Free Questions for 220-1102

Shared by Bartlett on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

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 2

Question Type: MultipleChoice

A user is unable to access a remote server from a corporate desktop computer using the appropriate terminal emulation program. The user contacts the help desk to report the issue. Which of the following clarifying questions would be most effective for the help desk technician to ask the user in

Options:

A- order to understand the issue?
B- What is the error message?
C- Does the program work on another computer?
D- Did the program ever work?
E- Is anyone else having this issue?

Answer:

A

Explanation:

The most effective clarifying question for the help desk technician to ask the user in order to understand the issue is

A) What is the error message? This question will help the technician to identify the possible cause and solution of the problem, as the error message will provide specific information about the nature and location of the error, such as the server name, the port number, the protocol, the authentication method, or the network status. The error message will also help the technician to troubleshoot the issue by following the suggested steps or searching for the error code online .

This question is more effective than the other choices because:

B) Does the program work on another computer? is not a very helpful question, as it will not reveal the source of the error or how to fix it. The program may work on another computer for various reasons, such as different network settings, firewall rules, permissions, or software versions. However, this question will not tell the technician what is wrong with the user's computer or the remote server, or what needs to be changed or updated to make the program work.

C) Did the program ever work? is not a very relevant question, as it will not address the current issue or how to resolve it. The program may have worked in the past, but it may have stopped working due to changes in the network configuration, the server status, the software updates, or

the user credentials. However, this question will not tell the technician what has changed or how to restore the program functionality.

D) Is anyone else having this issue? is not a very useful question, as it will not explain the reason or the solution for the error. The issue may affect only the user, or multiple users, depending on the scope and the impact of the error. However, this question will not tell the technician what is causing the error or how to fix it for the user or the others.

: How to Troubleshoot Terminal Emulation Problems - Techwalla : How to Read and Understand Windows Error Messages - Lifewire : How to Troubleshoot Network Connectivity Problems - How-To Geek : How to Troubleshoot Software Problems - dummies : How to Troubleshoot Common PC Issues For Users - MakeUseOf

Question 3

Question Type: MultipleChoice

Which of the following combinations meets the requirements for mobile device multifactor authentication?

Options:

A- Password and PIN
B- Password and swipe
C- Fingerprint and password
D- Swipe and PIN

Answer:

C

Explanation:

Multifactor authentication (MFA) requires the use of two or more verification factors to gain access to a resource such as an application, online account, or a VPN. The factors are categorized into something you know (like a password or PIN), something you have (like a security token or a smartphone), and something you are (like a biometric verification such as a fingerprint).

Fingerprint and password: This combination meets the criteria for MFA as it uses two different categories of authentication factors: 'something you are' (fingerprint) and 'something you know' (password). This enhances security by combining two distinct methods of authentication.

Other combinations mentioned:

Password and PIN: Both of these factors fall under the same category of 'something you know,' and hence, do not constitute multifactor authentication.

Password and swipe: Swiping a pattern is similar to a password in that it is something you know, so this does not qualify as multifactor authentication.

Swipe and PIN: Again, both of these are 'something you know' and do not qualify as multifactor authentication since they fall under the same category.

Question 4

Question Type: MultipleChoice

A user reports a computer is running slow. Which of the following tools will help a technician identify the issue?

Options:

A- Disk Cleanup
B- Group Policy Editor
C- Disk Management
D- Resource Monitor

Answer:

D

Explanation:

Resource Monitor is a Windows utility that can be used to monitor and analyze the system resources and processes running on a computer. It can be used to identify and troubleshoot any issues that might be causing the computer to run slowly, such as CPU usage, memory usage, disk I/O, and network usage.

Question 5

Question Type: MultipleChoice

A user is unable to start a computer following a failed Windows 10 update. When trying to start the computer, the user sees a blue screen of death. Which of the following steps should a technician take to diagnose the issue?

Options:

A- Perform a safe mode boot.
B- Run the System Restore wizard.
C- Start the computer in the last known-good configuration.
D- Reset the BIOS settinqs.

Answer:

A

Explanation:

Booting in safe mode is the initial step to diagnose a computer experiencing a blue screen of death (BSOD) following a failed Windows 10 update. Safe mode starts the computer with a minimal set of drivers and services, allowing troubleshooting and identification of the problematic software or driver causing the BSOD. This mode provides a safer environment to uninstall recent updates or drivers, perform system scans, and restore the system if necessary. Other options like System Restore wizard, last known-good configuration, and resetting BIOS settings may be subsequent steps but do not directly diagnose the issue as effectively as booting in safe mode.

Question 6

Question Type: MultipleChoice

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 7

Question Type: MultipleChoice

Which of the following environments allows for the testing of critical systems without the risk of them being negatively impacted by changes?

Options:

A- Regression
B- Cloud
C- Production
D- Sandbox

Answer:

D

Explanation:

A sandbox is an isolated environment that allows for the testing of critical systems without the risk of them being negatively impacted by changes. A sandbox can be used to simulate real-world scenarios, experiment with new features, debug errors, or evaluate the performance and security of a system. A sandbox can be created using virtualization, emulation, or containerization technologies. A sandbox prevents any changes made in the testing environment from affecting the production environment, which is the actual system that is used by the end users.

https://www.comptia.org/training/books/a-core-2-220-1102-study-guide

Question 8

Question Type: MultipleChoice

An employee has repeatedly contacted a technician about malware infecting a work computer. The technician has removed the malware several times, but the user's PC keeps getting infected. Which of the following should the technician do to reduce the risk of future infections?

Options:

A- Configure the firewall.
B- Restore the system from backups.
C- Educate the end user
D- Update the antivirus program.

Answer:

C

Explanation:

Malware is software that infects computer systems to damage, disable or exploit the computer or network for various malicious purposes5.Malware is typically distributed via email attachments, fake internet ads, infected applications or websites, and often relies on user interaction to execute6.Therefore, one of the most effective ways to prevent malware infections is to educate the end user about the common signs and sources of malware, and how to avoid them7. Configuring the firewall, restoring the system from backups, and updating the antivirus program are also important security measures, but they do not address the root cause of the user's repeated infections, which is likely due to a lack of awareness or caution.

Reference 5: Malware: what it is, how it works, and how to stop it - Norton 6: How to Prevent Malware: 15 Best Practices for Malware Prevention 7: 10 Security Tips for How to Prevent Malware Infections - Netwrix

Question 9

Question Type: MultipleChoice

In an organization with a standardized set of installed software, a developer submits a request to have new software installed. The company does not currently have a license for this software, but the developer already downloaded the installation file and is requesting that the technician install it. The developer states that the management team approved the business use of this software. Which of the following is the best action for the technician to take?

Options:

A- Contact the software vendor to obtain the license for the user, and assist the user with installation once the license is purchased.
B- Run a scan on the downloaded installation file to confirm that it is free of malicious software, install the software, and document the software installation process.
C- Indicate to the developer that formal approval is needed; then, the IT team should investigate the software and the impact it will have on the organization before installing the software.
D- Install the software and run a full system scan with antivirus software to confirm that the operating system is free of malicious software.

Answer:

C

Explanation:

Installing new software on an organization's system or device can have various implications, such as compatibility, security, performance, licensing, and compliance issues.Therefore, it is important to follow the best practices for software installation, such as doing research on the software, checking the system requirements, scanning the installation file for malware, and obtaining the proper license345. The technician should not install the software without formal approval from the management team, as this could violate the organization's policies or regulations. The technician should also not install the software without investigating the software and its impact on the organization, as this could introduce potential risks or problems to the system or device.The technician should indicate to the developer that formal approval is needed, and then work with the IT team to evaluate the software and its suitability for the organization before installing it

Question 10

Question Type: MultipleChoice

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 11

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.

To Get Premium Files for 220-1102 Visit
https://www.p2pexams.com/products/220-1102

For More Free Questions Visit
https://www.p2pexams.com/comptia/pdf/220-1102



P2P exams