CompTIA

Exam Questions SK0-005

CompTIA Server+ Certification Exam

NEW QUESTION 1
A new application server has been configured in the cloud to provide access to all clients within the network. On-site users are able to access all resources, but remote users are reporting issues connecting to the new application. The server administrator verifies that all users are configured with the appropriate group memberships. Which of the following is MOST likely causing the issue?

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

Answer: C

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

NEW QUESTION 2
A systems administrator is setting up a new server that will be used as a DHCP server. The administrator installs the OS but is then unable to log on using Active Directory credentials. The administrator logs on using the local administrator account and verifies the server has the correct IP address, subnet mask, and default gateway. The administrator then gets on another server and can ping the new server. Which of the following is causing the issue?

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

Answer: D

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

NEW QUESTION 3
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

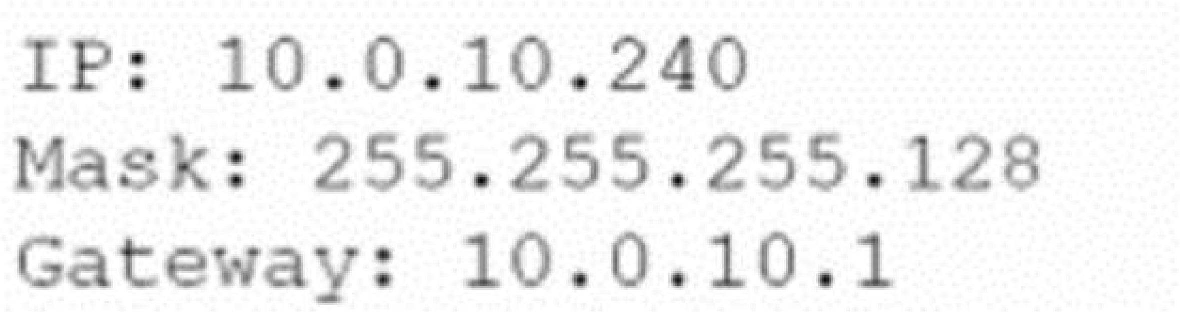
NEW QUESTION 4
A server administrator needs to harden a server by only allowing secure traffic and DNS inquiries. A port scan reports the following ports are open:

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

Answer: D

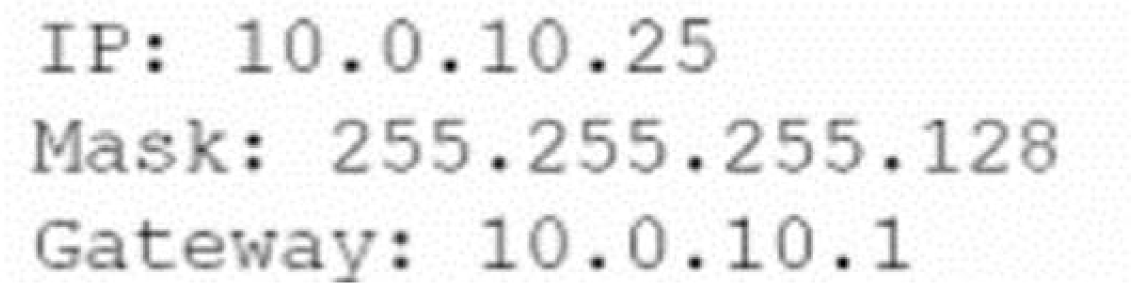
Explanation:
The administrator should only allow secure traffic and DNS inquiries on the server, which means that only ports 22, 53, and 443 should be open. Port 22 is used for SSH (Secure Shell), which is a protocol that allows secure remote login and command execution over a network connection using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

NEW QUESTION 5
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 6
A technician wants to limit disk usage on a server. Which of the following should the technician implement?

A. Formatting
B. Compression
C. Disk quotas
D. Partitioning

Answer: C

Explanation:
Disk quotas are a way to limit disk usage on a server by setting a maximum amount of space that each user or group can use. Disk quotas can help manage disk space allocation, prevent disk space exhaustion, and enforce fair usage policies. Disk quotas can be set at the volume level or at the folder level, depending on the file system and operating system used.Reference:https://docs.microsoft.com/en-us/windows- server/storage/ntfs/ntfs-disk-quotas-overview

NEW QUESTION 7
An administrator is configuring a server to communicate with a new storage array. To do so, the administrator enters the WWPN of the new array in the server's storage configuration. Which of the following technologies is the new connection using?

A. iSCSI
B. eSATA
C. NFS
D. FcoE

Answer: A

Explanation:
Reference:https://docs.oracle.com/cd/E26996_01/E18549/html/BABHBFHA.html

NEW QUESTION 8
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 shortsand 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 9
A security manager is concerned that a rogue employee could boot a server from an outside USB drive. Which of the following actions can be taken to reduce this risk? (Select TWO).

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

Answer: BC

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

NEW QUESTION 10
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 11
Which of the following physical security concepts would most likely be used to limit personnel access to a restricted area within a data center?

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

Answer: A

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

NEW QUESTION 12
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):" readdate
# Loop through all the files in the current directory forfilein*
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 file1

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 files1
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 files1
1: CompTIA Server+ Certification Exam Objectives

NEW QUESTION 13
The Chief Information Officer (CIO) of a datacenter is concerned that transmissions from the building can be detected from the outside. Which of the following would resolve this concern? (Choose two.)

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

Answer: CE

Explanation:
The best solutions to resolve the concern of transmissions from the building being detected from outside are signal blocking and reflective glass. Signal blocking is a method of preventing or interfering with electromagnetic signals from escaping or entering a certain area. Signal blocking can be achieved by using various materials or devices that create physical barriers or generate noise or jamming signals. Signal blocking can protect data transmissions from being intercepted or eavesdropped by unauthorized parties. Reflective glass is a type of glass that has a coating or film that reflects light and heat. Reflective glass can reduce glare and solar radiation, as well as prevent visual observation from outside. Reflective glass can enhance privacy and security for datacenter operations.

NEW QUESTION 14
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 15
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 16
A technician is monitoring a server and notices there is only one NIC plugged in. but the server has two. The NIC is oversaturated, and the technician would like to increase the available bandwidth. Which of the following solutions would be the BEST option to increase the speed of this NIC?

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

Answer: A

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

NEW QUESTION 17
A company recently implemented VolP across a multicampus environment with ten locations. The company uses many network technologies, including fiber, copper, and wireless. Users calling between three of the locations have reported that voices sound strange. Which of the following should be monitored to narrow down the issue?

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

Answer: D

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

NEW QUESTION 18
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 19
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 20
An administrator needs to disable root login over SSH. Which of the following tiles should be edited to complete this task?

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

Answer: B

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

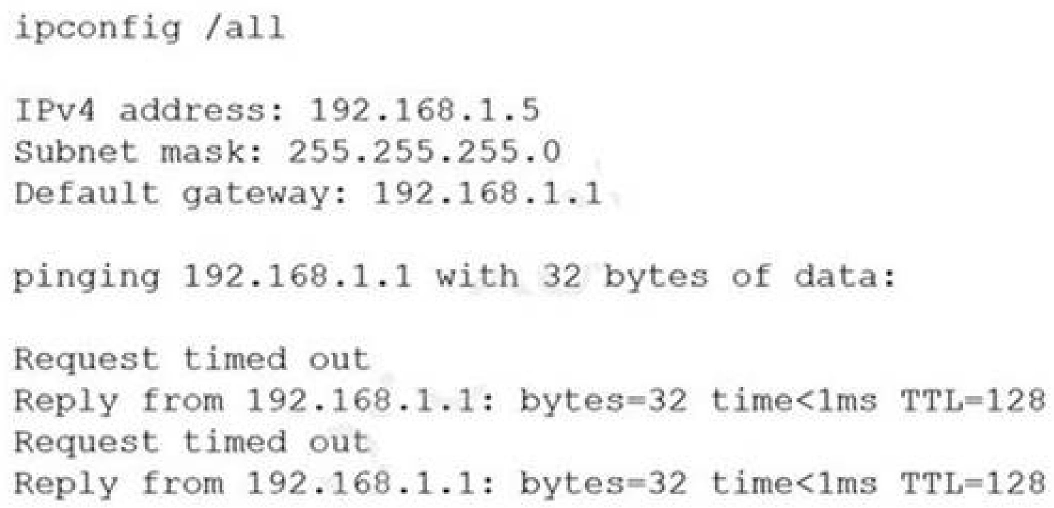
NEW QUESTION 21
A technician is decommissioning a server from a production environment. The technician removes the server from the rack but then decides to repurpose the system as a lab server instead of decommissioning it. Which of the following is the most appropriate NEXT step to recycle and reuse 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 22
A server technician installs a new NIC on a server and configures the NIC for IP connectivity. The technician then tests the connection using thepingcommand. Given the following partial output of thepingandipconfigcommands:



```
ipconfig /all

IPv4 address: 192.168.1.5
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.1

pinging 192.168.1.1 with 32 bytes of data:

Request timed out
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Request timed out
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
```

Which of the following caused the issue?

A. Duplicate IP address
B. Incorrect default gateway
C. DHCP misconfiguration
D. Incorrect routing table

Answer: A

Explanation:
? The ping command output shows that the NIC has an IP address of 192.168.1.100 and a default gateway of 192.168.1.1. However, when the technician tries to ping the default gateway, the reply comes from another IP address: 192.168.1.101. This means that there is another device on the network that has the same IP address as the default gateway, and it is responding to the ping request instead of the intended destination.
? A duplicate IP address can cause network connectivity problems, such as packet loss, routing errors, or unreachable hosts. To resolve this issue, the technician should either change the IP address of the default gateway or the device that is conflicting with it, or use DHCP to assign IP addresses automatically and avoid conflicts.
? The other options are not correct because they do not explain the ping output. An incorrect default gateway would cause no reply or a destination unreachable message, not a reply from a different IP address. A DHCP misconfiguration would cause an invalid or no IP address on the NIC, not a duplicate IP address on the network. An incorrect routing table would cause routing errors or unreachable destinations, not a reply from a different IP address.
References:
? https://askleo.com/what_is_ping_and_what_does_its_output_tell_me/
? https://learn.microsoft.com/en-us/windows-server/administration/windows- commands/ping

NEW QUESTION 23
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 24
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 PCle 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 25
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 26
A systems administrator is preparing to install two servers in a single rack. The administrator is concerned that having both servers in one rack will increase the chance of power issues due to the increased load. Which of the following should the administrator implement FIRST to address the issue?

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

Answer: A

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

NEW QUESTION 27
Which of the following licensing models is MOST appropriate tor a data center that has a variable daily equipment count?

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

Answer: D

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

NEW QUESTION 28
A server administrator has been creating new VMs one by one. The administrator notices the system requirements are very similar, even with different applications. Which of the following would help the administrator accomplish this task in the SHORTEST amount of time and meet the system requirements?

A. Snapshot
B. Deduplication
C. System Restore
D. Template

Answer: D

Explanation:
The method that would help the administrator accomplish the task of creating new VMs in the shortest amount of time and meet the system requirements is template. A template is a preconfigured virtual machine image that contains an operating system, applications, settings, and other components. A template can be used to create multiple identical or customized VMs quickly and easily, without having to install and configure each VM from scratch. A template can save time and ensure consistency across VMs.

NEW QUESTION 29
A server administrator needs to ensure all Window-based servers within a data center have RDP disabled. There are thousands of servers performing various roles. Which of the following is the best way to meet this requirement?

A. Run chkconfig ——1eve1 345 RDP off.
B. Create a PowerShell script to disable the RDP service.
C. Run chkconfig —— list RDP.
D. Create a Bash shell script to disable the Windows Remote Management service.
E. Create a GPO to disable the Windows Remote Management service.

Answer: B

Explanation:
The best way to meet this requirement is to create a PowerShell script to disable the RDP service on all Windows-based servers within a data center. PowerShell is a scripting language and command-line tool that can be used to automate tasks and manage Windows systems remotely. A PowerShell script can use cmdlets (commands) and parameters to perform actions on multiple servers at once, such as disabling a service or changing a configuration setting. RDP (Remote Desktop Protocol) is a service that allows remote access and control of a Windows system through a graphical user interface. Disabling RDP can improve security by preventing unauthorized or malicious access to the servers.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 4, Lesson 4.3, Objective 4.3; Chapter 7, Lesson 7.1, Objective 7.1

NEW QUESTION 30
The network's IDS is giving multiple alerts that unauthorized traffic from a critical application server is being sent to a known-bad public IP address.
One of the alerts contains the following information: Exploit Alert
Attempted User Privilege Gain 2/2/07-3: 09:09 10.1.200.32
--> 208.206.12.9:80
This server application is part of a cluster in which two other servers are also servicing clients. The server administrator has verified the other servers are not sending out traffic to that public IP address. The IP address subnet of the application servers is 10.1.200.0/26. Which of the following should the administrator perform to ensure only authorized traffic is being sent from the application server and downtime is minimized? (Select two).

A. Disable all services on the affected application server.
B. Perform a vulnerability scan on all the servers within the cluster and patch accordingly.
C. Block access to 208.206.12.9 from all servers on the network.
D. Change the IP address of all the servers in the cluster to the 208.206.12.0/26 subnet.
E. Enable GPO to install an antivirus on all the servers and perform a weekly reboot.
F. Perform an antivirus scan on all servers within the cluster and reboot each server.

Answer: BF

Explanation:
The administrator should perform an antivirus scan on all servers within the cluster and reboot each server, and block access to 208.206.12.9 from all servers on the network. These actions will help to remove any malware that may have infected the application server and prevent any further unauthorized traffic to the known-bad public IP address. An antivirus scan can detect and remove malicious software that may be sending data to an external source, and a reboot can clear any temporary files or processes that may be related to the malware. Blocking access to 208.206.12.9 from all servers on the network can prevent any future attempts to communicate with the malicious IP address.
References: CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.4, Objective 3.4; Chapter 6, Lesson 6.2, Objective 6.2

NEW QUESTION 31
......