Free Questions for 220-1102 by certsinside

Shared by Shannon on 15-04-2024

For More Free Questions and Preparation Resources

Question 1

A technician needs to configure security settings on a Windows 10 workstation. Which of the following should the technician configure to limit password attempts?

Options:

A- Account Lockout Policy

B- User Access Control

C- System Protection

D- Firewall

Answer:

A

Explanation:

Configuring the Account Lockout Policy in Windows 10 is the appropriate action to limit password attempts. This security setting determines the number of failed login attempts that will trigger a lockout, preventing unauthorized access due to repeated password

guessing. It is an effective measure to enhance security by deterring brute-force attacks.

Question 2

Question Type: MultipleChoice

Which of the following macOS file types requires mounting before installation?

Options:

A- .pkg

B- .zip

C- .app

D- .dmg

Answer:

D

Explanation:

The .dmg file type in macOS requires mounting before installation. .dmg files are disk image files used to distribute software on macOS. When opened, they mount a virtual disk on the desktop, from which the application can be installed. Other file types like .pkg, .zip, and .app have different processes for installation and do not require mounting in the same way.

Question 3

Question Type: **MultipleChoice**

A web developer installs and launches a new external web server. Immediately following the launch, the performance of all traffic traversing the firewall degrades substantially. Which of the following considerations was overlooked?

Options:

A- OS compatibility

B- Quality of service

C- 32- vs. 64-bit architecture

D- Storage requirements

Answer:

B

Explanation:

The performance degradation following the launch of a new external web server suggests that Quality of Service (QoS) considerations were overlooked. QoS settings help prioritize traffic to ensure that critical services like web servers receive the bandwidth they need without negatively impacting the overall network performance. Without proper QoS configuration, the new server's traffic could overwhelm the firewall, leading to widespread performance issues.

Question 4

Question Type: **MultipleChoice**

A user's workstation was infected with a newly discovered virus that the AV system detected. After a full virus scan and a workstation reboot, the virus is still present in the OS. Which of the following actions should the user take to remove the virus?

Options:

A- Enable the system firewall.

B- Use bootable antivirus media to scan the system.

C- Download software designed to specifically target the virus.

D- Run the operating system update process.

Answer:

B

Explanation:

Using bootable antivirus media to scan the system is an effective method for removing a persistent virus. Booting from external antivirus media allows the system to scan for and remove malware without the infected operating system running, which can prevent the virus from hiding or resisting removal efforts that might occur within the active OS environment.

Question 5

Question Type: MultipleChoice

A technician wants to update the local security policies on a Windows machine but is unable to launch the expected snap-in. Which of the following is the most likely reason?

A- The computer is running Windows Home.

B- The user did not sign the end user license agreement.

C- The user disabled the User Account Control.

D- An antivirus application is blocking access.

Answer:

A

Explanation:

The inability to launch the expected security policy snap-in is likely because the computer is running Windows Home edition, which does not include the Group Policy Editor or certain other administrative tools available in Professional, Enterprise, and Education editions. The Home edition is designed for general consumer use and lacks some of the advanced security and management features found in higher editions.

Question 6

A Windows 10 computer is not installing updates and continues to receive errors even during manual update installations. Which of the following should a technician do to fix the issues? (Select two).

Options:

A- Ensure that the Windows Update Utility is the latest version.

B- Refresh local WSUS settings on the computer.

C- Delete the Windows Update cache.

D- Run the System check to verify system files.

E- Reimage the operating system while retaining user files.

F- Reset WMI and re-register system .dlls.

Answer:

B, C

Explanation:

Refreshing local Windows Server Update Services (WSUS) settings and deleting the Windows Update cache are effective steps in resolving issues with Windows 10 not installing updates. These actions help in rectifying any corrupt update files and ensuring that the

workstation is properly communicating with the update servers, which can resolve errors during manual and automatic update installations.

Question 7

A 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:

Turning off inheritance on the specific folder requested by the manager and setting the requested permissions, followed by turning on inheritance under the child folders, ensures that only the immediate team has access to the confidential material while maintaining the broader permissions structure for other folders and files. This action isolates the folder's permissions from the top-level inheritance, providing a focused security measure for sensitive content.

Question 8

A customer service representative is unable to send jobs to a printer at a remote branch office. However, the representative can print successfully to a local network printer. Which of the following commands should a technician use to view the path of the network traffic from the PC?

Options:

A- netstat

B- ping

C- format

D- tracert

Answer:

D

Explanation:

The 'tracert' command is used to view the path that network traffic takes from a PC to a specified destination. It is helpful in identifying where along the path the traffic may be failing or experiencing delays. In the scenario where a customer service representative can't send jobs to a remote printer but can print locally, 'tracert' can help diagnose if there's a network routing issue affecting the connection to the remote branch office.

Question 9

Question Type: **MultipleChoice**

A technician is installing software on a user's workstation. The installation fails due to incompliance with the HCL. Which of the following components is most likely causing the installation to fail? (Select two).

Options:

A- NIC

B- CPU

C- PSU

D- KVM

E- RAM

F- DVI

Answer:

A, B

Explanation:

The Hardware Compatibility List (HCL) is a list that indicates hardware components that are compatible with a specific software or operating system. If software installation fails due to incompliance with the HCL, it's most likely due to core hardware components like the Network Interface Card (NIC) or the Central Processing Unit (CPU) not being supported or not meeting the software's minimum hardware requirements. The PSU, KVM, RAM, and DVI are less likely to directly impact software compatibility as defined by the HCL.