

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

<https://www.2passeasy.com/dumps/220-1102/>



NEW QUESTION 1

A help desk technician runs the following script: Inventory.py. The technician receives the following error message:

How do you want to Open this file?

Which of the following is the MOST likely reason this script is unable to run?

- A. Scripts are not permitted to run.
- B. The script was not built for Windows.
- C. The script requires administrator privileges,
- D. The runtime environment is not installed.

Answer: D

Explanation:

The error message is indicating that the script is not associated with any program on the computer that can open and run it. This means that the script requires a runtime environment, such as Python, to be installed in order for it to execute properly. Without the appropriate runtime environment, the script will not be able to run.

NEW QUESTION 2

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 3

A company installed a new backup and recovery system. Which of the following types of backups should be completed FIRST?

- A. Full
- B. Non-parity
- C. Differential
- D. Incremental

Answer: A

Explanation:

The type of backup that should be completed FIRST after installing a new backup and recovery system is a full backup. This is because a full backup is a complete backup of all data and is the foundation for all other backups. After a full backup is completed, other types of backups, such as differential and incremental backups, can be performed.

NEW QUESTION 4

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 5

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 6

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

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

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.

Show Question

Reset All Answers

	Date	Priority
ing to boot. Screen i...	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

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

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:

Resolution:

Verify/Resolve:

The screenshot displays a helpdesk application interface. On the left, a table lists tickets with columns for Date and Priority. The first ticket, dated 7/13/2022 with a High priority, is selected. To its right, a 'Details' panel shows ticket information: #6676309, Open status, High priority, Category 'Technical / Bug Reports', Assigned To 'helpdesk@fictional.com', and Assigned Date '7/13/2022'. Below this, the Subject is 'PC is failing to boot. Screen is displaying error message, see attachment.' and Attachments include 'bootmgr not found.png'. An 'Issue' dropdown menu is open, showing a list of common Windows problems such as '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'. At the bottom, a 'Verify/Resolve' dropdown is 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:

Graphical user interface, text, application Description automatically generated

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 7

When a user calls in to report an issue, a technician submits a ticket on the user's behalf. Which of the following practices should the technician use to make sure the ticket is associated with the correct user?

- A. Have the user provide a callback phone number to be added to the ticket
- B. Assign the ticket to the department's power user
- C. Register the ticket with a unique user identifier
- D. Provide the user with a unique ticket number that can be referenced on subsequent calls.

Answer: D

Explanation:

The technician should provide the user with a unique ticket number that can be referenced on subsequent calls to make sure the ticket is associated with the correct user. This is because registering the ticket with a unique user identifier, having the user provide a callback phone number to be added to the ticket, or assigning the ticket to the department's power user will not ensure that the ticket is associated with the correct user2.

NEW QUESTION 8

A technician is setting up a new laptop for an employee who travels, Which of the following is the BEST security practice for this scenario?

- A. PIN-based login
- B. Quarterly password changes
- C. Hard drive encryption
- D. A physical laptop lock

Answer: C

Explanation:

Encrypting the laptop's hard drive will ensure that any sensitive data stored on the laptop is secure, even if the laptop is lost or stolen. Encryption ensures that the data cannot be accessed by anyone without the correct encryption key. This is an important security measure for any laptop used by an employee who travels, as it helps to protect the data stored on the laptop from unauthorized access.

NEW QUESTION 9

A call center technician receives a call from a user asking how to update Windows Which of the following describes what the technician should do?

- A. Have the user consider using an iPad if the user is unable to complete updates
- B. Have the user text the user's password to the technician.
- C. Ask the user to click in the Search field, type Check for Updates, and then press the Enter key
- D. Advise the user to wait for an upcoming, automatic patch

Answer: C

Explanation:

The technician should guide the user to update Windows through the built-in "Check for Updates" feature. This can be done by having the user click in the Search field, type "Check for Updates", and then press the Enter key. This will bring up the Windows Update function, which will search for any available updates and give the user the option to install them.

NEW QUESTION 10

A department has the following technical requirements for a new application:

Quad Core processor
250GB of hard drive space
6GB of RAM
Touch screens

The company plans to upgrade from a 32-bit Windows OS to a 64-bit OS. Which of the following will the company be able to fully take advantage of after the upgrade?

- A. CPU
- B. Hard drive
- C. RAM
- D. Touch screen

Answer: C

Explanation:

<https://www.makeuseof.com/tag/difference-32-bit-64-bit-windows/>

After upgrading from a 32-bit Windows OS to a 64-bit OS, the company will be able to fully take advantage of the RAM of the computer. This is because a 64-bit operating system is able to use larger amounts of RAM compared to a 32-bit operating system, which may benefit the system's overall performance if it has more than 4GB of RAM installed

NEW QUESTION 10

Each time a user tries to go to the selected web search provider, a different website opens. Which of the following should the technician check FIRST?

- A. System time
- B. IP address
- C. DNS servers
- D. Windows updates

Answer: C

Explanation:

When a user experiences unexpected or erratic behavior while browsing the internet, it could be caused by the DNS servers. DNS translates human-readable domain names (like google.com) into IP addresses, which computers can use to communicate with web servers. If the DNS servers are not functioning correctly or have been compromised, it can result in the browser being redirected to unintended websites.

NEW QUESTION 13

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. SQL 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 18

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 21

A technician has been tasked with using the fastest and most secure method of logging in to laptops. Which of the following log-in options meets these requirements?

- A. PIN
- B. Username and password
- C. SSO
- D. Fingerprint

Answer: A

Explanation:

This is because a PIN is a fast and secure method of logging in to laptops, and it is more secure than a password because it is not susceptible to keyloggers.

NEW QUESTION 22

A user contacted the help desk to report pop-ups on a company workstation indicating the computer has been infected with 137 viruses and payment is needed to remove them. The user thought the company-provided antivirus software would prevent this issue. The help desk ticket states that the user only receives these messages when first opening the web browser. Which of the following steps would MOST likely resolve the issue? (Select TWO)

- A. Scan the computer with the company-provided antivirus software
- B. Install a new hard drive and clone the user's drive to it
- C. Deploy an ad-blocking extension to the browser.
- D. Uninstall the company-provided antivirus software
- E. Click the link in the messages to pay for virus removal
- F. Perform a reset on the user's web browser

Answer: CF

Explanation:

"The user thought the company-provided antivirus software would prevent this issue."

The most likely steps to resolve the issue are to deploy an ad-blocking extension to the browser and perform a reset on the user's web browser. Ad-blocking extensions can help to prevent pop-ups and other unwanted content from appearing in the browser, and resetting the browser can help to remove any malicious extensions or settings that may be causing the issue.

NEW QUESTION 24

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 27

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 29

During a recent flight an executive unexpectedly received several dog and cat pictures while trying to watch a movie via in-flight Wi-Fi on an iPhone. The executive has no records of any contacts sending pictures like these and has not seen these pictures before. To BEST resolve this issue, the executive should:

- A. set AirDrop so that transfers are only accepted from known contacts
- B. completely disable all wireless systems during the flight
- C. discontinue using iMessage and only use secure communication applications
- D. only allow messages and calls from saved contacts

Answer: A

Explanation:

To best resolve this issue, the executive should set AirDrop so that transfers are only accepted from known contacts (option A). AirDrop is a feature on iOS devices that allows users to share files, photos, and other data between Apple devices. By setting AirDrop so that it only accepts transfers from known contacts, the executive can ensure that unwanted files and photos are not sent to their device. Additionally, the executive should ensure that the AirDrop setting is only enabled when it is necessary, as this will protect their device from any unwanted files and photos.

NEW QUESTION 32

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

NEW QUESTION 33

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 36

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:

A risk analysis must be completed before a change request for an upcoming server deployment can be approved 1

Risk analysis is an important step in the change management process because it helps identify and mitigate potential risks before changes are implemented. Once the risks have been analyzed and the appropriate measures have been taken to minimize them, the change can be approved and implemented.

NEW QUESTION 40

A user's smartphone data usage is well above average. The user suspects an installed application is transmitting data in the background. The user would like to be alerted when an application attempts to communicate with the internet. Which of the following BEST addresses the user's concern?

- A. Operating system updates
- B. Remote wipe
- C. Antivirus
- D. Firewall

Answer: D

Explanation:

A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. In this scenario, the user is concerned about an installed application transmitting data in the background, so a firewall would be the best solution to address their concern. By installing and configuring a firewall, the user can block unauthorized connections to and from the device, and receive alerts whenever an application tries to access the internet.

NEW QUESTION 43

A systems administrator is tasked with configuring desktop systems to use a new proxy server that the organization has added to provide content filtering. Which of the following Windows utilities IS the BEST choice for accessing the necessary configuration to complete this goal?

- A. Security and Maintenance
- B. Network and Sharing Center
- C. Windows Defender Firewall
- D. Internet Options

Answer: D

Explanation:

The best choice for accessing the necessary configuration to configure the desktop systems to use a new proxy server is the Internet Options utility. This utility can be found in the Control Panel and allows you to configure the proxy settings for your network connection. As stated in the CompTIA A+ Core 2 exam objectives, technicians should be familiar with the Internet Options utility and how to configure proxy settings.

NEW QUESTION 47

A technician has an external SSD. The technician needs to read and write to an external SSD on both Macs and Windows PCs. Which of the following filesystems is supported by both OS types?

- A. NTFS

- B. APFS
- C. ext4
- D. exFAT

Answer: D

Explanation:

The filesystem that is supported by both Macs and Windows PCs is D. exFAT. exFAT is a file system that is designed to be used on flash drives like USB sticks and SD cards. It is supported by both Macs and Windows PCs, and it can handle large files and volumes
<https://www.diskpart.com/articles/file-system-for-mac-and-windows-0310.html>

NEW QUESTION 50

An Android user reports that when attempting to open the company's proprietary mobile application it immediately doses. The user states that the issue persists, even after rebooting the phone. The application contains critical information that cannot be lost. Which of the following steps should a systems administrator attempt FIRST?

- A. Uninstall and reinstall the application
- B. Reset the phone to factory settings
- C. Install an alternative application with similar functionality
- D. Clear the application cache.

Answer: D

Explanation:

The systems administrator should clear the application cache
 If clearing the application cache does not work, the systems administrator should uninstall and reinstall the application
 Resetting the phone to factory settings is not necessary at this point
 Installing an alternative application with similar functionality is not necessary at this point

NEW QUESTION 52

A user reports a PC is running slowly. The technician suspects high disk I/O. Which of the following should the technician perform NEXT?

- A. resmon.exe
- B. dfrgui.exe
- C. msinfo32.exe
- D. msconfig.exe

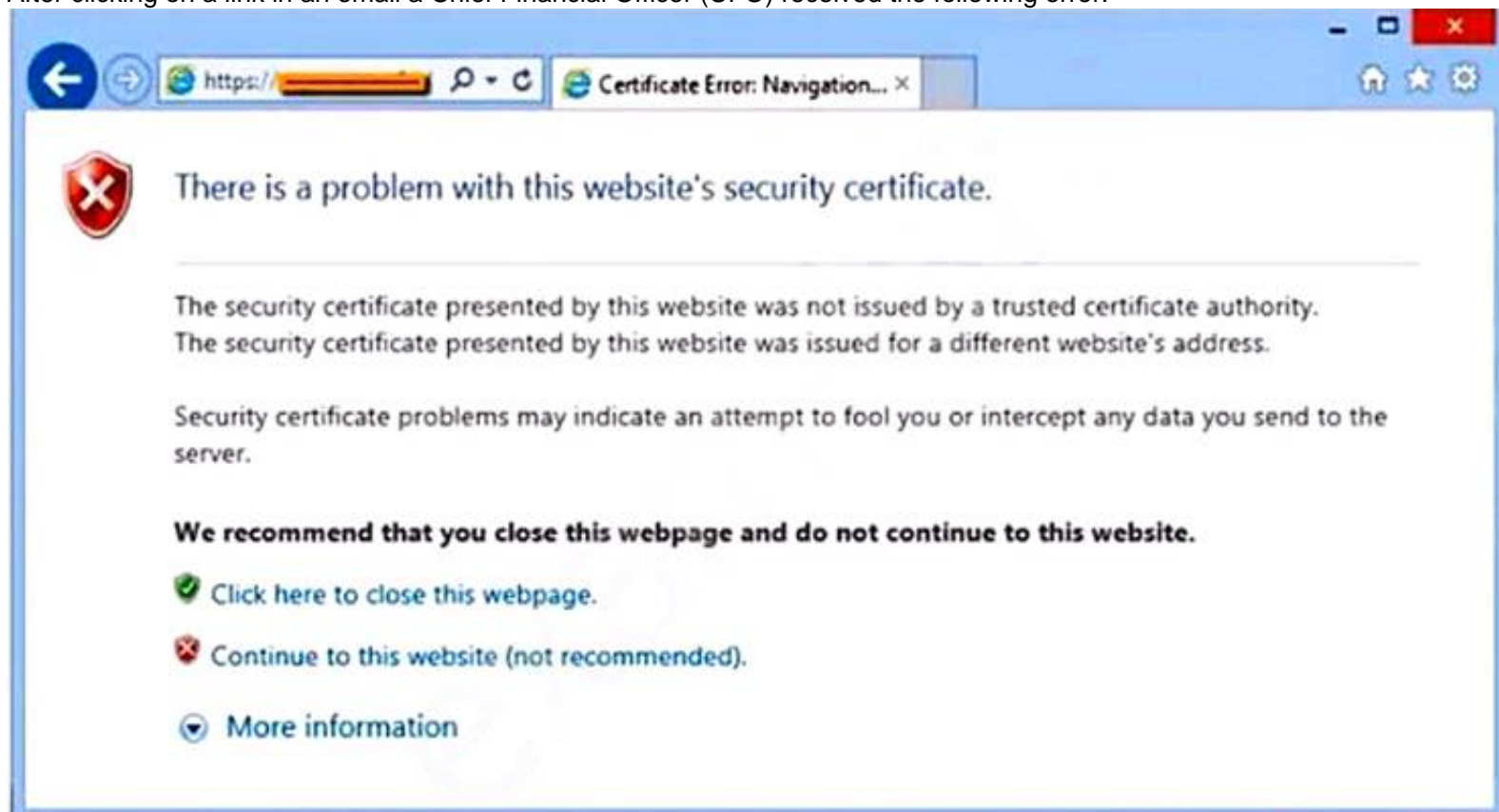
Answer: A

Explanation:

If a technician suspects high disk I/O, the technician should use the Resource Monitor (resmon.exe) to identify the process that is causing the high disk I/O. Resource Monitor provides detailed information about the system's resource usage, including disk I/O. The technician can use this information to identify the process that is causing the high disk I/O and take appropriate action.

NEW QUESTION 53

After clicking on a link in an email a Chief Financial Officer (CFO) received the following error:



The CFO then reported the incident to a technician. The link is purportedly to the organization's bank. Which of the following should the technician perform FIRST?

- A. Update the browser's CRLs
- B. File a trouble ticket with the bank.
- C. Contact the ISP to report the CFCs concern
- D. Instruct the CFO to exit the browser

Answer: A

Explanation:

The technician should update the browser's CRLs first. The error message indicates that the certificate revocation list (CRL) is not up to date. Updating the CRLs will ensure that the browser can verify the authenticity of the bank's website.

NEW QUESTION 58

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 60

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:

This will ensure that the antivirus software is up-to-date, and can detect any new viruses that may have been released since the last virus definition update. The CompTIA A+ Core 2 220-1002 exam covers this topic in the following domains: 1.3 Explain the importance of security awareness and 2.2 Given a scenario, use secure data management and disaster recovery principles.

NEW QUESTION 64

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 65

A technician suspects the boot disk of a user's computer contains bad sectors. Which of the following should the technician verify in the command prompt to address the issue without making any changes?

- A. Run sfc / scannow on the drive as the administrator.
- B. Run cleanmgr on the drive as the administrator
- C. Run chkdsk on the drive as the administrator.
- D. Run dfrgui on the drive as the administrator.

Answer: C

Explanation:

The technician should verify bad sectors on the user's computer by running chkdsk on the drive as the administrator. Chkdsk (check disk) is a command-line utility that detects and repairs disk errors, including bad sectors. It runs a scan of the disk and displays any errors that are found

NEW QUESTION 68

A company is issuing smartphones to employees and needs to ensure data is secure if the devices are lost or stolen. Which of the following provides the BEST solution?

- A. Anti-malware
- B. Remote wipe
- C. Locator applications
- D. Screen lock

Answer: B

Explanation:

This is because remote wipe allows the data on the smartphone to be erased remotely, which helps to ensure that sensitive data does not fall into the wrong hands.

NEW QUESTION 69

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 74

An administrator has received approval for a change request for an upcoming server deployment. Which of the following steps should be completed NEXT?

- A. Perform a risk analysis.
- B. Implement the deployment.
- C. Verify end user acceptance
- D. Document the lessons learned.

Answer: A

Explanation:

Before making any changes to the system, it is important to assess the risks associated with the change and determine whether it is worth implementing. Risk analysis involves identifying potential risks, assessing their likelihood and impact, and determining what steps can be taken to mitigate them. It is important to perform this step before making any changes, as this allows the administrator to make an informed decision about whether or not the change should be implemented. Once the risks have been assessed and the administrator has decided to go ahead with the change, the next step is to implement the deployment.

NEW QUESTION 78

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 82

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

NEW QUESTION 85

A technician is installing new network equipment in a SOHO and wants to ensure the equipment is secured against external threats on the Internet. Which of the following actions should the technician do FIRST?

- A. Lock all devices in a closet.
- B. Ensure all devices are from the same manufacturer.
- C. Change the default administrative password.
- D. Install the latest operating system and patches

Answer: C

Explanation:

The technician should change the default administrative password FIRST to ensure the network equipment is secured against external threats on the Internet. Changing the default administrative password is a basic security measure that can help prevent unauthorized access to the network equipment. Locking all

devices in a closet is a physical security measure that can help prevent theft or damage to the devices, but it does not address external threats on the Internet. Ensuring all devices are from the same manufacturer is not a security measure and does not address external threats on the Internet. Installing the latest operating system and patches is important for maintaining the security of the network equipment, but it is not the first action the technician should take¹

NEW QUESTION 87

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 (2FA)²

NEW QUESTION 92

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 percentage^{12 3}

NEW QUESTION 94

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. Data-in-transit encryption
- B. File encryption
- C. USB drive encryption
- D. Disk encryption

Answer: D

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 99

Which of the following should be used to control security settings on an Android phone in a domain environment?

- A. MDM
- B. MFA
- C. ACL
- D. SMS

Answer: A

Explanation:

The best answer to control security settings on an Android phone in a domain environment is to use "Mobile Device Management (MDM)". MDM is a type of software that is used to manage and secure mobile devices such as smartphones and tablets. MDM can be used to enforce security policies, configure settings, and remotely wipe data from devices. In a domain environment, MDM can be used to manage Android phones and enforce security policies such as password requirements, encryption, and remote wipe capabilities¹²

NEW QUESTION 100

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. Escalate the ticket to Tier 2.
- B. Run a virus scan.
- C. Utilize a Windows restore point.
- D. Reimage the computer.

Answer: B

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 102

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 user's 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 107

Which of the following is the MOST basic version of Windows that includes BitLocker?

- A. Home
- B. pro
- C. Enterprise
- D. Pro for Workstations

Answer: D

Explanation:

The most basic version of Windows that includes BitLocker is Windows Pro. BitLocker is a feature of Windows Pro that provides full disk encryption for all data on a storage drive [1]. It helps protect data from unauthorized access or theft and can help secure data from malicious attacks. Pro for Workstations includes this feature, as well as other features such as support for up to 6 TB of RAM and ReFS.

NEW QUESTION 111

A suite of security applications was installed a few days ago on a user's home computer. The user reports that the computer has been running slowly since the installation. The user notices the hard drive activity light is constantly solid. Which of the following should be checked FIRST?

- A. Services in Control Panel to check for overutilization
- B. Performance Monitor to check for resource utilization
- C. System File Checker to check for modified Windows files
- D. Event Viewer to identify errors

Answer: C

Explanation:

System File Checker to check for modified Windows files. System File Checker (SFC) is a Windows utility that can be used to scan for and restore corrupt Windows system files. SFC can be used to detect and fix any modified or corrupted system files on a computer, and thus should be checked first when a user reports that their computer has been running slowly since the installation of security applications [1][2]. By checking SFC, any modified or corrupted system files can be identified and fixed, potentially improving the overall performance of the computer.

NEW QUESTION 112

A user calls the help desk to report that none of the files on a PC will open. The user also indicates a program on the desktop is requesting payment in exchange for file access. A technician verifies the user's PC is infected with ransomware. Which of the following should the technician do FIRST?

- A. Scan and remove the malware
- B. Schedule automated malware scans
- C. Quarantine the system
- D. Disable System Restore

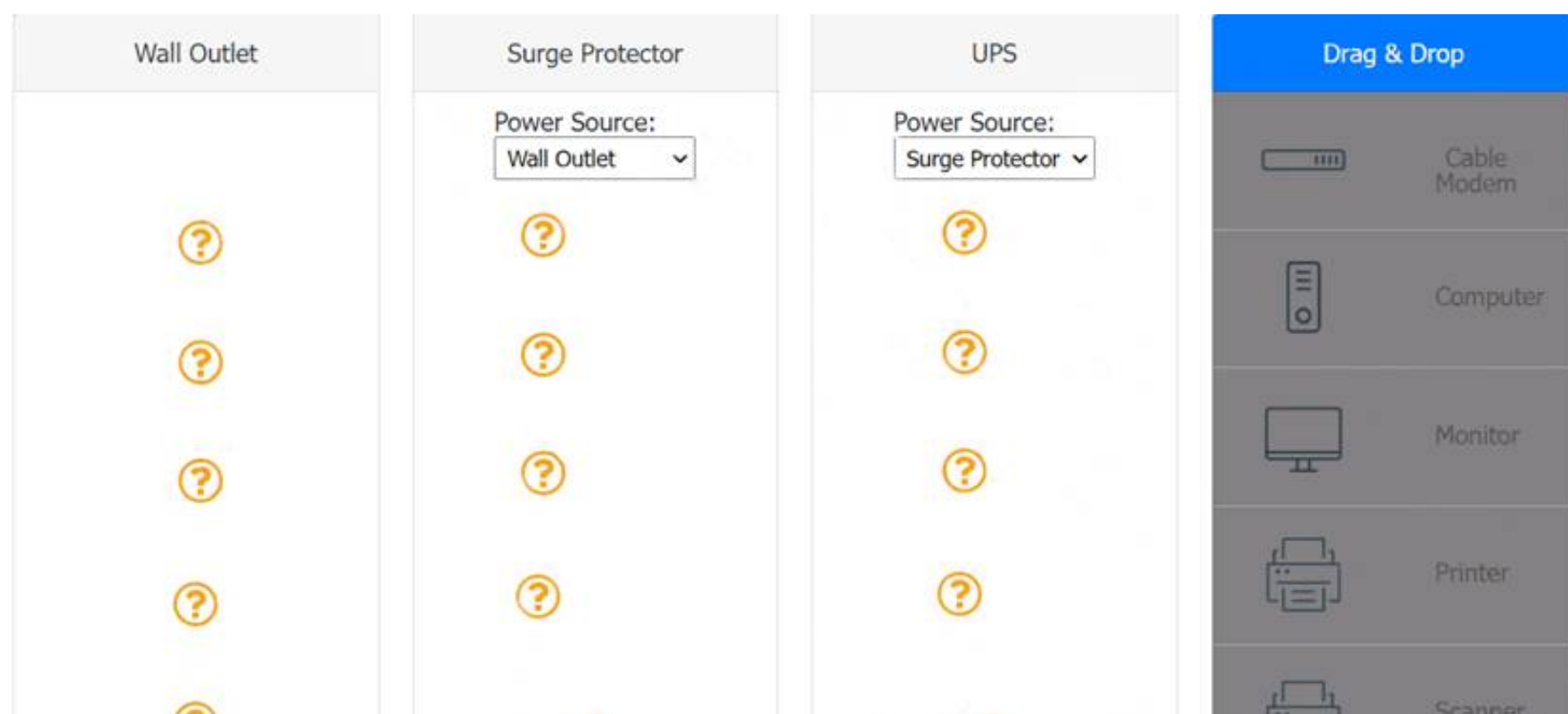
Answer: C

Explanation:

The technician should quarantine the system first.

NEW QUESTION 117

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 120

A user is unable to access a website, which is widely used across the organization, and receives the following error message:

The security certificate presented by this website has expired or is not yet valid.

The technician confirms the website works when accessing it from another computer but not from the user's computer. Which of the following should the technician perform NEXT to troubleshoot the issue?

- A. Reboot the computer.
- B. Reinstall the OS.
- C. Configure a static IP.
- D. Check the computer's date and time.

Answer: D

Explanation:

The error message indicates that the security certificate presented by the website has either expired or is not yet valid. This can happen if the computer's clock has the wrong date or time, as SSL/TLS certificates have a specific validity period. If the clock is off by too much, it may cause the certificate to fail to validate. Therefore, the technician should check the computer's date and time and ensure that they are correct.

NEW QUESTION 123

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 network.

NEW QUESTION 124

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 128

A user calls the help desk and reports a workstation is infected with malicious software. Which of the following tools should the help desk technician use to remove the malicious software? (Select TWO).

- A. File Explorer
- B. User Account Control
- C. Windows Backup and Restore
- D. Windows Firewall
- E. Windows Defender
- F. Network Packet Analyzer

Answer: AE

Explanation:

The correct answers are E. Windows Defender and A. File Explorer. Windows Defender is a built-in antivirus program that can detect and remove malicious software from a workstation. File Explorer can be used to locate and delete files associated with the malicious software1

NEW QUESTION 129

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.

Details

#8675310

Open

Priority

Low

Category

Technical / Bug Reports

Assigned To

helpdesk@fictional.com

Assigned Date

7/13/2022

Subject

Unable to access Z: on my computer, but I can manually enter the location in the window.

Attachments

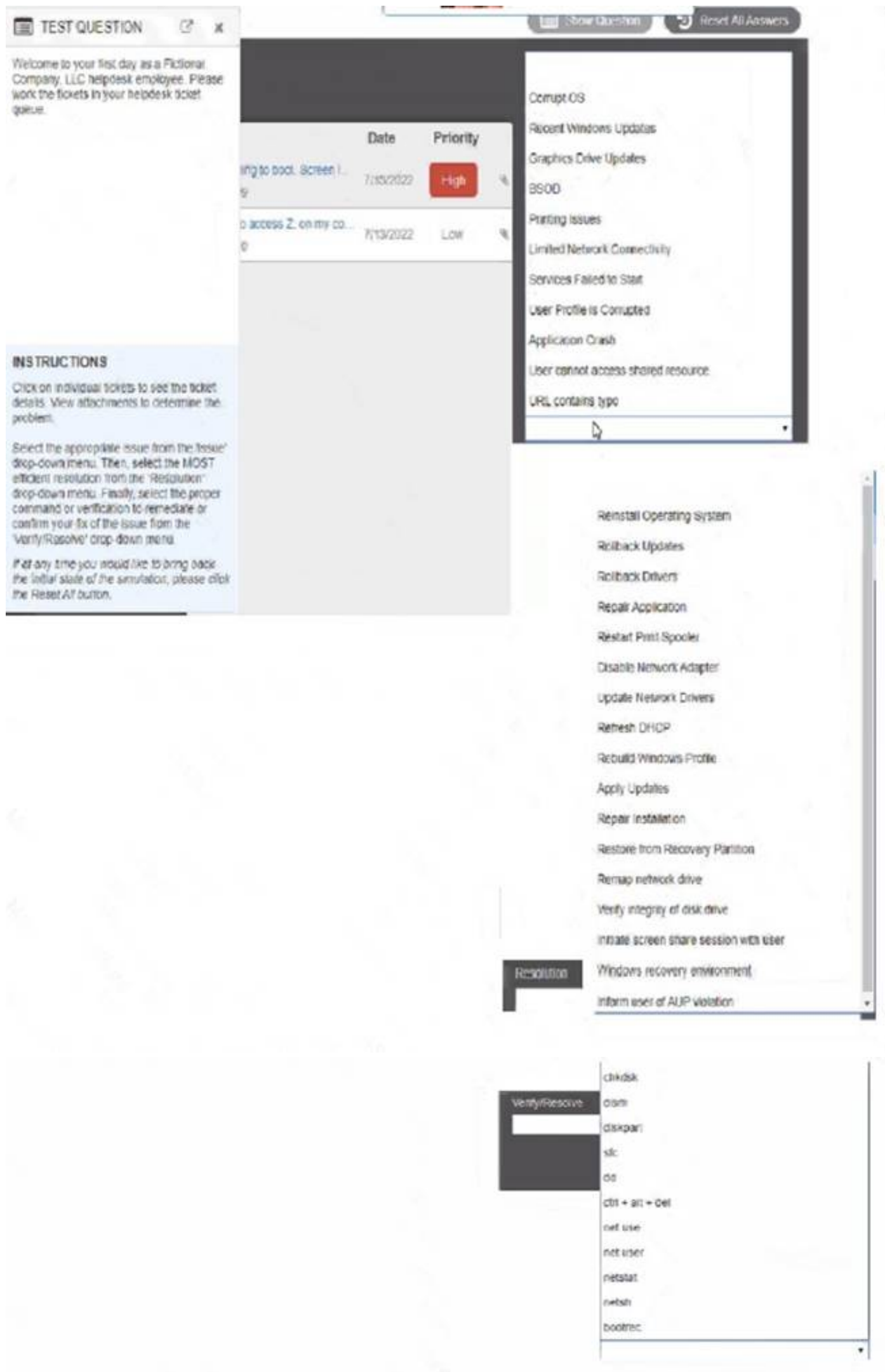
[File Explorer.jpg](#)

Issue

Resolution

Verify/Resolve

Close Ticket



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Details

#8675310

Open

Priority

Low

Category

Technical / Bug Reports

Assigned To

helpdesk@fictional.com

Assigned Date

7/13/2022

Subject

Unable to access Z: on my computer, but I can manually enter the location in the window.

Attachments

[File Explorer.jpg](#)

Issue

Corrupt OS

Resolution

Reinstall Operating System

Verify/Resolve

chkdsk

Close Ticket

NEW QUESTION 132

Which of the following must be maintained throughout the forensic evidence life cycle when dealing with a piece of evidence?

- A. Acceptable use
- B. Chain of custody
- C. Security policy
- D. Information management

Answer: B

Explanation:

The aspect of forensic evidence life cycle that must be maintained when dealing with a piece of evidence is chain of custody. This is because chain of custody is the documentation of the movement of evidence from the time it is collected to the time it is presented in court, and it is important to maintain the integrity of the evidence

NEW QUESTION 136

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.

TEST QUESTION

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.

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.

Telecom.

Please follow the new mobile device guide provided on our website.

the latest update, here is a screenshot

IMAP >

SSL >

10.0.200.1 >

100 >

on your mail settings to 143.

Send

Protocol

IMAP >

Security

SSL >

Server Address

10.0.200.1 >

Port

100 >

Please change the port number on your mail settings to 143.

Thanks for helping.

Which of the following should be done NEXT?

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

Answer: A

NEW QUESTION 138

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 142

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 147

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 152

Which of the following should be done NEXT?

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

Answer: D

Explanation:

educating the user on the solution that was performed is a good next step after resolving an issue. This can help prevent similar issues from happening again and empower users to solve problems on their own.

NEW QUESTION 153

A user reports that antivirus software indicates a computer is infected with viruses. The user thinks this happened while browsing the internet. The technician does not recognize the interface with which the antivirus message is presented. Which of the following is the NEXT step the technician should take?

- A. Shut down the infected computer and swap it with another computer
- B. Investigate what the interface is and what triggered it to pop up
- C. Proceed with initiating a full scan and removal of the viruses using the presented interface
- D. Call the phone number displayed in the interface of the antivirus removal tool

Answer: B

Explanation:

The technician should not proceed with initiating a full scan and removal of the viruses using the presented interface or call the phone number displayed in the interface of the antivirus removal tool¹²

Shutting down the infected computer and swapping it with another computer is not necessary at this point¹² The technician should not immediately assume that the message is legitimate or perform any actions without knowing what the interface is and what triggered it to pop up. It is important to investigate the issue further, including checking the legitimacy of the antivirus program and the message it is displaying.

NEW QUESTION 154

A technician is upgrading the backup system for documents at a high-volume law firm. The current backup system can retain no more than three versions of full backups before failing. The law firm is not concerned about restore times but asks the technician to retain more versions when possible. Which of the following backup methods should the technician MOST likely implement?

- A. Full
- B. Mirror
- C. Incremental
- D. Differential

Answer: C

Explanation:

The law firm wants to retain more versions of the backups when possible, so the best backup method for the technician to implement in this scenario would be Incremental backup. Incremental backups only save the changes made since the last backup, which allows for more frequent backups and minimizes the amount of storage required. This would allow the law firm to retain more than three versions of backups without risking backup failure.

To retain more versions of backups, the technician should implement an Incremental backup method¹⁰

An incremental backup method only backs up the data that has changed since the last backup, so it requires less storage space than a full backup¹²

NEW QUESTION 157

A laptop user is visually impaired and requires a different cursor color. Which of the following OS utilities is used to change the color of the cursor?

- A. Keyboard
- B. Touch pad
- C. Ease of Access Center
- D. Display settings

Answer: C

Explanation:

The OS utility used to change the color of the cursor in Windows is Ease of Access Center.

The user can change the cursor color by opening the Settings app, selecting Accessibility in the left sidebar selecting Mouse pointer and touch under Vision, and choosing one of the cursor options. The user can select Custom to pick a color and use the Size slider to make the cursor larger or smaller.

The Ease of Access Center in the Windows OS provides accessibility options for users with disabilities or impairments. One of these options allows the user to change the color and size of the cursor, making it more visible and easier to locate on the screen. The Keyboard and Touchpad settings do not offer the option to change cursor color, and Display Settings are used to adjust the resolution and other properties of the display. Therefore, C is the best answer. This information is covered in the CompTIA A+ Core2 documents/guide under the Accessibility section.

NEW QUESTION 162

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 166

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. The user is not connected to the VPN.
- B. The file server is offline.
- C. A low battery is preventing the connection.
- D. The log-in script failed.

Answer: A

NEW QUESTION 168

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 is 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 editions. 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 edition.

NEW QUESTION 172

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 network.

NEW QUESTION 173

Following a recent power outage, several computers have been receiving errors when booting. The technician suspects file corruption has occurred. Which of the following steps should the technician try FIRST to correct the issue?

- A. Rebuild the Windows profiles.
- B. Restore the computers from backup.
- C. Reimage the computers.
- D. Run the System File Checker.

Answer: D

Explanation:

The technician should run the System File Checker (SFC) first to correct file corruption errors on computers after a power outage. SFC is a command-line utility that scans for and repairs corrupted system files. It can be run from the command prompt or from the Windows Recovery Environment. Rebuilding the Windows profiles, restoring the computers from backup, and reimaging the computers are more drastic measures that should be taken only if SFC fails to correct the issue¹

NEW QUESTION 178

Which of the following change management documents includes how to uninstall a patch?

- A. Purpose of change
- B. Rollback plan
- C. Scope of change
- D. Risk analysis

Answer: B

Explanation:

The change management document that includes how to uninstall a patch is called the “rollback plan”. The rollback plan is a document that outlines the steps that should be taken to undo a change that has been made to a system. In the case of a patch, the rollback plan would include instructions on how to uninstall the patch if it causes problems or conflicts with other software¹²

NEW QUESTION 183

The Chief Executive Officer at a bank recently saw a news report about a high-profile cybercrime where a remote-access tool that the bank uses for support was also used in this crime. The report stated that attackers were able to brute force passwords to access systems. Which of the following would BEST limit the bank's risk? (Select TWO)

- A. Enable multifactor authentication for each support account
- B. Limit remote access to destinations inside the corporate network
- C. Block all support accounts from logging in from foreign countries
- D. Configure a replacement remote-access tool for support cases.
- E. Purchase a password manager for remote-access tool users
- F. Enforce account lockouts after five bad password attempts

Answer: AF

Explanation:

The best ways to limit the bank's risk are to enable multifactor authentication for each support account and enforce account lockouts after five bad password attempts. Multifactor authentication adds an extra layer of security to the login process, making it more difficult for attackers to gain access to systems. Account lockouts after five bad password attempts can help to prevent brute force attacks by locking out accounts after a certain number of failed login attempts.

NEW QUESTION 187

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 192

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 195

Security software was accidentally uninstalled from all servers in the environment. After requesting the same version of the software be reinstalled, the security analyst learns that a change request will need to be filled out. Which of the following is the BEST reason to follow the change management process in this scenario?

- A. Owners can be notified a change is being made and can monitor it for performance impact
- B. Most Voted
- C. A risk assessment can be performed to determine if the software is needed.
- D. End users can be aware of the scope of the change.
- E. A rollback plan can be implemented in case the software breaks an application.

Answer: A

Explanation:

change management process can help ensure that owners are notified of changes being made and can monitor them for performance impact (A). This can help prevent unexpected issues from arising.

NEW QUESTION 199

A technician is setting up a SOHO wireless router. The router is about ten years old. The customer would like the most secure wireless network possible. Which of the following should the technician configure?

- A. WPA2 with TKIP
- B. WPA2 with AES
- C. WPA3withAES-256
- D. WPA3 with AES-128

Answer: B

Explanation:

This is because WPA2 with AES is the most secure wireless network configuration that is available on a ten-year-old SOHO wireless router.

NEW QUESTION 202

A user received the following error upon visiting a banking website:

The security presented by website was issued a different website' s address . A technician should instruct the user to:

- A. clear the browser cache and contact the bank.
- B. close out of the site and contact the bank.
- C. continue to the site and contact the bank.
- D. update the browser and contact the bank.

Answer: A

Explanation:

The technician should instruct the user to clear the browser cache and contact the bank (option A). This error indicates that the website the user is visiting is not the correct website and is likely due to a cached version of the website being stored in the user's browser. Clearing the browser cache should remove any stored versions of the website and allow the user to access the correct website. The user should also contact the bank to confirm that they are visiting the correct website and to report the error.

NEW QUESTION 205

A technician is attempting to mitigate micro power outages, which occur frequently within the area of operation. The outages are usually short, with the longest occurrence lasting five minutes. Which of the following should the technician use to mitigate this issue?

- A. Surge suppressor
- B. Battery backup
- C. CMOS battery
- D. Generator backup

Answer: B

Explanation:

A battery backup, also known as an uninterruptible power supply (UPS), is a device that provides backup power during a power outage. When the power goes out, the battery backup provides a short amount of time (usually a few minutes up to an hour, depending on the capacity of the device) to save any work and safely shut down the equipment.

NEW QUESTION 206

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 211

A technician is investigating an employee's smartphone that has the following symptoms

- The device is hot even when it is not in use.
- Applications crash, especially when others are launched
- Certain applications, such as GPS, are in portrait mode when they should be in landscape mode

Which of the following can the technician do to MOST likely resolve these issues with minimal impact? (Select TWO).

- A. Turn on autorotation
- B. Activate airplane mode.
- C. Close unnecessary applications
- D. Perform a factory reset
- E. Update the device's operating system
- F. Reinstall the applications that have crashed.

Answer: AC

Explanation:

The technician can close unnecessary applications and turn on autorotation to resolve these issues with minimal impact. Autorotation can help the device to switch between portrait and landscape modes automatically. Closing unnecessary applications can help to free up the device's memory and reduce the device's temperature¹

NEW QUESTION 214

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 216

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 .app. This is because .app is the file extension for applications on macOS.

NEW QUESTION 221

A technician found that an employee is mining cryptocurrency on a work desktop. The company has decided that this action violates its guidelines. Which of the following should be updated to reflect this new requirement?

- A. MDM
- B. EULA
- C. IRP
- D. AUP

Answer: D

Explanation:

AUP (Acceptable Use Policy) should be updated to reflect this new requirement. The AUP is a document that outlines the acceptable use of technology within an organization. It is a set of rules that employees must follow when using company resources. The AUP should be updated to include a policy on cryptocurrency mining on work desktops

NEW QUESTION 226

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 220-1102 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 220-1102 Product From:

<https://www.2passeasy.com/dumps/220-1102/>

Money Back Guarantee

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