CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

NEW QUESTION 1
A macOS user reports seeing a spinning round cursor on a program that appears to be frozen. Which of the following methods does the technician use to force the program to close in macOS?

A. The technician presses the Ctrl+Alt+Del keys to open the Force Quit menu, selects the frozen application in the list, and clicks Force Quit.
B. The technician clicks on the frozen application and presses and holds the Esc key on the keyboard for 10 seconds Which causes the application to force quit.
C. The technician opens Finder, navigates to the Applications folder, locates the application that is frozen in the list, right-clicks on the application, and selects the Force Quit option.
D. The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit.

Answer: D

Explanation:
The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit. This is the most common method of force quitting a program in macOS. This can be done by clicking on the Apple icon in the top left of the screen, selecting Force Quit, selecting the frozen application in the list, and then clicking Force Quit. This will force the application to quit and the spinning round cursor will disappear.

NEW QUESTION 2
A user turns on a new laptop and attempts to log in to specialized software, but receives a message stating that the address is already in use. The user logs on to the old desktop and receives the same message. A technician checks the account and sees a comment that the user requires a specifically allocated address before connecting to the software. Which of the following should the technician do to MOST likely resolve the issue?

A. Bridge the LAN connection between the laptop and the desktop.
B. Set the laptop configuration to DHCP to prevent conflicts.
C. Remove the static IP configuration from the desktop.
D. Replace the network card in the laptop, as it may be defective.

Answer: C

Explanation:
The new laptop was set up with the static IP it needs to connect to the software. The old desktop is still configured with that IP, hence the conflict.

NEW QUESTION 3
A wireless network is set up, but it is experiencing some interference from other nearby SSIDs. Which of the following can BEST resolve the interference?

A. Changing channels
B. Modifying the wireless security
C. Disabling the SSIO broadcast
D. Changing the access point name

Answer: A

Explanation:
Changing channels can best resolve interference from other nearby SSIDs. Wireless networks operate on different channels, and changing the channel can help to avoid interference from other nearby networks.

NEW QUESTION 4
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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated

NEW QUESTION 5
A technician is reimaging a desktop PC. The technician connects the PC to the network and powers it on. The technician attempts to boot the computer via the NIC to image the computer, but this method does not work. Which of the following is the MOST likely reason the computer is unable to boot into the imaging system via the network?

A. The computer's CMOS battery failed.
B. The computer's NIC is faulty.
C. The PXE boot option has not been enabled
D. The Ethernet cable the technician is using to connect the desktop to the network is faulty.

Answer: C

Explanation:
The most likely reason the computer is unable to boot into the imaging system via the network is that the PXE boot option has not been enabled. PXE (Preboot Execution Environment) is an environment that allows computers to boot up over the network, instead of from a local disk. In order for this to work, the PXE boot option must be enabled in the computer's BIOS settings. As stated in the CompTIA A+ Core 2 exam objectives, technicians should know how to enable PXE in BIOS to enable network booting on a computer.

NEW QUESTION 6
A company discovered that numerous computers from multiple geographic locations are sending a very high number of connection requests which is causing the company’s web server to become unavailable to the general public. Which of the following attacks is occurring?

A. Zero day
B. SOL injection
C. Cross-site scripting
D. Distributed denial of service

Answer: D

Explanation:
The company is experiencing a distributed denial of service (DDoS) attack. A DDoS attack is a type of cyber attack in which multiple compromised systems are used to target a single system, causing a denial of service for users of the targeted system.

NEW QUESTION 7
A technician receives a ticket indicating the user cannot resolve external web pages However, specific IP addresses are working. Which of the following does the technician MOST likely need to change on the workstation to resolve the issue?

A. Default gateway
B. Host address
C. Name server
D. Subnet mask

Answer: A

Explanation:
The technician most likely needs to change the default gateway on the workstation to resolve the issue. The default gateway is the IP address of the router that connects the workstation to the internet, and it is responsible for routing traffic between the workstation and the internet. If the default gateway is incorrect, the workstation will not be able to access external web pages.

NEW QUESTION 8
A Chief Executive Officer has learned that an exploit has been identified on the web server software, and a patch is not available yet. Which of the following attacks MOST likely occurred?

A. Brute force
B. Zero day
C. Denial of service
D. On-path

Answer: B

Explanation:
A zero-day attack is an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on “day zero” of awareness of the vulnerability

Configuring AAA Services. Retrieved from https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/security/configuration/guide/sc40crsb

NEW QUESTION 9
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 10
A user has requested help setting up the fingerprint reader on a Windows 10 laptop. The laptop is equipped with a fingerprint reader and is joined to a domain Group Policy enables Windows Hello on all computers in the environment. Which of the following options describes how to set up Windows Hello Fingerprint for the user?

A. Navigate to the Control Panel utility, select the Security and Maintenance submenu, select Change Security and Maintenance settings, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete
B. Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign in options, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.
C. Navigate to the Windows 10 Settings menu, select the Update & Security submenu select Windows Security, select Windows Hello Fingerprint and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete
D. Navigate to the Control Panel utility, select the Administrative Tools submenu, select the user account in the list, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.

Answer: B

Explanation:
Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign in options, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete. Windows Hello Fingerprint can be set up by navigating to the Windows 10 Settings menu, selecting the Accounts submenu, selecting Sign in options, and then selecting Windows Hello Fingerprint. The user will then be asked to place a fingerprint on the fingerprint reader repeatedly until Windows indicates that setup is complete. Windows Hello Fingerprint allows the user to log into the laptop using just their fingerprint, providing an additional layer of security.

NEW QUESTION 10
A technician needs to document who had possession of evidence at every step of the process. Which of the following does this process describe?

A. Rights management
B. Audit trail
C. Chain of custody

D. Data integrity

Answer: C

Explanation:
The process of documenting who had possession of evidence at every step of the process is called chain of custody

NEW QUESTION 13
The findings from a security audit indicate the risk of data loss from lost or stolen laptops is high. The company wants to reduce this risk with minimal impact to users who want to use their laptops when not on the network. Which of the following would BEST reduce this risk for Windows laptop users?

A. Requiring strong passwords
B. Disabling cached credentials
C. Requiring MFA to sign on
D. Enabling BitLocker on all hard drives

Answer: D

Explanation:
BitLocker is a disk encryption tool that can be used to encrypt the hard drive of a Windows laptop. This will protect the data stored on the drive in the event that the laptop is lost or stolen, and will help to reduce the risk of data loss. Additionally, BitLocker can be configured to require a PIN or other authentication in order to unlock the drive, providing an additional layer of security.

NEW QUESTION 14
A company has just refreshed several desktop PCs. The hard drives contain PII. Which of the following is the BEST method to dispose of the drives?

A. Drilling
B. Degaussing
C. Low-level formatting
D. Erasing/wiping

Answer: D

Explanation:
Erasing/wiping the hard drives is the best method to dispose of the drives containing PII

NEW QUESTION 17
A technician is asked to resize a partition on the internal storage drive of a computer running macOS. Which of the followings tools should the technician use to accomplish this task?

A. Consoltf
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 21
A user's system is infected with malware. A technician updates the anti-malware software and runs a scan that removes the malware. After the user reboots the system, it once again becomes infected with malware. Which of the following will MOST likely help to permanently remove the malware?

A. Enabling System Restore
B. Educating the user
C. Booting into safe mode
D. Scheduling a scan

Answer: B

Explanation:
Although updating the anti-malware software and running scans are important steps in removing malware, they may not be sufficient to permanently remove the malware if the user keeps engaging in behaviors that leave the system vulnerable, such as downloading unknown files or visiting malicious websites. Therefore, educating the user on safe computing practices is the best way to prevent future infections and permanently remove the malware.
Enabling System Restore, Booting into safe mode, and scheduling a scan are not the most efficient ways to permanently remove the malware. Enabling System Restore and Booting into safe mode may help in some cases, but they may not be sufficient to permanently remove the malware. Scheduling a scan is also important for detecting and removing malware, but it may not be sufficient to prevent future infections.
https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0)

NEW QUESTION 26
Ann, a CEO, has purchased a new consumer-class tablet for personal use, but she is unable to connect it to the company's wireless network. All the corporate laptops are connecting without issue. She has asked you to assist with getting the device online.
INSTRUCTIONS
Review the network diagrams and device configurations to determine the cause of the problem and resolve any discovered issues.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated

Click on 802.11 and Select ac
Graphical user interface, application Description automatically generated

Click on SSID and select CORP
Graphical user interface, text, application, Teams Description automatically generated

Click on Frequency and select 5GHz
A picture containing background pattern Description automatically generated

At Wireless Security Mode, Click on Security Mode
Graphical user interface, text, application Description automatically generated

Select the WPA2
Graphical user interface, application, Teams Description automatically generated with medium confidence

Ann needs to connect to the BYOD SSID, using 2.4GHZ. The selected security method chose should be WPA PSK, and the password should be set to TotallySecret.
Graphical user interface, application Description automatically generated

NEW QUESTION 30
A desktop support technician is tasked with migrating several PCs from Windows 7 Pro to Windows 10 Pro, The technician must ensure files and user preferences are retained, must perform the operation locally, and should migrate one station at a time. Which of the following methods would be MOST efficient?

A. Golden image
B. Remote network install
C. In-place upgrade
D. Clean install

Answer: C

Explanation:
An in-place upgrade is the most efficient method for migrating from Windows 7 Pro to Windows 10 Pro, as it will retain all user files and preferences, can be done locally, and can be done one station at a time. An
in-place upgrade involves installing the new version of Windows over the existing version, and can be done quickly and easily.

NEW QUESTION 32
A technician is unable to join a Windows 10 laptop to a domain Which of the following is the MOST likely reason?

A. The domain's processor compatibility is not met
B. The laptop has Windows 10 Home installed
C. The laptop does not have an onboard Ethernet adapter
D. The Laptop does not have all current Windows updates installed

Answer: B

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

NEW QUESTION 33
A user reports that text on the screen is too small. The user would like to make the text larger and easier to see. Which of the following is the BEST way for the user to increase the size of text, applications, and other items using the Windows 10 Settings tool?

A. Open Settings select Devices, select Display, and change the display resolution to a lower resolution option
B. Open Settings, select System, select Display, and change the display resolution to a lower resolution option.
C. Open Settings Select System, select Display, and change the Scale and layout setting to a higher percentage.
D. Open Settings select Personalization, select Display and change the Scale and layout setting to a higher percentage

Answer: C

Explanation:
Open Settings, select System, select Display, and change the Scale and layout setting to a higher percentage12 3

NEW QUESTION 34
A user receives a notification indicating the data plan on the user's corporate phone has reached its limit. The user has also noted the performance of the phone is abnormally slow. A technician discovers a third-party GPS application was installed on the phone. Which of the following is the MOST likely cause?

A. The GPS application is installing software updates.
B. The GPS application contains malware.
C. The GPS application is updating its geospatial map data.
D. The GPS application is conflicting with the built-in GPS.

Answer: B

Explanation:
The GPS application contains malware. The third-party GPS application is likely the cause of the slow performance of the phone. The application may contain malware that is using up system resources and slowing down the phone. The user should uninstall the application and run a malware scan on the phon1e

NEW QUESTION 35
A technician receives a call from a user who is on vacation. The user provides the necessary credentials and asks the technician to log in to the users account and read a critical email that the user has been expecting. The technician refuses because this is a violation of the:

A. acceptable use policy.
B. regulatory compliance requirements.
C. non-disclosure agreement
D. incident response procedures

Answer: A

Explanation:
Logging into a user's account without their explicit permission is a violation of the acceptable use policy, which outlines the rules and regulations by which a user must abide while using a computer system. By logging into the user's account without their permission, the technician would be violating this policy. Additionally, this action could be seen as a breach of confidentiality, as the technician would have access to information that should remain confidential.

NEW QUESTION 38
A technician is installing a new business application on a user's desktop computer. The machine is running Windows 10 Enterprise 32-bit operating system. Which

of the following files should the technician execute in order to complete the installation?

A. Installer_x64.exe
B. Installer_Files.zip
C. Installer_32.msi
D. Installer_x86.exe
E. Installer_Win10Enterprise.dmg

Answer: D

Explanation:
The 32-bit operating system can only run 32-bit applications, so the technician should execute the 32-bit installer. The “x86” in the file name refers to the 32-bit architecture.
https://www.digitaltrends.com/computing/32-bit-vs-64-bit-operating-systems/

NEW QUESTION 42
A technician is configuring a new Windows laptop Corporate policy requires that mobile devices make use of full disk encryption at all limes Which of the following encryption solutions should the technician choose?

A. Encrypting File System
B. FileVault
C. BitLocker
D. Encrypted LVM

Answer: A

Explanation:
The encryption solution that the technician should choose when configuring a new Windows laptop and corporate policy requires that mobile devices make use of full disk encryption at all times is BitLocker. This is because BitLocker is a full-disk encryption feature that encrypts all data on a hard drive and is included with Window

NEW QUESTION 46
A field technician applied a Group Policy setting to all the workstations in the network. This setting forced the workstations to use a specific SNTP server. Users are unable to log in now. Which of the following is the MOST likely cause of this issue?

A. The SNTP server is offline.
B. A user changed the time zone on a local machine.
C. The Group Policy setting has disrupted domain authentication on the system,
D. The workstations and the authentication server have a system clock difference.

Answer: D

Explanation:
The workstations and the authentication server have a system clock difference. If a Group Policy setting is applied that forces the workstations to use a specific SNTP server, but the system clock on the workstations and the authentication server are out of sync, then this can cause authentication issues and users will be unable to log in. In this case, the most likely cause of the issue is a difference in system clocks and the technician should ensure that the clocks on the workstations and the authentication server are in sync.

NEW QUESTION 47
A user wants to set up speech recognition on a PC In which of the following Windows Settings tools can the user enable this option?

A. Language
B. System
C. Personalization
D. Ease of Access

Answer: D

Explanation:
The user can enable speech recognition on a PC in the Ease of Access settings tool. To set up Speech Recognition on a Windows PC, the user should open Control Panel, click on Ease of Access, click on Speech Recognition, and click the Start Speech Recognition link. Language settings can be used to change the language of the speech recognition feature, but they will not enable the feature. System settings can be used to configure the hardware and software of the PC, but they will not enable the speech recognition
feature. Personalization settings can be used to customize the appearance and behavior of the PC, but they will not enable the speech recognition feature1
Open up ease of access, click on speech, then there is an on and off button for speech recognition.

NEW QUESTION 52
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 Agreenment Reference:

https://www.youtube.com/watch?v=Ru77iZxuElA&list=PLG49S3nxzAnna96gzhJrzkii4hH_mgW4b&index=59

NEW QUESTION 54
A user reports that the hard drive activity light on a Windows 10 desktop computer has been steadily lit for more than an hour, and performance is severely degraded. Which of the following tabs in Task Manager would contain the information a technician would use to identify the cause of this issue?

A. Services
B. Processes
C. Performance
D. Startup

Answer: B

Explanation:
Processes tab in Task Manager would contain the information a technician would use to identify the cause of this issue. The Processes tab in Task Manager displays all the processes running on the computer, including the CPU and memory usage of each process. The technician can use this tab to identify the process that is causing the hard drive activity light to remain lit and the performance degradation1

NEW QUESTION 58
A bank would like to enhance building security in order to prevent vehicles from driving into the building while also maintaining easy access for customers. Which of the following BEST addresses this need?

A. Guards
B. Bollards
C. Motion sensors
D. Access control vestibule

Answer: B

Explanation:
Bollards are the best solution to enhance building security in order to prevent vehicles from driving into the building while also maintaining easy access for customers4
References: 2. Bollards. Retrieved from https://en.wikipedia.org/wiki/Bollard

NEW QUESTION 62
Which of the following provide the BEST way to secure physical access to a data cento 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 63
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 67
A technician suspects a rootkit has been installed and needs to be removed. Which of the following would BEST resolve the issue?

A. Application updates
B. Anti-malware software
C. OS reinstallation
D. File restore

Answer: C

Explanation:
If a rootkit has caused a deep infection, then the only way to remove the rootkit is to reinstall the operating system. This is because rootkits are designed to be difficult to detect and remove, and they can hide in the operating system's kernel, making it difficult to remove them without reinstalling the operating system
https://www.minitool.com/backup-tips/how-to-get-rid-of-rootkit-windows-10.html

NEW QUESTION 69
A technician is setting up a desktop computer in a small office. The user will need to access files on a drive shared from another desktop on the network. Which of the following configurations should the technician employ to achieve this goal?

A. Configure the network as private
B. Enable a proxy server
C. Grant the network administrator role to the user
D. Create a shortcut to public documents

Answer: A

Explanation:
The technician should configure the network as private to allow the user to access files on a drive shared from another desktop on the network1

NEW QUESTION 72
A Windows user reported that a pop-up indicated a security issue. During inspection, an antivirus system identified malware from a recent download, but it was unable to remove the malware. Which of the following actions would be BEST to remove the malware while also preserving the user's files?

A. Run the virus scanner in an administrative mode.
B. Reinstall the operating system.
C. Reboot the system in safe mode and rescan.
D. Manually delete the infected files.

Answer: C

Explanation:
Rebooting the system in safe mode will limit the number of programs and processes running, allowing the antivirus system to more effectively identify and remove the malware. Rescanning the system will allow the antivirus system to identify and remove the malware while preserving the user's files.

NEW QUESTION 75
A manager reports that staff members often forget the passwords to their mobile devices and applications. Which of the following should the systems administrator do to reduce the number of help desk tickets submitted?

A. Enable multifactor authentication.
B. Increase the failed log-in threshold.
C. Remove complex password requirements.
D. Implement a single sign-on with biometrics.

Answer: A

Explanation:
Multifactor authentication (MFA) is a security measure that requires users to provide multiple pieces of evidence when logging in to an account or system. This can include a combination of something the user knows (e.g. a password or PIN), something the user has (e.g. a security token or smartphone) and something the user is (e.g. biometrics such as a fingerprint or face scan). By enabling MFA, the systems administrator can ensure that users are required to provide multiple pieces of evidence when logging in, making it more difficult for unauthorized users to gain access to the system. This can help reduce the number of help desk tickets submitted due to forgotten passwords.

NEW QUESTION 80
A developer is creating a shell script to automate basic tasks in Linux. Which of the following file types are supported by default?

A. .py
B. .js
C. .vbs
D. .sh

Answer: D

Explanation:
https://www.educba.com/shell-scripting-in-linux/

NEW QUESTION 83
A user purchased a netbook that has a web-based, proprietary operating system. Which of the following operating systems is MOST likely installed on the netbook?

A. macOS
B. Linux
C. Chrome OS
D. Windows

Answer: C

Explanation:

* 4. Chrome OS. Retrieved from https://en.wikipedia.org/wiki/Chrome_OS 5. What is Chrome OS? Retrieved from https://www.google.com/chromebook/chrome-os/ A netbook with a web-based, proprietary operating system is most likely running Chrome OS. Chrome OS is a web-based operating system developed by Google that is designed to work with web applications and cloud storage. It is optimized for netbooks and other low-power devices and is designed to be fast, secure, and easy to use.

NEW QUESTION 84
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 86
An architecture firm is considering upgrading its computer-aided design (CAD) software to the newest version that forces storage of backups of all CAD files on the software's cloud server. Which of the following is MOST likely to be of concern to the IT manager?

A. All updated software must be tested with alt system types and accessories
B. Extra technician hours must be budgeted during installation of updates
C. Network utilization will be significantly increased due to the size of CAD files
D. Large update and installation files will overload the local hard drives.

Answer: C

Explanation:
The IT manager is most likely to be concerned about network utilization being significantly increased due to the size of CAD files. Backing up all CAD files to the software’s cloud server can result in a large amount of data being transferred over the network, which can cause network congestion and slow down other network traffic.

NEW QUESTION 90
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. DRM
B. NDA
C. EULA
D. MOU

Answer: C

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 93
A technician is installing new software on a macOS computer. Which of the following file types will the technician MOST likely use?

A. .deb
B. .vbs
C. .exe
D. .app

Answer: D

Explanation:
The file type that the technician will MOST likely use when installing new software on a macOS computer is
.a pp. This is because .app is the file extension for applications on macO1S.

NEW QUESTION 96
A help desk technician is troubleshooting a workstation in a SOHO environment that is running above normal system baselines. The technician discovers an unknown executable with a random string name running on the system. The technician terminates the process, and the system returns to normal operation. The technician thinks the issue was an infected file, but the antivirus is not detecting a threat. The technician is concerned other machines may be infected with this unknown virus. Which of the following is the MOST effective way to check other machines on the network for this unknown threat?

A. Run a startup script that removes files by name.
B. Provide a sample to the antivirus vendor.
C. Manually check each machine.
D. Monitor outbound network traffic.

Answer: C

Explanation:
The most effective way to check other machines on the network for this unknown threat is to manually check each machine. This can help to identify any other machines that may be infected with the unknown virus and allow them to be cleaned.

NEW QUESTION 101
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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