Vendor: CompTIA

Exam Code: SK0-005

Exam Name: CompTIA Server+ Certification Exam

Version: DEMO

QUESTION 1
A server technician is installing a Windows server OS on a physical server. The specifications for the installation call for a 4TB data volume. To ensure the partition is available to the OS, the technician must verify the:

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

Answer: B
Explanation:
GPT was developed to replace the limitations of MBR, and it is part of UEFI development to replace PC BIOS.
So the Hardware has to UEFI compatible for GPT to be fully effective.

QUESTION 2
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: BC
Explanation:
While some vulnerable services have continuing utility, legacy services such as Telnet on TCP port 23 were fundamentally unsafe from the start.
Port 22, the designated Secure Shell port that enables access to remote shells on physical server hardware is vulnerable where the credentials include default or easily guessed user names and passwords, according to David Widen, systems engineer at BoxBoat Technologies.
https://www.csoonline.com/article/3191531/securing-risky-network-ports.html

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

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

Answer: AB
Explanation:

1. **Remotely Access Computers and Software**

Take control of all remote computers, servers and virtual machines on your LAN or WAN by connecting your KVM switches over your existing IP network. KVM over IP combines the advantages of remote access software with the benefits of KVM switching technology. Like most KVM switches, KVMoIP products don't require any software to be loaded on the host computers. They interface directly with the keyboard, monitor, and mouse connectors of the host computer or KVM switch. The KVM over IP switch digitises the incoming video signal and processes it into digital data that is communicated to a remote client computer over a LAN/WAN or the public Internet.

https://www.blackbox.be/en-be/page/27559/Resources/Technical-Resources/Black-Box-Explains/kvm/Benefits-of-using-KVM-over-IP

QUESTION 4
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:
Constant Replication
The primary system replicates data changed data blocks continually. Constant replication is also referred to as "continuous replication." The replication process occurs in the background, permitting users to access the data without interruption.
Constant replication is different than regular backups, where files must be closed to be duplicated.

QUESTION 5
Which of the following would be BEST to help protect an organization against social engineering?

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

Answer: B
Explanation:
User awareness and training is the number one defense against most security threats.

QUESTION 6
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:
Command will display file sizes in human readable format.

https://www.linuxteck.com/df-command-in-linux-with-examples/

QUESTION 7
Which of the following documents would be useful when trying to restore IT infrastructure operations after a non-planned interruption?

A. Service-level agreement
B. Disaster recovery plan
C. Business impact analysis
D. Business continuity plan

Answer: B
Explanation:
A disaster recovery (DR) plan is used to bring failed systems online as quickly and efficiently as possible. The DR plan must be updated periodically to reflect changing threats.
The DR plan contains step-by-step procedures detailing exactly how systems are to be quickly recovered. All stakeholders must know their roles for the effective recovery of failed systems.
The DR plan includes the following:
• Table of contents
• DR scope
• Contact information
• Recovery procedures
• Document revision history
• Glossary

QUESTION 8
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: C
Explanation:
Power distribution units (PDUs) provide power outlets to racks in server rooms and data centers. To eliminate a single point of failure, redundant PDUs should be plugged into separate circuits. To extend this point, redundant server power supplies should each plug into separate PDUs. Data centers normally have alternate sources or providers of power, such as diesel generators, in the case of a power outage.
Because many different types of items can draw power from PDUs, you should check your PDU's rating to ensure that your equipment doesn't draw more power than the PDU's load capacity can accommodate.

QUESTION 9

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

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

Answer: A
Explanation:
The first line of physical defense is perimeter security, which comes from the following:
• Fencing
• Bollard posts to protect buildings from vehicle incursion
• Lighting
• Locked gates
• Security guards
• Guard dogs
• Limited access to areas of a facility
• Motion-sensing security systems

QUESTION 10
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:
Always load servers from the bottom up. This prevents servers from becoming top-heavy and tipping also we do not alternate the direction of the airflow because that would have already been setup on the room with airflow sensors.

QUESTION 11
Which of the following is an example of load balancing?

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

Answer: B
Explanation:
Active-active clusters use a load balancer device to distribute server requests between the nodes. This design provides high availability and also increases performance. The load balancer distributes the workload among the cluster nodes.
There are many scheduling types for load balancers. Three of them are round robin, most recently used, and weighted scheduling.

QUESTION 12
A server technician is configuring the IP address on a newly installed server. The documented configuration specifies using an IP address of 10.20.10.15 and a default gateway of 10.20.10.254. Which of the following subnet masks would be appropriate for this setup?

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

Answer: A
Explanation:
10.20.10.15 and 10.20.10.254 should be in the same subnet
255.255.255.0 must be the subnet mask.

QUESTION 13
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 sucessful. 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: C
Explanation:
The IP address in the command output is different on each machine.
hosts.allow and hosts.deny are for ACL not direction.
a host file that is different on each machine would cause the IP address to be different.

QUESTION 14
A security analyst suspects a remote server is running vulnerable network applications. The analyst does not have administrative credentials for the server. Which of the following would MOST likely help the analyst determine if the applications are running?

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

Answer: D
Explanation:
You can run nmap to determine what ports are open and what services are running on them and could even run a -sV to determine version.

QUESTION 15
Ann, an administrator, is configuring a two-node cluster that will be deployed. To check the cluster's functionality, she shuts down the active node. Cluster behavior is as expected, and the passive node is now active. Ann powers on the server again and wants to return to the original configuration. Which of the following cluster features will allow Ann to complete this task?

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

Answer: B
Explanation:
When you research server clustering, you frequently hear the terms failover and failback. Failover refers to the failure of the active service provider node and passive node's taking over of its responsibilities. At that point, the server that was the passive node becomes the active node. It services clients and handles the cluster's duties. Once the original active node returns to service, you may set it to act as the new passive node, or you may shift the services back to it, causing it to take back its active node role and relegating the formerly passive server to its original role. The term failback refers to the service returning to the original active node.

QUESTION 16
A server technician is deploying a server with eight hard drives. The server specifications call for a RAID configuration that can handle up to two drive failures but also allow for the least amount of drive space lost to RAID overhead. Which of the following RAID levels should the technician configure for this drive array?

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

Answer: C
Explanation:
RAID 6 Disk Striping with Double Parity
The RAID 6 design distributes data across a minimum of four HDDs the same way that RAID 0 and RAID 5 do, but it also distributes parity information across two disks. The result is that a RAID 6 array can recover data even with the failure of two HDDs. Reads are quick, like RAID 5, but writes are slower due to the duplication of the parity data. It is a good general solution as long as the performance hit on write tasks is not a problem for your environment.
RAID 6 requires a minimum of four HDDs.

QUESTION 17
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:
Out-of-band administration provides hardware-level remote access to a host without relying on the OS software running. Common solutions include Dell's iDRAC and HP's iLO; the server hardware must support this type of remote administration, and it must be configured with IP settings.

QUESTION 18
Which of the following steps in the troubleshooting theory should be performed after a solution has been implemented? (Choose two.)

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

Answer: AC
Explanation:
The following list represents the basic steps in a troubleshooting methodology:
Identify the problem
Determine the scope of the problem
Establish a theory of probable cause/question the obvious
Test the theory to determine the cause
Establish a plan of action
Implement the solution or escalate the issue
Verify full system functionality
Implement preventive measures
Perform a root cause analysis
Document findings, actions, and outcomes throughout the process.

QUESTION 19
An administrator needs to perform bare-metal maintenance on a server in a remote datacenter. Which of the following should the administrator use to access the server's console?

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

Answer: A
Explanation:
If a system is bare metal, there is no way to access the BIOS and Hardware without a crash cart, KVM, console, or remote management (iLO, etc). Since only one of those options (ip KVM or iLO) can be done remotely, that would be the correct answer.
RDP would allow you to manage the operating system running on the server, but not the bare metal system itself.

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: ASTR14