



CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

NEW QUESTION 1

After a failed update, an application no longer launches and generates the following error message: Application needs to be repaired. Which of the following Windows 10 utilities should a technician use to address this concern?

- A. Device Manager
- B. Administrator Tools
- C. Programs and Features
- D. Recovery

Answer: D

Explanation:

Recovery is a Windows 10 utility that can be used to address the concern of a failed update that prevents an application from launching. Recovery allows the user to reset the PC, go back to a previous version of Windows, or use advanced startup options to troubleshoot and repair the system. Device Manager, Administrator Tools, and Programs and Features are not Windows 10 utilities that can fix a failed update.

NEW QUESTION 2

An executive has contacted you through the help-desk chat support about an issue with a mobile device. Assist the executive to help resolve the issue.

The screenshot shows a chat window titled 'TEST QUESTION'. The chat history includes:

- User: An executive has contacted you through the help-desk chat support about an issue with a mobile device. Assist the executive to help resolve the issue.
- Telecom: Please follow the new mobile device guide provided on our website.
- User: [Screenshot of mail settings showing IMAP, SSL, 10.0.200.1, and 100]
- Telecom: Please change the port number on your mail settings to 143.
- User: Thanks for helping.

Instructions for the question:

INSTRUCTIONS
 Select the MOST appropriate statement for each response.
 If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Which of the following should be done NEXT?

- A. Educate the user on the solution that was performed.
 Tell the user to take time to fix it themselves next time.
- B. Close the ticket out.
- D. Send an email to Telecom to inform them of the Issue and prevent reoccurrence.

Answer: A

NEW QUESTION 3

When trying to access a secure internal network, the user receives an error messaging stating, "There is a problem with this website's security certificate." The user reboots the desktop and tries to access the website again, but the issue persists. Which of the following should the user do to prevent this error from reoccurring?

- A. Reimage the system and install SSL.
- B. Install Trusted Root Certificate.

- C. Select View Certificates and then Install Certificate.
- D. Continue to access the website.

Answer: C

Explanation:

The error message indicates that the website's security certificate is not trusted by the user's device, which may prevent the user from accessing the secure internal network. To resolve this issue, the user can view the certificate details and install it on the device, which will add it to the trusted root certificate store. Reimaging the system and installing SSL, installing Trusted Root Certificate, or continuing to access the website are not recommended solutions, as they may compromise the security of the device or the network.

NEW QUESTION 4

Which of the following data is MOST likely to be regulated?

- A. Name in a Phone book
- B. Name on a medical diagnosis
- C. Name on a job application
- D. Name on a employer's website

Answer: B

Explanation:

A name on a medical diagnosis (B) is most likely to be regulated. This is because it falls under the category of protected health information (PHI), which is subject to regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. These regulations aim to protect the privacy and security of individuals' health information.

NEW QUESTION 5

A technician installs specialized software on a workstation. The technician then attempts to run the software. The workstation displays a message indicating the software is not authorized to run. Which of the following should the technician do to most likely resolve the issue?

- A. Install the software in safe mode.
- B. Attach the external hardware token.
- C. Install OS updates.
- D. Restart the workstation after installation.

Answer: B

Explanation:

A hardware token is a physical device that provides an additional layer of security for software authorization. Some specialized software may require a hardware token to be attached to the workstation in order to run. A hardware token may contain a cryptographic key, a password, or a one-time code that verifies the user's identity or permission. Installing the software in safe mode, installing OS updates, and restarting the workstation after installation are not likely to resolve the issue of software authorization.

NEW QUESTION 6

A technician is in the process of installing a new hard drive on a server but is called away to another task. The drive has been unpackaged and left on a desk. Which of the following should the technician perform before leaving?

- A. Ask coworkers to make sure no one touches the hard drive.
- B. Leave the hard drive on the table; it will be okay while the other task is completed.
- C. Place the hard drive in an antistatic bag and secure the area containing the hard drive.
- D. Connect an electrostatic discharge strap to the drive.

Answer: C

Explanation:

The technician should place the hard drive in an antistatic bag and secure the area containing the hard drive before leaving. This will protect the hard drive from electrostatic discharge (ESD), dust, moisture, and physical damage. Asking coworkers to make sure no one touches the hard drive is not a reliable or secure way to prevent damage. Leaving the hard drive on the table exposes it to ESD and other environmental hazards. Connecting an electrostatic discharge strap to the drive is not enough to protect it from dust, moisture, and physical damage.

NEW QUESTION 7

A user notices a small USB drive is attached to the user's computer after a new vendor visited the office. The technician notices two files named grabber.exe and output.txt. Which of the following attacks is MOST likely occurring?

- A. Trojan
- B. Rootkit
- C. Cryptominer
- D. Keylogger

Answer: D

Explanation:

A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote attacker. A keylogger can be used to steal passwords, credit card numbers, personal information, and other sensitive data. A keylogger can be delivered through a USB drive that contains a malicious executable file, such as grabber.exe, and an output file that stores the captured keystrokes, such as output.txt. The other options are not likely to use this method of attack. References: : <https://www.comptia.org/training/resources/exam-objectives/comptia-a-core-2-exam-objectives> : <https://www.kaspersky.com/resource-center/definitions/keylogger>

NEW QUESTION 8

A systems administrator is configuring centralized desktop management for computers on a domain. The management team has decided that all users' workstations should have the same network drives, printers, and configurations. Which of the following should the administrator use to accomplish this task?

- A. Network and Sharing Center
- B. net use
- C. User Accounts
- D. regedit
- E. Group Policy

Answer: E

Explanation:

Group Policy is a feature of Windows that allows administrators to centrally manage and apply policies and settings to computers and users on a domain³. Group Policy can be used to configure network drives, printers, security settings, desktop preferences, and other configurations for all users' workstations³. Network and Sharing Center, net use, User Accounts, and regedit are not tools that can accomplish this task.

NEW QUESTION 9

Which of the following filesystem formats would be the BEST choice to ensure read and write compatibility of USB flash drives across several generations of Microsoft operating systems?

- A. APFS
- B. ext4
- C. CDFS
- D. FAT32

Answer: D

Explanation:

The best filesystem format to ensure read and write compatibility of USB flash drives across several generations of Microsoft operating systems is FAT32. FAT32 stands for File Allocation Table 32-bit and is a filesystem format that organizes and manages files and folders on storage devices using 32-bit clusters. FAT32 is compatible with most Microsoft operating systems since Windows 95 OSR2, as well as other operating systems such as Linux and Mac OS X. FAT32 can support storage devices up to 2TB in size and files up to 4GB in size. APFS stands for Apple File System and is a filesystem format that organizes and manages files and folders on storage devices using encryption, snapshots and cloning features. APFS is compatible with Mac OS X 10.13 High Sierra and later versions but not with Microsoft operating systems natively. Ext4 stands for Fourth Extended File System and is a filesystem format that organizes and manages files and folders on storage devices using journaling, extents and delayed allocation features. Ext4 is compatible with Linux operating systems but not with Microsoft operating systems natively.

NEW QUESTION 10

A user is having phone issues after installing a new application that claims to optimize performance. The user downloaded the application directly from the vendor's website and is now experiencing high network utilization and is receiving repeated security warnings. Which of the following should the technician perform FIRST to mitigate the issue?

- A. Reset the phone to factory settings
- B. Uninstall the fraudulent application
- C. Increase the data plan limits
- D. Disable the mobile hotspot.

Answer: B

Explanation:

Installing applications directly from a vendor's website can be risky, as the application may be malicious or fraudulent. Uninstalling the application can help mitigate the issue by removing the source of the problem.

NEW QUESTION 10

An administrator has submitted a change request for an upcoming server deployment. Which of the following must be completed before the change can be approved?

- A. Risk analysis
- B. Sandbox testing
- C. End user acceptance
- D. Lessons learned

Answer: A

Explanation:

Risk analysis is the process of identifying and evaluating the potential threats and impacts of a change on the system, network, or service. It is an essential step before approving a change request, as it helps to determine the level of risk, the mitigation strategies, and the contingency plans. Risk analysis also helps to prioritize the change requests based on their urgency and importance¹².

References: 1 The Change Request Process and Best Practices(<https://www.processmaker.com/blog/it-change-request-process-best-practices/>)2 Risk Assessment and Analysis Methods: Qualitative and Quantitative(<https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods>).

NEW QUESTION 12

An office is experiencing constant connection attempts to the corporate Wi-Fi. Which of the following should be disabled to mitigate connection attempts?

- A. SSID

- B. DHCP
- C. Firewall
- D. SSD

Answer: A

Explanation:

The SSID (Service Set Identifier) is the name of a wireless network that is broadcasted by the router or the Wi-Fi base station. The SSID helps nearby devices to identify and connect to the available networks. However, broadcasting the SSID also exposes the network to potential connection attempts from unauthorized or malicious users. Therefore, disabling the SSID can mitigate connection attempts by making the network invisible or hidden to the devices that are not already connected to it. To connect to a hidden network, the user would need to know the exact SSID and enter it manually. The other options are not related to mitigating connection attempts to the corporate Wi-Fi. DHCP (Dynamic Host Configuration Protocol) is a protocol that assigns IP addresses to the devices on a network. Firewall is a software or hardware device that filters the incoming and outgoing network traffic based on predefined rules. SSD (Solid State Drive) is a type of storage device that uses flash memory to store data. Disabling any of these options would not prevent connection attempts to the Wi-Fi network, and may cause other problems or issues for the network functionality and performance.

References:

- ? What is SSID + how to find (and change) it¹
- ? Choosing an SSID²
- ? SSID Meaning: Finding Your Network's Name³

NEW QUESTION 16

An Android user contacts the help desk because a company smartphone failed to complete a tethered OS update. A technician determines there are no error messages on the device. Which of the following should the technician do NEXT?

- A. Verify all third-party applications are disabled
- B. Determine if the device has adequate storage available.
- C. Check if the battery is sufficiently charged
- D. Confirm a strong internet connection is available using Wi-Fi or cellular data

Answer: C

Explanation:

Since there are no error messages on the device, the technician should check if the battery is sufficiently charged¹. If the battery is low, the device may not have enough power to complete the update².

In this scenario, the technician has already determined that there are no error messages on the device. The next best step would be to check if the battery is sufficiently charged. If the battery is low, it could be preventing the device from completing the update process. Verifying that third-party applications are disabled, determining if the device has adequate storage available, and confirming a strong internet connection are all important steps in troubleshooting issues with mobile devices. However, since the problem in this scenario is related to a failed OS update, it is important to first check the battery level before proceeding with further troubleshooting steps.

NEW QUESTION 19

A user attempts to open some files, but a message appears stating that the files are encrypted. The user was able to access these files before without receiving this message and no changes have been made within the company. Which of the following has infected the computer?

- A. Cryptominer
- B. Phishing
- C. Ransomware
- D. Keylogger

Answer: C

Explanation:

Ransomware is malicious software that encrypts files on a computer, making them inaccessible until a ransom is paid. In this case, the user was able to access the files before without issue, and no changes have been made within the company, so it is likely that the computer was infected with ransomware.

NEW QUESTION 21

Which of the following is used as a password manager in the macOS?

- A. Terminal
- B. FileVault
- C. Privacy
- D. Keychain

Answer: D

Explanation:

Keychain is a feature of macOS that securely stores passwords, account numbers, and other confidential information for your Mac, apps, servers, and websites¹. You can use the Keychain Access app on your Mac to view and manage your keychains and the items stored in them¹. Keychain can also sync your passwords across your devices using iCloud Keychain¹. Keychain can be used as a password manager in macOS to help you keep track of and protect your passwords. References: 1: Manage passwords using keychains on Mac (<https://support.apple.com/guide/mac-help/use-keychains-to-store-passwords-mchlf375f392/mac>)

NEW QUESTION 23

The courts determined that a cybercrimes case could no longer be prosecuted due to the agency's handling of evidence. Which of the following was MOST likely violated during the investigation?

- A. Open-source software

- B. EULA
- C. Chain of custody
- D. AUP

Answer: C

Explanation:

Chain of custody is a process that documents how evidence is collected, handled, stored and transferred during a cybercrime investigation. It ensures that the evidence is authentic, reliable and admissible in court. If the chain of custody is violated during an investigation, it can compromise the integrity of the evidence and lead to the case being dismissed. Open-source software, EULA (end-user license agreement) and AUP (acceptable use policy) are not related to cybercrime investigations or evidence handling. Verified References: <https://www.comptia.org/blog/what-is-chain-of-custody> <https://www.comptia.org/certifications/a>

NEW QUESTION 26

A company acquired a local office, and a technician is attempting to join the machines at the office to the local domain. The technician notes that the domain join option appears to be missing. Which of the following editions of Windows is MOST likely installed on the machines?

- A. Windows Professional
- B. Windows Education
- C. Windows Enterprise
- D. Windows Home

Answer: D

Explanation:

Windows Home is the most likely edition of Windows installed on the machines that do not have the domain join option. Windows Home is a consumer-oriented edition that does not support joining a domain or using Group Policy. Only Windows Professional, Education, and Enterprise editions can join a domain

NEW QUESTION 28

Which of the following would MOST likely be deployed to enhance physical security for a building? (Select TWO).

- A. Multifactor authentication
- B. Badge reader
- C. Personal identification number
- D. Firewall
- E. Motion sensor
- F. Soft token

Answer: BE

Explanation:

Badge reader and motion sensor are devices that can be deployed to enhance physical security for a building. A badge reader is a device that scans and verifies an identification card or tag that grants access to authorized personnel only. A badge reader can help prevent unauthorized entry or intrusion into a building or a restricted area. A motion sensor is a device that detects movement and triggers an alarm or an action when motion is detected. A motion sensor can help deter or alert potential intruders or trespassers in a building or an area. Multifactor authentication is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. Multifactor authentication is not a device that can be deployed to enhance physical security for a building but a technique that can be used to enhance logical security for systems or services. Personal identification number is a numeric code that can be used as part of authentication or access control. Personal identification number is not a device that can be deployed to enhance physical security for a building but an example of something you know factor in multifactor authentication. Firewall is a device or software that filters network traffic based on rules and policies. Firewall is not a device that can be deployed to enhance physical security for a building but a device that can be used to enhance network security for systems or services. Soft token is an application or software that generates one-time passwords or codes for authentication purposes. Soft token is not a device that can be deployed to enhance physical security for a building but an example of something you have factor in multifactor authentication. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 3.3

NEW QUESTION 31

Windows updates need to be performed on a department's servers. Which of the following methods should be used to connect to the server?

- A. MSRA
- B. RDP
- C. VPN
- D. FIP

Answer: C

Explanation:

RDP (Remote Desktop Protocol) is a protocol that allows a user to connect to and control a remote computer over a network. RDP can be used to perform Windows updates on a department's servers without physically accessing them. Reference: CompTIA A+ Core 2 Exam Objectives, Section 5.6

NEW QUESTION 35

A technician has verified a computer is infected with malware. The technician isolates the system and updates the anti-malware software. Which of the following should the technician do next?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Malware is malicious software that can cause damage or harm to a computer system or network⁴. A technician has verified a computer is infected with malware by observing unusual behavior, such as slow performance, pop-ups, or unwanted ads. The technician isolates the system and updates the anti-malware software to prevent further infection or spread of the malware. The next step is to run repeated remediation scans until the malware is removed. A remediation scan is a scan that detects and removes malware from the system. Running one scan may not be enough to remove all traces of malware, as some malware may hide or regenerate itself.

NEW QUESTION 40

A technician is troubleshooting application crashes on a Windows workstation. Each time the workstation user tries to open a website in a browser, the following message is displayed:

crypt32.dll is missing not found

Which of the following should the technician attempt FIRST?

- A. Rebuild Windows profiles.
- B. Reimage the workstation
- C. Roll back updates
- D. Perform a system file check

Answer: D

Explanation:

If this file is missing or corrupted, it can cause application crashes or errors when trying to open websites in a browser. To fix this, the technician can perform a system file check, which is a utility that scans and repairs corrupted or missing system files¹. To perform a system file check, the technician can follow these steps:

? Open the Command Prompt as an administrator. To do this, type cmd in the

search box on the taskbar, right-click on Command Prompt, and select Run as administrator.

? In the Command Prompt window, type sfc /scannow and hit Enter. This will start

the scanning and repairing process, which may take some time.

? Wait for the process to complete. If any problems are found and fixed, you will see a message saying Windows Resource Protection found corrupt files and successfully repaired them. If no problems are found, you will see a message saying Windows Resource Protection did not find any integrity violations.

? Restart your computer and check if the issue is resolved.

NEW QUESTION 41

A company-owned mobile device is displaying a high number of ads, receiving data-usage limit notifications, and experiencing slow response. After checking the device, a technician notices the device has been jailbroken. Which of the following should the technician do next?

- A. Run an antivirus and enable encryption.
- B. Restore the defaults and reimage the corporate OS.
- C. Back up the files and do a system restore.
- D. Undo the jailbreak and enable an antivirus.

Answer: B

Explanation:

The best course of action for the technician is to restore the defaults and reimage the corporate OS on the device. This will remove the jailbreak and any unauthorized or malicious apps that may have been installed on the device, as well as restore the security features and policies that the company has set for its devices. This will also ensure that the device can receive the latest updates and patches from the manufacturer and the company, and prevent any data leakage or compromise from the device.

Jailbreaking is a process of bypassing the built-in security features of a device to install software other than what the manufacturer has made available for that device¹. Jailbreaking allows the device owner to gain full access to the root of the operating system and access all the features¹. However, jailbreaking also exposes the device to various risks, such as:

? The loss of warranty from the device manufacturers².

? Inability to update software until a jailbroken version becomes available².

? Increased security vulnerabilities^{3,2}.

? Decreased battery life².

? Increased volatility of the device².

Some of the signs of a jailbroken device are:

? A high number of ads, which may indicate the presence of adware or spyware on the device³.

? Receiving data-usage limit notifications, which may indicate the device is sending or receiving data in the background without the user's knowledge or consent³.

? Experiencing slow response, which may indicate the device is running unauthorized or malicious apps that consume resources or interfere with the normal functioning of the device³.

? Finding apps or icons that the user did not install or recognize, such as Cydia, which is a storefront for jailbroken iOS devices¹.

The other options are not sufficient or appropriate for dealing with a jailbroken device. Running an antivirus and enabling encryption may not detect or remove all the threats or vulnerabilities that the jailbreak has introduced, and may not restore the device to its original state or functionality. Backing up the files and doing a system restore may not erase the jailbreak or the unauthorized apps, and may also backup the infected or compromised files. Undoing the jailbreak and enabling an antivirus may not be possible or effective, as the jailbreak may prevent the device from updating or installing security software, and may also leave traces of the jailbreak or the unauthorized apps on the device.

References:

? CompTIA A+ Certification Exam Core 2 Objectives⁴

? CompTIA A+ Core 2 (220-1102) Certification Study Guide⁵

? What is Jailbreaking & Is it safe? - Kaspersky¹

? Is Jailbreaking Safe? The ethics, risks and rewards involved - Comparitech³

? Jailbreaking : Security risks and moving past them²

NEW QUESTION 45

A technician downloads a validated security tool and notes the vendor hash of a58e87a2. When the download is complete, the technician again validates the hash, but the value returns as 2a876a7d3. Which of the following is the MOST likely cause of the issue?

- A. Private-browsing mode

- B. Invalid certificate
- C. Modified file
- D. Browser cache

Answer: C

Explanation:

The most likely cause of the issue of having different hash values for a downloaded security tool is a modified file. A hash value is a unique and fixed-length string that is

generated from an algorithm that processes data or files. A hash value can be used to verify the integrity and authenticity of data or files by comparing it with a known or expected value. If the hash values do not match, it means that the data or file has been altered or corrupted in some way. A modified file may result from intentional or unintentional changes, such as editing, encryption, compression or malware infection. Private-browsing mode is a feature that allows users to browse the web without storing any browsing history, cookies or cache on their browser. Private-browsing mode does not affect the hash value of a downloaded file but only how the browser handles user data. Invalid certificate is an error that occurs when a website or a server does not have a valid or trusted digital certificate that proves its identity and secures its communication. Invalid certificate does not affect the hash value of a downloaded file but only how the browser verifies the website or server's credibility. Browser cache is a temporary storage that stores copies of web pages, images and other content that users have visited on their browser.

NEW QUESTION 47

A homeowner recently moved and requires a new router for the new ISP to function correctly. The internet service has been installed and has been confirmed as functional. Which of the following is the FIRST step the homeowner should take after installation of all relevant cabling and hardware?

- A. Convert the PC from a DHCP assignment to a static IP address.
- B. Run a speed test to ensure the advertised speeds are met.
- C. Test all network sharing and printing functionality the customer uses.
- D. Change the default passwords on new network devices.

Answer: D

Explanation:

When a homeowner moves and sets up a new router for the new ISP it is important to take appropriate security measures to protect their network from potential security threats. The FIRST step that the homeowner should take after installation of all relevant cabling and hardware is to change the default passwords on new network devices. Most modern routers come with default usernames and passwords that are widely known to potential attackers. If these defaults are not changed, it could make it easier for external attackers to gain unauthorized access to the network. Changing the passwords on new network devices is a simple but effective way to improve the security posture of the network.

NEW QUESTION 51

An IT security team is implementing a new Group Policy that will return a computer to the login after three minutes. Which of the following BEST describes the change in policy?

- A. Login times
- B. Screen lock
- C. User permission
- D. Login lockout attempts

Answer: B

Explanation:

Screen lock is a feature that returns a computer to the login screen after a period of inactivity, requiring the user to enter their credentials to resume their session. Screen lock can be configured using Group Policy settings, such as Screen saver timeout and Interactive logon: Machine inactivity limit. Screen lock can help prevent unauthorized access to a computer when the user is away from their desk. Login times are not a feature that returns a computer to the login screen, but a measure of how long it takes for a user to log in to a system. User permission is not a feature that returns a computer to the login screen, but a set of rights and privileges that determine what a user can do on a system. Login lockout attempts are not a feature that returns a computer to the login screen, but a security policy that locks out a user account after a number of failed login attempts. <https://woshub.com/windows-lock-screen-after-idle-via-gpo/>

NEW QUESTION 53

A team of support agents will be using their workstations to store credit card data. Which of the following should the IT department enable on the workstations in order to remain compliant with common regulatory controls? (Select TWO).

- A. Encryption
- B. Antivirus
- C. AutoRun
- D. Guest accounts
- E. Default passwords
- F. Backups

Answer: AF

Explanation:

Encryption is a way of protecting cardholder data by transforming it into an unreadable format that can only be decrypted with a secret key¹. Backups are a way of ensuring that cardholder data is not lost or corrupted in case of a disaster or system failure². Both encryption and backups are part of the PCI DSS requirements that apply to any entity that stores, processes, or transmits cardholder data¹. The other options are not directly related to credit card data security or compliance.

NEW QUESTION 56

A new employee was hired recently. Which of the following documents will the new employee need to sign before being granted login access to the network?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A new employee will need to sign an AUP before being granted login access to the network. An AUP is an Acceptable Use Policy that defines the rules and guidelines for using network resources and services in an organization. An AUP typically covers topics such as security, privacy, ethics, compliance and liability issues related to network usage. An AUP helps protect the organization and its users from legal, regulatory and reputational risks associated with network activities. An MSDS is a Material Safety Data Sheet that provides information about hazardous substances and how to handle them safely. An MSDS is not related to network access or usage. A EULA is an End User License Agreement that specifies the terms and conditions for using a software product or service. A EULA is usually provided by software vendors or developers and does not apply to network access or usage in general. A UAC is a User Account Control that is a security feature that prompts users for permission or confirmation before performing certain actions that require elevated privileges or affect system settings. A UAC is not a document that needs to be signed by users but a mechanism that helps prevent unauthorized changes or malware infections on a system. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 5.1

NEW QUESTION 60

A user recently purchased a second monitor and wants to extend the Windows desktop to the new screen. Which of the following Control Panel options should a technician adjust to help the user?

- A. Color Management System
- B. Troubleshooting**
- D. Device Manager
- E. Administrative Tools

Answer: D

NEW QUESTION 62

A help desk technician determines a motherboard has failed. Which of the following is the most logical next step in the remediation process?

- A. Escalating the issue to Tier 2
- B. Verifying warranty status with the vendor**
- C. Replacing the motherboard
- D. Purchasing another PC

Answer: B

Explanation:

Verifying warranty status with the vendor is the most logical next step in the remediation process after determining that a motherboard has failed. A warranty is a guarantee from the vendor that covers the repair or replacement of defective or faulty products within a specified period of time. Verifying warranty status with the vendor can help the technician determine if the motherboard is eligible for warranty service and what steps to take to obtain it. Escalating the issue to Tier 2, replacing the motherboard, and purchasing another PC are not the most logical next steps in the remediation process.

NEW QUESTION 63

A technician has verified that a user's computer has a virus and the antivirus software is out of date. Which of the following steps should the technician take next?

- A. Quarantine the computer.
- B. Use a previous restore point.
- C. Educate the end user about viruses.
- D. Download the latest virus definitions.**

Answer: D

Explanation:

The first step in removing a virus from a computer is to update the antivirus software with the latest virus definitions. Virus definitions are files that contain information about the characteristics and behavior of known viruses and malware. They help the antivirus software to identify and remove the malicious threats from the computer. Without the latest virus definitions, the antivirus software may not be able to detect or remove the virus that infected the user's computer. Therefore, the technician should download the latest virus definitions from the antivirus vendor's website or use the update feature in the antivirus program before scanning the computer for viruses.

References:

- ? How to remove malware or viruses from my Windows 10 PC, section 21
- ? How to Remove a Virus From a Computer in 2023, section 32
- ? The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2193

NEW QUESTION 65

A user visits a game vendor's website to view the latest patch notes, but this information is not available on the page. Which of the following should the user perform before reloading the page?

- A. Synchronize the browser data.
- B. Enable private browsing mode.
- C. Mark the site as trusted.
- D. Clear the cached file.**

Answer: D

Explanation:

Clearing the cached file is an action that can help resolve the issue of not seeing the latest patch notes on a game vendor's website. A cached file is a copy of a web page or file that is stored locally on the user's browser or device for faster loading and offline access. However, sometimes a cached file may become outdated or corrupted and prevent the user from seeing the most recent or accurate version of a web page or file. Clearing the cached file can force the browser to download and display the latest version from the server instead of using the old copy from the cache. Synchronizing the browser data, enabling private browsing mode, and marking the site as trusted are not actions that can help resolve this issue.

NEW QUESTION 70

Which of the following options should MOST likely be considered when preserving data from a hard drive for forensic analysis? (Select TWO).

- A. Licensing agreements
- B. Chain of custody
- C. Incident management documentation
- D. Data integrity
- E. Material safety data sheet
- F. Retention requirements

Answer: B

Explanation:

Chain of custody and data integrity are two options that should most likely be considered when preserving data from a hard drive for forensic analysis. Chain of custody refers to the documentation and tracking of who has access to the data and how it is handled, stored, and transferred. Data integrity refers to the assurance that the data has not been altered, corrupted, or tampered with during the preservation process

NEW QUESTION 75

A user's corporate phone was stolen, and the device contains company trade secrets. Which of the following technologies should be implemented to mitigate this risk? (Select TWO).

- A. Remote wipe
- B. Firewall
- C. Device encryption
- D. Remote backup
- E. Antivirus
- F. Global Positioning System

Answer: AC

Explanation:

Remote wipe is a feature that allows data to be deleted from a device or system remotely by an administrator or owner¹. It is used to protect data from being compromised if the device is lost, stolen, or changed hands¹. Device encryption is a feature that helps protect the data on a device by making it unreadable to unauthorized users². It requires a key or a password to access the data². Both features can help mitigate the risk of losing company trade secrets if a corporate phone is stolen.

References: 1: How to remote wipe Windows laptop (<https://www.thewindowsclub.com/remote-wipe-windows-10>) 2: Device encryption in Windows (<https://support.microsoft.com/en-us/windows/device-encryption-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d>)

NEW QUESTION 78

A hard drive that previously contained PII needs to be repurposed for a public access workstation. Which of the following data destruction methods should a technician use to ensure data is completely removed from the hard drive?

- A. Shredding
- B. Degaussing
- C. Low-level formatting
- D. Recycling

Answer: A

Explanation:

Shredding is a data destruction method that physically destroys the hard drive by cutting it into small pieces using a machine. Shredding ensures that data is completely removed from the hard drive and cannot be recovered by any means. Shredding is suitable for hard drives that contain PII (personally identifiable information) which is any information that can be used to identify, contact, or locate an individual. Degaussing, low-level formatting, and recycling are not data destruction methods that can guarantee complete data removal from a hard drive.

NEW QUESTION 80

A technician is troubleshooting a customer's PC and receives a phone call. The technician does not take the call and sets the phone to silent. Which of the following BEST describes the technician's actions?

- A. Avoid distractions
- B. Deal appropriately with customer's confidential material
- C. Adhere to user privacy policy
- D. Set and meet timelines

Answer: A

Explanation:

The technician has taken the appropriate action by not taking the call and setting the phone to silent in order to avoid any distractions and remain focused on the task at hand. This is a good example of how to maintain focus and productivity when working on a customer's PC, and will help to ensure that the job is completed in a timely and efficient manner.

NEW QUESTION 85

A technician downloaded software from the Internet that required the technician to scroll through a text box and at the end of the text box, click a button labeled Accept Which of the following agreements IS MOST likely in use?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The most likely agreement in use here is a EULA (End User License Agreement). This is a legally binding agreement between the user and the software developer, outlining the terms and conditions that the user must agree to in order to use the software. It is important that the user understands and agrees to the EULA before they can proceed with downloading and installing the software. As stated in the CompTIA A+ Core 2 exam objectives, users should be aware of the EULA before downloading any software.

NEW QUESTION 89

A user in a corporate office reports the inability to connect to any network drives. No other users have reported this issue. Which of the following is the MOST likely reason the user is having this issue?

- A. Mastered
- B. Not Mastered

Answer: A

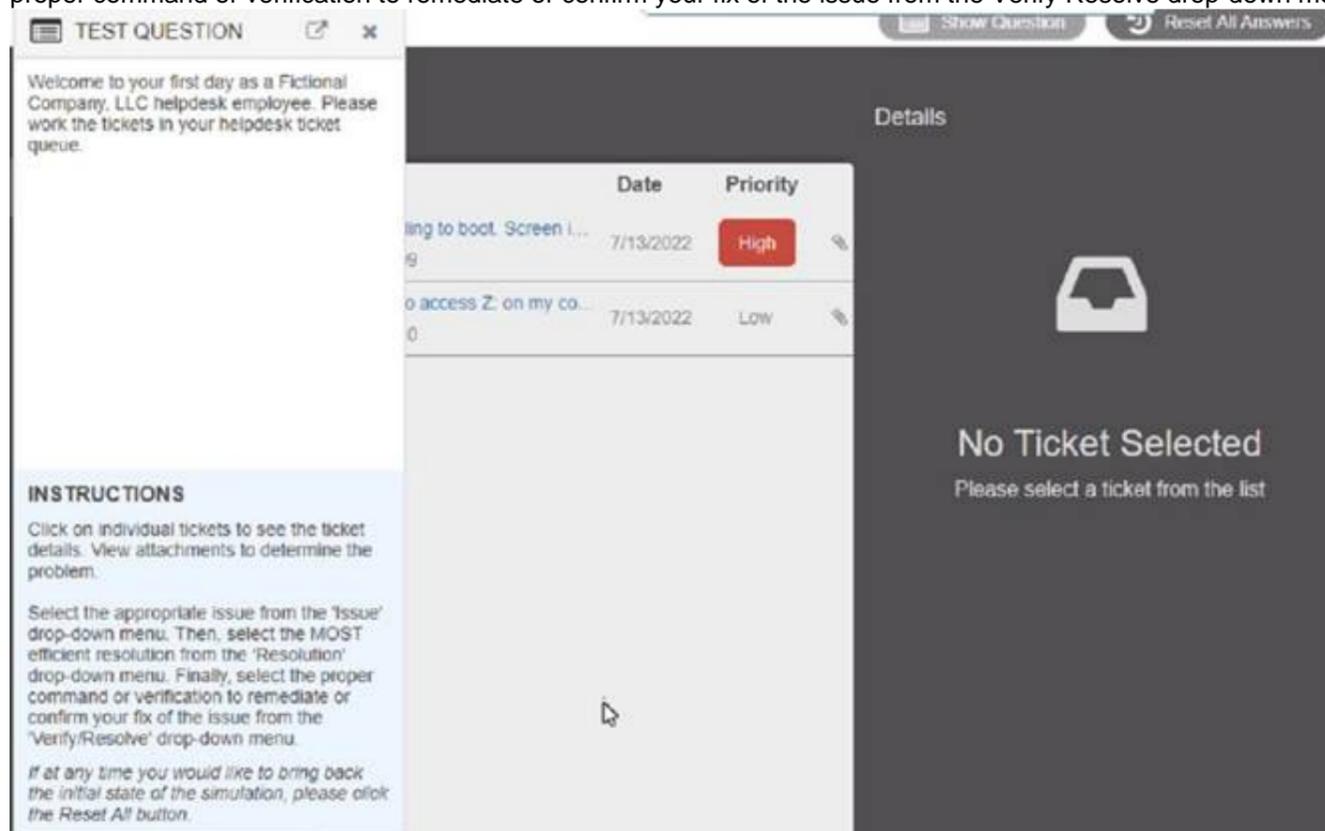
NEW QUESTION 92

HOTSPOT

Welcome to your first day as a Fictional Company, LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

Click on individual tickers to see the ticket details. View attachments to determine the problem.

Select the appropriate issue from the 'issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the Verify Resolve drop-down menu.



TEST QUESTION [Show Question] [Reset All Answers]

Welcome to your first day as a Fictional Company, LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

	Date	Priority
ing to boot. Screen l...	7/13/2022	High
o access Z: on my co...	7/13/2022	Low

Details

No Ticket Selected
Please select a ticket from the list

INSTRUCTIONS

Click on individual tickets to see the ticket details. View attachments to determine the problem.

Select the appropriate issue from the 'Issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the 'Verify/Resolve' drop-down menu.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Date	Priority
ing to boot. Screen l... 9	7/13/2022 High
to access Z: on my co... 0	7/13/2022 Low

#8675309	Open
Priority	High
Category	Technical / Bug Reports
Assigned To	helpdesk@fictional.com
Assigned Date	7/13/2022
Subject	PC is failing to boot. Screen is displaying error message, see attachment.
Attachments	bootmgr not found.png
Issue	<input type="text"/>
Resolution	<input type="text"/>
Verify/Resolve	<input type="text"/>

The screenshot shows a helpdesk ticket interface. On the left, a table lists tickets with columns for Date and Priority. The main area displays details for ticket #8678309, which is 'Open' with a 'High' priority. The subject is 'PC is failing to boot. Screen is displaying error message, see attachment'. An attachment named 'locklog_not_found.png' is listed. Below the details, there are two dropdown menus. The first is labeled 'Resolution' and is open, showing a list of options including 'Corrupt OS', 'Recent Windows Updates', 'Graphics Drive Updates', 'BSOD', 'Printing Issues', 'Limited Network Connectivity', 'Services Failed to Start', 'User Profile is Corrupted', 'Application Crash', 'User cannot access shared resource', 'URL contains typo', 'Reinstall Operating System', 'Rollback Updates', 'Rollback Drivers', 'Repair Application', 'Restart Print Spooler', 'Disable Network Adapter', 'Update Network Drivers', 'Refresh DHCP', 'Rebuild Windows Profile', 'Apply Updates', 'Repair installation', 'Restore from Recovery Partition', 'Remap network drive', 'Verify integrity of disk drive', 'Initiate screen share session with user', 'Windows recovery environment', and 'Inform user of AUP violation'. The second dropdown menu is labeled 'Verify/Resolve' and is also open, showing a list of commands: 'chkdsk', 'dism', 'diskpart', 'sfc', 'dd', 'ctrl + alt + del', 'net use', 'net user', 'netstat', 'netsh', and 'bootrec'.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Details

#8675309	Open
Priority	High
Category	Technical / Bug Reports
Assigned To	helpdesk@fictional.com
Assigned Date	7/13/2022

Subject PC is failing to boot. Screen is displaying error message, see attachment.

Attachments [bootmgr_not_found.png](#)

Issue

Corrupt OS ▼

Resolution

Reinstall Operating System ▼

Verify/Resolve

chkdsk ▼

Close Ticket

NEW QUESTION 95

A user reports a workstation has been performing strangely after a suspicious email was opened on it earlier in the week. Which of the following should the technician perform FIRST?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

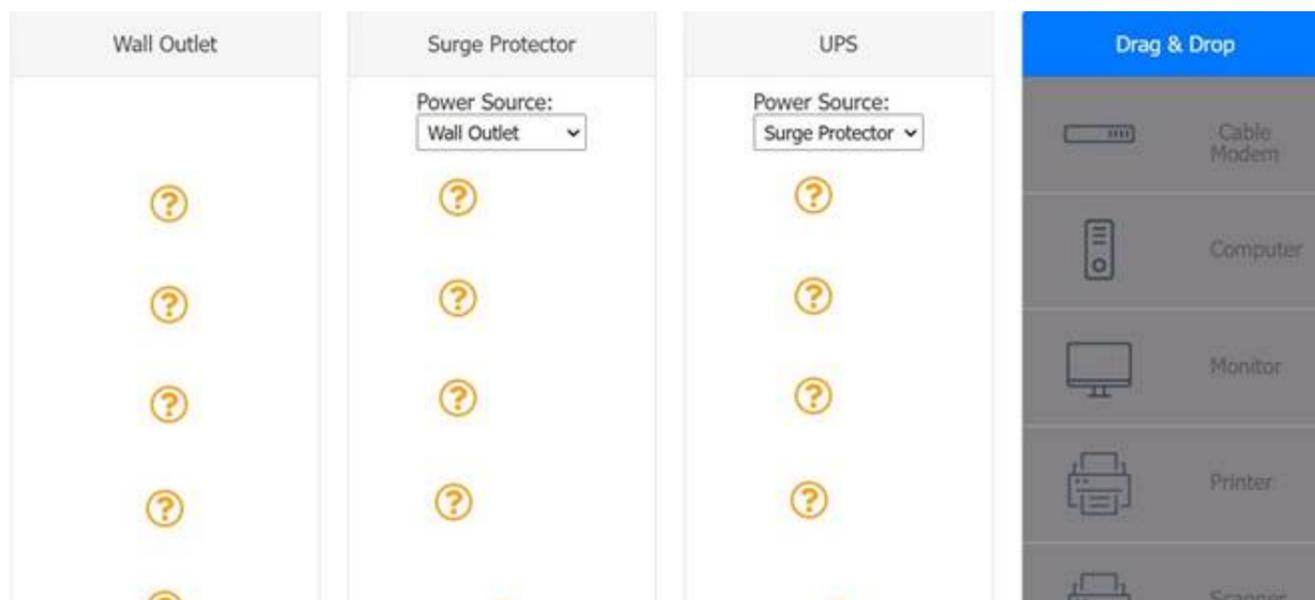
[https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-\(3-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0))

When a user reports that their workstation is behaving strangely after opening a suspicious email, the first step a technician should take is to run a virus scan on the computer. This is because opening a suspicious email is a common way for viruses and malware to infect a computer. Running a virus scan can help identify and remove any infections that may be causing the computer to behave strangely.

NEW QUESTION 96

DRAG DROP

A customer recently experienced a power outage at a SOHO. The customer does not think the components are connected properly. A print job continued running for several minutes after the power failed, but the customer was not able to interact with the computer. Once the UPS stopped beeping, all functioning devices also turned off. In case of a future power failure, the customer wants to have the most time available to save cloud documents and shut down the computer without losing any data.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

UPS > Surge protector = Computer, wifi router, cable modem
 Surge protector = wallOutlet , printer and scanner

NEW QUESTION 100

Which of the following wireless security features can be enabled to allow a user to use login credentials to attach to available corporate SSIDs?

- A. TACACS+
- B. Kerberos
- C. Preshared key
- D. WPA2/AES

Answer: D

Explanation:

WPA2/AES (Wi-Fi Protected Access 2/Advanced Encryption Standard) is a wireless security standard that supports enterprise mode, which allows a user to use login credentials (username and password) to authenticate to available corporate SSIDs (service set identifiers). TACACS+ (Terminal Access Controller Access-Control System Plus) and Kerberos are network authentication protocols, but they are not wireless security features. Preshared key is another wireless security feature, but it does not use login credentials. Verified References: <https://www.comptia.org/blog/wireless-security-standards>
<https://www.comptia.org/certifications/a>

NEW QUESTION 102

A technician is installing RAM in a new workstation and needs to protect against electrostatic discharge. Which of the following will best resolve this concern?

- A. Battery backup
- B. Thermal paste
- C. ESD strap
- D. Consistent power

Answer: C

Explanation:

An ESD strap, also known as an antistatic wrist strap, is a device that prevents electrostatic discharge (ESD) from damaging sensitive electronic components such as RAM. ESD is the sudden flow of electricity between two objects with different electrical charges, which can cause permanent damage or malfunction to electronic devices. An ESD strap connects the technician's wrist to a grounded surface, such as a metal case or a mat, and equalizes the electrical potential between the technician and the device. Battery backup, thermal paste, and consistent power are not devices that can protect against ESD.

NEW QUESTION 106

The network was breached over the weekend. System logs indicate that a single user's account was successfully breached after 500 attempts with a dictionary attack. Which of the following would BEST mitigate this threat?

- A. Encryption at rest
- B. Account lockout
- C. Automatic screen lock
- D. Antivirus

Answer: B

Explanation:

Account lockout would best mitigate the threat of a dictionary attack.

NEW QUESTION 107

A user wants to back up a Windows 10 device. Which of the following should the user select?

- A. Devices and Printers
- B. Email and Accounts
- C. Update and Security
- D. Apps and Features

Answer: C

Explanation:

Update and Security is the section in Windows 10 Settings that allows the user to back up their device. Backing up a device means creating a copy of the data and settings on the device and storing it in another location, such as an external drive or a cloud service. Backing up a device can help the user restore their data and settings in case of data loss, corruption, or theft. Devices and Printers, Email and Accounts, and Apps and Features are not sections in Windows 10 Settings that allow the user to back up their device.

NEW QUESTION 110

An IT services company that supports a large government contract replaced the Ethernet cards on several hundred desktop machines to comply With regulatory requirements. Which of the following disposal methods for the non-compliant cards is the MOST environmentally friendly?

- A. incineration
- B. Resale
- C. Physical destruction
- D. Dumpster for recycling plastics

Answer: D

Explanation:

When disposing of non-compliant Ethernet cards, the most environmentally friendly option is to use a dumpster for recycling plastics. This method is the most effective way to reduce the amount of waste that is sent to landfills, and it also helps to reduce the amount of energy used in the production of new materials. Additionally, recycling plastics helps to reduce the amount of toxic chemicals that can be released into the environment. According to CompTIA A+ Core 2 documents, "The most environmentally friendly disposal method for non-compliant Ethernet cards is to use a dumpster for recycling plastics. This method is the most effective way to reduce the amount of waste that is sent to landfills, and it also helps to reduce the amount of energy used in the production of new materials." <https://sustainability.yale.edu/blog/how-sustainably-dispose-your-technological-waste>

NEW QUESTION 113

A user rotates a cell phone horizontally to read emails, but the display remains vertical, even though the settings indicate autorotate is on. Which of the following will MOST likely resolve the issue?

- A. Recalibrating the magnetometer
- B. Recalibrating the compass
- C. Recalibrating the digitizer
- D. Recalibrating the accelerometer

Answer: D

Explanation:

When a user rotates a cell phone horizontally to read emails and the display remains vertical, even though the settings indicate autorotate is on, this is typically due to a problem with the phone's accelerometer. The accelerometer is the sensor that detects changes in the phone's orientation and adjusts the display accordingly. If the accelerometer is not calibrated correctly, the display may not rotate as expected. Recalibrating the accelerometer is the most likely solution to this issue. The process for recalibrating the accelerometer can vary depending on the specific device and operating system, but it typically involves going to the device's settings and finding the option to calibrate or reset the sensor. Users may need to search their device's documentation or online resources to find specific instructions for their device.

NEW QUESTION 114

Remote employees need access to information that is hosted on local servers at the company. The IT department needs to find a solution that gives employees secure access to the company's resources as if the employees were on premises. Which of the following remote connection services should the IT team implement?

- A. SSH
- B. VNC
- C. VPN
- D. RDP

Answer: C

Explanation:

A VPN (Virtual Private Network) is a service that allows remote employees to access the company's network resources securely over the internet as if they were on premises. A VPN encrypts the data traffic between the employee's device and the VPN server, and assigns the employee a virtual IP address that belongs to the company's network. This way, the employee can access the local servers, files, printers, and other resources without exposing them to the public internet. A VPN also protects the employee's privacy and identity by masking their real IP address and location.

NEW QUESTION 118

A user wants to acquire antivirus software for a SOHO PC. A technician recommends a licensed software product, but the user does not want to pay for a license. Which of the following license types should the technician recommend?

- A. Corporate
- B. Open-source
- C. Personal

D. Enterprise

Answer: B

Explanation:

Open-source software is software that has its source code available for anyone to inspect, modify, and distribute. Open-source software is usually free of charge and does not require a license to use. Some examples of open-source antivirus software are ClamAV, Comodo, and Immunit12. The other license types are either suitable for a SOHO PC. Corporate and enterprise licenses are designed for large-scale organizations and networks, and they usually require a subscription fee. Personal licenses are for individual users and may have limited features or support.

References: 1 What is Open Source Software? - Definition from Techopedia(<https://www.tomsguide.com/us/best-antivirus,review-2588.html>). 2 7 Best Lifetime License Antivirus Tools [2023 Guide] - Windows Report(<https://windowsreport.com/antivirus-with-unlimited-validity/>).

NEW QUESTION 119

A customer calls a service support center and begins yelling at a technician about a feature for a product that is not working to the customer's satisfaction. This feature is not supported by the service support center and requires a field technician to troubleshoot. The customer continues to demand service. Which of the following is the BEST course of action for the support center representative to take?

- A. Inform the customer that the issue is not within the scope of this department.
- B. Apologize to the customer and escalate the issue to a manager.
- C. Ask the customer to explain the issue and then try to fix it independently.
- D. Respond that the issue is something the customer should be able to fix.

Answer: B

Explanation:

Apologizing to the customer and escalating the issue to a manager is the best course of action for the support center representative to take. This shows empathy and professionalism and allows the manager to handle the situation and provide the appropriate service or resolution for the customer.

NEW QUESTION 121

Which of the following is a consequence of end-of-life operating systems?

- A. Operating systems void the hardware warranty.
- B. Operating systems cease to function.
- C. Operating systems no longer receive updates.
- D. Operating systems are unable to migrate data to the new operating system.

Answer: C

Explanation:

End-of-life operating systems are those which have reached the end of their life cycle and are no longer supported by the software developer. This means that the operating system will no longer receive updates, security patches, or other new features. This can leave users vulnerable to security threats, as the system will no longer be protected against the latest threats. Additionally, this can make it difficult to migrate data to a newer operating system, as the old system is no longer supported.

NEW QUESTION 122

A technician needs administrator access on a Windows workstation to facilitate system changes without elevating permissions. Which of the following would best accomplish this task?

- A. Group Policy Editor
- B. Local Users and Groups
- C. Device Manager
- D. System Configuration

Answer: B

Explanation:

Local Users and Groups is the best option to accomplish this task. Local Users and Groups is a tool that allows managing the local user accounts and groups on a Windows workstation. The technician can use this tool to create a new user account with administrator privileges or add an existing user account to the Administrators group. This way, the technician can log in with the administrator account and make system changes without elevating permissions. Group Policy Editor, Device Manager, and System Configuration are not correct answers for this question. Group Policy Editor is a tool that allows configuring policies and settings for users and computers in a domain environment. Device Manager is a tool that allows managing the hardware devices and drivers on a Windows workstation. System Configuration is a tool that allows modifying the startup options and services on a Windows workstation. None of these tools can directly grant administrator access to a user account. References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 13

? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 103

NEW QUESTION 125

The command `cat cor.ptia.txt` was issued on a Linux terminal. Which of the following results should be expected?

- A. The contents of the text `comptia.txt` will be replaced with a new blank document
- B. The contents of the text `compti`
- C. `txt` would be displayed.
- D. The contents of the text `comptia.txt` would be categorized in alphabetical order.
- E. The contents of the text `compti`
- F. `txt` would be copied to another `compti`
- G. `txt` file

Answer: B

Explanation:

The command `cat cor.ptia.txt` was issued on a Linux terminal. This command would display the contents of the text `comptia.txt`.

NEW QUESTION 127

A technician needs to remotely connect to a Linux desktop to assist a user with troubleshooting. The technician needs to make use of a tool natively designed for Linux. Which of the following tools will the technician MOST likely use?

- A. VNC
- B. MFA
- C. MSRA
- D. RDP

Answer: A

Explanation:

The tool that the technician will most likely use to remotely connect to a Linux desktop is VNC. VNC stands for Virtual Network Computing and is a protocol that allows remote access and control of a graphical desktop environment over a network. VNC is natively designed for Linux and can also support other operating systems, such as Windows and Mac OS. VNC can be used to assist users with troubleshooting by viewing and interacting with their desktops remotely. MFA stands for Multi-Factor Authentication and is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. MFA is not a tool that can be used to remotely connect to a Linux desktop but a technique that can be used to enhance security

for systems or services. MSRA stands for Microsoft Remote Assistance and is a feature that allows remote access and control of a Windows desktop environment over a network. MSRA is not natively designed for Linux and may not be compatible or supported by Linux systems. RDP stands for Remote Desktop Protocol and is a protocol that allows remote access and control of a Windows desktop environment over a network. RDP is not natively designed for Linux and may not be compatible or supported by Linux systems. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

NEW QUESTION 131

A company would like to implement multifactor authentication for all employees at a minimal cost. Which of the following best meets the company's requirements?

- A. Biometrics
- B. Soft token
- C. Access control lists
- D. Smart card

Answer: B

Explanation:

A soft token, also known as a software token or an OTP (one-time password) app, is a type of multifactor authentication that generates a temporary code or password on a user's device, such as a smartphone or a tablet. The user must enter this code or password along with their username and password to access their account or service. A soft token can help improve security by adding an extra layer of verification and preventing unauthorized access even if the user's credentials are compromised. A soft token can also be implemented at a minimal cost, as it does not require any additional hardware or infrastructure. Biometrics, access control lists, and smart card are not types of multifactor authentication that can be implemented at a minimal cost.

NEW QUESTION 133

Which of the following is used to explain issues that may occur during a change implementation?

- A. Scope change
- B. End-user acceptance
- C. Risk analysis
- D. Rollback plan

Answer: C

Explanation:

Risk analysis is used to explain issues that may occur during a change implementation. Risk analysis is a process of identifying, assessing and prioritizing potential risks that may affect a project or an activity. Risk analysis can help determine the likelihood and impact of various issues that may arise during a change implementation, such as technical errors, compatibility problems, security breaches, performance degradation or user dissatisfaction. Risk analysis can also help plan and prepare for mitigating or avoiding these issues. Scope change is a modification of the original goals, requirements or deliverables of a project or an activity. Scope change is not used to explain issues that may occur during a change implementation but to reflect changes in expectations or needs of the stakeholders. End-user acceptance is a measure of how well the users are satisfied with and adopt a new system or service. End-user acceptance is not used to explain issues that may occur during a change implementation but to evaluate the success and effectiveness of the change. Rollback plan is a contingency plan that describes how to restore a system or service to its previous state in case of a failed or problematic change implementation. Rollback plan is not used to explain issues that may occur during a change implementation but to recover from them. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.2

NEW QUESTION 137

A technician is troubleshooting boot times for a user. The technician attempts to use MSConfig to see which programs are starting with the OS but receives a message that it can no longer be used to view startup items. Which of the following programs can the technician use to view startup items?

- A. msinfo32
- B. perfmon
- C. regedit
- D. taskmgr

Answer: D

Explanation:

When troubleshooting boot times for a user, a technician may want to check which programs are starting with the operating system to identify any that may be slowing down the boot process. MSConfig is a tool that can be used to view startup items on a Windows system, but it may not always be available or functional. In this scenario, the technician receives a message that MSConfig cannot be used to view startup items. As an alternative, the technician can use Task Manager (taskmgr), which can

also display the programs that run at startup. To access the list of startup items in Task Manager, the technician can follow these steps:

- ? Open Task Manager by pressing Ctrl+Shift+Esc.
- ? Click the "Startup" tab.
- ? The list of programs that run at startup will be displayed.

NEW QUESTION 138

A user is unable to access a web-based application. A technician verifies the computer cannot access any web pages at all. The computer obtains an IP address from the DHCP server. Then, the technician verifies the user can ping localhost, the gateway, and known IP addresses on the internet and receive a response. Which of the following is the MOST likely reason for the issue?

- A. A firewall is blocking the application.
- B. The wrong VLAN was assigned.
- C. The incorrect DNS address was assigned.
- D. The browser cache needs to be cleared

Answer: C

Explanation:

DNS (domain name system) is a protocol that translates domain names to IP addresses. If the computer has an incorrect DNS address assigned, it will not be able to

resolve the domain names of web-based applications and access them. A firewall, a VLAN (virtual local area network) and a browser cache are not the most likely reasons for the issue, since the computer can ping known IP addresses on the internet and receive a response. Verified References: <https://www.comptia.org/blog/what-is-dns> <https://www.comptia.org/certifications/a>

NEW QUESTION 142

All the desktop icons on a user's newly issued PC are very large. The user reports that the PC was working fine until a recent software patch was deployed. Which of the following would BEST resolve the issue?

- A. Rolling back video card drivers
- B. Restoring the PC to factory settings
- C. Repairing the Windows profile
- D. Reinstalling the Windows OS

Answer: A

Explanation:

Rolling back video card drivers is the best way to resolve the issue of large desktop icons on a user's newly issued PC. This means restoring the previous version of the drivers that were working fine before the software patch was deployed. The software patch may have caused compatibility issues or corrupted the drivers, resulting in display problems

NEW QUESTION 144

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?

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.

References:

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

NEW QUESTION 146

A technician wants to enable BitLocker on a Windows 10 laptop and is unable to find the BitLocker Drive Encryption menu item in Control Panel. Which of the following explains why the technician unable to find this menu item?

- A. The hardware does not meet BitLocker's minimum system requirements.
- B. BitLocker was renamed for Windows 10.
- C. BitLocker is not included on Windows 10 Home.
- D. BitLocker was disabled in the registry of the laptop

Answer: C

Explanation:

BitLocker is only available on Windows 10 Pro, Enterprise, and Education editions¹. Therefore, the technician is unable to find the BitLocker Drive Encryption menu item in Control Panel because it is not included in the Windows 10 Home edition¹.

NEW QUESTION 147

A technician has spent hours trying to resolve a computer issue for the company's Chief Executive Officer (CEO). The CEO needs the device returned as soon as possible. Which of the following steps should the technician take NEXT?

- A. Continue researching the issue
- B. Repeat the iterative processes
- C. Inform the CEO the repair will take a couple of weeks
- D. Escalate the ticket

Answer: D

Explanation:

The technician should escalate the ticket to ensure that the CEO's device is returned as soon as possible¹

NEW QUESTION 148

A technician is setting up a backup method on a workstation that only requires two sets of

tapes to restore. Which of the following would BEST accomplish this task?

- A. Differential backup
- B. Off-site backup
- C. Incremental backup
- D. Full backup

Answer: D

Explanation:

To accomplish this task, the technician should use a Full backup method

A full backup only requires two sets of tapes to restore because it backs up all the data from the workstation. With a differential backup, the backups need to be taken multiple times over a period of time, so more tapes would be needed to restore the data

NEW QUESTION 151

A user updates a mobile device's OS. A frequently used application becomes consistently unresponsive immediately after the device is launched. Which of the following troubleshooting steps should the user perform FIRST?

- A. Delete the application's cache.
- B. Check for application updates.
- C. Roll back the OS update.
- D. Uninstall and reinstall the application.

Answer: B

Explanation:

Checking for application updates is the first troubleshooting step that the

user should perform, because the application may not be compatible with the new OS version and may need an update to fix the issue.

Deleting the application's cache, rolling back the OS update, or uninstalling and reinstalling the application are possible solutions, but they are more time-consuming and disruptive than checking for updates. References: : <https://www.comptia.org/training/resources/exam-objectives/comptia-a-core-2-exam-objectives>
: <https://www.lifewire.com/how-to-update-apps-on-android-4173855>

NEW QUESTION 155

A department manager submits a help desk ticket to request the migration of a printer's port utilization from USB to Ethernet so multiple users can access the printer. This will be a new network printer, thus a new IP address allocation is required. Which of the following should happen immediately before network use is authorized?

- A. Document the date and time of the change.
- B. Submit a change request form.
- C. Determine the risk level of this change.
- D. Request an unused IP address.

Answer: B

Explanation:

A change request form is a document that describes the proposed change, the reason for the change, the impact of the change, and the approval process for the change. A change request form is required for any planned changes to the network, such as adding a new network printer, to ensure that the change is authorized, documented, and communicated to all stakeholders. Submitting a change request form should happen immediately before network use is authorized, as stated in the Official CompTIA A+ Core 2 Study Guide. The other options are either too late (documenting the date and time of the change) or too early (determining the risk level of the change and requesting an unused IP address) in the change management process.

NEW QUESTION 158

The audio on a user's mobile device is inconsistent when the user uses wireless headphones and moves around. Which of the following should a technician perform to troubleshoot the issue?

- A. Verify the Wi-Fi connection status.
- B. Enable the NFC setting on the device.
- C. Bring the device within Bluetooth range.
- D. Turn on device tethering.

Answer: C

Explanation:

Bringing the device within Bluetooth range is the best way to troubleshoot the issue of inconsistent audio when using wireless headphones and moving around. Bluetooth is a wireless technology that allows devices to communicate over short distances, typically up to 10 meters or 33 feet. If the device is too far from the headphones, the Bluetooth signal may be weak or interrupted, resulting in poor audio quality or loss of connection.

NEW QUESTION 161

A technician sees a file that is requesting payment to a cryptocurrency address. Which of the following should the technician do first?

- A. Quarantine the computer.
- B. Disable System Restore.
- C. Update the antivirus software definitions.
- D. Boot to safe mode.

Answer: A

Explanation:

Quarantining the computer means isolating it from the network and other devices to prevent the spread of malware or ransomware. Ransomware is a type of malware that encrypts the files on a computer and demands payment (usually in cryptocurrency) to restore them. If a technician sees a file that is requesting payment to a cryptocurrency address, it is likely that the computer has been infected by ransomware. Quarantining the computer should be the first step to contain the infection and prevent further damage. Disabling System Restore, updating the antivirus software definitions, and booting to safe mode are not steps that should be done before quarantining the computer.

NEW QUESTION 165

Which of the following could be used to implement secure physical access to a data center?

- A. Geofence
- B. Alarm system
- C. Badge reader
- D. Motion sensor

Answer: C

Explanation:

Badge readers are used to implement secure physical access to a data center. They are used to read the identification information on an employee's badge and grant access to the data center if the employee is authorized.

This system requires individuals to have an access badge that contains their identification information or a unique code that can be scanned by a reader. After the badge is scanned, the system compares the information on the badge with the authorized personnel database to authenticate if the individual has the required clearance to enter that area. The other options listed, such as a geofence, alarm system, or motion sensor are security measures that may be used in conjunction with badge readers, but do not provide identification and authentication features.

NEW QUESTION 170

Which of the following would typically require the most computing resources from the host computer?

- A. Chrome OS
- B. Windows
- C. Android
- D. macOS
- E. Linux

Answer: B

Explanation:

Windows is the operating system that typically requires the most computing resources from the host computer, compared to the other options. Computing resources include hardware components such as CPU, RAM, disk space, graphics card, and network adapter. The minimum system requirements for an operating system indicate the minimum amount of computing resources needed to install and run the operating system on a computer. The higher the minimum system requirements, the more computing resources the operating system consumes.

According to the web search results, the minimum system requirements for Windows 10 and Windows 11 are as follows:

- ? CPU: 1 GHz or faster with two or more cores (Windows 10); 1 GHz or faster with two or more cores on a compatible 64-bit processor (Windows 11)
- ? RAM: 1 GB for 32-bit or 2 GB for 64-bit (Windows 10); 4 GB (Windows 11)
- ? Disk space: 16 GB for 32-bit or 32 GB for 64-bit (Windows 10); 64 GB (Windows 11)
- ? Graphics card: DirectX 9 or later with WDDM 1.0 driver (Windows 10); DirectX 12 compatible with WDDM 2.0 driver (Windows 11)
- ? Network adapter: Ethernet or Wi-Fi (Windows 10); Ethernet or Wi-Fi that supports 5 GHz (Windows 11)

The minimum system requirements for macOS Ventura are as follows:

- ? CPU: Intel Core i3 or higher, or Apple M1 chip
- ? RAM: 4 GB
- ? Disk space: 35.5 GB
- ? Graphics card: Metal-capable

? Network adapter: Ethernet or Wi-Fi

The minimum system requirements for Chrome OS are as follows:

? CPU: Intel Celeron or higher

? RAM: 2 GB

? Disk space: 16 GB

? Graphics card: Integrated

? Network adapter: Ethernet or Wi-Fi

The minimum system requirements for Android are as follows:

? CPU: 1 GHz or higher

? RAM: 512 MB

? Disk space: 8 GB

? Graphics card: OpenGL ES 2.0

? Network adapter: Ethernet or Wi-Fi

The minimum system requirements for Linux vary depending on the distribution, but a common example is Ubuntu, which has the following minimum system requirements:

? CPU: 2 GHz dual core processor or better

? RAM: 4 GB

? Disk space: 25 GB

? Graphics card: 1024 x 768 screen resolution

? Network adapter: Ethernet or Wi-Fi

Based on the comparison of the minimum system requirements, Windows has the highest requirements for CPU, RAM, disk space, and graphics card, while Chrome OS and Android have the lowest requirements. macOS and Linux have moderate requirements, depending on the hardware and software configuration.

Therefore, Windows is the operating system that typically requires the most computing resources from the host computer.

References:

? Windows, macOS, Chrome OS, or Linux: Which Operating System Is Right for You?1

? Comparison of operating systems3

? Windows 10 vs 11 Minimum System Requirements: Why Need a New One?2

? macOS Monterey - Technical Specifications

? Chrome OS - Wikipedia

? Android - Wikipedia

? Installation/SystemRequirements - Community Help Wiki

NEW QUESTION 171

A change advisory board just approved a change request. Which of the following is the MOST likely next step in the change process?

- A. End user acceptance
- B. Perform risk analysis
- C. Communicate to stakeholders
- D. Sandbox testing

Answer: D

Explanation:

The risk analysis should be performed before it's taken to the board. The step after the board approves the change is End User Agreement Reference:

https://www.youtube.com/watch?v=Ru77iZxuEIA&list=PLG49S3nxzAnna96gzhJrzki4hH_mgW4b&index=59

NEW QUESTION 173

A remote user is having issues accessing an online share. Which of the following tools would MOST likely be used to troubleshoot the issue?

- A. Screen-sharing software
- B. Secure shell
- C. Virtual private network
- D. File transfer software

Answer: A

Explanation:

Screen-sharing software is a tool that allows a technician to remotely view and control a user's screen over the internet. It can be used to troubleshoot issues with accessing an online share, as well as other problems that require visual inspection or guidance. Secure shell (SSH) is a protocol that allows remote access and command execution on another device, but it does not allow screen-sharing. Virtual private network (VPN) is a protocol that creates a secure tunnel between two devices over the internet, but it does not allow remote troubleshooting. File transfer software is a tool that allows transferring files between two devices over the internet, but it does not allow screen-sharing. Verified References: <https://www.comptia.org/blog/what-is-screen-sharing-software>

<https://www.comptia.org/certifications/a>

NEW QUESTION 174

A technician is troubleshooting a customer's PC and receives a phone call. The technician does not take the call and sets the phone to silent. Which of the following BEST describes

the technician's actions?

- A. Avoid distractions
- B. Deal appropriately with customer's confidential material .
- C. Adhere to user privacy policy
- D. Set and meet timelines

Answer: A

Explanation:

The technician's action of setting the phone to silent while troubleshooting the customer's PC is an example of avoiding distractions. By setting the phone to silent, the technician is ensuring that they are able to focus on the task at hand without any distractions that could potentially disrupt their workflow. This is an important practice when handling customer's confidential material, as it ensures that the technician is able to focus on the task and not be distracted by any external sources. Furthermore, it also adheres to user privacy policies, as the technician is not exposing any confidential information to any external sources.

NEW QUESTION 177

A technician is trying to encrypt a single folder on a PC. Which of the following should the technician use to accomplish this task?

- A. FAT32
- B. exFAT
- C. BitLocker
- D. EFS

Answer: D

Explanation:

EFS (Encrypting File System) is a feature that allows a user to encrypt a single folder or file on a Windows PC. It uses a public key encryption system to protect the data from unauthorized access. FAT32 and exFAT are file system formats that do not support encryption. BitLocker is a feature that encrypts the entire drive, not a single folder or file. Verified References: <https://www.comptia.org/blog/what-is-efs> <https://www.comptia.org/certifications/a>

NEW QUESTION 180

A customer has a USB-only printer attached to a computer. A technician is configuring an arrangement that allows other computers on the network to use the printer. In which of the following locations on the customer's desktop should the technician make this configuration?

- A. Printing Preferences/Advanced tab
- B. Printer Properties/Sharing tab
- C. Printer Properties/Security tab
- D. Printer Properties/Ports tab

Answer: B

Explanation:

The correct answer is B. Printer Properties/Sharing tab. This is the location where the technician can enable printer sharing and assign a share name for the USB printer. This will allow other computers on the network to access the printer by using the share name or the IP address of the computer that has the printer attached1.

1: CompTIA A+ Certification Exam: Core 2 Objectives, page 15, section 1.9.

NEW QUESTION 182

Which of the following is an example of MFA?

- A. Fingerprint scan and retina scan
- B. Password and PIN
- C. Username and password
- D. Smart card and password

Answer: D

Explanation:

Smart card and password is an example of two-factor authentication (2FA), not multi-factor authentication (MFA). MFA requires two or more authentication factors. Smart card and password is an example of two-factor authentication (2FA2)

NEW QUESTION 184

Which of the following is used to ensure users have the appropriate level of access to perform their job functions?

- A. Access control list
- B. Multifactor authentication
- C. Least privilege
- D. Mobile device management

Answer: C

Explanation:

Least privilege is the principle that is used to ensure users have the appropriate level of access to perform their job functions. Least privilege means granting users only the minimum amount of access rights and permissions they need to perform their tasks, and nothing more. Least privilege reduces the risk of unauthorized access, data leakage, malware infection, or accidental damage by limiting what users can do on the system or network. Access control list, multifactor authentication, and mobile device management are not principles, but rather mechanisms or methods that can implement least privilege. Access control list is a list that specifies the users or groups that are allowed or denied access to a resource, such as a file, folder, or printer. Multifactor authentication is a method that requires users to provide two or more pieces of evidence to prove their identity, such as a password, a token, or a biometric factor. Mobile device management is a tool that allows managing and securing mobile devices, such as smartphones or tablets, that are used by employees to access corporate data or applications. References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25

? [CompTIA Security+ SY0-601 Certification Study Guide], page 1003

NEW QUESTION 185

Once weekly a user needs Linux to run a specific open-source application that is not available for the currently installed Windows platform. The user has limited bandwidth throughout the day. Which of the following solutions would be the MOST efficient, allowing for parallel execution of the Linux application and Windows

applications?

- A. Install and run Linux and the required application in a PaaS cloud environment
- B. Install and run Linux and the required application as a virtual machine installed under the Windows OS
- C. Use a swappable drive bay for the boot drive and install each OS with applications on its own drive Swap the drives as needed
- D. Set up a dual boot system by selecting the option to install Linux alongside Windows

Answer: B

Explanation:

The user should install and run Linux and the required application as a virtual machine installed under the Windows OS. This solution would allow for parallel execution of the Linux application and Windows applications.

The MOST efficient solution that allows for parallel execution of the Linux application and Windows applications is to install and run Linux and the required application as a virtual machine installed under the Windows OS. This is because it allows you to run both Linux and Windows together without the need to keep the Linux portion confined to a VM window.

NEW QUESTION 187

Which of the following is the MOST important environmental concern inside a data center?

- A. Battery disposal
- B. Electrostatic discharge mats
- C. Toner disposal
- D. Humidity levels

Answer: D

Explanation:

One of the most important environmental concerns inside a data center is the level of humidity. High levels of humidity can cause condensation, which can result in corrosion of components and other equipment. Low levels of humidity can cause static electricity to build up, potentially leading to electrostatic discharge (ESD) and damage to components. Therefore, it is crucial to maintain a relative humidity range of 40-60% in a data center to protect the equipment and ensure proper operation.

NEW QUESTION 189

A user tries to access commonly used web pages but is redirected to unexpected websites. Clearing the web browser cache does not resolve the issue. Which of the following should a technician investigate NEXT to resolve the issue?

- A. Enable firewall ACLs.
- B. Examine the localhost file entries.
- C. Verify the routing tables.
- D. Update the antivirus definitions.

Answer: B

Explanation:

A possible cause of the user being redirected to unexpected websites is that the localhost file entries have been modified by malware or hackers to point to malicious or unwanted websites. The localhost file is a text file that maps hostnames to IP addresses and can override DNS settings. By examining the localhost file entries, a technician can identify and remove any suspicious or unauthorized entries that may cause the redirection issue. Enabling firewall ACLs may not resolve the issue if the firewall rules do not block the malicious or unwanted websites. Verifying the routing tables may not resolve the issue if the routing configuration is correct and does not affect the web traffic. Updating the antivirus definitions may help prevent future infections but may not remove the existing malware or changes to the localhost file. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.3

NEW QUESTION 192

An organization's Chief Financial Officer (CFO) is concerned about losing access to very sensitive, legacy unmaintained PII on a workstation if a ransomware outbreak occurs. The CFO has a regulatory requirement to retain this data for many years. Which of the following backup methods would BEST meet the requirements?

- A. A daily, incremental backup that is saved to the corporate file server
- B. An additional, secondary hard drive in a mirrored RAID configuration
- C. A full backup of the data that is stored off-site in cold storage
- D. Weekly, differential backups that are stored in a cloud-hosting provider

Answer: C

Explanation:

According to CompTIA A+ Core 2 objectives, a full backup stored off-site provides the greatest protection against data loss in the event of a ransomware attack or other data disaster. By storing the backup in a separate physical location, it is less likely to be affected by the same event that could cause data loss on the original system. Cold storage is a term used for data archiving, which typically refers to a long-term storage solution that is used for retaining data that is infrequently accessed, but still needs to be kept for regulatory or compliance reasons.

NEW QUESTION 196

During an enterprise rollout of a new application, a technician needs to validate compliance with an application's EULA while also reducing the number of licenses to manage. Which of the following licenses would best accomplish this goal?

- A. Personal use license
- B. Corporate use license
- C. Open-source license
- D. Non-expiring license

Answer: B

Explanation:

A corporate use license, also known as a volume license, is a type of software license that allows an organization to purchase and use multiple copies of a software product with a single license key. A corporate use license can help validate compliance with an application's EULA (end-user license agreement), which is a legal contract that defines the terms and conditions of using the software. A corporate use license can also reduce the number of licenses to manage, as it eliminates the need to activate and track individual licenses for each copy of the software. Personal use license, open-source license, and non-expiring license are not types of licenses that can best accomplish this goal.

NEW QUESTION 200

A technician is asked to resize a partition on the internal storage drive of a computer running macOS. Which of the following tools should the technician use to accomplish this task?

- A. Console
- B. Disk Utility
- C. Time Machine
- D. FileVault

Answer: B

Explanation:

The technician should use Disk Utility to resize a partition on the internal storage drive of a computer running macOS. Disk Utility is a built-in utility that allows users to manage disks, partitions, and volumes on a Mac. It can be used to resize, create, and delete partitions, as well as to format disks and volumes.

NEW QUESTION 203

A police officer often leaves a workstation for several minutes at a time. Which of the following is the BEST way the officer can secure the workstation quickly when walking away?

- A. Use a key combination to lock the computer when leaving.
- B. Ensure no unauthorized personnel are in the area.
- C. Configure a screensaver to lock the computer automatically after approximately 30 minutes of inactivity.
- D. Turn off the monitor to prevent unauthorized visibility of information.

Answer: A

Explanation:

The BEST way to secure the workstation quickly when walking away is to use a key combination to lock the computer when leaving.

NEW QUESTION 206

A network administrator is deploying a client certificate to be used for Wi-Fi access for all devices in an organization. The certificate will be used in conjunction with the user's existing username and password. Which of the following BEST describes the security benefits realized after this deployment?

- A. Multifactor authentication will be forced for Wi-Fi.
- B. All Wi-Fi traffic will be encrypted in transit.
- C. Eavesdropping attempts will be prevented.
- D. Rogue access points will not connect.

Answer: B

Explanation:

The security benefits realized after deploying a client certificate to be used for Wi-Fi access for all devices in an organization are that all Wi-Fi traffic will be encrypted in transit. This means that any data transmitted over the Wi-Fi network will be protected from eavesdropping attempts. Rogue access points will not connect to the network because they will not have the client certificate. However, multifactor authentication will not be forced for Wi-Fi because the client certificate is being used in conjunction with the user's existing username and password.

NEW QUESTION 208

A technician needs to access a Windows 10 desktop on the network in a SOHO using RDP. Although the connection is unsuccessful, the technician is able to ping the computer successfully. Which of the following is MOST likely preventing the connection?

- A. The Windows 10 desktop has Windows 10 Home installed.
- B. The Windows 10 desktop does not have DHCP configured.
- C. The Windows 10 desktop is connected via Wi-Fi.
- D. The Windows 10 desktop is hibernating.

Answer: A

Explanation:

The Windows 10 desktop has Windows 10 Home installed, which does not support RDP (Remote Desktop Protocol) as a host. Only Windows 10 Pro, Enterprise, and Education editions can act as RDP hosts and allow remote access to their desktops. The Windows 10 desktop does not have DHCP configured, is connected via Wi-Fi, or is hibernating are not likely to prevent the RDP connection if the technician is able to ping the computer successfully.

NEW QUESTION 212

Which of the following command options is used to display hidden files and directories?

- A. -a
- B. -s

- C. -lh
- D. -t

Answer: A

Explanation:

The -a option is used to display hidden files and directories in a command-line interface. Hidden files and directories are those that start with a dot (.) and are normally not shown by default. The -a option stands for "all" and shows all files and directories, including the hidden ones. The -a option can be used with commands such as ls, dir, or find to list or search for hidden files and directories. The -s, -lh, and -t options are not used to display hidden files and directories. The -s option stands for "size" and shows the size of files or directories in bytes. The -lh option stands for "long human-readable" and shows the size of files or directories in a more readable format, such as KB, MB, or GB. The -t option stands for "time" and sorts the files or directories by modification time. References:
 ? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 17
 ? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 107

NEW QUESTION 216

A technician successfully removed malicious software from an infected computer after running updates and scheduled scans to mitigate future risks. Which of the following should the technician do next?

- A. Educate the end user on best practices for security.
- B. Quarantine the host in the antivirus system.
- C. Investigate how the system was infected with malware.
- D. Create a system restore point.

Answer: A

Explanation:

Educating the end user on best practices for security is the next step that the technician should take after successfully removing malicious software from an infected computer. Educating the end user on best practices for security is an important part of preventing future infections and mitigating risks. The technician should explain to the end user how to avoid common sources of malware, such as phishing emails, malicious websites, or removable media. The technician should also advise the end user to use strong passwords, update software regularly, enable antivirus and firewall protection, and backup data frequently. Educating the end user on best practices for security can help the end user become more aware and responsible for their own security and reduce the likelihood of recurrence of malware infections. Quarantining the host in the antivirus system, investigating how the system was infected with malware, and creating a system restore point are not the next steps that the technician should take after successfully removing malicious software from an infected computer. Quarantining the host in the antivirus system is a step that the technician should take before removing malicious software from an infected computer. Quarantining the host in the antivirus system means isolating the infected computer from the network or other devices to prevent the spread of malware. Investigating how the system was infected with malware is a step that the technician should take during or after removing malicious software from an infected computer. Investigating how the system was infected with malware means identifying the source, type, and impact of malware on the system and documenting the findings and actions taken. Creating a system restore point is a step that the technician should take before removing malicious software from an infected computer. Creating a system restore point means saving a snapshot of the system's configuration and settings at a certain point in time, which can be used to restore the system

In case of failure or corruption. References:

- ? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15
- ? CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 458

NEW QUESTION 217

A systems administrator installed the latest Windows security patch and received numerous tickets reporting slow performance the next day. Which of the following should the administrator do to resolve this issue?

- A. Rebuild user profiles.
- B. Roll back the updates.
- C. Restart the services.
- D. Perform a system file check.

Answer: B

Explanation:

Rolling back the updates is the best way to resolve the issue of slow performance caused by installing the latest Windows security patch. This can be done by using the System Restore feature or by uninstalling the specific update from the Control Panel. Rebuilding user profiles, restarting the services and performing a system file check are not likely to fix the issue, since they do not undo the changes made by the update. Verified References: <https://www.comptia.org/blog/how-to-roll-back-windows-updates> <https://www.comptia.org/certifications/a>

NEW QUESTION 220

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

- A. Professional
- Home
- B. 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. References¹: BitLocker overview - Windows Security | Microsoft Learn²: Device encryption in Windows - Microsoft Support³: Can You Turn on BitLocker on Windows 10 Home?⁴: How to enable device encryption on Windows 10 Home

NEW QUESTION 223

After a company installed a new SOHO router customers were unable to access the company-hosted public website. Which of the following will MOST likely allow customers to access the website?

- A. Port forwarding
- B. Firmware updates
- C. IP filtering
- D. Content filtering

Answer: B

Explanation:

If customers are unable to access the company-hosted public website after installing a new SOHO router, the company should check for firmware updates¹. Firmware updates can fix bugs and compatibility issues that may be preventing customers from accessing the website¹. The company should also ensure that the router is properly configured to allow traffic to the website¹. If the router is blocking traffic to the website, the company should configure the router to allow traffic to the website¹.

NEW QUESTION 226

A user reports seeing random, seemingly non-malicious advertisement notifications in the Windows 10 Action Center. The notifications indicate the advertisements are coming from a web browser. Which of the following is the best solution for a technician to implement?

- A. Disable the browser from sending notifications to the Action Center.
- B. Run a full antivirus scan on the computer.
- C. Disable all Action Center notifications.
- D. Move specific site notifications from Allowed to Block.

Answer: A

Explanation:

The best solution for a technician to implement is to disable the browser from sending notifications to the Action Center. This will prevent the random advertisement notifications from appearing in the Windows 10 Action Center, which can be annoying and distracting for the user. The technician can follow these steps to disable the browser notifications¹:

? Open the browser that is sending the notifications, such as Microsoft Edge, Google Chrome, or Mozilla Firefox.

? Go to the browser settings or options menu, and look for the privacy and security section.

? Find the option to manage site permissions or notifications, and click on it.

? You will see a list of sites that are allowed or blocked from sending notifications to the browser and the Action Center. You can either block all sites from sending notifications, or select specific sites that you want to block or allow.

? Save the changes and close the browser settings. This solution is better than the other options because:

? Running a full antivirus scan on the computer (B) is not necessary, as the advertisement notifications are not malicious or harmful, and they are not caused by a virus or malware infection. Running a scan will not stop the notifications from appearing, and it will consume system resources and time.

? Disabling all Action Center notifications © is not advisable, as the Action Center is a useful feature that shows notifications and alerts from various apps and system events, such as email, calendar, security, updates, etc. Disabling all notifications will make the user miss important information and reminders, and reduce the functionality of the Action Center.

? Moving specific site notifications from Allowed to Block (D) is not the best solution,

as it will only stop the notifications from some sites, but not from others. The user may still receive advertisement notifications from other sites that are not blocked, or from new sites that are added to the Allowed list. This solution will also require the user to manually manage the list of sites, which can be tedious and time-consuming.

References:

1: How to Disable Annoying Browser Notifications - PCMag

NEW QUESTION 230

Before leaving work, a user wants to see the traffic conditions for the commute home. Which of the following tools can the user employ to schedule the browser to automatically launch a traffic website at 4:45 p.m.?

- A. taskschd.msc
- B. perfmon.msc
- C. lusrmgr.msc
- D. Eventvwr.msc

Answer: A

Explanation:

The user can use the Task Scheduler (taskschd.msc) to schedule the browser to automatically launch a traffic website at 4:45 p.m. The Task Scheduler is a tool in Windows that allows users to schedule tasks to run automatically at specified times or in response to certain events.

NEW QUESTION 235

Which of the following provide the BEST way to secure physical access to a data center server room? (Select TWO).

- A. Biometric lock
- B. Badge reader
- C. USB token
- D. Video surveillance
- E. Locking rack
- F. Access control vestibule

Answer: AB

Explanation:

A biometric lock requires an authorized user to provide a unique biometric identifier, such as a fingerprint, in order to gain access to the server room. A badge

reader requires an authorized user to swipe an access card in order to gain access. Both of these methods ensure that only authorized personnel are able to access the server room. Additionally, video surveillance and access control vestibules can be used to further secure the server room. Finally, a locking rack can be used to physically secure the servers, so that they cannot be accessed without the appropriate key.

NEW QUESTION 236

A call center handles inquiries into billing issues for multiple medical facilities. A security analyst notices that call center agents often walk away from their workstations, leaving patient data visible for anyone to see. Which of the following should a network administrator do to BEST prevent data theft within the call center?

- A. Encrypt the workstation hard drives.
- B. Lock the workstations after five minutes of inactivity.
- C. Install privacy screens.
- D. Log off the users when their workstations are not in use.

Answer: B

Explanation:

The BEST solution for preventing data theft within the call center in this scenario would be to lock the workstations after a period of inactivity. This would prevent unauthorized individuals from accessing patient data if call center agents were to step away from their workstations without logging out.

NEW QUESTION 241

A technician receives a help desk ticket from a user who is unable to update a phone. The technician investigates the issue and notices the following error message: Insufficient storage space

While analyzing the phone, the technician does not discover any third-party applications or photos. Which of the following is the best way to resolve the issue?

- A. Exchange the device for a newer one.
- B. Upgrade the onboard storage
- C. Allocate more space by removing factory applications
- D. Move factory applications to external memory.

Answer: D

Explanation:

The best way to resolve the issue is to move factory applications to external memory. This will free up some space on the phone's internal storage, which is required for updating the phone. To do this, you can follow these steps:

? Insert a microSD card into your phone if you don't have one already.

? Go to Settings > Apps and tap on the app you want to move.

? Tap on Storage and then on Change.

? Select the SD card option and tap on Move.

You may need to repeat this process for multiple apps until you have enough space to update your phone. Alternatively, you can also clear the cache and data of some apps, or uninstall the apps that you don't use frequently. You can find more information on how to fix insufficient storage error on your phone in these articles²³⁴. I hope this helps.

NEW QUESTION 243

A technician has been tasked with installing a workstation that will be used for point-of-sale transactions. The point-of-sale system will process credit cards and loyalty cards. Which of the following encryption technologies should be used to secure the workstation in case of theft?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Disk encryption should be used to secure the workstation in case of theft. Disk encryption can help to protect data on the hard drive by encrypting it so that it cannot be accessed without the correct encryption key.

NEW QUESTION 248

While staying at a hotel, a user attempts to connect to the hotel Wi-Fi but notices that multiple SSIDs have very similar names. Which of the following social-engineering attacks is being attempted?

- A. Evil twin
- B. Impersonation
- C. Insider threat
- D. Whaling

Answer: A

Explanation:

An evil twin is a type of social-engineering attack that involves setting up a rogue wireless access point that mimics a legitimate one. The attacker can then intercept

or modify the traffic of the users who connect to the fake SSID. The attacker may also use phishing or malware to steal credentials or personal information from the users

NEW QUESTION 250

An organization is creating guidelines for the incorporation of generative AI solutions. In which of the following would these guidelines be published?

- A. Standard operating procedure

- B. Acceptable use policy
- C. Security protocols
- D. Data flow diagram

Answer: B

Explanation:

An acceptable use policy (AUP) is a document that defines the rules and expectations for the users of a system, network, or service. It typically covers topics such as the purpose, scope, responsibilities, and restrictions of using the system, network, or service¹. An AUP is a suitable place to publish the guidelines for the incorporation of generative AI solutions, as it can inform the users of the benefits, risks, and ethical implications of using such tools. It can also specify the conditions and limitations for using generative AI solutions, such as the types of data, content, and applications that are allowed or prohibited, the security and privacy requirements, the legal and regulatory compliance, and the accountability and reporting mechanisms²³.

References: 1 What is an Acceptable Use Policy (AUP)? - Definition from Techopedia([https://security.stackexchange.com/questions/84168/the-difference-of-security-](https://security.stackexchange.com/questions/84168/the-difference-of-security-policy-and-acceptable-use-policy)

[policy-and-acceptable-use-policy](https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-use-generative-ai.html)). 2 Guide on the use of Generative AI -

[Canada.ca\(https://www.canada.ca/en/government/system/digital-government/digital-](https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-use-generative-ai.html)

[government-innovations/responsible-use-ai/guide-use-generative-ai.html](https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-44/key-considerations-for-developing-organizational-generative-ai-policies))³
Key Considerations for Developing Organizational Generative AI Policies - ISACA(<https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-44/key-considerations-for-developing-organizational-generative-ai-policies>).

NEW QUESTION 253

A new employee is having difficulties using a laptop with a docking station. The laptop is connected to the docking station, and the laptop is closed. The external monitor works for a few seconds, but then the laptop goes to sleep. Which of the following options should the technician configure in order to fix the issue?

- A. Hibernate
- B. Sleep/suspend
- C. Choose what closing the lid does
- D. Turn on fast startup

Answer: C

Explanation:

The correct answer is C. Choose what closing the lid does. This option allows you to configure how the laptop behaves when you close the lid, such as whether it goes to sleep, hibernates, shuts down, or does nothing. To access this option, you can follow these steps:

? Go to Settings > System > Power & sleep.

? Click on Additional power settings on the right side.

? Click on Choose what closing the lid does on the left side.

? Under When I close the lid, select Do nothing for both On battery and Plugged in.

? Click on Save changes.

This will prevent the laptop from going to sleep when you close the lid while it is connected to the docking station and the external monitor.

Hibernate, sleep/suspend, and turn on fast startup are not the options that should be configured to fix the issue. Hibernate and sleep/suspend are both power-saving modes that allow you to resume your work without losing any data. However, they also turn off the display and other components of the laptop, which means you will not be able to use the external monitor when the laptop is closed. Turn on fast startup is a feature that reduces the boot time of Windows by saving some system information to a file when you shut down. It does not affect how the laptop behaves when you close the lid.

NEW QUESTION 256

Someone who is fraudulently claiming to be from a reputable bank calls a company employee. Which of the following describes this incident?

- A. Pretexting
- B. Spoofing
- C. Vishing
- D. Scareware

Answer: C

Explanation:

Vishing is a type of social engineering attack where a fraudulent caller impersonates a legitimate entity, such as a bank or financial institution, in order to gain access to sensitive information. The caller will typically use a variety of techniques, such as trying to scare the target or providing false information, in order to get the target to provide the information they are after. Vishing is often used to gain access to usernames, passwords, bank account information, and other sensitive data.

NEW QUESTION 258

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?

- 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

NEW QUESTION 259

A user is having issues with document-processing software on a Windows workstation. Other users that log in to the same device do not have the same issue. Which of the following should a technician do to remediate the issue?

- A. Roll back the updates.
- B. Increase the page file.
- C. Update the drivers.
- D. Rebuild the profile.

Answer: D

Explanation:

The issue is specific to the user's profile, so the technician should rebuild the profile. Rebuilding the profile will create a new profile and transfer the user's data to the new profile

NEW QUESTION 264

A technician installed Windows 10 on a workstation. The workstation only has 3.5GB of usable RAM, even though the technician installed 8GB. Which of the following is the MOST likely reason this system is not utilizing all the available RAM?

- A. The system is missing updates.
- B. The system is utilizing a 32-bit OS.
- C. The system's memory is failing.
- D. The system requires BIOS updates

Answer: B

Explanation:

The most likely reason that the system is not utilizing all the available RAM is that the system is utilizing a 32-bit OS. A 32-bit OS is an operating system that uses 32 bits to address memory locations and perform calculations. A 32-bit OS can only support up to 4GB of RAM, and some of that RAM may be reserved for hardware devices or system functions, leaving less than 4GB of usable RAM for applications and processes. A 32-bit OS cannot recognize or utilize more than 4GB of RAM, even if more RAM is installed on the system. To utilize all the available RAM, the system needs to use a 64-bit OS, which can support much more RAM than a 32-bit OS. The system missing updates may cause some performance or compatibility issues, but it does not affect the amount of usable RAM on the system. The system's memory failing may cause some errors or crashes, but it does not affect the amount of usable RAM on the system. The system requiring BIOS updates may cause some configuration or compatibility issues, but it does not affect the amount of usable RAM on the system. References: CompTIA A+ Core 2 (220-1102) Certification

Exam Objectives Version 4.0, Domain 1.1

NEW QUESTION 269

A computer technician is investigating a computer that is not booting. The user reports that the computer was working prior to shutting it down last night. The technician notices a removable USB device is inserted, and the user explains the device is a prize the user received in the mail yesterday. Which of the following types of attacks does this describe?

- A. Phishing
- B. Dumpster diving
- C. Tailgating
- D. Evil twin

Answer: A

Explanation:

Phishing is the correct answer for this question. Phishing is a type of attack that uses fraudulent emails or other messages to trick users into revealing sensitive information or installing malicious software. Phishing emails often impersonate legitimate entities or individuals and offer incentives or threats to lure users into clicking on malicious links or attachments. In this scenario, the user received a removable USB device in the mail as a prize, which could be a phishing attempt to infect the user's computer with malware or gain access to the user's data. Dumpster diving, tailgating, and evil twin are not correct answers for this question. Dumpster diving is a type of attack that involves searching through trash bins or recycling containers to find discarded documents or devices that contain valuable information. Tailgating is a type of attack that involves following an authorized person into a restricted area without proper identification or authorization. Evil twin is a type of attack that involves setting up a rogue wireless access point that mimics a legitimate one to intercept or manipulate network traffic. References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25

? [CompTIA Security+ SY0-601 Certification Study Guide], page 1004

NEW QUESTION 273

Which of the following should be used to secure a device from known exploits?

- A. Encryption
- B. Remote wipe
- C. Operating system updates
- D. Cross-site scripting

Answer: C

Explanation:

Operating system updates are used to secure a device from known exploits. Operating system updates are patches or fixes that are released by the vendor to address security vulnerabilities, bugs, or performance issues. Operating system updates can also provide new features or enhancements to the device. It is important to keep the operating system updated to prevent attackers from exploiting known flaws or weaknesses.

NEW QUESTION 274

A technician needs to format a USB drive to transfer 20GB of data from a Linux computer to a Windows computer. Which of the following filesystems will the technician MOST likely use?

- A. FAT32
- B. ext4
- C. NTFS
- D. exFAT

Answer: D

Explanation:

exFAT is a file system that is supported by both Linux and Windows and can handle large files1.

NEW QUESTION 278

An organization implemented a method of wireless security that requires both a user and the user's computer to be in specific managed groups on the server in order to connect to Wi-Fi. Which of the following wireless security methods BEST describes what this organization implemented?

- A. TKIP
- B. RADIUS
- C. WPA2
- D. AES

Answer: B

Explanation:

RADIUS stands for Remote Authentication Dial-In User Service and it is a protocol that provides centralized authentication, authorization, and accounting for network access. RADIUS can be used to implement a method of wireless security that requires both a user and the user's computer to be in specific managed groups on the server in order to connect to Wi-Fi. This is also known as 802.1X authentication or EAP-TLS authentication

NEW QUESTION 279

Which of the following allows access to the command line in macOS?

- A. PsExec
- B. command.com
- C. Terminal
- D. CMD

Answer: C

Explanation:

Terminal is an application that allows access to the command line in macOS. The command line is an interface that allows users to interact with the operating system and perform various tasks by typing commands and arguments. Terminal can be used to launch programs, manage files and folders, configure settings, troubleshoot issues, and run scripts in macOS. PsExec, command.com, and CMD are not applications that allow access to the command line in macOS.

NEW QUESTION 281

A user has a license for an application that is in use on a personal home laptop. The user approaches a systems administrator about using the same license on multiple computers on the corporate network. Which of the following BEST describes what the systems administrator should tell the user?

- A. Use the application only on the home laptop because it contains the initial license.
- B. Use the application at home and contact the vendor regarding a corporate license.
- C. Use the application on any computer since the user has a license.
- D. Use the application only on corporate computers.

Answer: B

Explanation:

Use the application at home and contact the vendor regarding a corporate license. The user should use the application only on the home laptop because it contains the initial license. The user should contact the vendor regarding a corporate license if they want to use the application on multiple computers on the corporate network1

NEW QUESTION 282

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

220-1102 Practice Exam Features:

- * 220-1102 Questions and Answers Updated Frequently
- * 220-1102 Practice Questions Verified by Expert Senior Certified Staff
- * 220-1102 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 220-1102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 220-1102 Practice Test Here](#)