

DUMPS ARENA

CompTIA Server+ Certification Exam

CompTIA SK0-005

Version Demo

Total Demo Questions: 15

Total Premium Questions: 208

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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 plan would be useful when trying to restore IT infrastructure operations after a non-planned interruption. A disaster recovery plan is a document that outlines the steps and procedures to recover from a major disruption of IT services caused by natural or man-made disasters, such as fire, flood, earthquake, cyberattack, etc. A disaster recovery plan typically includes:

A disaster recovery plan helps IT organizations to minimize downtime, data loss, and financial impact of a disaster, as well as to resume normal operations as quickly as possible.

QUESTION NO: 2

An organization implements split encryption keys for sensitive files. Which of the following types of risks does this mitigate?

- A. Hardware failure
- B. Malware
- C. Data corruption
- D. Insider threat

ANSWER: D**QUESTION NO: 3**

A technician needs to set up a server backup method for some systems. The company's management team wants to have quick restores but minimize the amount of backup media required. Which of the following are

the BEST backup methods to use to support the management's priorities? (Choose two.)

- A. Differential

- B. Synthetic full
- C. Archive
- D. Full
- E. Incremental
- F. Open file

ANSWER: A E

Explanation:

The best backup methods to use to support the management's priorities are differential and incremental. A backup is a process of copying data from a source to a destination for the purpose of restoring it in case of data loss or corruption. There are different types of backup methods that vary in terms of speed, efficiency, and storage requirements. Differential and incremental backups are two types of partial backups that only copy the data that has changed since the last full backup. A full backup is a type of backup that copies all the data from the source to the destination. A full backup provides the most complete and reliable restore option, but it also takes the longest time and requires the most storage space. A differential backup copies only the data that has changed since the last full backup. A differential backup provides a faster restore option than an incremental backup, but it also takes more time and requires more storage space than an incremental backup. An incremental backup copies only the data that has changed since the last backup, whether it was a full or an incremental backup. An incremental backup provides the fastest and most efficient backup option, but it also requires multiple backups to restore the data completely.

QUESTION NO: 4

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: A C

QUESTION NO: 5

A Linux administrator created a script that will run at startup. After successfully writing the script, the administrator received the following output when trying to execute the script:

```
Bash ./startup,sh:Permission denied
```

Which of the following commands would BEST resolve the error message?

- A. Chmod +w startup.sh
- B. Chmod 444 startup.sh
- C. Chmod+x startup.sh
- D. Chmod 466 startUp,sh

ANSWER: C

QUESTION NO: 6

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

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

ANSWER: A B H

QUESTION NO: 7

A backup application is copying only changed files each time it runs. During a restore, however, only a single file is used. Which of the following backup methods does this describe?

- A. Open file
- B. Synthetic full
- C. Full incremental
- D. Full differential

ANSWER: B

QUESTION NO: 8

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: A C**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>

QUESTION NO: 9

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

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

ANSWER: B F**Explanation:**

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

QUESTION NO: 10

An administrator is installing a new file server that has four drive bays available. Which of the following RAID types would provide the MOST storage as well as disk redundancy?

- A. RAID0
- B. RAID 1
- C. RAID 5
- D. RAID 10

ANSWER: C**QUESTION NO: 11**

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: C E**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.

QUESTION NO: 12

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.

QUESTION NO: 13

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

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

ANSWER: B**Explanation:**

To ensure the partition is available to the OS, the technician must verify that the volume is formatted as GPT. GPT (GUID Partition Table) is a partitioning scheme that defines how data is organized on a hard disk drive (HDD) or a solid state drive (SSD). GPT uses globally unique identifiers (GUIDs) to identify partitions and supports up to 128 primary partitions per disk. GPT also supports disks larger than 2 TB and has a backup copy of the partition table at the end of the disk for data recovery. GPT is required for installing Windows on UEFI-based PCs, which offer faster boot time and better security than legacy BIOS-based PCs.

QUESTION NO: 14

A systems administrator needs to configure a new server and external storage for a new production application environment. Based on end-user specifications, the new solution needs to adhere to the following basic requirements:

1. The OS must be installed in a separate disk partition. In case of hard drive failure, it cannot be affected.
2. Application data IOPS performance is a must.
3. Data availability is a high priority, even in the case of multiple hard drive failures.

Which of the following are the BEST options to comply with the user requirements? (Choose three.)

- A. Install the OS on a RAID 0 array.
- B. Install the OS on a RAID 1 array.
- C. Configure RAID 1 for the application data.
- D. Configure RAID 5 for the application data.
- E. Use SSD hard drives for the data application array.
- F. Use SATA hard drives for the data application array.
- G. Use a single JBOD for OS and application data.

ANSWER: B D E

Explanation:

References:

QUESTION NO: 15

A server administrator receives the following output when trying to ping a local host:

```
ping imhrh-vc.net
Reply from imhrh-vc.net: Destination host unreachable.
Reply from imhrh-vc.net: Destination host unreachable.
Reply from imhrh-vc.net: Destination host unreachable.
Reply from imhrh-vc.net: Destination host unreachable.
```

Which of the following is MOST likely the issue?

- A. Firewall
- B. DHCP
- C. DNS
- D. VLAN

ANSWER: A

Explanation:

A firewall is a network device or software that filters and controls the incoming and outgoing traffic based on predefined rules. A firewall can block or allow certain types of packets, ports, protocols, or IP addresses. The output of the ping command shows that the local host is unreachable, which means that there is no network connectivity between the source and the destination. This could be caused by a firewall that is blocking the ICMP (Internet Control Message Protocol) packets that ping uses to test the connectivity. References: <https://www.comptia.org/training/resources/exam-objectives/comptia-server-sk0-005-exam-objectives> (Objective 2.2)