Free Questions for SK0-005 by go4braindumps

Shared by Klein on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- MTBF

B- RTO

C- MTTR

D- RPO

Answer:

B

Explanation:

Recovery Time Objective (RTO) refers to the target time set for the recovery of IT and business activities after a disaster has struck, which includes restoring server, network, and data access. The policy requirement mentioned in the question aligns with the definition of

RTO, as it specifies the maximum allowable downtime or the time within which functionality must be restored. Mean Time Between Failures (MTBF) and Mean Time To Repair (MTTR) are metrics related to the reliability and repair times of systems but do not specifically pertain to disaster recovery time frames. Recovery Point Objective (RPO) describes the acceptable amount of data loss measured in time, not the restoration of operations.

Question 2

Question Type: MultipleChoice

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

Options:

A- Check the RAID controller (or background rebuild tasks

B- Check the firmware version on the newly replaced disk.

C- Check the RPM speed on the newly replaced disk-

D- Check the cache settings on the RAID controller.

Answer:

C

Explanation:

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

Question 3

Question Type: **MultipleChoice**

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

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

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

Options:

A- chown

B- sestatus

C- setenforce

D- getenforce

E- chmod

Answer:

E

Explanation:

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

Question 4

Question Type: MultipleChoice

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

Options:

A- Use the keyboard command AH+F12 to switch to the kernel log screen

B- Perform a hard reboot on the server and monitor the server startup

C- Collect a screenshot of the PSOD and note the details after the line detailing the OS version

D- Collect a core dump from the server and store locally before rebooting the hardware

Answer:

C

Explanation:

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

Question 5

Question Type: MultipleChoice

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

Options:

A- Check the power cables

B- Clean the fans.

C- Replace the RAM.

D- Reattach the CPU heat sink

Answer:

A

Explanation:

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

Question 6

Question Type: MultipleChoice

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

will best meet the administrator's requirements?

Options:

A- Deploying each server from a VM template

B- Using a kickstart file during installation

C- Configuring each server manually one at a time

D- Copying/pasting configuration commands into each server through SSH sessions

E- Configuring a single server and then creating clones of it

Answer:

B

Explanation:

Kickstart Files (Linux):Kickstart files are configuration files that automate the Linux installation process. They contain pre-determined answers to installation prompts, allowing for identical and rapid deployment of multiple systems. (CompTIA Server+ Objectives SK0-004: 3.1, Red Hat documentation on Kickstart:https://access.redhat.com/documentation/)

Why other options are less ideal:

VM Template (A):Templates are useful for replicating the OS & some software, but might not capture all configurations.

Manual Configuration (C):Time-consuming and prone to errors when replicating across many servers.

Copy/Paste via SSH (D):Tedious, error-prone, and requires servers to be online before configuration.

Cloning (E):Can work but has version compatibility risks if the OS of the cloned server isn't identical to the new ones.

Question 7

Question Type: **MultipleChoice**

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?

Options:

A- 25

B- 53

C- 443

D- 3389

E- 8080

Answer:

C

Explanation:

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

Why other options are not essential:

25 (SMTP):Used for email transmission

53 (DNS):Used for domain name resolution

**3389 (RDP): ** Used for remote desktop connections

**8080 (Alternate HTTP): ** Sometimes used for web servers, but not the standard secure port

Question 8

Question Type: MultipleChoice

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

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

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

Options:

A- 1,2, 4, and 6

B- 1, 2, 3, 5, and 6

C- 1, 2, 4, 5, and 6

D- 1, 2, 3, 4, and 6

Answer:

C

Explanation:

RAID 5 configuration:Using five of the available drives in a RAID 5 configuration meets the requirements for:

Storage capacity:Four 600GB drives (2, 5, and 6) provide a total usable capacity of 2.4TB (4 * 600 * 0.8), exceeding the minimum requirement of 2TB. RAID 5 introduces parity data for fault tolerance, sacrificing some usable space (one drive's worth).

Performance:The combination of multiple drives in a RAID 5 array improves read performance compared to a single drive setup.

Fault tolerance:Even with a single drive failure (any of the five drives used in the RAID 5), the remaining drives can reconstruct the lost data, allowing the server to continue operating.

Question 9

Question Type: MultipleChoice

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

Options:

A- Applying OS updates

B- Disabling unused services

C- Implementing HIDS

D- Installing anti-malware

Answer:

C

Explanation:

HIDS (Host Intrusion Detection System):Continuously monitors a system for suspicious activity and logs or raises alerts when potential threats are identified. This proactive approach is crucial for identifying and mitigating threats on a web server exposed to the external network.

Applying OS updates:While essential for maintaining system security, updates address vulnerabilities and may not necessarily identify ongoing threats.

Disabling unused services:Reduces the attack surface by minimizing potential entry points for malicious actors, but doesn't actively identify threats.

Installing anti-malware:Primarily designed to detect and remove malware after infection, not for ongoing threat identification.

CompTIA Server+ Objectives(Exam codes SK0-004 or SK0-005): Search for sections on intrusion detection and prevention.

To Get Premium Files for SK0-005 Visit

https://www.p2pexams.com/products/sk0-005

For More Free Questions Visit

https://www.p2pexams.com/comptia/pdf/sk0-005