Free Questions for 220-1102 by dumpshq

Shared by Riley on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following Windows 10 editions is the most cost-effective and appropriate for a single user who needs to access their computer remotely?

Options:

A- Education

B- Pro

C- Enterprise

D- Home

Answer:

B

Explanation:

For a single user who needs to access their computer remotely, the Windows 10 Pro edition is the most cost-effective and appropriate choice. It includes features such as Remote Desktop, which are essential for remote access.

Option A: Education This edition is designed for academic institutions and includes educational features. It is not the most cost-effective for a single user.

Option B: Pro Windows 10 Pro includes Remote Desktop and other business features. It is suitable and cost-effective for single users needing remote access.

Option C: Enterprise This edition includes advanced features for large organizations and is more expensive, making it less cost-effective for a single user.

Option D: Home While cost-effective, Windows 10 Home does not include the Remote Desktop feature, making it unsuitable for this requirement.

CompTIA A+ 220-1102 Objective 1.1 (Identify basic features of Microsoft Windows editions), particularly comparing editions based on features and cost.

Question 2

Question Type: **MultipleChoice**

A technician is investigating a workstation that has not received the latest policy changes. Which of the following commands should the technician use to apply the latest domain policy changes?

Options:

A- sfc /scannow

B- gpupdare /force

C- chkdsk /y

D- xcopy Zp

Answer:

B

Explanation:

When a workstation has not received the latest policy changes, the gpupdate command is used to manually apply the latest group policies from the domain controller.

Option A: sfc /scannow This command is used to scan and repair corrupted system files, not to update group policies.

Option B: gpupdate /force This command forces the workstation to reapply all group policies, ensuring that the latest policies are applied immediately.

Option C: chkdsk /y This command checks the integrity of the file system and fixes logical file system errors, not to update group policies.

Option D: xcopy /Zp This command is used for copying files and directories, not for updating group policies.

CompTIA A+ 220-1102 Objective 1.6 (Configure Microsoft Windows networking features on a client/desktop), particularly managing and applying group policies.

Question 3

Question Type: **MultipleChoice**

Which of the following filesystems supports journaling?

Options:

A- NTFS

B- exFAT

C- HFS

D- ext2

Answer:

A

Explanation:

Journaling is a feature that helps maintain the integrity of the filesystem by keeping a record of changes not yet committed to the main file system. This feature is supported by various filesystems, but not all.

Option A: NTFS NTFS (New Technology File System) is a filesystem used by Windows that supports journaling. This makes it resilient to corruption from unexpected shutdowns or crashes by keeping a log of file changes.

Option B: exFAT exFAT (Extended File Allocation Table) does not support journaling. It is optimized for flash drives and large files but lacks advanced features like journaling.

Option C: HFS HFS (Hierarchical File System) is an older filesystem used by Apple. HFS+ (also known as Mac OS Extended) supports journaling, but HFS itself does not.

Option D: ext2 ext2 (Second Extended File System) is a filesystem for Linux that does not support journaling. Its successor, ext3, introduced journaling.

CompTIA A+ 220-1102 Objective 1.8 (Explain common OS types and their purposes), particularly filesystems and their features.

Question 4

Question Type: MultipleChoice

Which of the following provides disk encryption on computers running a Windows OS?

Options:

A- FileVault

B- BitLocker

C- Private Key

D- PowerShell

Answer:

B

Explanation:

BitLocker is a full-disk encryption feature included with certain editions of Windows, designed to protect data by providing encryption for entire volumes.

Option A: FileVault FileVault is a disk encryption program in macOS, not Windows.

Option B: BitLocker BitLocker is the correct tool for disk encryption on Windows operating systems, providing full disk encryption.

Option C: Private Key A private key is part of public key infrastructure (PKI) used in encryption, but it is not a tool for disk encryption by itself.

Option D: PowerShell PowerShell is a task automation and configuration management framework from Microsoft, not a tool for disk encryption.

CompTIA A+ 220-1102 Objective 2.5 (Manage and configure basic security settings in the Windows OS), particularly BitLocker for disk encryption.

Question 5

Question Type: **MultipleChoice**

The company uses shared drives as part of a workforce collaboration process. To ensure the correct access permissions, inheritance at the top-level folder is assigned to each department. A manager's team is working on confidential material and wants to ensure only the immediate team can view a specific folder and its subsequent files and subfolders. Which of the following actions should the technician most likely take?

Options:

A- Turn off inheritance on the requested folder only and set the requested permissions to each file manually.

B- Turn off inheritance at the top-level folder and remove all inherited permissions.

C- Turn off Inheritance at the top-level folder and set permissions to each file and subfolder manually.

D- Turn off inheritance on the requested folder only, set the requested permissions, and then turn on inheritance under the child folders.

Answer:

D

Explanation:

For managing permissions where a specific folder needs to have different access controls than its parent, turning off inheritance for that specific folder is the correct approach.

Option A: Turn off inheritance on the requested folder only and set the requested permissions to each file manually This is partially correct, but setting permissions manually for each file is inefficient and error-prone.

Option B: Turn off inheritance at the top-level folder and remove all inherited permissions This action would disrupt permissions for all other folders and files, not just the confidential folder.

Option C: Turn off inheritance at the top-level folder and set permissions to each file and subfolder manually This approach is overly broad and inefficient, impacting more than just the specific folder that needs restricted access.

Option D: Turn off inheritance on the requested folder only, set the requested permissions, and then turn on inheritance under the child folders This ensures the specific folder has unique permissions while allowing those permissions to propagate to its children, maintaining

security and ease of management.

CompTIA A+ 220-1102 Objective 2.5 (Manage and configure basic security settings in the Windows OS), particularly file and folder permissions and inheritance settings.

Question 6

Question Type: MultipleChoice

A workstation does not recognize a printer. However, the previous day. the printer successfully received a job from the workstation. Which of the following tools should a technician use to see what happened before the failure?

Options:

A- Performance Monitor

B- Devices and Printers

C- Task Scheduler

D- Event Viewer

Answer:

D

Explanation:

When troubleshooting a printer that was previously working but is no longer recognized by a workstation, Event Viewer is the most appropriate tool to check for historical logs and events related to the printer and the system.

Option A: Performance Monitor Performance Monitor is used for monitoring system performance and resources in real-time and does not provide specific historical event logs related to device failures.

Option B: Devices and Printers Devices and Printers show the status and properties of connected devices but do not provide a historical log of events or errors.

Option C: Task Scheduler Task Scheduler manages and monitors scheduled tasks but does not log hardware events or errors.

Option D: Event Viewer Event Viewer logs system events, including errors, warnings, and information related to hardware and software. It is ideal for checking what happened prior to the printer failure.

CompTIA A+ 220-1102 Objective 3.1 (Troubleshoot common Windows OS problems), particularly using Event Viewer for diagnosing issues.

Question 7

Question Type: MultipleChoice

A user's Android phone has been randomly restarting. A technician investigates and finds several applications have been installed that are not available within the standard marketplace. Which of the following is most likely the cause of the issue?

Options:

A- The OS update failed.

B- The user downloaded malware.

C- The device is In developer mode.

D- The over-the-air carrier update failed.

Answer:

B

Explanation:

Random restarting of an Android phone and the presence of applications not from the standard marketplace strongly suggest the possibility of malware.

Option A: The OS update failed While an OS update failure can cause issues, it is less likely to result in random restarts compared to malware.

Option B: The user downloaded malware Malware is a common cause of erratic behavior, including random restarts, especially when applications are installed from unofficial sources.

Option C: The device is in developer mode Developer mode alone does not typically cause random restarts. It may make the device more susceptible to issues if improper apps are installed.

Option D: The over-the-air carrier update failed Similar to the OS update, this would more likely cause consistent issues rather than random restarts.

CompTIA A+ 220-1102 Objective 2.3 (Detect, remove, and prevent malware) and Objective 3.5 (Mobile OS and application security issues).

Question 8

Question Type: **MultipleChoice**

A technician is configuring security for a computer that is located in a common are

a. A sign above the computer indicates only authorized users can use the computer. Guests visiting the office must walk past the computer to enter and leave the office. Which of the following will offer the best protection against physical threats?

Options:

A- Using screen lock

B- Installing a privacy screen

C- Implementing password complexity

D- Locking the computer case

E- Enabling drive encryption

Answer:

D

Explanation:

The best protection against physical threats, especially in a common area where the computer is publicly accessible, involves physically securing the hardware.

Option A: Using screen lock Screen locks are good for securing access temporarily but do not protect against physical tampering or theft.

Option B: Installing a privacy screen Privacy screens prevent visual access but do not secure the hardware.

Option C: Implementing password complexity Password complexity helps secure digital access but does not prevent physical threats.

Option D: Locking the computer case Physically securing the case prevents unauthorized individuals from tampering with internal components or stealing the computer.

Option E: Enabling drive encryption Encryption protects data but does not prevent physical access to the hardware itself.

CompTIA A+ 220-1102 Objective 2.1 (Physical security), particularly physical security measures like locking the computer case.