Free Questions for 220-1102 by actualtestdumps

Shared by Cash on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

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 2

Question Type: MultipleChoice

Applications on a computer are not updating, which is preventing the user from opening certain files. Which of the following MMC snap-ins should the technician launch next to continue troubleshooting the issue?

Options:

A- gpedit.msc

B- perfmon.msc

C- devmgmt.msc

Answer:

C

Explanation:

devmgmt.msc is the MMC snap-in that opens the Device Manager, a tool that allows the technician to view and manage the hardware devices and their drivers on the computer1. If the applications are not updating properly, it could be due to outdated, corrupted, or incompatible drivers that prevent the hardware from functioning normally.The technician can use the Device Manager to update, uninstall, rollback, or disable the drivers, as well as scan for hardware changes, troubleshoot problems, and view device properties2.

gpedit.msc is the MMC snap-in that opens the Group Policy Editor, a tool that allows the technician to configure the local or domain group policy settings for the computer or a group of computers3. Group policy settings can affect the security, performance, and functionality of the system, but they are not directly related to the application updates or the hardware drivers.

perfmon.msc is the MMC snap-in that opens the Performance Monitor, a tool that allows the technician to monitor and analyze the performance of the system and its components, such as processor, memory, disk, network, etc4.Performance Monitor can display real-time data or collect log data for later analysis, as well as generate reports and alerts based on the performance counters5. Performance Monitor can help the technician identify and diagnose performance issues, but it does not provide a way to manage the hardware drivers.

The Official CompTIA A+ Core 2 Study Guide6, page 223, 225, 227, 228.

Question 3

Question Type: MultipleChoice

A technician wants to mitigate unauthorized data access if a computer is lost or stolen. Which of the following features should the technician enable?

Options:

A- Network share

B- Group Policy

C- BitLocker

D- Static IP

Answer:

C

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 helps mitigate unauthorized data access by enhancing file and system protections, rendering data inaccessible when BitLocker-protected devices are decommissioned or recycled1. Network share, Group Policy, and Static IP are not features that can prevent unauthorized data access if a computer is lost or stolen.

BitLocker overview - Windows Security | Microsoft Learn1

The Official CompTIA A+ Core 2 Study Guide2, page 315.

Question 4

Question Type: MultipleChoice

Which of the following protocols supports fast roaming between networks?

Options:

A- WEP

B- WPA

C- WPA2

D- LEAP

E- PEAP

Answer:

B

Explanation:

WPA2 is the only protocol among the options that supports fast roaming between networks.Fast roaming, also known as IEEE 802.11r or Fast BSS Transition (FT), enables a client device to roam quickly in environments implementing WPA2 Enterprise security, by ensuring that the client device does not need to re-authenticate to the RADIUS server every time it roams from one access point to another1. WEP, WPA, LEAP, and PEAP do not support fast roaming and require the client device to perform the full authentication process every time it roams, which can cause delays and interruptions in the network service.

The Official CompTIA A+ Core 2 Study Guide2, page 263.

WiFi Fast Roaming, Simplified3

Question 5

Question Type: MultipleChoice

A user's company phone was stolen. Which of the following should a technician do next?

Options:

A- Perform a low-level format.

B- Remotely wipe the device.

C- Degauss the device.

D- Provide the GPS location of the device.

Answer:

B

Explanation:

Remotely wiping the device is the best option to prevent unauthorized access to the company data stored on the phone. A low-level format, degaussing, or providing the GPS location of the device are not feasible or effective actions to take in this scenario.

Question 6

Question Type: MultipleChoice

A user's antivirus software reports an infection that it is unable to remove. Which of the following is the most appropriate way to remediate the issue?

Options:

A- Disable System Restore.

B- Utilize a Linux live disc.

C- Quarantine the infected system.

D- Update the anti-malware.

Answer:

C

Explanation:

Quarantining the infected system is the most appropriate way to remediate the issue of an infection that the antivirus software cannot remove. Quarantining means isolating the system from the network and other devices to prevent the infection from spreading or causing

further damage. Quarantining also allows the technician to perform further analysis and removal of the infection without risking the security of other systems or data.

Some of the steps involved in quarantining an infected system are:

Disconnect the system from the internet and any local network connections, such as Wi-Fi, Ethernet, Bluetooth, or USB.

Disable any file-sharing or remote access services on the system, such as Windows File Sharing, Remote Desktop, or TeamViewer.

Use a separate device to download and update the antivirus software and any other tools that may be needed to remove the infection, such as malware scanners, rootkit removers, or bootable rescue disks.

Transfer the updated antivirus software and tools to the infected system using a removable media, such as a CD, DVD, or USB flash drive. Scan the removable media for any infections before and after using it on the infected system.

Run the antivirus software and tools on the infected system and follow the instructions to delete or quarantine the infection. If the infection is persistent or complex, it may require booting the system from a rescue disk or using a Linux live disc to access and clean the system files.

After the infection is removed, restore the system to a previous clean state using System Restore, backup, or recovery partition. Scan the system again to ensure that it is clean and secure. Reconnect the system to the network and update the system and the antivirus software.

How to Identify and Repair Malware or Virus Infected Computers, section 31

Uninstalling Antivirus Software, the Clean Way: 40 Removal Tools & Instructions, section 22

How to manually remove an infected file from a Windows computer3

The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2194

Question 7

Question Type: MultipleChoice

A technician cannot uninstall a system driver because the driver is currently in use. Which of the following tools should the technician use to help uninstall the driver?

Options:

A- msinfo32.exe

B- dxdiag.exe

C- msconfig.exe

D- regedit.exe

Answer:

C

Explanation:

The msconfig.exe tool, also known as the System Configuration utility, is a tool that allows users to modify various system settings, such as startup options, services, boot options, and more. One of the features of msconfig.exe is the ability to disable or enable device drivers that are loaded during the system startup. By using msconfig.exe, a technician can prevent a driver from being loaded and used by the system, which will allow them to uninstall it without any errors. To use msconfig.exe to disable a driver, the technician can follow these steps:

Open the Run dialog box by pressing the Windows key + R.

Type msconfig.exe and press Enter.

Click on the Boot tab and then click on Advanced options.

Check the box next to No GUI boot and click OK. This will prevent the graphical user interface from loading during the boot process, which will also prevent some drivers from loading.

Click on the Services tab and check the box next to Hide all Microsoft services. This will show only the third-party services and drivers that are running on the system.

Find the service or driver that corresponds to the device that the technician wants to uninstall and uncheck the box next to it. This will disable the service or driver from starting during the system startup.

Click Apply and OK and then restart the computer.

After the computer restarts, the technician can use the Device Manager or the Control Panel to uninstall the driver that was previously in use.

How to Completely Remove/Uninstall a Driver in Windows, section 31

The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2212