Free Questions for 220-1102

Shared by Keller on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following features can be used to ensure a user can access multiple versions of files?

Options:

A- Multiple desktops

B- Remote Disc

C- Time Machine

D- FileVault

Answer:

C

Explanation:

Time Machine is a backup feature available in macOS that automatically makes hourly backups for the past 24 hours, daily backups for the past month, and weekly backups for all previous months to an external drive or NAS. It allows users to recover the entire system or specific files from any point in time, ensuring access to multiple versions of files. This feature is particularly useful for reverting to earlier versions of a document or recovering a file that has been accidentally deleted or altered. The other options, such as Multiple Desktops, Remote Disc, and FileVault, do not provide versioning capabilities for file access.

Question 2

Question Type: MultipleChoice

A user is setting up a new Windows 10 laptop. Which of the following Windows settings should be used to input the SSID and password?

Options:

A- Network & Internet

B- System

C- Personalization

D- Accounts

Answer:

A

Explanation:

The Network & Internet settings in Windows 10 allow the user to input the SSID and password of a Wi-Fi network, as well as manage other network-related options, such as airplane mode, mobile hotspot, VPN, proxy, etc1.To access the Network & Internet settings, the user can select the Start button, then select Settings > Network & Internet2.Alternatively, the user can right-click the Wi-Fi icon on the taskbar and click 'Open Network & Internet Settings'3.

The System settings in Windows 10 allow the user to configure the display, sound, notifications, power, storage, and other system-related options1.The Personalization settings in Windows 10 allow the user to customize the background, colors, lock screen, themes, fonts, and other appearance-related options1.The Accounts settings in Windows 10 allow the user to manage the user accounts, sign-in options, sync settings, and other account-related options1. None of these settings can be used to input the SSID and password of a Wi-Fi network.

The Official CompTIA A+ Core 2 Study Guide1, page 221, 222, 223, 224.

Question 3

Question Type: MultipleChoice

A technician is hardening a company file server and needs to prevent unauthorized LAN devices from accessing stored files. Which of the following should the technician use?

Options:

A- Software firewall

B- Password complexity

C- Antivirus application

D- Anti-malware scans

Answer:

A

Explanation:

A software firewall is a program that monitors and controls the incoming and outgoing network traffic on a computer or a server. A software firewall can help prevent unauthorized LAN devices from accessing stored files on a company file server by applying rules and policies that filter the network packets based on their source, destination, protocol, port, or content.A software firewall can also block or allow specific applications or services from communicating with the network, and alert the administrator of any suspicious or malicious activity12.

A software firewall is a better option than the other choices because:

Password complexity (B) is a good practice to protect the file server from unauthorized access, but it is not sufficient by itself. Password complexity refers to the use of strong passwords that are hard to guess or crack by attackers, and that are changed frequently and securely.Password complexity can prevent brute force attacks or credential theft, but it cannot stop network attacks that exploit vulnerabilities in the file server software or hardware, or that bypass the authentication process34.

Antivirus application and anti-malware scans (D) are important tools to protect the file server from viruses and malware that can infect, damage, or encrypt the stored files. However, they are not effective in preventing unauthorized LAN devices from accessing the files in the first place. Antivirus and anti-malware tools can only detect and remove known threats, and they may not be able to stop zero-day attacks or advanced persistent threats that can evade or disable them.Moreover, antivirus and anti-malware tools cannot control the network traffic or the file server permissions, and they may not be compatible with all file server platforms or configurations56.

1: What is a Firewall and How Does it Work?- Cisco12: How to Harden Your Windows Server - ServerMania23: Password Security: Complexity vs.Length - Norton74: Password Hardening: 5 Ways to Protect Your Passwords - Infosec5: What is Antivirus Software and How Does it Work?- Kaspersky6: What is Anti-Malware? - Malwarebytes

Question 4

Question Type: MultipleChoice

Which of the following Windows 10 editions is the most appropriate for a single user who wants to encrypt a hard drive with BitLocker?

Options:

A- Professional

B- Home

C- Enterprise
D- Embedded

Answer:

A

Explanation:

BitLocker is a Windows security feature that provides encryption for entire volumes, addressing the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned devices1.BitLocker is available on supported devices running Windows 10 or 11 Pro, Enterprise, or Education2.Windows 10 Home does not support BitLocker3, and Windows 10 Embedded is designed for specialized devices and does not offer BitLocker as a feature4. Therefore, the most appropriate Windows 10 edition for a single user who wants to encrypt a hard drive with BitLocker is Professional.

Reference 1: BitLocker overview - Windows Security | Microsoft Learn 2: Device encryption in Windows - Microsoft Support 3: Can You Turn on BitLocker on Windows 10 Home? 4: How to enable device encryption on Windows 10 Home

Question 5

Question Type: MultipleChoice

A user is experiencing frequent malware symptoms on a Windows workstation. The user has tried several times to roll back the state but the malware persists. Which of the following would MOST likely resolve the issue?

Options:

A- Quarantining system files
B- Reimaging the workstation
C- Encrypting the hard drive
D- Disabling TLS 1.0 support

Answer:

C

Explanation:

Encrypting the hard drive would most likely resolve the issue1

Question 6

Question Type: MultipleChoice

A user received an alert from a Windows computer indicating low storage space. Which of the following will best resolve this issue?

Options:

A- Reviewing System Information
B- Running Disk Cleanup
C- Editing the Registry
D- Checking the Performance Monitor
E- Increasing the memory

Answer:

B

Question 7

Question Type: MultipleChoice

A customer recently upgraded their computer to the latest Windows version and is now having issues with the display. The icons and text are too large, and the colors are not accurate. Which of the following Control Panel options should the technician adjust to help the customer?

Options:

A- Ease of Access
B- Device Manager
C- Network and Sharing Center
D- Programs andFeatures

Answer:

B

Explanation:

When a customer experiences display issues such as large icons and inaccurate colors after a Windows upgrade, the most appropriate Control Panel option to address these issues is 'Device Manager.' The technician can use Device Manager to check and update display drivers, which are often the cause of such problems after an OS upgrade. Updating or reinstalling the correct drivers can help resolve display resolution and color issues.

A . Ease of Access focuses on accessibility features and does not directly address display driver issues.

C . Network and Sharing Center is related to network settings and does not affect display settings.

D . Programs and Features is used for managing installed programs and features but is not relevant for updating display drivers.

CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 1.3: Using features and tools of the Microsoft Windows OS, including Device Manager for managing hardware drivers.

Question 8

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 9

Question Type: MultipleChoice

After a computer upgrade at an imaging lab. the upgraded computers are not able to obtain an IP address. Which of the following is most likely the issue?

Options:

A- The switch Is only providing IPv6 addresses.
B- The OS must be updated to be compatible with the imaging software.
C- The switch has port security enabled.
D- The switch does not support multicast traffic.

Answer:

C

Explanation:

When upgraded computers are not able to obtain an IP address, the issue often lies in the network configuration. Here's a detailed explanation:

Option A: The switch is only providing IPv6 addresses. This is unlikely because if the switch were providing IPv6 addresses, the devices would still receive an IP address, albeit an IPv6 one. The issue described indicates no IP address is being obtained at all.

Option B: The OS must be updated to be compatible with the imaging software. This option is unrelated to obtaining an IP address. Compatibility with imaging software would not prevent the devices from getting an IP address.

Option C: The switch has port security enabled. Correct Answer. Port security on a switch restricts access based on MAC addresses. If the MAC addresses of the upgraded computers are not recognized or have not been added to the allowed list, the switch will not provide network access, resulting in the computers not obtaining an IP address.

Option D: The switch does not support multicast traffic. This is unrelated to obtaining an IP address. Multicast traffic deals with specific types of network communication and would not affect the basic DHCP IP address assignment process.

Question 10

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.