CompTIA

Exam Questions SK0-005

CompTIA Server+ Certification Exam

NEW QUESTION 1
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

Answer: A

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.

NEW QUESTION 2
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 haveaccess without granting excessive access to others?

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

Answer: C

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

NEW QUESTION 3
A systems administrator is performing maintenance on 12 Windows servers that are in different racks at a large datacenter. Which of the following would allow the administrator to perform maintenance on all 12 servers without having to physically be at each server? (Choose two.)

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

Answer: AB

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

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

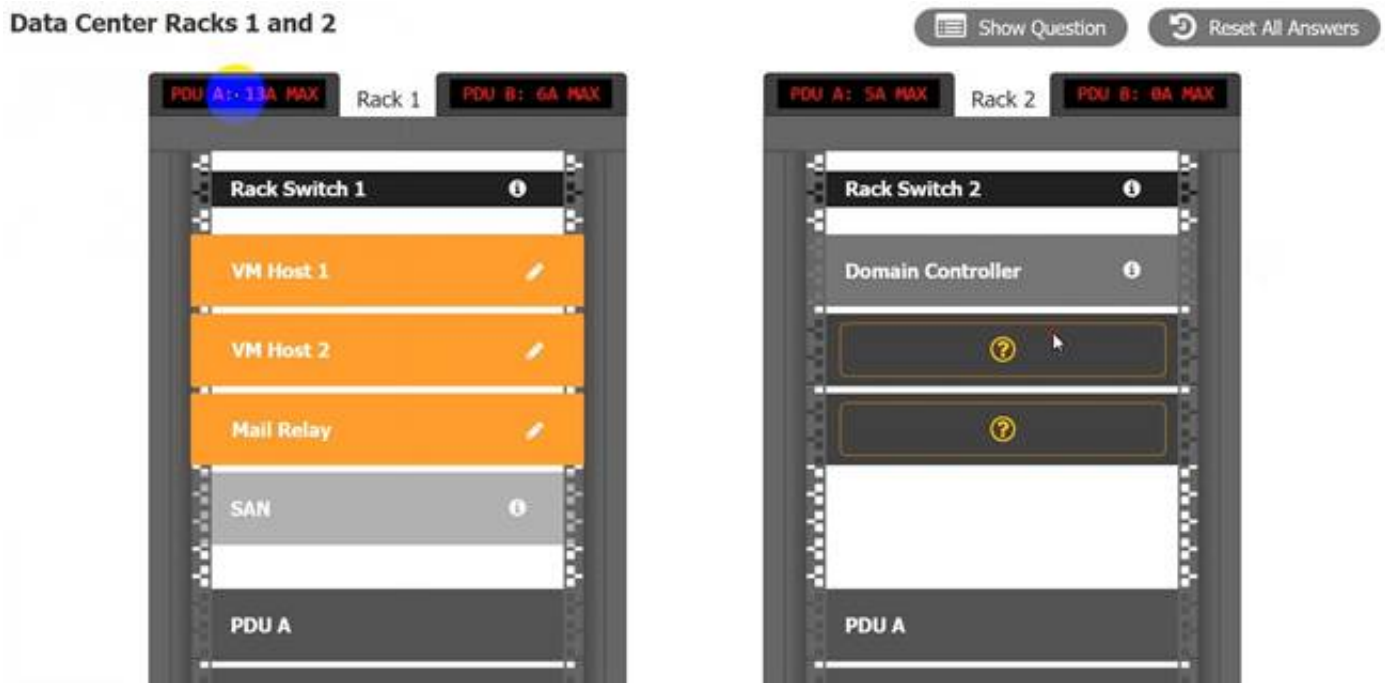
A. RAID 1
B. RAID 5
C. RAID 6
D. RAID 10

Answer: B

Explanation:
RAID 5 is a RAID level that uses disk striping with parity. It requires a minimum of three disks and can handle one disk failure. RAID 5 distributes the parity information across all the disks in the array, which improves the read performance and reduces the write penalty. The capacity of a RAID 5 array is (N-1) times the

size of the smallest disk, where N is the number of disks in the array. Therefore, for six 4TB disks, the capacity of a RAID 5 array would be (6-1) x 4TB = 20TB, which meets the minimum disk space requirement of 19TB. RAID 5 also has the leastamount of disk space lost to RAID overhead among the options, as it only uses onedisk's worth of space for parity

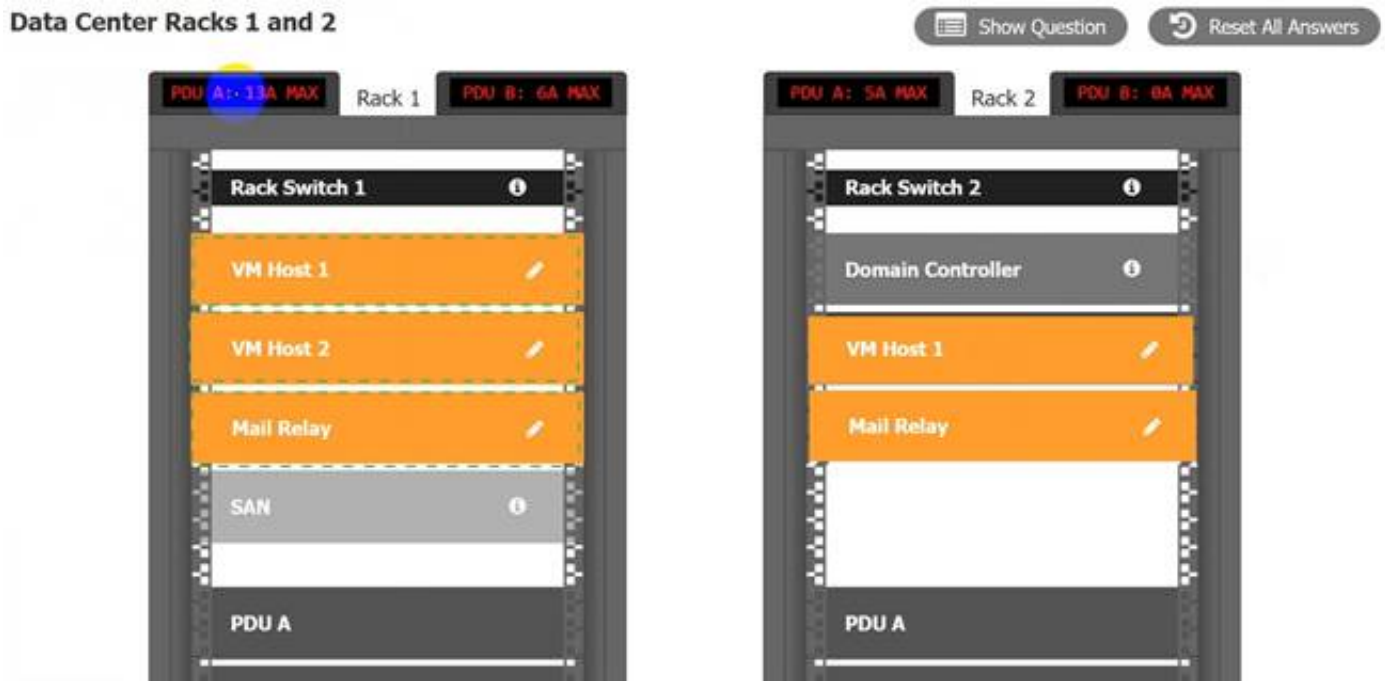
NEW QUESTION 5
DRAG DROP
A recent power Outage caused email services to go down. A sever administrator also received alerts from the datacenter's UPS.
After some investigation, the server administrator learned that each POU was rated at a maximum Of 12A.
INSTRUCTIONS
Ensure power redundancy is implemented throughout each rack and UPS alarms are resolved. Ensure the maximum potential PDU consumption does not exceed 80% or 9.6A).
* a. PDU selections must be changed using the pencil icon.
* b. VM Hosts 1 and 2 and Mail Relay can be moved between racks.
* c. Certain devices contain additional details



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 6
The management team has mandated the use of data-at-rest encryption for all data. Which of the following forms of encryption best achieves this goal?

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

Answer: A

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

NEW QUESTION 7
Alter rack mounting a server, a technician must install four network cables and two power cables for the server. Which of the following is the MOST appropriate way to complete this task?

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

Answer: B

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

NEW QUESTION 8
A systems administrator is setting up a new server that will be used as a DHCP server. The administrator installs the OS but is then unable to log on using Active Directory credentials. The administrator logs on using the local administrator account and verifies the server has the correct IP address, subnet mask, and default gateway. The administrator then gets on another server and can ping the new server. Which of the following is causing the issue?

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

Answer: D

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

NEW QUESTION 9
Which of the following backup types resets the archive bit each time it is run?

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

Answer: C

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.References: https://www.comptia.org/training/resources/exam- objectives/comptia-server-sk0-005-exam-objectives (Objective 3.1)

NEW QUESTION 10
A server administrator is currently working on an incident. Which of the following steps should the administrator perform before resolving the issue?

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

Answer: C

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

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

NEW QUESTION 10
A technician is laying out a filesystem on a new Linux server. Which of the following tools would work BEST to allow the technician to increase a partition's size in the future without reformatting it?

A. LVM
B. DiskPart
C. fdisk
D. Format

Answer: A

Explanation:
LVM (Logical Volume Manager) is a tool that allows the technician to increase a partition's size in the future without reformatting it on a Linux server. LVM creates logical volumes that can span across multiple physical disks or partitions and can be resized dynamically without losing data. LVM also provides other features such as snapshots, encryption, and RAID. DiskPart, fdisk, and Format are tools that can be used to partition and format disks, but they do not allow increasing a partition's size without reformatting it. References: https://www.howtogeek.com/howto/40702/how-to-manage-and- use-lvm-logical-volume-management-in-ubuntu/ https://www.howtogeek.com/school/using- windows-admin-tools-like-a-pro/lesson2/https://www.howtogeek.com/howto/17001/how-to- format-a-usb-drive-in-ubuntu-using-gparted/

NEW QUESTION 14
Following a recent power outage, a server in the datacenter has been constantly going offline and losing its configuration. Users have been experiencing access issues while using the application on the server. The server technician notices the data and time are incorrect when the server is online. All other servers are working. Which of the following would MOST likely cause this issue? (Choose two.)

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

Answer: BF

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

NEW QUESTION 19
Hackers recently targeted a company with an attack that resulted in a system breach, which compromised the organization's data. Because of the system breach, the administrator had to bypass normal change management procedures. Which of the following change management activities was necessary?

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

Answer: C

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

NEW QUESTION 23
Users have noticed a server is performing below Baseline expectations. While diagnosing me server, an administrator discovers disk drive performance has degraded. The administrator checks the diagnostics on the RAID controller and sees the battery on me controller has gone bad. Which of the following is causing the poor performance on the RAID array?

A. The controller has disabled the write cache.
B. The controller cannot use all the available channels.
C. The drive array is corrupt.
D. The controller has lost its configuration.

Answer: A

Explanation:
The write cache is a feature of some RAID controllers that allows them to temporarily store data in a fast memory buffer before writing it to the disk drives. This improves the performance and efficiency of write operations, especially for random and small writes. However, if the battery on the controller goes bad, the controller may disable the write cache to prevent data loss in case of a power failure. This can degrade the disk drive performance significantly, as every write operation will have to wait for the disk drives to complete. References: https://www.dell.com/support/kbdoc/en-us/000131486/understanding-raid-controller-battery-

learn-cyclehttps://www.techrepublic.com/article/understanding-raid-controller-write-cache/

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

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

Answer: B

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 third-party 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.

NEW QUESTION 28
A server technician is installing a new server OS on legacy server hardware. Which of the following should the technician do FIRST to ensure the OS will work as intended?

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

Answer: A

Explanation:
The first thing that the technician should do before installing a new server OS on legacy server hardware is to consult the HCL (Hardware Compatibility List) to ensure everything is supported. The HCL is a list of hardware devices and components that are tested and certified to work with a specific OS or software product. The HCL helps to avoid compatibility issues and performance problems that may arise from using unsupported or incompatible hardware. Migrating the physical server to a virtual server may be a good option to improve scalability and flexibility, but it requires additional hardware and software resources and may not be feasible for legacy server hardware. Low-level formatting the hard drives may be a good practice to erase any old data and prepare the drives for a new OS installation, but it does not guarantee that the hardware will work with the new OS. Making sure the case and the fans are free from dust may be a good practice to ensure proper cooling and prevent overheating, but it does not guarantee that the hardware will work with the new OS. References:
https://www.howtogeek.com/190014/virtualization- basics-understanding-techniques-and-fundamentals/ https://www.howtogeek.com/173353/how-to-low-level-format-or-write-zeros-to-a-hard- drive/https://www.howtogeek.com/303282/how-to-manage-your-pcs-fans-for-optimal- airflow-and-cooling/

NEW QUESTION 33
After configuring IP networking on a newly commissioned server, a server administrator installs a straight- through network cable from the patch panel to the switch. The administrator then returns to the server to test network connectivity using the ping command. The partial output of the ping and ipconfig commands are displayed below:

```
ipconfig/all

IPv4 address: 192.168.1.5
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: Request timed out
Reply from 192.168.1.2: Request timed out
Reply from 192.168.1.2: Request timed out
Reply from 192.168.1.2: Request timed out
```

The administrator returns to the switch and notices an amber link light on the port where the server is connected. Which of the following is the MOST likely reason for the lack of network connectivity?

A. Network port security
B. An improper VLAN configuration
C. A misconfigured DHCP server
D. A misconfigured NIC on the server

Answer: D

Explanation:
A misconfigured NIC on the server is the most likely reason for the lack of network connectivity. The output of the ping command shows that the server is unable to reach its default gateway (10.0.0.1) or any other IP address on the network. The output of the ipconfig command shows that the server has a valid IP address (10.0.0.10) and subnet mask (255.255.255.0) but no default gateway configured. This indicates that there is a problem with the NIC settings on the server, such as an incorrect IP address, subnet mask, default gateway, DNS server, etc. A misconfigured NIC can also cause an amber link light on the switch port, which indicates a speed or duplex mismatch between the NIC and the switch.

NEW QUESTION 34

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

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

Answer: B

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

NEW QUESTION 37
Users at a company work with highly sensitive data. The security department implemented an administrative and technical control to enforce least-privilege access assigned to files. However, the security department has discovered unauthorized data exfiltration. Which of the following is the BEST way to protect the data from leaking?

A. Utilize privacy screens.
B. Implement disk quotas.
C. Install a DLP solution.
D. Enforce the lock-screen feature.

Answer: C

Explanation:
Components of a Data Loss Solution Reference:https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/
The best way to protect the data from leaking is to install a DLP solution. A DLP (Data Loss Prevention) solution is a software that helps businesses prevent confidential data from being leaked or stolen by unauthorized parties. A DLP solution can identify, monitor, and protect data as it moves across networks and devices, such as endpoints, email, web, cloud applications, or removable media. A DLP solution can also enforce security policies based on content and context for data in use, in motion, and at rest. A DLP solution can detect and prevent data breaches by using various techniques, such as content inspection, contextual analysis, encryption, blocking, alerting, warning, quarantining, or other remediation actions.

NEW QUESTION 41
A server administrator is completing an OS installation for a new server. The administrator patches the server with the latest vendor-suggested software, configures DHCP, and verifies all network cables are properly connected in the IDF, but there is no network connectivity. Which of the following is the MOST likely reason for the lack of connectivity?

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

Answer: A

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

NEW QUESTION 46
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

Answer: D

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 References: [Data in transit], [Encryption]

NEW QUESTION 51

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

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

Answer: D

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

NEW QUESTION 52
A company wants to find an affordable way to simulate a fail over of a critical application. The company does not currently have a solution for it. The application consists of 15 servers, and the company would like to simulate on production configurations and IP address schemes. Which of the following would be the most cost-effective solution?

A. Build a warm site and perform a fail over of the application.
B. Build a cloud laaS and perform a fail over of the application.
C. Build a hot site and perform a fail over of the application.
D. Build a cold site and perform a fail over of the application.
E. Perform a tabletop fail over of the application.

Answer: B

Explanation:
Cloud IaaS (Infrastructure as a Service) is a service model that allows users to rent virtualized computing resources over the internet, such as servers, storage, network, and software. Cloud IaaS can provide several benefits for disaster recovery and failover scenarios, such as:
? Lower cost: Cloud IaaS can reduce the capital and operational expenses of
building and maintaining a physical disaster recovery site, asusers only pay for the resources they use on demand12.
? Scalability: Cloud IaaS can offer flexible and elastic scalability of resources, as
users can easily provision or deprovision resources according to their needs and workload12.
? Availability: Cloud IaaS can ensure high availability and reliability of the
application, as users can leverage the cloud provider's redundant and geographically distributed infrastructure12.
? Simplicity:Cloud IaaS can simplify the failover process, as users can use the cloud provider's tools and services to automate and orchestrate the failover operations12.
Therefore, building a cloud IaaS and performing a failover of the application would be the most cost-effective solution for the company, as it would allow them to simulate a failover of a critical application on production configurations and IP address schemes without investing in a physical disaster recovery site.

NEW QUESTION 54
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.

Answer: BC

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

NEW QUESTION 55
A technician recently replaced a NIC that was not functioning. Since then, no device driver is found when starting the server, and the network card is not functioning. Which of the following should the technician check first?

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

Answer: C

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

NEW QUESTION 58

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

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

Answer: D

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

NEW QUESTION 61
A server administrator wants to ensure a storage array can survive the failure of two drives without the loss of data. Which of the following RAID levels should the administrator choose?

A. 1
B. 5
C. 6

Answer: D

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

NEW QUESTION 64
A technician is attempting to update a server's firmware. After inserting the media for the firmware and restarting the server, the machine starts normally into the OS. Which of the following should the technician do NEXT to install the firmware?

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

Answer: B

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

NEW QUESTION 65
An analyst is planning a new point-to-point Ethernet connection between a university campus and a newly acquired space downtown that is about 5mi (8km) away. The analyst would like the fastest possible connection speed. Which of the following would best meet the analyst's needs?

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

Answer: A

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

NEW QUESTION 70
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 thedatabasefrom 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.

Answer: C

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

NEW QUESTION 71
A company is building a new datacenter next to a busy parking lot. Which of the following is the BEST strategy to ensure wayward vehicle traffic does not interfere with datacenter operations?

A. Install security cameras
B. Utilize security guards
C. Install bollards
D. Install a mantrap

Answer: C

Explanation:
The best strategy to ensure wayward vehicle traffic does not interfere with datacenter operations is to install bollards. Bollards are sturdy posts that are installed around a perimeter to prevent vehicles from entering or crashing into a protected area. Bollards can provide physical security and deterrence for datacenters that are located near busy roads or parking lots. Bollards can also prevent accidental damage or injury caused by vehicles that lose control or have faulty brakes.

NEW QUESTION 73
An administrator has been asked to deploy a database server that provides the highest performance with fault tolerance. Which of the following RAID levels will fulfill this request?

A. RAIDO
B. RAID1
C. RAID 5
D. RAID 6
E. RAID 10

Answer: E

Explanation:
RAID 10 is the best option to deploy a database server that provides the highest performance with fault tolerance. RAID 10 is a type of RAID level that combines RAID 1 (mirroring) and RAID 0 (striping) to create an array of mirrored stripes. RAID 10 offers high performance by distributing data across multiple disks in parallel (striping), which improves read/write speed and I/O operations. RAID 10 also offers fault tolerance by duplicating data across two or more disks in each stripe (mirroring), which provides redundancy and data protection in case of disk failure. RAID 10 requires at least four disks to implement and has a high storage overhead, as half of the disk space is used for mirroring. References: [CompTIA Server+ Certification Exam Objectives]

NEW QUESTION 76
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

Answer: C

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.References:https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html

NEW QUESTION 79
A company needs to increase the security controls on its servers. Anadministrator is implementing MFA on all servers using cost effective techniques. Which of the following should the administrator use to satisfy the MFA requirement?

A. Biometrics
B. Push notifications
C. Smart carts
D. Physical tokens

Answer: B

Explanation:
Push notifications are messages that are sent from an application or a service to a user's device without requiring the user to open or request them. They can be used as a cost- effective technique for implementing MFA (Multi-Factor Authentication) on servers by sending verification codes or approval requests to the user's

smartphone or tablet when they try to log in to the server. Verified References: [Push notifications], [MFA]

NEW QUESTION 81
A technician is connecting a Linux server to a share on a NAS. Which of the following is the MOST appropriate native protocol to use for this task?

A. CIFS
B. FTP
C. SFTP
D. NFS

Answer: D

Explanation:
The most appropriate native protocol to use for connecting a Linux server to a share on a NAS is NFS. NFS (Network File System) is a protocol that allows file sharing and remote access over a network. NFS is designed for Unix-like operating systems, suchas Linux, and supports features such as symbolic links, hard links, file locking, and file permissions. NFS uses mount points to attach remote file systems to local file systems, making them appear as if they are part of the local file system. NFS can provide fast and reliable access to files stored on a NAS (Network Attached Storage), which is a device that provides centralized storage for network devices.

NEW QUESTION 86
A technician has received multiple reports of issues with a server. The server occasionally has a BSOD, powers off unexpectedly, and has fans that run continuously. Which of the following BEST represents what the technician should investigate during troubleshooting?

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

Answer: B

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

NEW QUESTION 89
A technician is connecting a server's secondary NIC to a separate network. The technician connects the cable to the switch but then does not see any link lights on the NIC. The technician confirms there is nothing wrong on the network or with the physical connection. Which of the following should the technician perform NEXT?

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

Answer: C

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

NEW QUESTION 90
Which of the following symbols is used to write a text description per line within a PowerShell script?

A. %
B. @
C. &
D. #

Answer: D

Explanation:
The # symbol is used to write a text description per line within a PowerShell script. A text description is also known as a comment, which is a line of code that is ignored by the PowerShell interpreter and serves as documentation or explanation for human readers. The # symbol indicates that everything following it on the same line is a comment and not part of the script commands or expressions. For example:
This is a comment in PowerShellWrite-Host "Hello World" # This command prints Hello World to the console
References: CompTIA Server+ Certification Exam Objectives, Domain 6.0: Troubleshooting, Objective 6.3: Given a scenario, troubleshoot scripting errors using PowerShell commands.

NEW QUESTION 91
A server administrator wants to run a performance monitor for optimal system utilization. Which of the following metrics can the administrator use for monitoring? (Choose two.)

A. Memory
B. Page file

C. Services
D. Application
E. CPU
F. Heartbeat

Answer: AE

Explanation:
Memory and CPU are two metrics that can be used for monitoring system utilization. Memory refers to the amount of RAM that is available and used by the system and its processes. CPU refers to the percentage of processor time that is consumed by the system and its processes. Both memory and CPU can affect the performance and responsiveness of the system and its applications. Monitoring memory and CPU can help identify bottlenecks, resource contention, memory leaks, high load, etc.

NEW QUESTION 96
A server administrator noticesthe/var/log/audit/audit.logfileon a Linux server is rotating loo frequently. The administrator would like to decrease the number of times the leg rotates without losing any of the information in the logs. Which of the following should the administrator configure?

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

Answer: A

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

NEW QUESTION 101
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

Answer: B

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.References:https://azure.microsoft.com/en-us/overview/what-is-hybrid-cloud- computing/

NEW QUESTION 105
A senior administrator instructs a technician to run the following script on a Linux server: for i in {1..65536); do echo Si; telnet localhost $i; done
The script mostly returns the following message: Connection refused. However, there are several entries in the console display that look like this:
80
Connected to localhost 443
Connected to localhost
Which of the following actions should the technician perform NEXT?

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

Answer: A

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

NEW QUESTION 110
A company wants to deploy software to all users, Out very few of men will be using the software at any one point in time. Which of the following licensing models

would be BEST lot the company?

A. Per site
B. Per concurrent user
C. Per core
D. Per instance

Answer: B

Explanation:
Per concurrent user licensing is a model that allows a fixed number of users to access the software at any one point in time. This model is best for the company that wants to deploy software to all users, but very few of them will be using the software at any one point in time. This way, the company can save money by paying only for the number of simultaneous users, rather than for every user who has access to the software. Per site licensing is a model that allows unlimited users within a specific location to use the software. Per core licensing is a model that charges based on the number of processor cores on the server where the software is installed. Per instance licensing is a model that charges based on the number of copies of the software running on different servers or virtual machines.References: https://www.pcmag.com/encyclopedia/term/concurrent-use-licensehttps://www.techopedia.com/definition/1440/software-licensing

NEW QUESTION 115
A VLAN needs to be configured within a virtual environment for a new VM. Which of the following will ensure the VM receives a correct IP address?

A. A virtual router
B. A host NIC
C. A VPN
D. A virtual switch
E. A vNIC

Answer: D

Explanation:
The correct answer is D. A virtual switch.
A virtual switch is a software-based network device that connects the virtual machines (VMs) in a virtual environment and allows them to communicate with each other and with the physical network. A virtual switch can also create and manage virtual LANs (VLANs), which are logical segments of a network that separate the traffic of different VMs or groups of VMs. A VLAN needs a DHCP server to assign IP addresses to the VMs that belong to it. A virtual switch can act as a DHCP relay agent and forward the DHCP requests from the VMs to the DHCP server on the physical network.This way, the VMs can receive correct IP addresses for their VLANs123
A virtual router is a software-based network device that routes packets between different networks or subnets. A virtual router can also create and manage VLANs, but it is not necessary for a VM to receive a correct IP address.A virtual router can be used to provide additional security, redundancy, or load balancing for the VMs12
A host NIC is a physical network interface card that connects the host machine to the physical network. A host NIC can also support VLAN tagging, which allows the host machine to communicate with different VLANs on the network. However, a host NIC alone cannot ensure that a VM receives a correct IP address for its VLAN.The host NIC needs to be connected to a virtual switch that can relay the DHCP requests from the VMs to the DHCP server12
A VPN is a virtual private network that creates a secure tunnel between two or more devices over the internet. A VPN can be used to encrypt and protect the data traffic of the VMs, but it is not related to the configuration of VLANs or IP addresses.A VPN does not affect how a VM receives a correct IP address for its VLAN14
A vNIC is a virtual network interface card that connects a VM to a virtual switch or a virtual router. A vNIC can also support VLAN tagging, which allows the VM to communicate with different VLANs on the network.However, a vNIC alone cannot ensure that a VM receives a correct IP address for its VLAN.The vNIC needs to be connected to a virtual switch or a virtual router that can relay the DHCP requests from the VMs to the DHCP server12

NEW QUESTION 117
A technician has moved a data drive from a new Windows server to an order Windows server. The hardware recognizes the drive, but the data is not visible to the OS. Which of the following is the MOST Likely cause of the issue?

A. Thedisk uses GPT.
B. Thepartition is formatted with ext4.
C. The -partition is formatted with FAT32.
D. Thedisk uses MBn.

Answer: A

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. However, GPT is not compatible with older versions of Windows, such as Windows XP or Windows Server 2003, which use MBR (Master Boot Record) as the partitioning scheme. If a disk uses GPT, it may not be recognized or accessible by an older Windows server. Verified References: [GPT], [MBR]

NEW QUESTION 121
A user can successfully connect to a database server from a home office but is unable to access it from a hotel room. Which of the following authentication methods is most likely
configured?

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

Answer: D

Explanation:
Scope-based authentication is a method of restricting access to resources based on the location, network, or device of the user. It can be used to prevent unauthorized access from outside the organization’s network or from untrusted devices. In this case, the user can connect to the database server from the home office, which is likely within the scope of the authentication policy, but not from the hotel room, which is outside the scope.

References:
CompTIA Server+ Certification Exam Objectives1, page 15 CompTIA Server+: Authentication & Authorization2

NEW QUESTION 123
An administrator has been asked to increase the storage capacity of a stand-alone file server but no further expansion slots are available. Whichof the following would be the FASTEST solution to implement with no downtime?

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

Answer: D

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

NEW QUESTION 125
A remote, embedded loT server is having a Linux OS upgrade installed. Which of the following is the best method to stage the new media for the default boot device of the server?

A. Copy and send an SSD to the site.
B. Copy and send a DVD to the site.
C. Copy and send a SATA drive to the site.
D. Copy and send a microSD card to the site.

Answer: D

Explanation:
A microSD card is the best method to stage the new media for the default boot device of a remote embedded IoT server that is having a Linux OS upgrade installed. A microSD card is a small and portable storage device that can store large amounts of data. It can be easily inserted into the slot of an embedded IoT server, which is a small and low-power device that performs specific tasks and connects to other devices over a network. A microSD card can also be formatted with different file systems, such as FAT32 or ext4, which are compatible with Linux OS. References: CompTIA Server+ Certification Exam Objectives, Domain 4.0: Networking, Objective 4.3: Given a scenario, configure servers for IoT applications.

NEW QUESTION 130
Due to a recent application migration, a company's current storage solution does not meet the necessary requirements tor hosting data without impacting performance when the data is accessed in real time by multiple users. Which of the following is the BEST solution for this Issue?

A. Install local external hard drives for affected users.
B. Add extra memory to the server where data is stored.
C. Compress the data to increase available space.
D. Deploy a new Fibre Channel SAN solution.

Answer: D

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

NEW QUESTION 132
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

Answer: A

Explanation:
Insider threat is the most likely system vulnerability in a company that deploys antivirus, anti-malware, 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.

NEW QUESTION 134
Which of the following would MOST likely be part of the user authentication process when implementing SAML across multiple applications?

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

Answer: A

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

NEW QUESTION 135
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

Answer: B

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.

NEW QUESTION 139
An administrator needs to disable root login over SSH. Which of the following tiles should be edited to complete this task?

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

Answer: B

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

NEW QUESTION 141
A newly installed server is accessible to local users, but remote users are unable to connect. Which of the following is MOST likely misconfigured?

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

Answer: B

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

NEW QUESTION 143
A company is reviewing options for its current disaster recovery plan and potential changes to it. The security team will not allow customer data to egress to non-company equipment, and the company has requested recovery in the shortest possible time. Which of the following will BEST meet these goals?

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

Answer: B

Explanation:

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

NEW QUESTION 147
A user has been unable to authenticate to the company's external, web-based database after clicking a link in an email that required the user to change the account password. Which of the following steps should the company take next?

A. Disable the user's account and inform the security team.
B. Create a new log-in to the external database.
C. Ask the user to use the link again to reset the password.
D. Reset the user's password and ask the user to log in again.

Answer: A

Explanation:
The user has likely fallen victim to a phishing scam, which is a fraudulent attempt to obtain sensitive information, such as passwords, by disguising as a legitimate entity. The link in the email that required the user to change the account password was probably a fake website that mimicked the company’s external database, and captured the user’s credentials when they entered them. This could compromise the security and integrity of the company’s data, as well as the user’s identity and privacy12.
The company should take immediate action to prevent further damage and investigate the incident. The first step is to disable the user’s account and inform the security team. Disabling the user’s account can prevent unauthorized access to the external database by the attackers, who may use the stolen credentials to log in and manipulate or steal data. Informing the security team can alert them of the breach and allow them to take appropriate measures, such as scanning for malware, changingpasswords, notifying other users, and reporting the incident34.

NEW QUESTION 148
Due to a disaster incident on a primary site, corporate users are redirected to cloud services where they will be required to be authenticated just once in order to use all cloud services.
Which of the following types of authentications is described in this scenario?

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

Answer: D

NEW QUESTION 149
A staff memberwho 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

Answer: A

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

NEW QUESTION 152
A systems administrator needs to back up changes made to a data store on a daily basis during a short time frame. The administrator wants to maximize RTO when restoring data. Which of the following backup methodologies would best fit this scenario?

A. Off-site backups
B. Full backups
C. Differential backups
D. Incremental backups

Answer: D

Explanation:
An incremental backup is a backup method that only backs up the files that have changed since the last backup, whether it was a full or an incremental backup. An incremental backup can save disk space and time, as it only copies the new or modified data. An incremental backup can also improve the RTO (Recovery Time Objective), which is the maximum acceptable time to restore data after a disaster. This is because an incremental backup can restore data faster than a full or a differential backup, as it only needs to apply the latest changes to the previous backup1.

NEW QUESTION 156
A technician recently upgraded several pieces of firmware on a server. Ever since the technician rebooted the server, it no longer communicates with the network. Which of the following should the technician do FIRST to return the server to service as soon as possible?

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

Answer: D

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

NEW QUESTION 161
A server administrator purchased a single license key to use for all the new servers that will be imaged this year. Which of the following MOST likely refers to the licensing type that will be used?

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

Answer: D

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

NEW QUESTION 163
Which of the following steps in the troubleshooting theory should be performed after a solution has been implemented? (Choose two.)

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

Answer: CF

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

NEW QUESTION 166
A server administrator receives a report that Ann, a new user, is unable to save a file to her home directory on a server. The administrator checks Ann's home directory permissions and discovers the following:
dr-xr-xr-- /home/Ann
Which of the following commands should the administrator use to resolve the issue without granting unnecessary permissions?

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

Answer: D

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

Reference:
https://linuxize.com/post/what-does-chmod-777-mean/

NEW QUESTION 170
A company created a new DR plan. The management team would like to begin performing a review of this plan without endangering company data and with a minimal time commitment. Which of the following testing methods would best allow for this type of review?

A. Simulated
B. Tabletop
C. Live
D. Non-production

Answer: B

Explanation:
Tabletop testing is a method of reviewing a DR plan without endangering company data and with a minimal time commitment. Tabletop testing involves a simulated scenario where the participants discuss their roles and responsibilities, identify potential issues, and evaluate the effectiveness of the plan. Simulated, live, and non-production testing are methods that involve more time and resources, and may pose some risks to company data. References: [CompTIA Server+ Certification Exam Objectives], Domain 6.0: Disaster Recovery, Objective 6.3: Compare and contrast various backup techniques.

NEW QUESTION 175
A server administrator is configuring the IP address on a newly provisioned server in the testing environment. The network VLANs are configured as follows:

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

The administrator configures the IP address for the new server as follows: IP address: 192.168.1.1/24
Default gateway: 192.168.10.1
A ping sent to the default gateway is not successful. Which of the following IP address/default gateway combinations should the administrator have used for the new server?

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

Answer: A

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

NEW QUESTION 177
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

Answer: A

Explanation:
A SD card is a type of flash memory card that can be used to store data and run applications. A SD card can be used to install a Type 1 hypervisor on a server, as it provides fast boot time, low power consumption, and high reliability. A Type 1 hypervisor runs directly on the underlying computer's physical hardware, interacting directly with its CPU, memory, and physical storage. For this reason, Type 1 hypervisors are also referred to as bare-metal hypervisors. A Type 1 hypervisor takes the place of a host operating system and VM resources are scheduled directly to the hardware by the hypervisor123. A NAS drive (B) is a type of network-attached storage (NAS) device that provides shared access to files and data over a network. A NAS drive cannot be used to install a Type 1 hypervisor on a server, as it requires a network connection and a host operating system to function. A SATA drive © is a type of hard disk drive (HDD) or solid state drive (SSD) that uses the Serial ATA (SATA) interface to connect to a computer. A SATA drive can be used to install a Type 1 hypervisor on a server, but it may have some disadvantages compared to a SD card, such as slower boot time, higher power consumption, and lower reliability. A SAS drive (D) is a type of hard disk drive (HDD) or solid state drive (SSD) that uses the Serial Attached SCSI (SAS) interface to connect to a computer. A SAS drive can also be used to install a Type 1 hypervisor on a server, but it may have similar disadvantages as a SATA drive, and it may also be more expensive and less compatible than a SD card.References: 1 https://phoenixnap.com/kb/what-is-hypervisor-type-1-22
https://www.ibm.com/topics/hypervisors3 https://www.redhat.com/en/topics/virtualization/what-is-a-hypervisor

NEW QUESTION 180
A company's servers are all displaying the wrong time. The server administrator confirms the time source is correct. Which of the following is MOST likely preventing the servers from obtaining the correct time?

A. A firewall
B. An antivirus
C. AHIDS
D. User account control

Answer: A

Explanation:
The most likely cause of the servers displaying the wrong time is A. A firewall. A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predefined rules. A firewall can block or allow certain ports, protocols, or applications that are used for network communication. One of the protocols that is used for time synchronization is the Network Time Protocol (NTP), which requires the use of UDP port 123 for all time synchronization1. If a firewall blocks this port, it can prevent the servers from obtaining the correct time from the time source. Therefore, the server administrator should check the firewall settings and make sure that UDP port 123 is allowed for NTP traffic.

NEW QUESTION 183
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

Answer: C

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 References: [Rack layout], [Data center]

NEW QUESTION 188
A server in a remote datacenter is no longer responsive. Which of the following is the BEST solution to investigate this failure?

A. Remote desktop
B. Access via a crash cart
C. Out-of-band management
D. A Secure Shell connection

Answer: C

Explanation:
The best solution to investigate the failure of a server in a remote datacenter is out-of-band management. Out-of-band management is a method of accessing and controlling a server or a device using a dedicated channel that is separate from its normal network connection. Out-of-band management can use various technologies, such as serial ports, modems, KVM switches, or dedicated management cards or interfaces. Out- of-band management can provide remote access to servers or devices even when they are powered off, unresponsive, or disconnected from the network. Out-of-band management
can enable troubleshooting, configuration, maintenance, or recovery tasks without requiring physical presence at the server location.
Reference:
https://www.lantronix.com/wp-content/uploads/pdf/Data_Center_Mgmt_WP.pdf

NEW QUESTION 191
Which of thefollowinglicensing concepts is based on the number of logical processorsa serverhas?

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

Answer: A

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

NEW QUESTION 193
A technician has several possible solutions to a reported server issue. Which of the following BEST represents how the technician should proceed with troubleshooting?

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

Answer: C

Explanation:
This is the best way to proceed with troubleshooting when the technician has several possible solutions to a reported server issue. Making one change at a time and testing allows the technician to isolate the cause and effect of each solution and determine which one works best. It also helps to avoid introducing new problems or complicating existing ones by making multiple changes at once. Determining whether there is a common element in the symptoms causing multiple

problems is a good step to perform before identifying possible solutions, but not after. Performing a root cause analysis is a good step to perform after resolving the issue, but not during. Documenting the findings, actions, and outcomes throughout the process is a good practice to follow at every step of troubleshooting, but not a specific way to proceed with testing possible solutions. References: https://www.howtogeek.com/174288/how-to-tell-if-your-computer-is-overheating-and-what-to-do-about-it/https://www.howtogeek.com/428483/what-is-end-to- end-encryption-and-why-does-it-matter/

NEW QUESTION 195
A newly hired systems administrator is concerned about fileshare access at the company. The administrator turns on DLP for the fileshare and lets it propagate for a week. Which of the following can the administrator perform now?

A. Manage the fileshare from an RDP session.
B. Audit the permissions of the fileshare.
C. Audit the access to the physical fileshare.
D. Manage the permissions from the fileshare.

Answer: B

Explanation:
DLP, or Data Loss Prevention, is a type of security measure that aims to prevent unauthorized access, use, or transfer of sensitive data. DLP can be applied to various types of data, such as email, cloud storage, network traffic, or fileshares1. DLP for fileshares can help monitor and control who can access, modify, or share files on a network share2. By turning on DLP for the fileshare and letting it propagate for a week, the administrator can audit the permissions of the fileshare and see if there are any violations
or anomalies in the access patterns. This can help the administrator identify and remediate any potential risks or compliance issues related to the fileshare2. The other options are incorrect because they are not directly related to DLP for fileshares. Managing the fileshare from an RDP session or from the fileshare itself are administrative tasksthat do not require DLP. Auditing the access to the physical fileshare is a physical security measure that is not affected by DLP.

NEW QUESTION 197
An organization stores backup tapes of its servers at cold sites. The organization wants to ensure the tapes are properly maintained and usable during a DR scenario. Which of the following actions should the organization perform?

A. Have the facility inspect and inventory the tapes on a regular basis.
B. Have duplicate equipment available at the cold site.
C. Retrieve the tapes from the cold site and test them.
D. Use the test equipment at the cold site to read the tapes.

Answer: C

Explanation:
The organization should retrieve the tapes from the cold site and test them to ensure they are properly maintained and usable during a DR scenario. A cold site is a location that has space and power for backup equipment, but no actual equipment installed or configured. The organization stores backup tapes of its servers at cold sites as a precaution in case of a disaster that affects its primary site. However, backup tapes can degrade over time due to environmental factors such as temperature, humidity, dust, or magnetic fields. Therefore, the organization should periodically retrieve the tapes from the cold site and test them on compatible equipment to verify their integrity and readability. References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 6, Lesson 6.4, Objective 6.4

NEW QUESTION 198
The Chief Information Officer of a data center is concerned that transmissions from the building can be detected from the outside. Which of the following would resolve this concern? (Select TWO).

A. RFID
B. Proximity readers
C. Signal blocking
D. Camouflage
E. Reflective glass
F. Bollards

Answer: CD

Explanation:
Signal blocking is a technique that prevents or reduces the transmission of electromagnetic signals from a building to the outside. Signal blocking can be achieved by using materials that absorb, reflect, or scatter the signals, such as metal, concrete, or mesh. Signal blocking can protect the data center from eavesdropping, interference, or jamming by unauthorized parties1.
Camouflage is a technique that disguises or conceals the appearance of a building to make
it less noticeable or identifiable from the outside. Camouflage can be achieved by using colors, patterns, shapes, or vegetation that blend in with the surrounding environment. Camouflage can protect the data center from detection, reconnaissance, or targeting by hostile parties

NEW QUESTION 200
The management team has mandated the encryption of all server administration traffic. Which of the following should MOST likely be implemented?

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

Answer: A

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

NEW QUESTION 202
An administrator is troubleshooting connectivity to a remote server. The goal is to remotely connect to the server to make configuration changes. To further troubleshoot, a port scan revealed the ports on the
server as follows:
Port 22: Closed
Port 23: Open
Port 990: Closed
Which of the following next steps should the administrator take?
Reboot the workstation and then the server.

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

Answer: B

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

NEW QUESTION 205
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

Answer: C

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).References:https://en.wikipedia.org/wiki/Standard_RAID_levels#RAID_5

NEW QUESTION 210
Which of the following is the most effective way to mitigate risks associated with privacy- related data leaks when sharing with a third party?

A. Third-party acceptable use policy
B. Customer data encryption and masking
C. Non-disclosure and indemnity agreements
D. Service- and operational-level agreements

Answer: B

Explanation:
The most effective way to mitigate risks associated with privacy-related data leaks when sharing with a third party is customer data encryption and masking. Encryption is a process of transforming data into an unreadable format that can only be decrypted with a key or password. Masking is a process of hiding or replacing sensitive data with fake or meaningless data. By encrypting and masking customer data, the organization can protect the confidentiality and integrity of the data and prevent unauthorized access or disclosure by the third party.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.3, Objective 3.3

NEW QUESTION 214
A systems administrator is attempting to install a package on a server. After downloading the package from the internet and trying to launch it, the installation is blocked by the antivirus on the server. Which of the following must be completed before launching the installation package again?

A. Creating an exclusion to the antivirus for the application
B. Disabling real-time scanning by the antivirus
C. Validating the checksum for the downloaded installation package
D. Checking for corruption of the downloaded installation package

Answer: C

Explanation:
A checksum is a value that is calculated from a data set to verify its integrity and authenticity. A checksum can be used to compare a downloaded installation package with theoriginal source to ensure that the package has not been corrupted or tampered with during the download or transmission process. If the checksums match, then the package is safe to install. If the checksums do not match, then the package may be infected with malware or contain errors that could cause installation problems. Therefore, validating the checksum for the downloaded installation package is a necessary step before launching the installation again12

1: CompTIA Server+ Certification Exam Objectives 2: How to Verify File Integrity Using Checksums on Linux

NEW QUESTION 216
A technician learns users are unable to tog in to a Linux server with known-working LDAP credentials. The technician logs in to the server with a local account and confirms the system is functional can communicate over the network, and is configured correctly However, the server log has entries regarding Kerberos errors. Which of the following is the MOST likely source of the issue?

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

Answer: C

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

NEW QUESTION 217
A datacenter in a remote location lost power. The power has since been restored, but one ol the servers has not come back online. After some investigation, the server is found to still be powered off. Which of the following is the BEST method to power on the server
remotely?

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

Answer: B

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

NEW QUESTION 219
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

Answer: A

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.

NEW QUESTION 223
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

Answer: D

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 References: [JBOD], [RAID]

NEW QUESTION 224
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

Answer: E

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.

NEW QUESTION 229
An administrator is working locally in a data center with multiple server racks. Which of the following is the best low-cost option to connect to any server while on site?

A. Crash cart
B. IPKVM
C. Remote console access
D. IPMI

Answer: A

Explanation:
A crash cart is the best low-cost option to connect to any server while on site in a data center with multiple server racks. A crash cart is a mobile unit that contains a monitor, a keyboard, a mouse, and cables that can be plugged into any server for direct access and control. A crash cart can be used for troubleshooting, maintenance, or configuration of servers without requiring remote access or network connectivity. A crash cart is also easy to move around and store in a data center. References: [CompTIA Server+ Certification Exam Objectives], Domain 2.0: Hardware, Objective 2.4: Given a scenario involving server management issues (e.g., remote access), troubleshoot using appropriate tools.

NEW QUESTION 230
A server administrator is setting up a disk with enforcement policies on how much data each home share can hold. The amount of data that is redundant on the server must also be minimized. Which of the following should the administrator perform on the server? (Select two).

A. Partitioning
B. Deduplication
C. Disk quotas
D. Compression
E. Cloning
F. Provisioning

Answer: BC

Explanation:
Deduplication is a process that eliminates redundant data blocks and reduces the amount of storage space needed. Disk quotas are policies that limit the amount of disk space that each user or group can use on a volume.
References:
? CompTIA Server+ Certification Exam Objectives1, page 8
? Data Deduplication interoperability2

NEW QUESTION 231
A technician is attempting to reboot a remote physical Linux server. However, attempts to command a shutdown -----now result in the loss of the SSH connection. The server still responds to pings. Which of the following should the technician use to command a remote shutdown?

A. virtual serial console
B. A KVM
C. An IDRAC
D. A crash cart

Answer: C

Explanation:
An IDRAC (Integrated Dell Remote Access Controller) is a tool that can be used to command a remote shutdown of a physical Linux server. An IDRAC is a hardware device that provides out-of-band management for Dell servers. It allows the technician to access the server's console, power cycle, reboot, or shut down the server remotely using a web interface or a command-line interface. An IDRAC does not depend on the operating system or network connectivity of the server. A virtual serial console is a tool that can be used to access a remote virtual machine's console using a serial port connection. A KVM (Keyboard, Video, Mouse) switch is a device that allows the technician to switch between different computer sources using the same keyboard, monitor, and mouse. A crash cart is a mobile unit that contains a keyboard, monitor, mouse, and other tools that can be connected to a physical server for troubleshooting purposes. References: https://www.dell.com/support/kbdoc/en-us/000131486/understanding-the-idrac https://www.howtogeek.com/799968/what-is-a-kvm-switch/https://www.techopedia.com/definition/1032/business-impact-analysis-bia

NEW QUESTION 236
Which of the following would a systems administrator most likely implement to encrypt data in transit for remote administration?

A. Telnet

B. SSH
C. TFTP
D. rlogin

Answer: B

Explanation:
SSH (Secure Shell) is a protocol that would most likely be implemented to encrypt data in transit for remote administration. SSH provides secure communication between two devices over an unsecured network by using public-key cryptography and symmetric encryption. SSH can be used to remotely execute commands, transfer files, or tunnel other protocols. Telnet, TFTP, and rlogin are protocols that do not encrypt data in transit and are considered insecure for remote administration. References: [CompTIA Server+ Certification Exam Objectives], Domain 2.0: Networking, Objective 2.4: Given a scenario involving network security/access methods, implement an appropriate solution.

NEW QUESTION 238
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

Answer: AC

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.

NEW QUESTION 240
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

Answer: A

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.

NEW QUESTION 243
A systems administrator recently installed a new virtual server. After completing the installation, the administrator was only able to reach a few of the servers on the network. While testing, the administrator discovered only servers that had similar IP addresses were reachable. Which of the following is the most likely cause of the issue?

A. The jumbo frames are not enabled.
B. The subnet mask is incorrect.
C. There is an IP address conflict.
D. There is an improper DNS configuration.

Answer: B

Explanation:
A subnet mask is a number that distinguishes the network address and the host address within an IP address1. A subnet mask allows network traffic to understand IP addresses by splitting them into the network and host addresses. If the subnet mask is incorrect, the network traffic may not be able to determine the correct destination for the packets, and only reach some of the servers that have similar IP addresses. For example, if the new virtual server has an IP address of 192.168.1.100 and a subnet mask of 255.255.0.0, it can only communicate with servers that have IP addressesin the range of 192.168.0.0 to 192.168.255.2552. To fix this issue, the systems administrator needs to check and correct the subnet mask of the new virtual server according to the network configuration.

NEW QUESTION 248
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

Answer: C

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

NEW QUESTION 253
A server administrator is taking advantage of all the available bandwidth of the four NICs on the server. Which of the following NIC-teaming technologies should the server administrator utilize?

A. Fail over
B. Fault tolerance
C. Load balancing
D. Link aggregation

Answer: D

Explanation:
Link aggregation is a technique that combines multiple physical network links into one logical link with higher bandwidth and redundancy. It can take advantage of all the available bandwidth of the NICs (Network Interface Cards) on the server and provide load balancing and failover capabilities for network traffic. Verified References: [Link aggregation], [NIC]

NEW QUESTION 258
An administrator is configuring a host-based firewall tor a server. The server needs to allow SSH, FTP, and LDAP traffic. Which of the following ports must be configured so this traffic will be allowed? (Select THREE).

A. 21
B. 22
C. 53
D. 67
E. 69
F. 110
G. 123
H. 389

Answer: ABH

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

NEW QUESTION 262
A server administrator was asked to build a storage array with the highest possible capacity. Which of the following RAID levels should the administrator choose?

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

Answer: A

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

NEW QUESTION 265
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

Answer: B

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.
References:https://www.sudo.ws/man/1.8.13/sudo.man.html

NEW QUESTION 266
A server administrator is gathering business requirements to determine how frequently backups need to be performed on an application server. Which of the following is the administrator attempting to establish?

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

Answer: B

Explanation:
The administrator is attempting to establish the recovery point objective (RPO) by determining how frequently backups need to be performed on an application server. RPO is a metric that defines how much data can be lost or how far back in time a recovery can go in case of a disaster or disruption, based on the business requirements and impact analysis of an organization or system. RPO is measured by the time interval between backups or snapshots of data, such as hourly, daily, weekly, etc., depending on how critical or sensitive the data is and how often it changes or updates. References: [CompTIA Server+ Certification Exam Objectives], Domain 5.0: Security, Objective 5.3: Given a scenario, explain methods and techniques to secure data.

NEW QUESTION 269
A technician needs to restore data from a backup. The technician has these files in the backup inventory:

Name	Size
01012020.bak	100MB
01022020.bak	10MB
01032020.bak	5MB
01042020.bak	7MB
01052020.bak	120MB
01062020.bak	8MB
01072020.bak	10MB

Which of the following backup types is being used if the file 01062020.bak requires another file to restore data?

A. Full
B. Incremental
C. Snapshot
D. Differential

Answer: B

Explanation:
An incremental backup only backs up files that have changed since the last backup, whether it was a full or an incremental backup. Therefore, an incremental backup file may require another file to restore data, depending on the sequence of backups. A full backup backs up all files and does not require any other file to restore data. A snapshot is a point- in-time copy of data that does not depend on other files. A differential backup backs up files that have changed since the last full backup and does not require any other file to restore data.

NEW QUESTION 273
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

SK0-005 Practice Exam Features:

* SK0-005 Questions and Answers Updated Frequently

* SK0-005 Practice Questions Verified by Expert Senior Certified Staff

* SK0-005 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SK0-005 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year