):Kickstart files are configuration files that automate the Linux installation process. They contain pre-determined answers to installation prompts, allowing for identical and rapid deployment of multiple systems. (CompTIA Server+ Objectives SK0-004: 3.1, Red Hat documentation on Kickstart:https://access.redhat.com/documentation/)
Why other options are less ideal:
VM Template (A):Templates are useful for replicating the OS & some software, but might not capture all configurations.
Manual Configuration (C):Time-consuming and prone to errors when replicating across many servers.
Copy/Paste via SSH (D):Tedious, error-prone, and requires servers to be online before configuration.
Cloning (E):Can work but has version compatibility risks if the OS of the cloned server isn't identical to the new ones.

QUESTION 154
An employee who was dismissed did not return company-issued equipment. Which of the following is the most important information the IT department needs to give to the legal department?

A. Labeling
B. Serial number
C. Warranty
D. Asset tag

Correct Answer: D
Section:
Explanation:
The most important piece of information needed by the legal department in the event that an employee does not return company-issued equipment is the asset tag. The asset tag is a unique identifier that is used to track assets throughout their lifecycle. It allows the company to keep precise records of the assets, monitor their location, and manage their overall inventory. In legal situations, the asset tag can be used to prove ownership and aid in the recovery process of the equipment. The serial number is also important, but it is the asset tag that ties the equipment directly to the company's asset management system and is therefore the most crucial for the legal department. Warranty and labeling information are less critical from a legal perspective when it comes to unreturned equipment.

QUESTION 155
Which of the following authentication types defines credentials as 'something you have'?

A. Swipe pattern
B. PIN
C. Fingerprint
D. Smart card

Correct Answer: D
Section:
Explanation:
The concept of authentication is rooted in the principle of verifying identity, which is commonly broken down into three categories: 'something you know' (like a password or PIN), 'something you have' (such as a smart card or a security token), and 'something you are' (biometric data, for example, fingerprints). The question asks for the authentication type defined by 'something you have.'

QUESTION 156
An administrator is tasked with building an environment consisting of four servers that can each serve the same website. Which of the following concepts is described?

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

Correct Answer: A
Section:
Explanation:
Load balancing is a technique used to distribute workloads evenly across multiple servers, ensuring no single server is overwhelmed. This is especially important in environments where high availability and reliability are critical, such as when multiple servers are serving the same website. By doing so, load balancing improves the responsiveness and availability of applications or websites.
Load balancing refers to the process of distributing network or application traffic across multiple servers to ensure no single server becomes overwhelmed, thereby improving responsiveness and availability of applications or websites. In the scenario described, where four servers are set up to each serve the same website, the concept of load balancing is applied. This setup aims to distribute incoming requests evenly among the servers to maximize speed and capacity utilization while ensuring no one server is overburdened, which can lead to improved overall performance of the website. Options B, C, and D do not accurately describe the scenario of distributing traffic for the same website across multiple servers.

QUESTION 157
An administrator has been asked to copy files from a Windows server that may not conform to Windows file-naming standards. Which of the following would best facilitate the copy process?

A. Robocopy
B. SCP
C. Drag and drop
D. FTP

Correct Answer: A
Section:
Explanation:
Robocopy (Robust File Copy) is a command-line tool in Windows that is designed for reliable copy or mirroring of files, and it can handle a broader range of file names and paths, including those that do not conform to traditional Windows file-naming standards. It's specifically designed to handle complex file copy demands and offers a wide range of options that can be tailored for different scenarios, which makes it suitable for the task mentioned. SCP (Secure Copy Protocol), Drag and Drop, and FTP (File Transfer Protocol) are all methods that can be used to copy files, but they might not handle non-standard Windows file names as well as Robocopy.

QUESTION 158
A server located in an IDF of a paper mill reboots every other day at random times. Which of the following should the technician perform on the server first?

A. Check the power cables

B. Clean the fans.
C. Replace the RAM.
D. Reattach the CPU heat sink

Correct Answer: A
Section:
Explanation:
In a situation where a server reboots randomly, the first step should be to check for any issues with the power supply. Random reboots can often be caused by intermittent power supply issues, which can be due to faulty power cables, loose connections, or problems with the power source itself. This is especially pertinent in environments like a paper mill where dust and debris might affect cable integrity. Since the issue occurs every other day and at random times, it's less likely to be caused by components that would typically fail due to overheating or other gradual issues (like RAM or CPU heat sink problems). Therefore, checking the power cables is the simplest and most direct first step to troubleshoot the issue.

QUESTION 159
An administrator receives an alert that one of the virtual servers has suddenly crashed. The administrator confirms the data center does not have any power failures and then connects to the remote console of the crashed server After connecting to the server console, which of the following should the administrator complete first?

A. Use the keyboard command AH+F12 to switch to the kernel log screen
B. Perform a hard reboot on the server and monitor the server startup
C. Collect a screenshot of the PSOD and note the details after the line detailing the OS version
D. Collect a core dump from the server and store locally before rebooting the hardware

Correct Answer: C
Section:
Explanation:
When a virtual server crashes and presents a Purple Screen of Death (PSOD), the immediate response should be to document the incident. Collecting a screenshot of the PSOD is crucial as it contains error codes and state information that can be used for diagnosing the root cause of the crash. Noting the details, especially those that come after the line detailing the OS version, can provide specific clues to what might have caused the server to crash. This is a standard best practice before rebooting the server, as it ensures that there is a record of the event to investigate and potentially prevent future occurrences. A hard reboot should only be done after this critical information has been recorded.

QUESTION 160
An IT administrator is configuring ten new desktops without an operating system. The infrastructure contains an imaging server and operating system loaded on a USB, a DVD, and an SD card. Which of the following options would minimize the amount of time the administrator needs to load the operating system on every machine?

A. SD card
B. Optical
C. Network
D. USB

Correct Answer: C
Section:
Explanation:
Using a network-based deployment, such as network booting (PXE - Preboot Execution Environment) or imaging through a server, is the most efficient way to load operating systems onto multiple machines simultaneously. This approach minimizes the manual intervention required for each device, as the administrator can initiate the operating system installation or imaging process across all desktops at once through the network. In contrast, using an SD card, DVD (Optical), or USB would require the administrator to physically move the media from one desktop to another, significantly increasing the setup time for each device.

QUESTION 161
A systems administrator is setting up a server farm for a new company. The company has a public range of IP addresses and uses the addresses internally. Which of the following IP addresses best fits this scenario?

A. 10.3.7.27
B. 127.0.0.1
C. 192.168.7.1
D. 216.176.128.10

Correct Answer: D
Section:
Explanation:
The IP address 216.176.128.10 falls within the range of public IP addresses, which are routable over the Internet. Since the company is using a public range of IP addresses internally, this address is suitable for the scenario. In contrast, 10.3.7.27 and 192.168.7.1 are private IP addresses typically used within internal networks and not routable on the public Internet. 127.0.0.1 is known as the loopback address, used by a computer to communicate with itself and not suitable for assigning to devices within a network.

QUESTION 162
A technician replaces a single faulted disk in the following array RAID 10, Four 15K SAS HDD The technician replaces it from a disk in spare parts, and the array rebuilds the data in a few minutes. After the array rebuild is complete, the system reports the IOPS on the disk array have dropped by almost 60% Which of the following should the technician investigate first?

A. Check the RAID controller (or background rebuild tasks
B. Check the firmware version on the newly replaced disk.
C. Check the RPM speed on the newly replaced disk-
D. Check the cache settings on the RAID controller.

Correct Answer: C
Section:
Explanation:
In RAID 10 arrays, disk performance is crucial, especially if they are high-speed 15K RPM SAS HDDs, as each disk in the array is part of a mirrored pair that also stripes data with another pair. When replacing a disk, it's essential that the new disk matches the specifications of the others, especially in terms of rotational speed (RPM). If the replaced disk is slower, it can significantly reduce the Input/Output operations per second (IOPS) of the entire array. This is because all disks need to work in tandem, and the slowest disk can become a bottleneck. Thus, checking the RPM of the newly replaced disk is a sensible first step to ensure it matches the performance of the other disks in the array.

QUESTION 163
A new company policy requires that any lost functionality must be restored within 24 hours in the event of a disaster. Which of the following describes this policy requirement?

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

Correct Answer: B
Section:
Explanation:
Recovery Time Objective (RTO) refers to the target time set for the recovery of IT and business activities after a disaster has struck, which includes restoring server, network, and data access. The policy requirement mentioned in the question aligns with the definition of RTO, as it specifies the maximum allowable downtime or the time within which functionality must be restored. Mean Time Between Failures (MTBF) and Mean Time To Repair (MTTR) are metrics related to the reliability and repair times of systems but do not specifically pertain to disaster recovery time frames. Recovery Point Objective (RPO) describes the acceptable amount of data loss measured in time, not the restoration of operations.

QUESTION 164
A technician is attempting to resolve an issue with a file server that is unable to download a file Given the following output:

```
root@server:~$ ls -Z /var/www/html/file
-rw-r--r--  root  root  unconfined_u:object_r:samba_share_t:s0  /var/www/html/file
```

Which of the following would best allow this file to be read?

A. chown
B. sestatus
C. setenforce
D. getenforce
E. chmod

Correct Answer: E
Section:
Explanation:
The given output in the image indicates that the file is present, but the permissions may not allow it to be read. The output indicates '-rw-------', which means that the file is set to be readable and writable by the owner only, with no permissions for group or others. To allow the file to be read by users other than the owner, the file's permissions will need to be changed. The chmod (change mode) command is used to change the file's permissions in Linux. For example, chmod 644 file would change the permissions of the file to be readable by everyone and writable by the owner, which is typically what's required for a file server. It is always recommended to apply the least permissive settings that still allow the required operation to maintain security.

QUESTION 165
A virtual host has four NICs and eight VMs. Which of the following should the technician configure to enable uplink redundancy?

A. VM
B. vNIC
C. vSwitch
D. vCPU
E. vHBA

Correct Answer: C
Section:
Explanation:
Uplink redundancy is a method used to ensure that if one physical network interface card (NIC) fails, the network connectivity for the virtual machines (VMs) does not go down. This is typically achieved by configuring multiple NICs to connect to a single virtual switch (vSwitch) and setting up NIC teaming or bonding. The vSwitch manages the internal network traffic between the VMs and the outside network by using the physical NICs assigned to it. By configuring the vSwitch with multiple NICs, you can create redundancy, so if one NIC fails, the other NICs can take over the traffic, ensuring continuous network connectivity.

QUESTION 166
A technician is configuring a server rack that will hold ten blade servers. Which of the following safety concerns should be observed? (Select three).

A. Floor load limitations
B. Rack balancing
C. Proper lifting techniques
D. Power connector type
E. KVM placement
F. Cable management
G. UPS power requirements
H. PDU installation
I. Separate circuits for power

Correct Answer: A, B, C
Section:
Explanation:
When configuring a server rack, it's important to consider:
A) Floor load limitations: Server racks can be extremely heavy, especially when filled with equipment like blade servers. It is crucial to ensure that the floor can handle the load to avoid structural damage or failure.
B) Rack balancing: Properly distributing the weight in a server rack is important for stability. Heavier equipment should generally be placed at the bottom to prevent the rack from becoming top-heavy and risking a tip-over.
C) Proper lifting techniques: Using correct lifting techniques when placing servers into a rack is vital to prevent personal injury.

QUESTION 167
A new company policy requires that any data loss in excess of one hour is unacceptable in the event of a disaster. Which of the following concepts is being referred to in this policy?

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

Correct Answer: C
Section:
Explanation:
The Recovery Point Objective (RPO) refers to the maximum tolerable period in which data might be lost from an IT service due to a major incident. The policy mentioned in the question highlights that data loss exceeding one hour is unacceptable, directly relating to the RPO concept. RPO is critical in disaster recovery and business continuity planning, indicating the age of the files that must be recovered from backup storage for normal operations to resume without significant losses. MTTR (Mean Time To Repair), RTO (Recovery Time Objective), and MTBF (Mean Time Between Failures) are related concepts but do not specifically address the amount of data loss that can be tolerated.

QUESTION 168
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) connectors are used in high-density, high-speed networking solutions such as 40 Gigabit Ethernet (40GbE) interfaces. When upgrading a server's network to 40Gbps, QSFP+ is the appropriate choice due to its capability to support such high-speed data transfer rates. 10 GigE, SFP, and SFP+ connectors are used for lower speed connections (10Gbps and below for SFP+ and 10 GigE, and even less for SFP), making them unsuitable for a 40Gbps network upgrade.

QUESTION 169
Which of the following should a technician verify first before decommissioning and wiping a file server?

A. The media destruction method
B. The recycling policy
C. Asset management documentation
D. Document retention policy

Correct Answer: C

Section:
Explanation:
Before decommissioning and wiping a file server, it's crucial to verify the asset management documentation. This documentation provides detailed records of the server's lifecycle, including procurement, usage, maintenance, and decommissioning information. Ensuring that asset management documentation is up-to-date and accurate is essential before proceeding with the server's decommissioning to maintain proper inventory control, comply with regulatory and organizational policies, and facilitate any potential audits. While the media destruction method, recycling policy, and document retention policy are important considerations in the decommissioning process, verifying asset management documentation is the first step to ensure the server is correctly identified and accounted for in the organization's asset registry.

QUESTION 170
Which of the following types of physical security controls would most likely be a target of a social engineering attack?

A. A security guard
B. An access control vestibule
C. Perimeter fencing
D. Biometric locks
E. Bollards

Correct Answer: A
Section:
Explanation:
A security guard is a human element in physical security, making them susceptible to social engineering attacks. Social engineering exploits human behavior, and a guard can be tricked into allowing unauthorized access through persuasion, manipulation, or deception.
Security guard (Answer A): Human elements are the most vulnerable to social engineering techniques like impersonation or manipulation.
Access control vestibule (Option B): This is a physical security barrier, which is harder to exploit through social engineering.
Perimeter fencing (Option C): This is a static physical barrier, not susceptible to social engineering.
Biometric locks (Option D): These rely on biological data and are not susceptible to social engineering in the same way a human would be.
Bollards (Option E): Physical barriers that are not vulnerable to social engineering.
CompTIA Server+
Reference:
This topic relates to SK0-005 Objective 4.4: Implement physical security controls.

QUESTION 171
Which of the following factors would most likely impact the selection of an organization's cloud provider?

A. Industry standards
B. Government regulations
C. Company policy
D. Organizational procedures

Correct Answer: B
Section:
Explanation:
Government regulations often dictate the legal requirements for data storage, privacy, and security, which can greatly impact the selection of a cloud provider. Compliance with regulations like GDPR, HIPAA, or other local laws is critical when choosing a cloud provider to avoid legal repercussions.
Government regulations (Answer B): Cloud providers must comply with legal and regulatory requirements, making this a significant factor in provider selection.
Industry standards (Option A): While important, standards can be more flexible and are often not legally binding.
Company policy (Option C): Internal policies are important but usually stem from the need to comply with regulations.
Organizational procedures (Option D): Procedures help guide operations but don't typically dictate the choice of cloud providers.
CompTIA Server+

Reference:
This topic is covered under SK0-005 Objective 1.6: Explain the importance of cloud-based concepts and services.

QUESTION 172
A bad actor leaves a USB drive with malicious code on it in a company's parking lot. Which of the following describes this scenario?

A. Hacking
B. Insider threat
C. Phishing
D. Social engineering

Correct Answer: D
Section:
Explanation:
Leaving a USB drive in a company parking lot is a classic example of social engineering, where the bad actor relies on human curiosity to prompt someone to pick up the USB drive and insert it into their computer, potentially infecting the system with malicious code.
Social engineering (Answer D): The attacker manipulates human behavior (in this case, curiosity) to exploit security weaknesses.
Hacking (Option A): Hacking refers to directly breaching security systems or exploiting software vulnerabilities, not manipulating humans.
Insider threat (Option B): This involves a legitimate insider within the organization carrying out malicious activities, which isn't the case here.
Phishing (Option C): Phishing typically involves emails or messages designed to deceive individuals into providing sensitive information.
CompTIA Server+
Reference:
This topic is covered under SK0-005 Objective 4.2: Explain server security concepts and best practices.

QUESTION 173
Which of the following describes when a site is considered a warm site?

A. It has basic technical facilities connected to it.
B. It has faulty air conditioning that is awaiting service.
C. It is almost ready to take over all operations from the primary site.
D. It is fully operational and continuously providing services.

Correct Answer: C
Section:
Explanation:
A warm site is a backup location that has partial infrastructure ready to support operations in the event of a failure at the primary site. It is almost ready to take over but requires some configuration or installation of data backups and software before it can become fully operational.
Warm site (Answer C): This site has the necessary equipment but requires some setup, making it a middle ground between cold and hot sites.
Basic technical facilities (Option A): This more accurately describes a cold site.
Faulty air conditioning (Option B): This is irrelevant to the definition of a warm site.
Fully operational (Option D): This describes a hot site, which is continuously ready to provide full services.
CompTIA Server+
Reference:
This topic is related to SK0-005 Objective 4.1: Summarize disaster recovery methods and concepts.

QUESTION 174
Which of the following would allow a server administrator to ensure all maximum available resources are being utilized?

A. Overprovisioning
B. Scalability
C. Thin clients
D. Resource Monitor

Correct Answer: D
Section:
Explanation:
Resource Monitor is a tool that allows administrators to monitor the system's CPU, memory, disk, and network usage in real-time, ensuring that maximum resources are being efficiently utilized.
Resource Monitor (Answer D): This tool provides real-time insights into resource utilization and can help ensure resources are not under- or over-utilized.
Overprovisioning (Option A): Refers to allocating more resources than physically available but doesn't directly monitor resource usage.
Scalability (Option B): Refers to the ability to increase or decrease resources based on demand.
Thin clients (Option C): Refer to lightweight computers that depend on servers for processing power, unrelated to resource utilization monitoring.
CompTIA Server+
Reference:
This topic is related to SK0-005 Objective 2.4: Monitor server performance.