Free Questions for SK0-005 by certscare

Shared by Montgomery on 15-04-2024

For More Free Questions and Preparation Resources

Question 1

An IT administrator is configuring ten new desktops without an operating system. The infrastructure contains an imaging server and operating system loaded on a USB, a DVD, and an SD card. Which of the following options

would minimize the amount of time the administrator needs to load the operating system on every machine?

Options:

A- SD card

B- Optical

C- Network

D- USB

Answer:

C

Explanation:

Using a network-based deployment, such as network booting (PXE - Preboot Execution Environment) or imaging through a server, is the most efficient way to load operating systems onto multiple machines simultaneously. This approach minimizes the manual intervention required for each device, as the administrator can initiate the operating system installation or imaging process across all desktops at once through the network. In contrast, using an SD card, DVD (Optical), or USB would require the administrator to physically move the media from one desktop to another, significantly increasing the setup time for each device.

Question 2

Question Type: MultipleChoice

An administrator is setting up a new employee's read/write access to a document on the file server. Currently, the user can open the file, but edits cannot be saved. Which of the following should the administrator do so the user

can save the updated file while maintaining least-privilege access?

Options:

A- Give the user 'read and execute' rights to the file.

B- Give the user 'modify' rights to the file.

C- Give the user 'list folder contents' rights to the folder.

D- Give the user 'full control' rights to the folder.

Answer:

B

Explanation:

To enable a user to both read and write to a file, the administrator needs to provide 'modify' rights. This permission level allows the user not only to open and view the file (read) but also to make changes and save those changes back to the file (write). 'Read and execute' rights would allow the user to open and run the file but not make any changes. 'List folder contents' rights would enable the user to view the files within a folder but not make changes to them. 'Full control' rights would provide the user with complete control over the file, including the ability to change permissions and delete the file, which exceeds the principle of least-privilege access necessary for this task.

Question 3

Question Type: MultipleChoice

A new company policy requires that any data loss in excess of one hour is unacceptable in the event of a disaster. Which of the following concepts is being referred to in this policy?

Options:

A- MTTR

B- RTO

C- RPO

D- MTBF

Answer:

C

Explanation:

The Recovery Point Objective (RPO) refers to the maximum tolerable period in which data might be lost from an IT service due to a major incident. The policy mentioned in the question highlights that data loss exceeding one hour is unacceptable, directly relating to the RPO concept. RPO is critical in disaster recovery and business continuity planning, indicating the age of the files that must be recovered from backup storage for normal operations to resume without significant losses. MTTR (Mean Time To Repair), RTO (Recovery Time Objective), and MTBF (Mean Time Between Failures) are related concepts but do not specifically address the amount of data loss that can be tolerated.

Question 4

Which of the following authentication types defines credentials as "something you have"?

Options:

A- Swipe pattern

B- PIN

C- Fingerprint

D- Smart card

Answer:

D

Explanation:

The concept of authentication is rooted in the principle of verifying identity, which is commonly broken down into three categories: 'something you know' (like a password or PIN), 'something you have' (such as a smart card or a security token), and 'something you are' (biometric data, for example, fingerprints). The question asks for the authentication type defined by 'something you have.'

Question 5

An employee who was dismissed did not return company-issued equipment. Which of the following is the most important information the IT department needs to give to the legal department?

Options:

A- Labeling

B- Serial number

C- Warranty

D- Asset tag

Answer:

D

Explanation:

The most important piece of information needed by the legal department in the event that an employee does not return company-issued equipment is the asset tag. The asset tag is a unique identifier that is used to track assets throughout their lifecycle. It allows the company to keep precise records of the assets, monitor their location, and manage their overall inventory. In legal situations, the asset tag can be used to prove ownership and aid in the recovery process of the equipment. The serial number is also important, but it is the asset tag that ties the equipment directly to the company's asset management system and is therefore the most crucial for the legal department. Warranty and labeling information are less critical from a legal perspective when it comes to unreturned equipment.

Question 6

Question Type: MultipleChoice

A virtual host has four NICs and eight VMs. Which of the following should the technician configure to enable uplink redundancy?

Options:

A- VM

B- vNIC

C- vSwitch

D- vCPU

E- vHBA

Answer:

C

Explanation:

Uplink redundancy is a method used to ensure that if one physical network interface card (NIC) fails, the network connectivity for the virtual machines (VMs) does not go down. This is typically achieved by configuring multiple NICs to connect to a single virtual switch (vSwitch) and setting up NIC teaming or bonding. The vSwitch manages the internal network traffic between the VMs and the outside network by using the physical NICs assigned to it. By configuring the vSwitch with multiple NICs, you can create redundancy, so if one NIC fails, the other NICs can take over the traffic, ensuring continuous network connectivity.

Question 7

Question Type: **MultipleChoice**

A technician is configuring a server rack that will hold ten blade servers. Which of the following safety concerns should be observed? (Select three).

Options:

A- Floor load limitations

B- Rack balancing

C- Proper lifting techniques

D- Power connector type

E- KVM placement

F- Cable management

G- UPS power requirements

H- PDU installation

I- Separate circuits for power

Answer:

A, B, C

Explanation:

When configuring a server rack, it's important to consider:

A) Floor load limitations: Server racks can be extremely heavy, especially when filled with equipment like blade servers. It is crucial to ensure that the floor can handle the load to avoid structural damage or failure.

B) Rack balancing: Properly distributing the weight in a server rack is important for stability. Heavier equipment should generally be placed at the bottom to prevent the rack from becoming top-heavy and risking a tip-over.

C) Proper lifting techniques: Using correct lifting techniques when placing servers into a rack is vital to prevent personal injury.