



CompTIA

Exam Questions SK0-005

CompTIA Server+ Certification Exam

About Exambible

[Your Partner of IT Exam](#)

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

An administrator needs to increase the size of an existing RAID 6 array that is running out of available space. Which of the following is the best way the administrator can perform this task?

- A. Replace all the array drives at once and then expand the array.
- B. Expand the array by changing the RAID level to 6.
- C. Expand the array by changing the RAID level to 10.
- D. Replace the array drives one at a time and then expand the array.

Answer: D

Explanation:

RAID 6 is a type of RAID that uses block-level striping with two parity blocks distributed across all member disks. It allows for two disk failures within the RAID set before any data is lost¹. A minimum of four disks is required to create RAID 6¹. To increase the size of an existing RAID 6 array, the administrator can replace the array drives one at a time with larger drives and then expand the array. This way, the data and parity are rebuilt on each new drive and the array remains operational during the process².

NEW QUESTION 2

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

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

Answer: D

Explanation:

RAID 6 is a type of RAID level that uses two parity blocks to provide fault tolerance and redundancy for data storage. RAID 6 can withstand the failure of up to two disks in the array without losing any data. RAID 6 requires a minimum of four disks to operate, and it distributes the data and parity blocks across all the disks in the array. RAID 6 has a high write penalty, which means that it takes more time and resources to write data to the disks than to read data from them. However, RAID 6 offers a high level of data protection and reliability, which makes it suitable for applications that require high availability and durability¹.

RAID 1 provides redundancy and fault tolerance by mirroring the data from one disk to another disk. RAID 1 offers high read performance and data security, but it has low capacity and write performance. RAID 1 requires a minimum of two disks to operate, and it can only tolerate the failure of one disk in the array. If more than one disk fails, all the data in the array is lost².

RAID 5 provides redundancy and fault tolerance by using one parity block to store information that can be used to reconstruct the data in case of a disk failure. RAID 5 requires a minimum of three disks to operate, and it distributes the data and parity blocks across all the disks in the array. RAID 5 offers a balance between performance, capacity, and data protection, but it can only tolerate the failure of one disk in the array. If more than one disk fails, all the data in the array is lost². Therefore, among these options, RAID 6 is the best solution for creating a data volume out of four disks with the most redundancy.

NEW QUESTION 3

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

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

Answer: A

Explanation:

A mantrap is a security device that consists of a small space with two sets of interlocking doors, such that the first set of doors must close before the second one opens. A mantrap can be used to control access to a data center by verifying the identity and weight of the person entering. A bollard is a sturdy post that prevents vehicles from entering a restricted area. Geofencing is a technology that uses GPS or RFID to create a virtual boundary around a location and trigger an action when a device crosses it. RFID is a technology that uses radio waves to identify and track objects or people. References:

? <https://www.techopedia.com/definition/16293/mantrap>

? <https://www.techopedia.com/definition/1437/bollard>

? <https://www.techopedia.com/definition/23961/geofencing>

? <https://www.techopedia.com/definition/506/radio-frequency-identification-rfid>

NEW QUESTION 4

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 5

A server administrator is connecting a new storage array to a server. The administrator has obtained multiple IP addresses for the array. Which of the following connection types is the server most likely using to connect to the array?

- A. eSATA
- B. USB
- C. FC
- D. iSCSI

Answer: D

Explanation:

iSCSI is a protocol that allows SCSI commands to be transmitted over IP networks, enabling remote access to storage devices. iSCSI uses IP addresses to identify and communicate with the storage array, so having multiple IP addresses for the array indicates that iSCSI is being used. eSATA, USB, and FC are other types of connections that use different protocols and connectors than iSCSI. References: CompTIA Server+ Certification Exam Objectives, Domain 3.0: Storage, Objective 3.1: Given a scenario, install and deploy primary storage devices based on given specifications and interfaces.

NEW QUESTION 6

A systems administrator recently upgraded the memory in a server, and now the server does not turn on, and nothing is displayed on the screen. Which of the following is the next step the administrator should take to diagnose the error without opening the machine?

- A. Perform a cold reboot.
- B. Listen for POST code beeps.
- C. Call technical support.
- D. Check the monitor connection.

Answer: B

Explanation:

A power-on self-test (POST) is a diagnostic process that runs when a server is turned on to check the basic functionality of the hardware components and report any errors or faults. A POST code is a series of beeps or flashes that indicate the status of the POST process and identify any problems that prevent the server from booting up. A POST code can be heard through a speaker or seen on a display attached to the server motherboard. A POST code is useful for diagnosing errors without opening the machine or using any software tools.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 5, Lesson 5.1, Objective 5.1

NEW QUESTION 7

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

Data Center Racks 1 and 2

Show Question Reset All Answers

Rack 1

PDU A: 13A MAX PDU B: 6A MAX

Rack Switch 1

VM Host 1

VM Host 2

Mail Relay

SAN

PDU A

Rack 2

PDU A: 5A MAX PDU B: 0A MAX

Rack Switch 2

Domain Controller

PDU A

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Data Center Racks 1 and 2



NEW QUESTION 8

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

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

Answer: B

Explanation:

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

NEW QUESTION 9

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

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

Answer: D

Explanation:

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

NEW QUESTION 10

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

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

Answer: C

Explanation:

The administrator should use 172.16.19.241 as an IP address to be in compliance with RFC 1918 standard. RFC 1918 defines three ranges of IP addresses that are reserved for private internets, meaning they are not globally routable on the public Internet and can be used within an enterprise without any risk of conflict or overlap with other networks. These ranges are:

* 10.0.0.0 - 10.255.255.255 (10/8 prefix) 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

* 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Out of these ranges, only 172.16.19.241 falls within one of them (172.16/12 prefix). The other options are either public IP addresses that belong to other organizations or networks (11.251.196.241, 171.245.198.241) or invalid IP addresses that do not conform to any standard (193.168.145.241).

Reference: <https://whatis.techtarget.com/definition/RFC-1918>

NEW QUESTION 10

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

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

Answer: C

Explanation:

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

NEW QUESTION 12

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

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

Answer: A

Explanation:

Retention policies are the guidelines that dictate when to delete data backups based on operational or compliance needs. They specify how long, how, where, and in what format the data backups are stored, and who has authority over them. The other options are not directly related to the deletion of data backups.

<https://backup.ninja/news/Database-Backups-101-Backup-Retention-Policy-Considerations>

NEW QUESTION 17

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

- A. pvdisplay
- B. mount
- C. df -h
- D. fdisk -l

Answer: C

Explanation:

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

NEW QUESTION 18

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

- A. Differential
- B. Snapshot
- C. Incremental
- D. Synthetic 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 21

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 23

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 27

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

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

Answer: C

Explanation:

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

NEW QUESTION 29

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

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

Answer: B

Explanation:

The most likely cause of this issue is that the UEFI boot was interrupted by a missing Linux boot file, such as `grub.cfg` or `vmlinuz`, which are essential for loading the Linux kernel and booting the system. The `£s>` prompt indicates that the system entered into UEFI Shell mode, which is a command-line interface for troubleshooting UEFI boot issues. The administrator can use UEFI Shell commands to locate and restore the missing boot file or change the boot order. Verified References: [UEFI Shell Guide]

NEW QUESTION 31

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

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

Answer: D

Explanation:

The BIOS (Basic Input/Output System) or UEFI (Unified Extensible Firmware Interface) setup is a program that allows users to configure the hardware settings of a computer, such as the CPU, memory, disk, and boot options. The BIOS/UEFI setup can be accessed by pressing a specific key (such as F2, F10, or Delete) during the boot process, before the operating system loads¹².

One of the settings that can be changed in the BIOS/UEFI setup is the CPU hyperthreading option. Hyperthreading is a technology that enables a single physical CPU core to execute two threads or tasks simultaneously, improving the performance and efficiency of multi-threaded applications. However, some software licenses may limit the number of CPU cores or threads that can be used, and therefore require disabling hyperthreading on the server³⁴.

To disable hyperthreading on a server, the administrator will likely need to enter the BIOS/UEFI setup and navigate to the processor options menu. There, the administrator will find a setting for Intel® Hyperthreading Technology or Hyperthreading Function, which can be enabled or disabled. The administrator will need to disable this setting and save the changes. This will turn off hyperthreading on the server and reduce the number of logical CPUs to match the number of physical cores⁵.

NEW QUESTION 36

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

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

Answer: B

Explanation:

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

NEW QUESTION 37

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

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

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

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

Which of the following most likely contains an error?

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

Answer: D

Explanation:

The subnet mask is most likely containing an error that prevents the application server from communicating with the newly installed database server. The subnet mask is a binary number that defines how many bits of an IP address are used for the network portion and how many bits are used for the host portion. The subnet mask determines which devices belong to the same network or subnet and can communicate directly with each other without routing or switching devices. The subnet mask of the database server is 255.255.O.O, which means that all 32 bits of its IP address are used for the network portion and none for the host portion, which is invalid and makes it unreachable by any other device on any network or subnet. The subnet mask of the application server is 255.O.O.O, which means that only 8 bits of its IP address are used for the network portion and 24 bits are used for the host portion, which is also uncommon and makes it incompatible with most networks or subnets. References: [CompTIA Server+ Certification Exam Objectives], Domain 4.0: Networking, Objective 4.1: Given a scenario, configure network settings for servers.

NEW QUESTION 39

An administrator is deploying a new secure web server. The only administration method that is permitted is to connect via RDP. Which of the following ports should be allowed? (Select TWO).

- A. 53
- B. 80
- C. 389
- D. 443
- E. 45
- F. 3389
- G. 8080

Answer: DF

Explanation:

Port 443 is the default port for HTTPS, which is the protocol used for secure web communication. HTTPS uses SSL/TLS certificates to encrypt the data between the web server and the browser. Port 443 is commonly used for web servers that need to provide secure services, such as online banking, e-commerce, or email. By allowing port 443, the administrator can access the web server's interface and manage its settings¹.

Port 3389 is the default port for RDP, which is the protocol used for remote desktop connection. RDP allows a user to remotely access and control another computer over a network. Port 3389 is commonly used for remote administration, technical support, or remote work. By allowing port 3389, the administrator can connect to the web server's desktop and perform tasks that require graphical user interface².

NEW QUESTION 42

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

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

Answer: BE

Explanation:

These are two measures that should be taken when a data breach occurs. A data breach is an unauthorized or illegal access to confidential or sensitive data by an internal or external actor. A data breach can result in financial losses, reputational damage, legal liabilities, and regulatory penalties for the affected organization. Disclosing the incident is a measure that involves informing the relevant stakeholders, such as customers, employees, partners, regulators, and law enforcement, about the nature, scope, and impact of the data breach. Disclosing the incident can help to mitigate the negative consequences of the data breach, comply with legal obligations, and restore trust and confidence. Identifying the exploited vulnerability is a measure that involves investigating and analyzing the root cause and source of the data breach. Identifying the exploited vulnerability can help to prevent further data loss, remediate the security gaps, and improve the security posture of the organization. Restoring the data from backup is a measure that involves recovering the lost or corrupted data from a secondary storage device or location. However, this does not address the underlying issue of how the data breach occurred or prevent future breaches. Disabling unnecessary ports is a measure that involves closing or blocking network communication endpoints that are not required for legitimate purposes. However, this does not address how the data breach occurred or what vulnerability was exploited. Running an antivirus scan is a measure that involves detecting and removing malicious software from a system or network. However, this does not address how the data breach occurred or what vulnerability was exploited. Moving the data to a different location is a measure that involves transferring the data to another storage device or location that may be more secure or less accessible. However, this does not address how the data breach occurred or what vulnerability was exploited. References: <https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-it-matter/> <https://www.howtogeek.com/202794/what-is-the-difference-between-127.0.0.1-and-0.0.0.0/> <https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual-files/>

NEW QUESTION 45

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

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

Answer: B

Explanation:

The port that must remain open for a secure website is port 443. Port 443 is used by Hypertext Transfer Protocol Secure (HTTPS), which is an extension of HTTP that encrypts and authenticates the communication between a web server and a web browser. HTTPS ensures that the data transmitted over the web is protected from eavesdropping, tampering, or spoofing. Therefore, port 443 must remain open for a secure website to function properly.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 2, Lesson 2.2, Objective 2.2

NEW QUESTION 47

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

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

Answer: D

Explanation:

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

NEW QUESTION 49

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

- A. RAID 0
- B. RAID 1

- C. RAID 5
- D. RAID 6

Answer: B

Explanation:

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

NEW QUESTION 54

The accounting department needs more storage and wants to retain the current data for quick read-write access. The accounting server does not have any internet drive bays available to keep both disks however the server does have USB 3.0 and eSATA ports available. Which of the following is the BEST way to accomplish the department's goals?

- A. Copy the existing data to an external USB 3.0 enclosure.
- B. Place the existing data on a DVD and use the internal DVD-ROM drive.
- C. Transfer the existing data to an external eSATA enclosure.
- D. Move the existing data to a new
- E. larger internal hard drive.

Answer: C

Explanation:

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

NEW QUESTION 58

A security technician generated a public/private key pair on a server. The technician needs to copy the key pair to another server on a different subnet. Which of the following is the most secure method to copy the keys?

- A. FTP
- B. SCP
- C. USB

Answer: C

Explanation:

SCP (Secure Copy Protocol) is a protocol that allows users to securely transfer files between servers using SSH (Secure Shell) encryption. SCP encrypts both the data and the authentication information, preventing unauthorized access, interception, or modification of the files. SCP also preserves the file attributes, such as permissions, timestamps, and ownership.

NEW QUESTION 61

Which of the following environmental controls must be carefully researched so the control itself does not cause the destruction of the server equipment?

- A. Humidity control system
- B. Sensors
- C. Fire suppression
- D. Heating system

Answer: C

Explanation:

Fire suppression systems are designed to extinguish or contain fires in a server room, but they can also damage the server equipment if they are not carefully researched and selected. For example, water-based fire suppression systems can cause electrical shorts and corrosion, while gas-based fire suppression systems can create thermal shock and reduce oxygen levels. Therefore, fire suppression systems must be compatible with the server environment and equipment. References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 1, Lesson 1.5, Objective 1.5

NEW QUESTION 64

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 with name 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 65

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, it will not be able to obtain an IP address or reach other network devices. The DNS configuration is not relevant for network connectivity, as DNS only resolves names to IP addresses. The OS version is not likely to be incompatible with the network switch vendor, as most network switches use standard protocols and interfaces. The HIDS (Host-based Intrusion Detection System) is not likely to prevent the connection, as HIDS only monitors and alerts on suspicious activities on the host. 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 66

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

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

Answer: A

Explanation:

Fibre Channel is a connectivity option that can transmit at 16Gb over an optical connection for SAN-based shared storage. Fibre Channel is a high-speed network technology that provides reliable and secure data transfer between servers and storage devices. Fibre Channel uses optical fiber cables to connect devices and supports various topologies and protocols. FCoE is another connectivity option that uses Fibre Channel over Ethernet, which encapsulates Fibre Channel frames into Ethernet packets. FCoE can also transmit at 16Gb over an optical connection, but it requires a converged network adapter (CNA) and a lossless Ethernet network. iSCSI is another connectivity option that uses SCSI commands over IP networks, which can use either copper or optical cables. iSCSI can transmit at 10Gb or 40Gb over an optical connection, but it has higher latency and lower performance than Fibre Channel. eSATA is another connectivity option that uses SATA commands over external cables, which are usually copper. eSATA can transmit at 6Gb over a copper connection, but it has limited cable length and device support compared to Fibre Channel. References:

? <https://www.ibm.com/topics/storage-area-network>

? <https://www.techopedia.com/definition/1369/fibre-channel-fc>

? <https://www.techopedia.com/definition/1368/fibre-channel-over-ethernet-fcoe>

? <https://www.techopedia.com/definition/1367/internet-small-computer-system-interface-iscsi>

? <https://www.techopedia.com/definition/1366/external-serial-advanced-technology-attachment-esata>

NEW QUESTION 67

A technician has been asked to check on a SAN. Upon arrival, the technician notices the red LED indicator shows a disk has failed. Which of the following should the technician do NEXT, given the disk is hot swappable?

- A. Stop sharing the volume
- B. Replace the disk
- C. Shut down the SAN
- D. Stop all connections to the volume

Answer: B

Explanation:

The next thing that the technician should do, given the disk is hot swappable, is to replace the disk. A hot swappable disk is a disk that can be removed and replaced without shutting down the system or affecting its operation. A hot swappable disk is typically used in a storage array that has RAID (Redundant Array of Independent Disks) configuration that provides fault tolerance and redundancy. If a disk fails in a RAID array, it can be replaced by a new disk without interrupting the service or losing any data. The new disk will automatically rebuild itself using the data from the other disks in the array.

NEW QUESTION 69

A server administrator has connected a new server to the network. During testing, the administrator discovers the server is not reachable via server but can be accessed by IP address. Which of the following steps should the server administrator take NEXT? (Select TWO).

- A. Check the default gateway.
- B. Check the route tables.
- C. Check the hosts file.
- D. Check the DNS server.
- E. Run the ping command.
- F. Run the tracert command

Answer: CD

Explanation:

If the server is not reachable by name but can be accessed by IP address, it means that there is a problem with name resolution. The hosts file and the DNS server are both responsible for mapping hostnames to IP addresses. Therefore, the server administrator should check these two files for any errors or inconsistencies that might prevent the server from being resolved by name. References: <https://www.howtogeek.com/662249/how-to-edit-the-hosts-file-on-linux/>
<https://www.howtogeek.com/164981/how-to-use-nslookup-to-check-domain-name-information-in-microsoft-windows/>

NEW QUESTION 73

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

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

Answer: D

Explanation:

The IP address that best fits this scenario is 216.176.128.10. This is a public IP address that belongs to a range of addresses that are assigned and registered by an Internet service provider (ISP) and can be accessed from anywhere on the Internet. The company has a public range of IP addresses and uses them internally, which means that they do not use private IP addresses or network address translation (NAT) to communicate within their network.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 2, Lesson 2.2, Objective 2.2

NEW QUESTION 76

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

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

Answer: B

Explanation:

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

NEW QUESTION 78

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

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

Answer: D

Explanation:

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

NEW QUESTION 82

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

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

Answer: C

Explanation:

To calculate the minimum number of disks needed for this application, we need to consider the RAID levels and their disk requirements. RAID 1 requires a

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

NEW QUESTION 86

A server administrator has been asked to implement a password policy that will help mitigate the chance of a successful brute-force attack. Which of the following password policies should the administrator implement first?

- A. Lockout
- B. Length
- C. Complexity
- D. Minimum age

Answer: B

Explanation:

Password length is the first password policy that the administrator should implement to help mitigate the chance of a successful brute-force attack. A brute-force attack is a method of guessing passwords by trying all possible combinations of characters until the correct one is found. The longer the password, the more combinations there are, and the more time and resources it takes to crack it. Therefore, password length is a key factor in password strength and security.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.2, Objective 3.2

NEW QUESTION 91

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

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

Answer: C

Explanation:

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

NEW QUESTION 96

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 101

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. RAID 0
- B. RAID 1
- 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 106

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

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

Answer: A

Explanation:

This is the best definition of overprovisioning in a virtual server environment because it means allocating more CPU, memory, disk, or network resources to the virtual machines than what is actually available on the physical host. This can lead to performance issues and resource contention.

References: <https://www.hpe.com/us/en/insights/articles/10-virtualization-mistakes-everyone-makes-1808.html>

NEW QUESTION 110

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 111

A server administrator is creating a script that will move files only if they were created before a date input by the user. Which of the following constructs will allow the script to apply this test until all available files are assessed?

- A. Variable
- B. Loop
- C. Comparator
- D. Conditional

Answer: B

Explanation:

A loop is a script construct that allows the script to repeat a block of code until a certain condition is met or for a specified number of times. A loop can be used to apply a test to each file in a directory and move the files that meet the criteria. For example, in a bash script, a loop can be written as:

```
#!/bin/bash
# Ask the user for the date echo "Enter the date (YYYY-MM-DD):" read date
# Loop through all the files in the current directory for file in *
do
# Check if the file was created before the date if [[ $(date -r "$file" +%F) < $date ]]
then
# Move the file to another location mv "$file" /path/to/destination
fi done Copy
```

A variable is a script construct that allows the script to store and manipulate data. A variable can be used to store the date input by the user, but it cannot apply a test to each file.

A comparator is a script construct that allows the script to compare two values and determine their relationship. A comparator can be used to check if a file was created before

the date, but it cannot repeat the test for all files.

A conditional is a script construct that allows the script to execute different blocks of code based on certain conditions. A conditional can be used to decide whether to move a file or not, but it cannot iterate over all files.

1: CompTIA Server+ Certification Exam Objectives

NEW QUESTION 115

A remote physical server is unable to communicate to the network through the available NICs, which were misconfigured. However, the server administrator is still able to configure the server remotely. Which of the following connection types is the server administrator using to access the server?

- A. Out-of-band management
- B. Crash cart access
- C. Virtual administrator console
- D. Local KVM setup
- E. RDP connection

Answer: A

Explanation:

The connection type that the server administrator is using to access the server remotely is out-of-band management. Out-of-band management is a method of accessing and controlling a server through a dedicated network interface or port that is separate from the regular data network. Out-of-band management allows administrators to perform tasks such as rebooting, configuring, troubleshooting, or updating a server even if the server is offline or unresponsive through the regular network. Out-of-band management can use protocols such as IPMI, iLO, DRAC, or BMC. Reference: <https://www.ibm.com/cloud/learn/out-of-band-management>

NEW QUESTION 118

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, such as 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 122

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 125

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 128

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 PowerShell: Write-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 129

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

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

Answer: C

Explanation:

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

NEW QUESTION 131

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 133

Several new components have been added to a mission-critical server, and corporate policy states all new components must meet server hardening requirements. Which of the following should be applied?

- A. Definition updates
- B. Driver updates
- C. OS security updates
- D. Application updates

Answer: B

Explanation:

Driver updates should be applied to the new components that have been added to a mission-critical server, as part of the server hardening requirements. Drivers are software programs that enable the communication and functionality of hardware devices, such as network cards, storage controllers, or graphics cards. Updating drivers can improve the performance, compatibility, and stability of the new components with the server operating system and applications. References: CompTIA Server+ Certification Exam Objectives, Domain 2.0: Hardware, Objective 2.2: Given a scenario, install, configure and maintain server components.

NEW QUESTION 138

An administrator discovers a Bash script file has the following permissions set in octal notation;
777

Which of the following is the MOST appropriate command to ensure only the root user can modify and execute the script?

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

Answer: A

Explanation:

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

NEW QUESTION 142

A technician is sizing a new server and, for service reasons, needs as many hot-swappable components as possible. Which of the following server components can most commonly be replaced without downtime? (Select three).

- A. Drives
- B. Fans
- C. CMOSIC
- D. Processor
- E. Power supplies
- F. Motherboard
- G. Memory
- H. BIOS

Answer: ABE

Explanation:

Drives, fans, and power supplies are server components that can most commonly be replaced without downtime if they are hot-swappable. Hot-swappable

components can be removed and inserted while the server is running, without affecting its operation or performance. Drives store data and applications, fans cool down the server components, and power supplies provide electricity to the server. Replacing these components can prevent data loss, overheating, or power failure. References: CompTIA Server+ Certification Exam Objectives, Domain 2.0: Hardware, Objective 2.2: Given a scenario, install, configure and maintain server components.

NEW QUESTION 145

A company wants to deploy software to all users, but very few of them will be using the software at any one point in time. Which of the following licensing models would be BEST for 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-license><https://www.techopedia.com/definition/1440/software-licensing>

NEW QUESTION 150

A server administrator is experiencing difficulty configuring MySQL on a Linux server. The administrator issues the `getenforce` command and receives the following output:

```
># Enforcing
```

Which of the following commands should the administrator issue to configure MySQL successfully?

- A. `setenforce 0`
- B. `setenforce permissive`
- C. `setenforce 1`
- D. `setenforce disabled`

Answer: A

Explanation:

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

to run by using commands such as `semanage` or `setsebool`.

Reference:

<https://blogs.oracle.com/mysql/selinux-and-mysql-v2>

NEW QUESTION 155

A company stores extremely sensitive data on an air-gapped system. Which of the following can be implemented to increase security against a potential insider threat?

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

Answer: A

Explanation:

Two-person integrity is a security measure that can be implemented to increase security against a potential insider threat on an air-gapped system. An air-gapped system is a system that is isolated from any network connection and can only be accessed physically. An insider threat is a malicious actor who has authorized access to an organization's system or data and uses it for unauthorized or harmful purposes. Two-person integrity is a system of storage and handling that requires the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures, for accessing certain sensitive data or material. This way, no single person can compromise the security or integrity of the data or material without being noticed by another person. SSO (Single Sign-On) is a feature that allows users to access multiple applications or systems with one set of credentials, but it does not prevent insider threats. SIEM (Security Information and Event Management) is a tool that collects and analyzes log data from various sources to detect and respond to security incidents, but it does not work on air-gapped systems. A Faraday cage is a structure that blocks electromagnetic signals from entering or leaving, but it does not prevent physical access or insider threats. MFA (Multi-Factor Authentication) is a method that requires users to provide two or more pieces of evidence to verify their identity, such as something they know, something they have, or something they are, but it does not prevent insider threats. References: <https://www.howtogeek.com/169080/air-gap-how-to-isolate-a-computer-to-protect-it-from-hackers/> <https://www.howtogeek.com/428483/what-is-end-to-end-encryption-and-why-does-it-matter/> <https://www.howtogeek.com/202794/what-is-the-difference-between-127.0.0.1-and-0.0.0.0/> <https://www.howtogeek.com/443611/how-to-encrypt-your-macs-system-drive-removable-devices-and-individual-files/>

NEW QUESTION 159

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 163

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

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

Answer: A

Explanation:

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 167

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 169

An administrator is setting up a new server and has been asked to install an operating system that does not have a GUI because the server has limited resources. Which of the following installation options should the administrator use?

- A. Bare metal
- B. Headless
- C. Virtualized
- D. Slipstreamed

Answer: B

Explanation:

A headless installation is an installation method that does not require a graphical user interface (GUI) or a monitor, keyboard, and mouse. It can be done remotely through a network connection or a command-line interface. A headless installation is suitable for a server that has limited resources and does not need a GUI.

References:

? CompTIA Server+ Certification Exam Objectives¹, page 14

? Server Management: Server Hardware Installation and Management2, Module 2, Lesson 5

NEW QUESTION 172

A server has experienced several component failures. To minimize downtime, the server administrator wants to replace the components while the server is running. Which of the following can MOST likely be swapped out while the server is still running? (Select TWO).

- A. The power supply
- B. The CPU
- C. The hard drive
- D. The GPU
- E. The cache
- F. The RAM

Answer: AC

Explanation:

The power supply and the hard drive are two components that can most likely be swapped out while the server is still running, if they support hot swapping or hot plugging. Hot swapping or hot plugging means that the device can be added or removed without shutting down the system. The operating system automatically recognizes the changes that have been made. This feature is useful for minimizing downtime and improving availability. The CPU, the GPU, the cache, and the RAM are not hot swappable and require the system to be powered off before replacing them. References: <https://www.geeksforgeeks.org/what-is-hot-swapping/><https://www.howtogeek.com/268249/what-is-hot-swapping-and-what-devices-support-it/>

NEW QUESTION 177

A technician is configuring a point-to-point heartbeat connection between two servers using IP addressing. Which of the following is the most efficient subnet mask for this connection?

- A. /28
- B. /29
- C. /30
- D. /32

Answer: C

Explanation:

The most efficient subnet mask for a point-to-point heartbeat connection between two servers using IP addressing is /30. A /30 subnet mask has 255.255.255.252 as its decimal representation and 11111111.11111111.11111111.11111100 as its binary representation. This means that there are only two bits available for the host portion of the IP address, which allows for four possible combinations: 00, 01, 10, and 11. However, the first and the last combinations are reserved for the network address and the broadcast address, respectively. Therefore, only two IP addresses are usable for the point-to-point connection, which is the minimum required for such a link. A /30 subnet mask is also known as a point-to-point prefix because it is commonly used for point-to-point links between routers or servers¹.

A /28 subnet mask has 255.255.255.240 as its decimal representation and 11111111.11111111.11111111.11110000 as its binary representation. This means that there are four bits available for the host portion of the IP address, which allows for 16 possible combinations. However, two of them are reserved for the network address and the broadcast address, respectively. Therefore, 14 IP addresses are usable for the subnet, which is more than needed for a point-to-point connection and would result in wasted addresses.

A /29 subnet mask has 255.255.255.248 as its decimal representation and 11111111.11111111.11111111.11111000 as its binary representation. This means that there are three bits available for the host portion of the IP address, which allows for eight possible combinations. However, two of them are reserved for the network address and the broadcast address, respectively. Therefore, six IP addresses are usable for the subnet, which is still more than needed for a point-to-point connection and would result in wasted addresses.

A /32 subnet mask has 255.255.255.255 as its decimal representation and 11111111.11111111.11111111.11111111 as its binary representation. This means that there are no bits available for the host portion of the IP address, which allows for only one possible combination: all ones. Therefore, only one IP address is usable for the subnet, which is not enough for a point-to-point connection and would result in an invalid configuration.

Therefore, a /30 subnet mask is the most efficient choice for a point-to-point heartbeat connection between two servers using IP addressing because it provides exactly two usable IP addresses without wasting any addresses or creating any conflicts¹.

NEW QUESTION 178

Which of the following BEST describes a warm site?

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

Answer: D

Explanation:

A warm site is a type of disaster recovery site that has some pre-installed hardware, software, and network connections, but not as much as a hot site. A warm site also has some backup data, but not as current as a hot site. A warm site requires some time and effort to become fully operational in the event of a disaster. A hot site is a disaster recovery site that has all infrastructure and live data, and can take over the primary site's operations immediately. A cold site is a disaster recovery site that has no infrastructure or data, and requires significant time and resources to set up. References:

? <https://www.enterprisestorageforum.com/management/disaster-recovery-site/>

? <https://www.techopedia.com/definition/3780/warm-site>

NEW QUESTION 180

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

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

Answer: C

Explanation:

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

NEW QUESTION 182

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

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

Answer: B

Explanation:

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

NEW QUESTION 186

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

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

Answer: A

Explanation:

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

NEW QUESTION 187

A Linux server was recently updated. Now, the server stops during the boot process with a blank screen and an f prompt. Which of the following is the most likely cause of this issue?

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

Answer: B

Explanation:

The most likely cause of this issue is that the UEFI boot was interrupted by a missing Linux boot file. UEFI (Unified Extensible Firmware Interface) is a standard that defines the interface and functionality of the firmware that initializes the hardware and software components of a system before loading the operating system. UEFI boot is a process that uses UEFI firmware to load and execute a boot loader, which is a program that loads the operating system kernel and other essential files. A Linux boot file is a file that contains information and instructions for the boot loader, such as the location of the kernel, the root file system, and the boot parameters. If a Linux boot file is missing or corrupted, the boot loader cannot find or load the kernel, and the system stops during the boot process with a blank screen and an f prompt.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 4, Lesson 4.1, Objective 4.1

NEW QUESTION 189

Which of the following would a systems administrator implement to ensure all web traffic is secure?

- A. SSH
- B. SSL
- C. SMTP
- D. PGP

Answer: B

Explanation:

Secure Sockets Layer (SSL): SSL and its successor Transport Layer Security (TLS) enable client and server computers to establish a secure connection session and manage encryption and decryption activities. Reference: <https://paginas.fe.up.pt/~als/mis10e/ch8/chpt8-4bullettext.htm>

NEW QUESTION 190

A server administrator has a system requirement to install the virtual OS on bare metal hardware. Which of the following hypervisor virtualization technologies should the administrator use to BEST meet the system requirements? (Select TWO)

- A. Host
- B. Template
- C. Clone
- D. Type1
- E. Type2
- F. Guest

Answer: BD

Explanation:

A template is a preconfigured virtual machine image that can be used to create new virtual machines quickly and easily. A template can include the operating system, applications, settings, and data that are required for a specific purpose or role. A type 1 hypervisor is a virtualization technology that runs directly on bare metal hardware, without requiring an underlying operating system. A type 1 hypervisor can provide better performance, security, and isolation for virtual machines than a type 2 hypervisor, which runs on top of an operating system. Verified References: [Template], [Type 1 hypervisor]

NEW QUESTION 194

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

- A. tracer
- B. telnet
- C. ipconfig
- D. ping

Answer: C

NEW QUESTION 197

A hardware technician is installing 19 1U servers in a 42U rack. The following unit sizes should be allocated per server?

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

Answer: A

Explanation:

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

NEW QUESTION 199

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

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

Answer: D

Explanation:

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

NEW QUESTION 203

A systems administrator has noticed performance degradation on a company file server, and one of the disks on it has a solid amber light. The administrator logs on to the disk utility and sees the array is rebuilding. Which of the following should the administrator do NEXT once the rebuild is finished?

- A. Restore the server from a snapshot.
- B. Restore the server from backup.
- C. Swap the drive and initialize the disk.
- D. Swap the drive and initialize the array.

Answer: C

Explanation:

The next action that the administrator should take once the rebuild is finished is to swap the drive and initialize the disk. This is to replace the faulty disk that has a solid amber light, which indicates a predictive failure or a SMART error. Initializing the disk will prepare it for use by the RAID controller and add it to the array. The administrator should also monitor the array status and performance after swapping the drive. Reference: <https://www.salvagedata.com/how-to-rebuild-a-failed-raid/>

NEW QUESTION 205

An administrator needs to disable root login over SSH. Which of the following files 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_sshd_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 208

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 210

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-site> <https://www.techopedia.com/definition/29836/cloud-recovery>

NEW QUESTION 215

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

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

Answer: AC

Explanation:

The administrator should close ports 21 and 23 to secure the server properly. Port 21 is used for FTP (File Transfer Protocol), which is an unsecure protocol that allows file transfer between a client and a server over a network connection. FTP does not encrypt the data or the credentials that are transmitted, making them vulnerable to interception or modification by attackers. Port 23 is used for Telnet, which is an unsecure protocol that allows remote login and command execution over a network connection using a CLI. Telnet does not encrypt the data or the credentials that are transmitted, making them vulnerable to interception or modification by attackers.

Reference:

<https://www.csoonline.com/article/3191531/securing-risky-network-ports.html>

NEW QUESTION 218

A server administrator needs to implement load balancing without purchasing any new hardware or implementing any new software. Which of the following will the administrator most likely implement?

- A. Round robin
- B. Link aggregation
- C. Most recently used
- D. Heartbeat

Answer: B

Explanation:

Link aggregation is a technique that allows multiple network interfaces to act as one logical interface, increasing the bandwidth and redundancy of the connection. This can improve the load balancing of network traffic without requiring any new hardware or software. Round robin, most recently used, and heartbeat are not load balancing methods, but rather scheduling algorithms or monitoring techniques. References: CompTIA Server+ Certification Exam Objectives, Domain 2.0: Networking, Objective 2.3: Given a scenario, configure NIC teaming.

NEW QUESTION 222

A staff member who is 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 heat 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 in 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 227

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

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

Answer: B

Explanation:

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

NEW QUESTION 230

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 232

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

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

Answer: A

Explanation:

Open-source software is software that is freely available and can be modified and distributed by anyone. It usually requires very little technical support and has no

licensing fees. Therefore, it would be the lowest cost solution for an application that does not need much support. References:
<https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives> (Objective 2.3)

NEW QUESTION 233

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 238

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

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

Answer: BE

Explanation:

A CMOS battery failure can cause the server to lose its BIOS settings, including the date and time, which can affect the server's functionality and connectivity. The servers have NTP (Network Time Protocol) configured to synchronize their clocks with a reliable time source, which can prevent time drift and ensure consistent timestamps. If one server has a wrong date and time, it can cause conflicts and errors with the other servers that have NTP configured.

References:

? CompTIA Server+ Certification Exam Objectives1, page 9

? Signs or symptoms of a CMOS battery failure2

? NTP: Network Time Protocol

NEW QUESTION 243

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

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

Answer: C

Explanation:

An emergency change request is a type of change request that is initiated in response to an urgent situation, such as a system breach, that requires immediate action to restore normal operations or prevent further damage. An emergency change request may bypass some of the normal change management procedures, such as approval, testing, or documentation, in order to expedite the implementation of the change. However, an emergency change request should still follow the basic steps of change management, such as identification, analysis, planning, execution, and evaluation, and should be reviewed and documented after the change is completed.

References: CompTIA Server+ Study Guide, Chapter 11: Change Management, page 443.

NEW QUESTION 246

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

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

Answer: A

Explanation:

The best way to complete the request to harden the server is to disable port 389 on the server. Port 389 is the default port used by LDAP (Lightweight Directory Access Protocol), which is a protocol that allows access and modification of directory services over a network. LDAP can be used for authentication, authorization, or information retrieval purposes. However, LDAP does not encrypt its data by default, which can expose sensitive information or credentials to attackers who can intercept or modify the network traffic.

Therefore, port 389 should be disabled on a web server that only hosts websites and does not need LDAP functionality. Alternatively, port 636 can be used instead

of port 389 to enable LDAPS (LDAP over SSL/TLS), which encrypts the data using SSL/TLS certificates.

NEW QUESTION 249

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

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

Answer: D

Explanation:

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

NEW QUESTION 253

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

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

Answer: A

Explanation:

The RAID level that should be implemented to maximize usable capacity without requiring redundancy is RAID 0. RAID (Redundant Array of Independent Disks) is a technology that combines multiple physical disks into a logical unit that provides improved performance, reliability, or both. RAID 0 is a RAID level that splits data evenly across two or more disks without parity or mirroring. RAID 0 does not provide any redundancy or fault tolerance, but it increases usable capacity and performance by allowing parallel read and write operations.

References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 1, Lesson 1.2, Objective 1.2

NEW QUESTION 258

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

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

Answer: A

Explanation:

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

NEW QUESTION 263

A company has implemented a requirement to encrypt all the hard drives on its servers as part of a data loss prevention strategy. Which of the following should the company also perform as a data loss prevention method?

- A. Encrypt all network traffic
- B. Implement MFA on all the servers with encrypted data
- C. Block the servers from using an encrypted USB
- D. Implement port security on the switches

Answer: B

Explanation:

The company should also implement MFA on all the servers with encrypted data as a data loss prevention method. MFA stands for multi-factor authentication, which is a method of verifying a user's identity by requiring two or more pieces of evidence, such as something they know (e.g., a password), something they have (e.g., a token), or something they are (e.g., a fingerprint). MFA adds an extra layer of security to prevent unauthorized access to sensitive data, even if the user's password is compromised or stolen. Encrypting the hard drives on the servers protects the data from being read or copied if the drives are physically removed or stolen, but it does not prevent unauthorized access to the data if the user's credentials are valid.

NEW QUESTION 266

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

- A. bash
- B. !execute
- C. #!
- D. @each off

Answer: C

Explanation:

#! is the symbol that should be placed at the top of a Bash script to ensure it can be executed. #! is also known as shebang or hashbang. It is a special notation that tells the operating system which interpreter to use to run the script. The shebang is followed by the path to the interpreter, such as /bin/bash for Bash, /bin/python for Python, or /bin/perl for Perl. For example, a Bash script that prints "Hello World" would start with:

```
#!/bin/bash echo "Hello World"
```

The shebang must be the first line of the script and must not have any spaces between the

and ! symbols. bash is not a valid shebang by itself, as it does not specify the path to the interpreter. !execute is not a valid shebang at all, as it does not start with #. @echo off is a command that disables the echoing of commands in a batch file on Windows, but it has nothing to do with Bash scripts on Linux.

References: <https://www.howtogeek.com/67469/the-beginners-guide-to-shell-scripting-the-basics/> <https://www.howtogeek.com/435903/what-is-a-shebang-line/>

NEW QUESTION 268

A server technician arrives at a data center to troubleshoot a physical server that is not responding to remote management software. The technician discovers the servers in the data center are not connected to a KVM switch, and their out-of-band management cards have not been configured. Which of the following should the technician do to access the server for troubleshooting purposes?

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

Answer: C

Explanation:

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

NEW QUESTION 272

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

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

Answer: D

Explanation:

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

Reference:

<https://www.dnsstuff.com/what-is-server-load-balancing>

NEW QUESTION 273

A server administrator is swapping out the GPU card inside a server. Which of the following actions should the administrator take FIRST?

- A. Inspect the GPU that is being installed.
- B. Ensure the GPU meets HCL guidelines.
- C. Shut down the server.
- D. Disconnect the power from the rack.

Answer: C

Explanation:

The first action that the administrator should take before swapping out the GPU card inside a server is to shut down the server. This is to ensure that the server is not running any processes that might be using the GPU card, and to prevent any damage to the hardware or data loss due to sudden power loss. Shutting down the server also reduces the risk of electrostatic discharge (ESD) that might harm the components. Reference: <https://pcgearhead.com/installing-a-new-gpu/>

NEW QUESTION 274

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

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

Answer: B

Explanation:

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

NEW QUESTION 277

Which of the following asset management documents is used to identify the location of a server 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 279

Users are able to connect to the wireless network, but they are unable to access the internet. The network administrator verifies connectivity to all network devices, and there are no ISP outages. The server administrator removes the old address leases from the active leases pool, which allows users to access the internet. Which of the following is most likely causing the internet issue?

- A. The DHCP exclusion needs to be removed.
- B. The DHCP scope is full.
- C. The DHCP scope options are misconfigured.
- D. The DHCP lease times are too short.
- E. The DHCP reservations need to be configured.

Answer: B

Explanation:

The most likely cause of the internet issue is B. The DHCP scope is full.

A DHCP scope is a range of IP addresses that a DHCP server can assign to DHCP clients on a network. A DHCP scope has a start address and an end address, and it can also have some excluded addresses that are not available for lease. A DHCP scope can have various options, such as subnet mask, default gateway, DNS server, etc., that are applied to the DHCP clients along with the IP address. A DHCP scope also has a lease time, which is the duration that a DHCP client can use an IP address before renewing it or releasing it. A DHCP scope can have reservations, which are fixed IP addresses that are assigned to specific DHCP clients based on their MAC addresses.

If a DHCP scope is full, it means that there are no more IP addresses available for lease in the scope. This can happen if the number of DHCP clients exceeds the number of IP addresses in the scope, or if the lease time is too long and the IP addresses are not released or reused frequently enough. If a DHCP scope is full, any new or existing DHCP clients that request an IP address from the DHCP server will not receive one, and they will not be able to access the network or the internet.

In this scenario, users are able to connect to the wireless network, but they are unable to access the internet. The network administrator verifies connectivity to all network devices, and there are no ISP outages. The server administrator removes the old address leases from the active leases pool, which allows users to access the internet. This indicates that the DHCP scope is full, and that removing the old leases frees up some IP addresses for lease in the scope. Therefore, option B is the most likely cause of the internet issue.

NEW QUESTION 283

A server technician has been asked to upload a few files from the internal web server to the internal FTP server. The technician logs in to the web server using PuTTY, but the connection to the FTP server fails. However, the FTP connection from the technician's workstation is successful. To troubleshoot the issue, the technician executes the following command on both the web server and the workstation:

```
ping ftp.acme.local
```

The IP address in the command output is different on each machine. Which of the following is the MOST likely reason for the connection failure?

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

Answer: D

Explanation:

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

NEW QUESTION 288

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 290

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

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

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 294

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 tasks that do not require DLP. Auditing the access to the physical fileshare is a physical security measure that is not affected by DLP.

NEW QUESTION 299

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

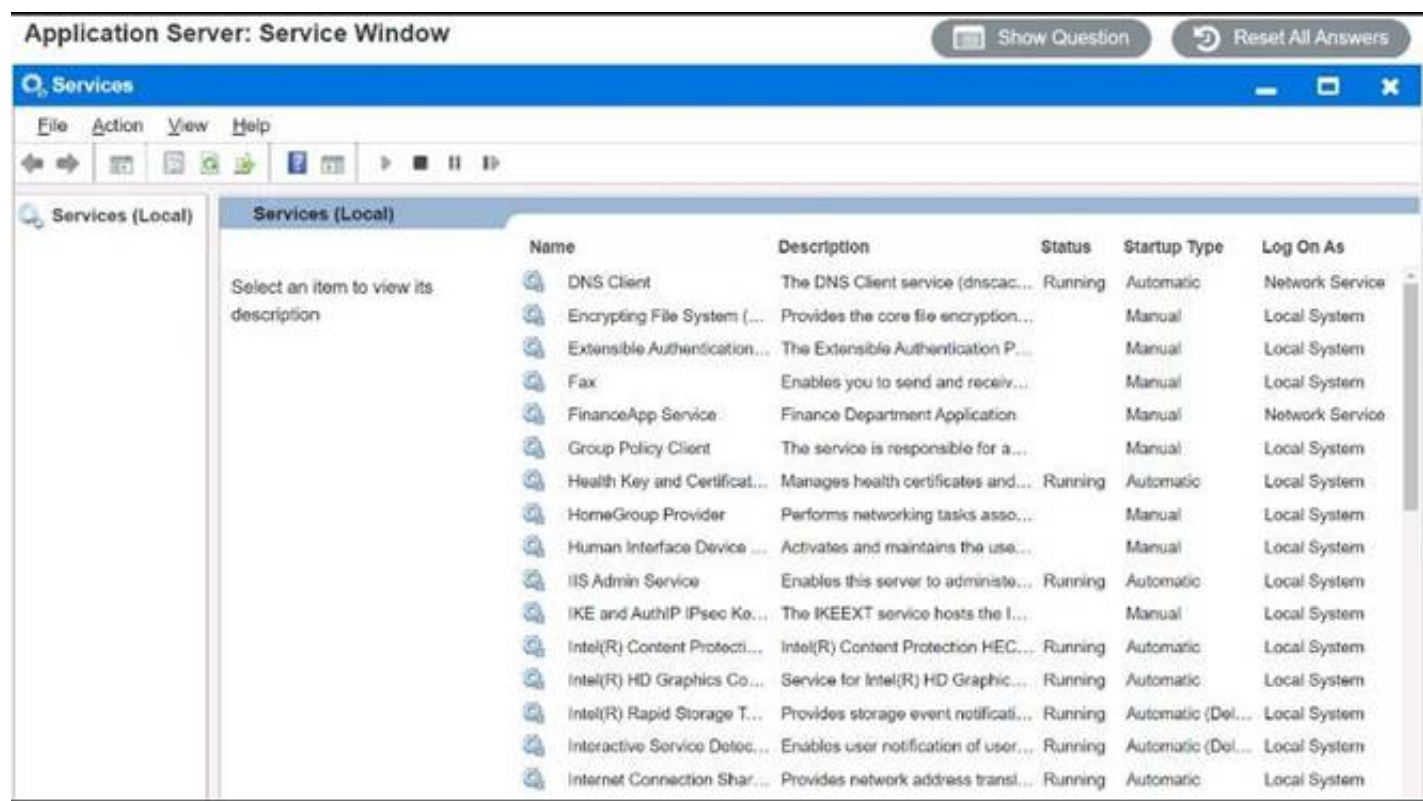
NEW QUESTION 303

SIMULATION

Users report that the FinanceApp software is not running, and they need immediate access. Issues with the FinanceApp software occur every week after the IT team completes server system updates. The users, however, do not want to contact the help desk every time the issue occurs. The users also report the new MarketApp software is not usable when it crashes, which can cause significant downtime. The technician who restarted the MarketApp software noticed it is running under a test account, which is a likely cause of the crashes.

INSTRUCTIONS

Using the Services menu provided, modify the appropriate application services to remedy the stated issues.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

FinanceApp software is running as a service named “FinanceApp Service”. The service description says “Provides financial data and calculations for the FinanceApp software”. The service status is “Stopped”, which means that the service is not running and the software is not functional. The service startup type is “Manual”, which means that the service needs to be started manually by the user or the administrator. The service log on as is “Local System”, which means that the service runs under a predefined local account that has extensive privileges on the local computer.

To fix the issue with the FinanceApp software, you need to do two things:

? First, you need to start the service, so that the software can run. To do this, you can right-click on the service name and select “Start” from the menu. Alternatively, you can select the service name and click on the “Start” button on the toolbar. You should see a message saying that the service has started successfully.

? Second, you need to change the service startup type, so that the service can start automatically every time the server boots up. This way, you don’t have to contact the help desk every time the issue occurs. To do this, you can right-click on the service name and select “Properties” from the menu. Alternatively, you can select the service name and click on the “Properties” button on the toolbar. You should see a window with several tabs and options. On the “General” tab, under “Startup type”, you can select “Automatic” from the drop-down list. Then, click on “OK” to save your changes.

By doing these two steps, you should be able to use the FinanceApp software without any problems.

The MarketApp software is running as a service named “MarketApp Service”. The service description says “Provides market data and analysis for the MarketApp software”. The service status is “Running”, which means that the service is running and the software is functional. However, as you reported, the software may crash sometimes, which can cause significant downtime. The service startup type is “Automatic”, which means that the service starts automatically every time the server boots up. The service log on as is “TestAccount”, which is a test account that was probably used for development or testing purposes.

To fix the issue with the MarketApp software, you need to do one thing:

? You need to change the service log on as, so that the service runs under a proper account that has sufficient permissions and security settings for production use. To do this, you can right-click on the service name and select “Properties” from the menu. Alternatively, you can select the service name and click on the “Properties” button on the toolbar. You should see a window with several tabs and options. On the “Log On” tab, under “Log on as”, you can select either “Local System account” or “This account”. If you choose “Local System account”, then the service will run under a predefined local account that has extensive privileges on the local computer. If you choose “This account”, then you will need to enter a valid username and password for an account that has appropriate permissions and security settings for running the service. You may need to consult with your IT team or your software vendor to determine which option is best for your situation. Then, click on “OK” to save your changes.

NEW QUESTION 308

.....

Relate Links

100% Pass Your SK0-005 Exam with ExamBible Prep Materials

<https://www.exambible.com/SK0-005-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>