

CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2



NEW QUESTION 1

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 shows the Windows Troubleshooting Center interface. On the left, a list of issues is displayed with columns for Date and Priority. The 'PC is failing to boot' issue is selected, showing a 'High' priority and a 'Details' pane. The details pane shows the issue description, category, assigned to, and assigned date. Below the details, there is a 'Resolution' section with a list of steps to follow. The 'Verify/Resolve' section is also visible, showing a list of commands to run.

Date	Priority	Issue
7/13/2022	High	PC is failing to boot. Screen is displaying error message, see attachment.
7/13/2022	Low	Access Z: on my computer

Details

#6675309
 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
 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

Resolution

- 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
- Inform user of AUP violation

Verify/Resolve

- chkdsk
- dism
- diskpart
- sfc
- dd
- ctrl + alt + del
- net use
- net user
- netstat
- netsh
- 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 2

A user is experiencing frequent malware symptoms on a Windows workstation. The user has tried several times to roll back the state but the malware persists. Which of the following would MOST likely resolve the issue?

- A. Quarantining system files
- B. Reimaging the workstation
- C. Encrypting the hard drive
- D. Disabling TLS 1.0 support

Answer: C

Explanation:

Encrypting the hard drive would most likely resolve the issue¹

NEW QUESTION 3

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

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

Answer: D

Explanation:

The issue is specific to the user's profile, so the technician should rebuild the profile. Rebuilding the profile will create a new profile and transfer the user's data to the new profile¹

NEW QUESTION 4

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 5

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 6

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 7

A technician just completed a Windows 10 installation on a PC that has a total of 16GB of RAM. The technician notices the Windows OS has only 4GB of RAM available for use. Which of the following explains why the OS can only access 4GB of RAM?

- A. The UEFI settings need to be changed.
- B. The RAM has compatibility issues with Windows 10.
- C. Some of the RAM is defective.
- D. The newly installed OS is x86.

Answer: D

Explanation:

The newly installed OS is x86. The x86 version of Windows 10 can only use up to 4GB of RAM. The x64 version of Windows 10 can use up to 2TB of RAM.

NEW QUESTION 8

A change advisory board did not approve a requested change due to the lack of alternative actions if implementation failed. Which of the following should be updated before requesting approval again?

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

Answer: C

Explanation:

The rollback plan should be updated before requesting approval again. A rollback plan is a plan for undoing a change if it causes problems, and it is an important part of any change management process. If the change advisory board did not approve the requested change due to the lack of alternative actions if implementation failed, then updating the rollback plan would be the best way to address this concern.

NEW QUESTION 9

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 10

A technician is replacing the processor in a desktop computer prior to opening the computer, the technician wants to ensure the internal components are protected.

Which of the following safety procedures would BEST protect the components in the PC? (Select TWO).

- A. Utilizing an ESD strap
- B. Disconnecting the computer from the power source
- C. Placing the PSU in an antistatic bag
- D. Ensuring proper ventilation
- E. Removing dust from the ventilation fans
- F. Ensuring equipment is grounded

Answer: AC

Explanation:

The two safety procedures that would best protect the components in the PC are:

- Utilizing an ESD strap
- Placing the PSU in an antistatic bag

<https://www.professormesser.com/free-a-plus-training/220-902/computer-safety-procedures-2/> <https://www.skillssoft.com/course/comptia-a-core-2-safety-procedures-environmental-impacts-cbdf0f2c-61c0-4f>

NEW QUESTION 10

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 13

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 18

The web browsing speed on a customer's mobile phone slows down every few weeks and then returns to normal after three or four days. Restarting the device does not usually restore performance. Which of the following should a technician check FIRST to troubleshoot this issue?

- A. Data usage limits
- B. Wi-Fi connection speed
- C. Status of airplane mode
- D. System uptime

Answer: B

Explanation:

The technician should check the Wi-Fi connection speed first to troubleshoot this issue. Slow web browsing speed on a mobile phone can be caused by a slow Wi-Fi connection. The technician should check the Wi-Fi connection speed to ensure that it is fast enough to support web browsing. If the Wi-Fi connection speed is slow, the technician should troubleshoot the Wi-Fi network to identify and resolve the issue.

NEW QUESTION 23

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 28

A technician has been asked to set up a new wireless router with the best possible security. Which of the following should the technician implement?

- A. WPS
- B. TKIP
- C. WPA3
- D. WEP

Answer: C

Explanation:

WPA3 (Wi-Fi Protected Access version 3) is the latest version of Wi-Fi security and offers the highest level of protection available. It is designed to protect against brute force password attempts and protect against eavesdropping and man-in-the-middle attacks. WPA3 also supports the use of stronger encryption algorithms, such as the Advanced Encryption Standard (AES), which provides additional protection for wireless networks. WPA3 should be implemented in order to ensure the best possible security for the new wireless router.

NEW QUESTION 31

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 35

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 cache1e2
If clearing the application cache does not work, the systems administrator should uninstall and reinstall the application12
Resetting the phone to factory settings is not necessary at this point12
Installing an alternative application with similar functionality is not necessary at this point12

NEW QUESTION 36

A technician is troubleshooting an issue involving programs on a Windows 10 machine that are loading on startup but causing excessive boot times. Which of the following should the technician do to selectively prevent programs from loading?

- A. Right-click the Windows button, then select Run entering shell startup and clicking OK, and then move items one by one to the Recycle Bin
- B. Remark out entries listed HKEY_LOCAL_MACHINE>SOFTWARE>Microsoft>Windows>CurrentVersion>Run
- C. Manually disable all startup tasks currently listed as enabled and reboot checking for issue resolution at startup
- D. Open the Startup tab and methodically disable items currently listed as enabled and reboot, checking for issue resolution at each startup.

Answer: D

Explanation:

This is the most effective way to selectively prevent programs from loading on a Windows 10 machine. The Startup tab can be accessed by opening Task Manager and then selecting the Startup tab. From there, the technician can methodically disable items that are currently listed as enabled, reboot the machine, and check

for issue resolution at each startup. If the issue persists, the technician can then move on to disabling the next item on the list.

NEW QUESTION 37

A user is being directed by the help desk to look up a Windows PC's network name so the help desk can use a remote administration tool to assist the user. Which of the following commands would allow the user to give the technician the correct information? (Select TWO).

- A. ipconfig /all
- B. hostname
- C. netstat /?
- D. nslookup localhost
- E. arp -a
- F. ping :: 1

Answer: AB

Explanation:

The user can use the following commands to give the technician the correct information: ipconfig /all and hostname.

The ipconfig /all command displays the IP address, subnet mask, and default gateway all adapters on the computer. The hostname command displays the name of the computer.

NEW QUESTION 39

Sensitive data was leaked from a user's smartphone. A technician discovered an unapproved application was installed, and the user has full access to the device's command shell. Which of the following is the NEXT step the technician should take to find the cause of the leaked data?

- A. Restore the device to factory settings.
- B. Uninstall the unapproved application.
- C. Disable the ability to install applications from unknown sources.
- D. Ensure the device is connected to the corporate WiFi network.

Answer: B

Explanation:

The technician should disable the user's access to the device's command shell. This will prevent the user from accessing sensitive data and will help to prevent further data leaks. The technician should then investigate the unapproved application to determine if it is the cause of the data leak. If the application is found to be the cause of the leak, the technician should uninstall the application and restore the device to factory settings. If the application is not the cause of the leak, the technician should investigate further to determine the cause of the leak. Disabling the ability to install applications from unknown sources can help to prevent future data leaks, but it is not the next step the technician should take in this scenario. Ensuring the device is connected to the corporate WiFi network is not relevant to this scenario.

NEW QUESTION 42

Which of the following is a proprietary Cisco AAA protocol?

- A. TKIP
- B. AES
- C. RADIUS
- D. TACACS+

Answer: D

Explanation:

TACACS+ is a proprietary Cisco AAA protocol.

NEW QUESTION 44

Which of the following is the MOST cost-effective version of Windows 10 that allows remote access through Remote Desktop?

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

Answer: D

Explanation:

The most cost-effective version of Windows 10 that allows remote access through Remote Desktop is Windows 10 Pro. Windows 10 Pro includes Remote Desktop, which allows users to connect to a remote computer and access its desktop, files, and applications. Windows 10 Home does not include Remote Desktop, while Windows 10 Pro for Workstations and Windows 10 Enterprise are more expensive versions of Windows 10 that include additional features for businesses.

NEW QUESTION 45

A technician received a call stating that all files in a user's documents folder appear to be Changed, and each of the files now has a .lock file extension. Which of the following actions is the FIRST step the technician should take?

- A. Run a live disk clone.
- B. Run a full antivirus scan.
- C. Use a batch file to rename the files.
- D. Disconnect the machine from the network.

Answer: D

Explanation:

The CompTIA A+ Core 2 220-1002 exam covers this topic in the following domains: 1.2 Given a scenario, use appropriate resources to support users and 1.3 Explain the importance of security awareness.

NEW QUESTION 49

Which of the following is a data security standard for protecting credit cards?

- A. PHI
- B. NIST
- C. PCI
- D. GDPR

Answer: C

Explanation:

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

NEW QUESTION 52

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

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

Answer: A

Explanation:

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

NEW QUESTION 53

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

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

Answer: A

Explanation:

The BEST way to secure the workstation quickly when walking away is to use a key combination to lock the computer when leaving1

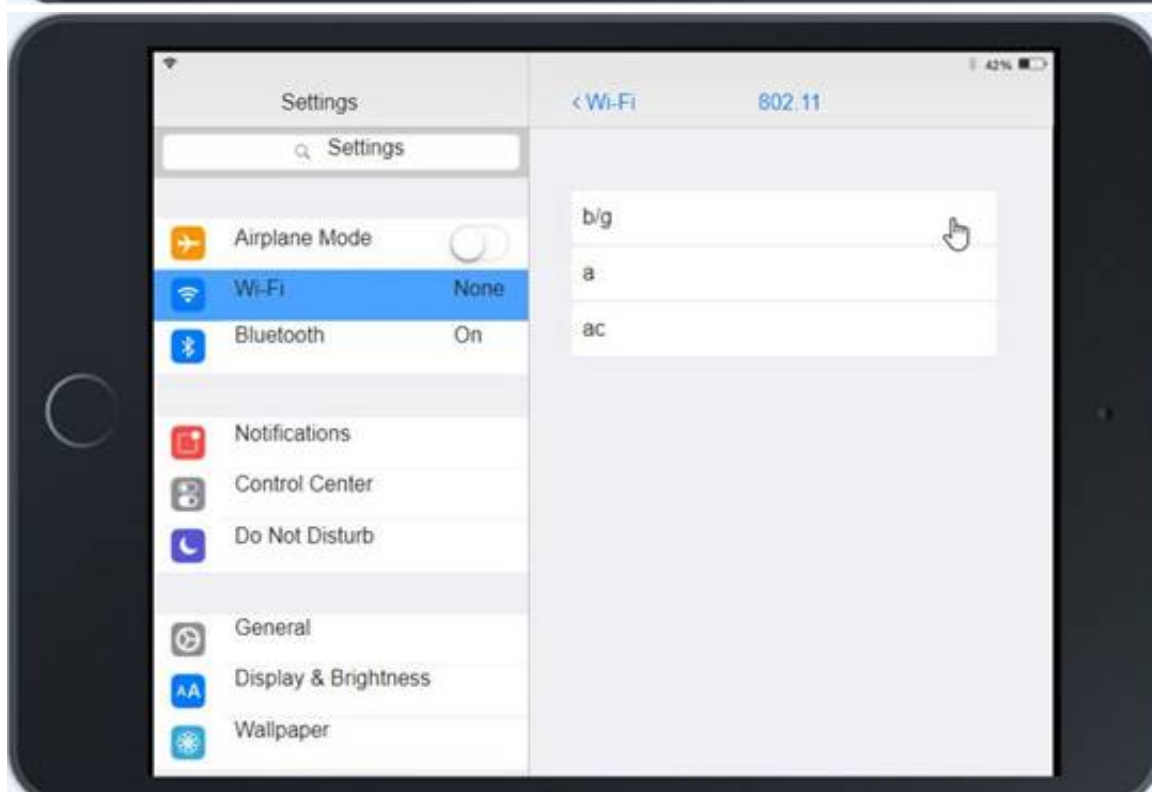
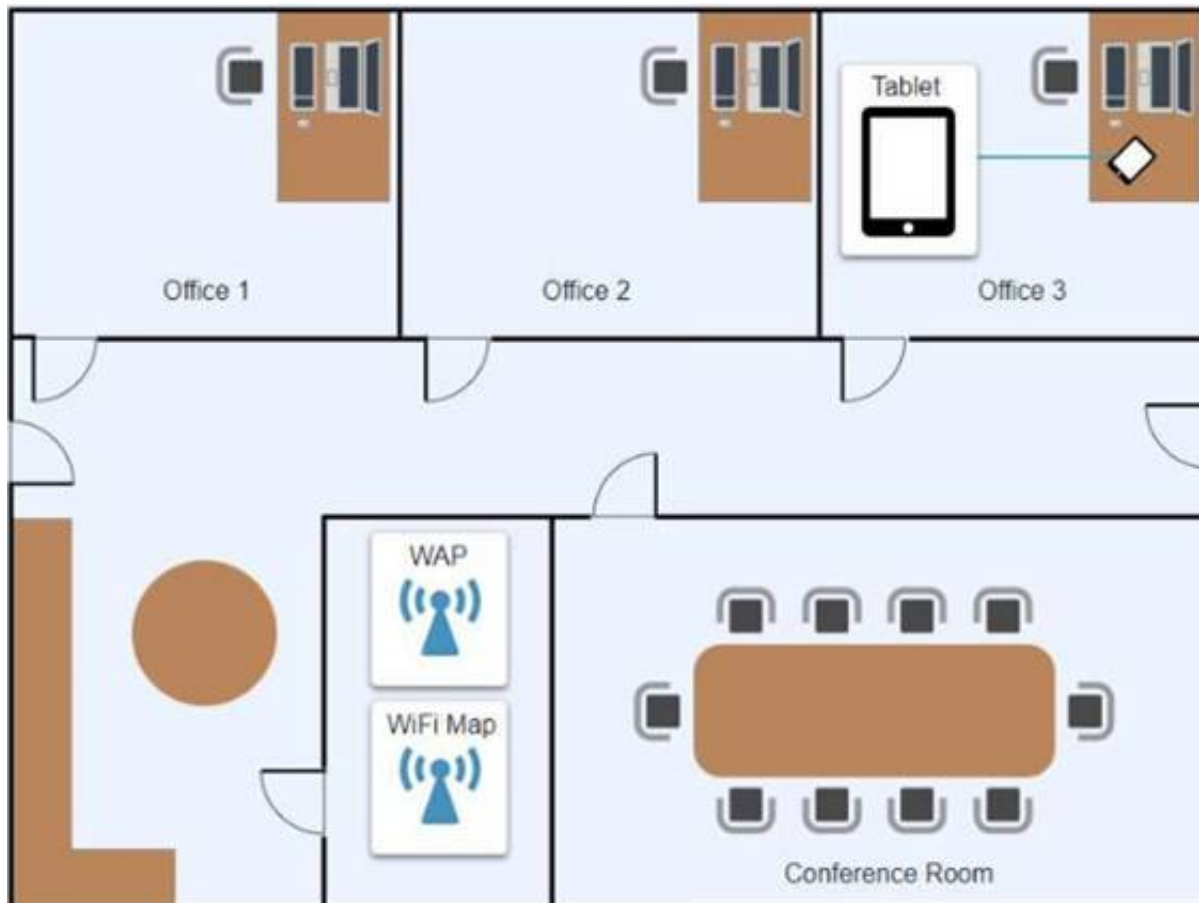
NEW QUESTION 55

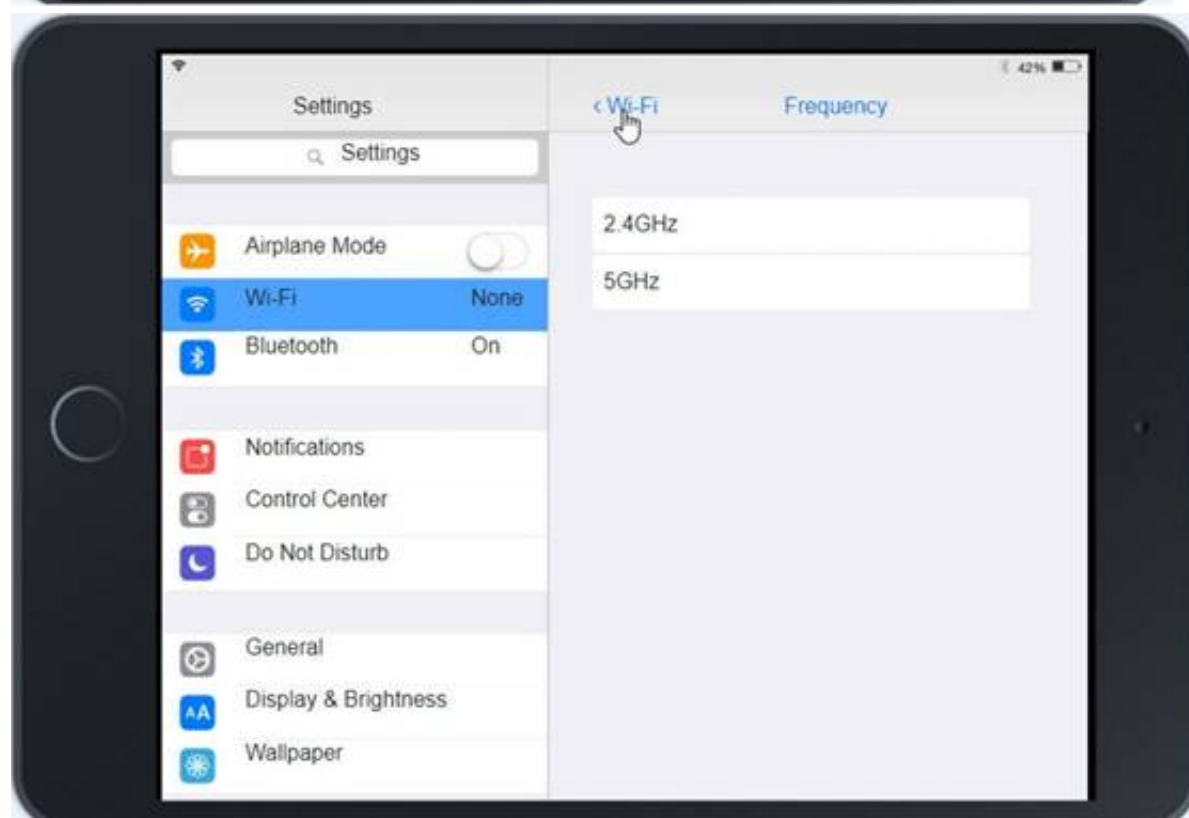
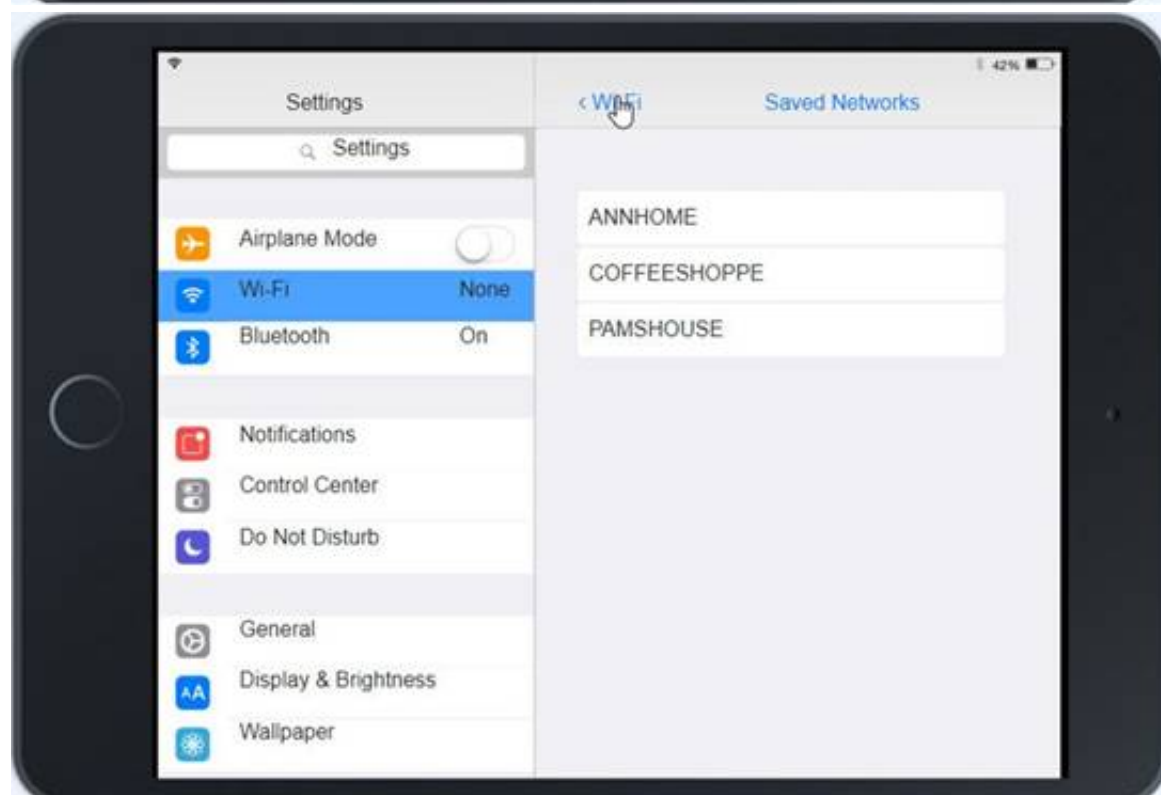
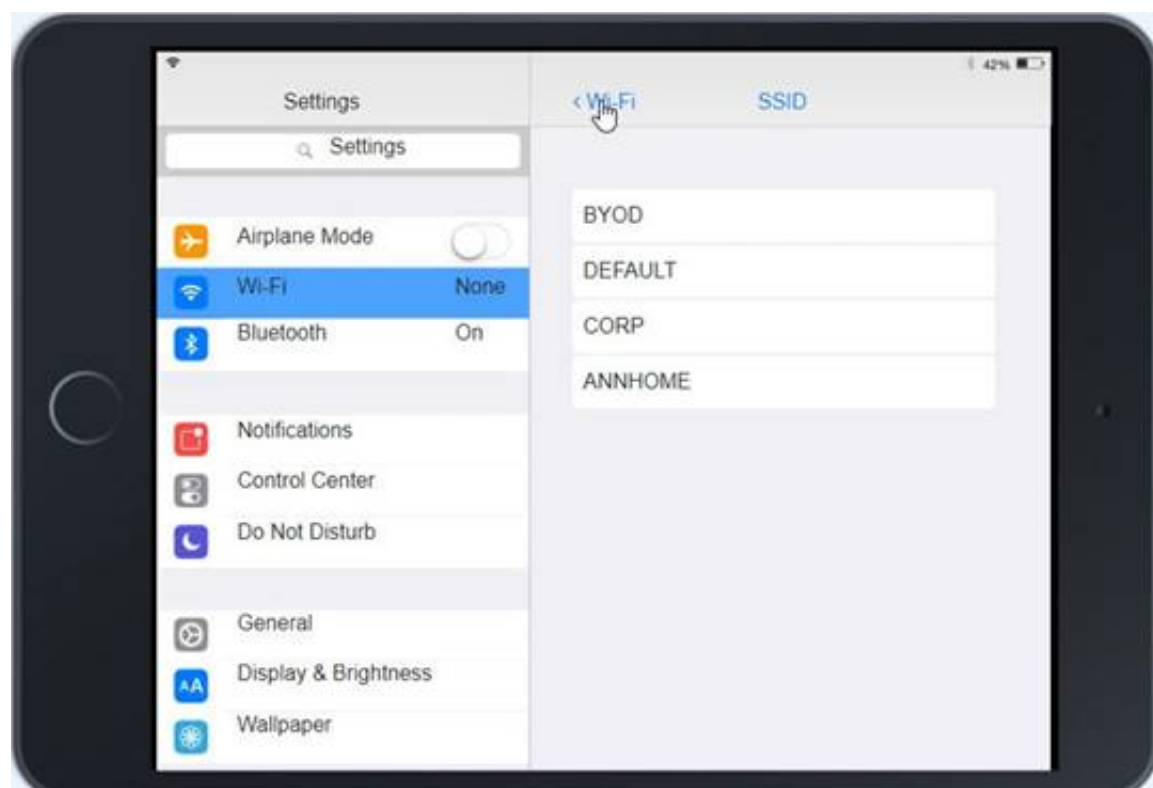
Ann, a CEO, has purchased a new consumer-class tablet for personal use, but she is unable to connect it to the company's wireless network. All the corporate laptops are connecting without issue. She has asked you to assist with getting the device online.

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.







x

Settings

Site

Wireless Networks

Networks

Guest Control

Admins

User Groups

VOIP

Controller

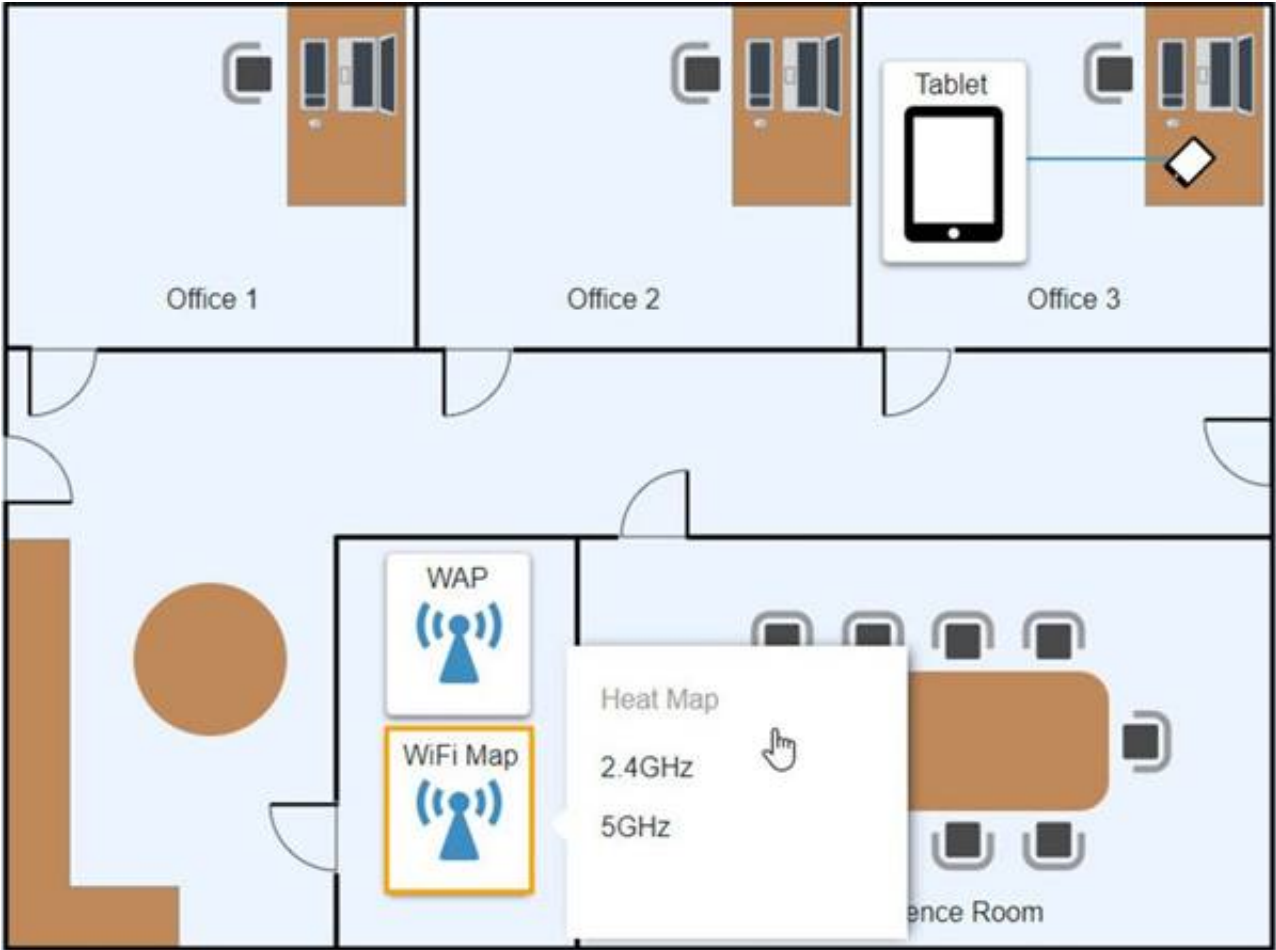
Cloud Access

Maintenance

Wireless Networks

SSID	Frequency	Security	Totally Secure!
CORP	2.4GHz/5GHz	WPA2	Corpsecure1
BYOD	2.4GHz/5GHz	WPA-PSK	TotallySecure1

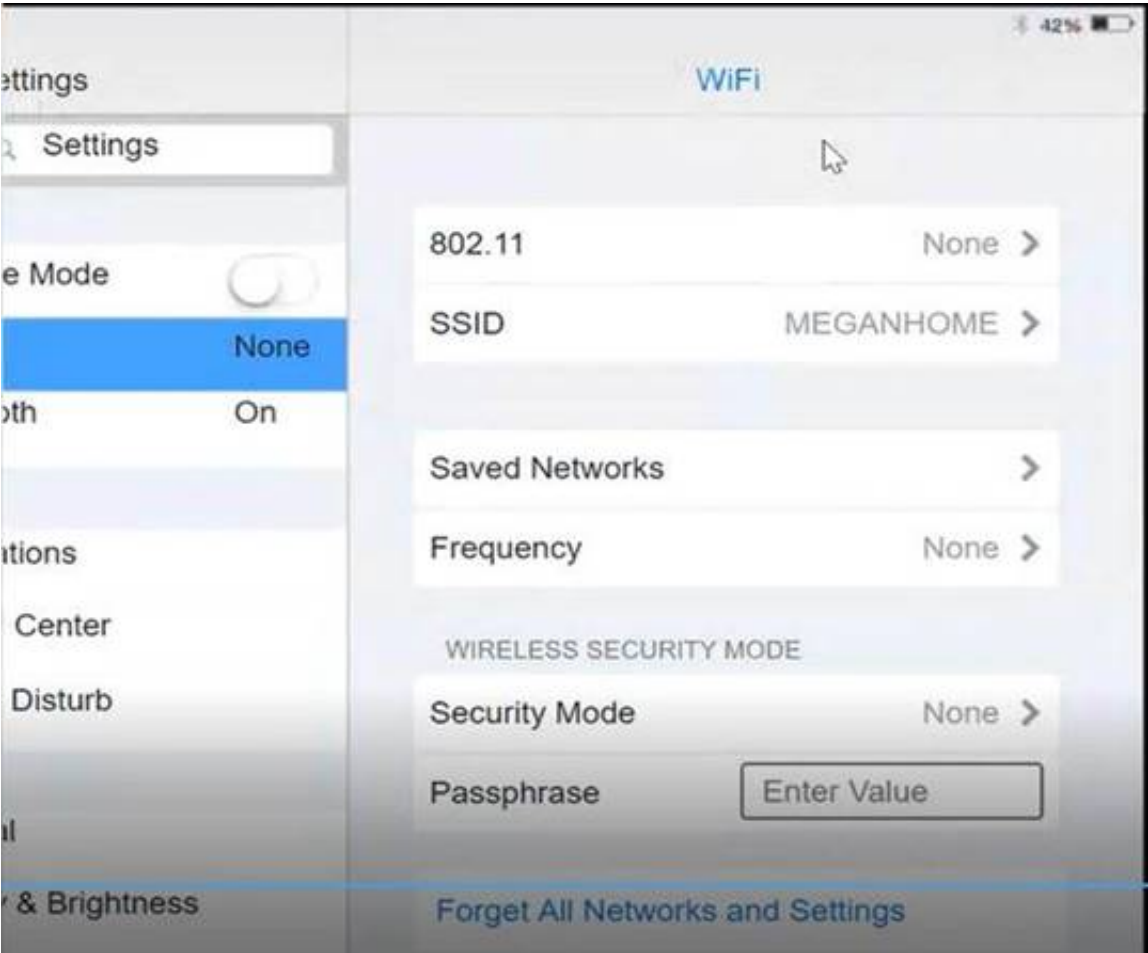
Create New Wireless Network



- A. Mastered
- B. Not Mastered

Answer: A

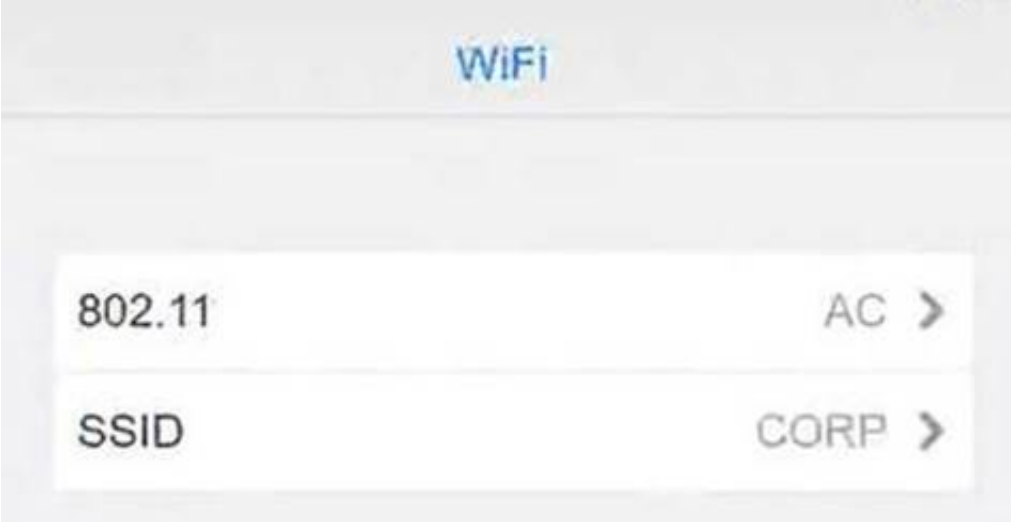
Explanation:
Graphical user interface, application Description automatically generated



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 58

A technician is tasked with configuring a computer for a visually impaired user. Which of the following utilities should the technician use?

- A. Device Manager
- B. System
- C. Ease of Access Center
- D. Programs and Features

Answer: C

Explanation:

The Ease of Access Center is a built-in utility in Windows that provides tools and options for making a computer easier to use for individuals with disabilities, including the visually impaired. In the Ease of Access Center, the technician can turn on options like high contrast display, screen magnification, and screen reader software to help the user better interact with the computer.

NEW QUESTION 59

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

requirements?

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

Answer: C

Explanation:

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

NEW QUESTION 62

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 65

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 66

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 first¹

NEW QUESTION 70

A company needs to securely dispose of data stored on optical discs. Which of the following is the MOST effective method to accomplish this task?

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

Answer: D

Explanation:

Shredding is the most effective method to securely dispose of data stored on optical discs¹² References: 4. How Can I Safely Destroy Sensitive Data CDs/DVDs? - How-To Geek. Retrieved from <https://www.howtogeek.com/174307/how-can-i-safely-destroy-sensitive-data-cdsdvds/> 5. Disposal — UK Data Service. Retrieved from <https://ukdataservice.ac.uk/learning-hub/research-data-management/store-your-data/disposal/>

NEW QUESTION 72

A technician is configuring a new Windows laptop Corporate policy requires that mobile devices make use of full disk encryption at all times 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 Windows

NEW QUESTION 76

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 79

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

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

Answer: D

Explanation:

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

NEW QUESTION 84

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 87

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 degradation

NEW QUESTION 88

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 method

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 backup

NEW QUESTION 89

A technician is setting up a backup method on a workstation that only requires two sets of tapes to restore. Which of the following would BEST accomplish this task?

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

Answer: D

Explanation:

A full backup involves creating a copy of all data on the workstation, including system files and user-created data, and storing it on a set of tapes. This ensures that all data is backed up, and ensures that the data can be restored in the event of a system failure or data loss.

NEW QUESTION 94

A small business owner wants to install newly purchased software on all networked PCs. The network is not configured as a domain, and the owner wants to use the easiest method possible. Which of the following is the MOST deficient way for the owner to install the application?

- A. Use a network share to share the installation files.
- B. Save software to an external hard drive to install.
- C. Create an imaging USB for each PC.
- D. Install the software from the vendor's website

Answer: B

Explanation:

Saving software to an external hard drive and installing it on each individual PC is the most inefficient method for the small business owner. This method requires manual intervention on each PC, and there is a higher risk of error or inconsistencies between PCs. Additionally, if the software needs to be updated or reinstalled in the future, this process would need to be repeated on each PC.

NEW QUESTION 99

A technician is setting up a backup method on a workstation that only requires two sets of tapes to restore. Which of the following would BEST accomplish this task?

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

Answer: D

Explanation:

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

A full backup only requires two sets of tapes to restore because it backs up all the data from the

workstation. With a differential backup, the backups need to be taken multiple times over a period of time, so more tapes would be needed to restore the data

NEW QUESTION 100

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 102

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 105

A technician needs to recommend the best backup method that will mitigate ransomware attacks. Only a few files are regularly modified, however, storage space is a concern. Which of the following backup methods would BEST address these concerns?

- A. Full
- B. Differential
- C. Off-site
- D. Grandfather-father-son

Answer: B

Explanation:

The differential backup method would best address these concerns. Differential backups only back up files that have changed since the last full backup, which means that only a few files would be backed up each time. This would help to mitigate the risk of ransomware attacks, as only a few files would be affected if an attack occurred. Additionally, differential backups require less storage space than full backups.

NEW QUESTION 107

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 112

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 115

A technician needs to transfer a large number of files over an unreliable connection. The technician should be able to resume the process if the connection is interrupted. Which of the following tools can be used?

- A. afc
- B. ehkdsd
- C. git clone
- D. zobocopy

Answer: A

Explanation:

The technician should use afc to transfer a large number of files over an unreliable connection and be able to resume the process if the connection is interrupted1

NEW QUESTION 120

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 121

A technician needs to exclude an application folder from being cataloged by a Windows 10 search. Which of the following utilities should be used?

- A. Privacy
- B. Indexing Options
- C. System
- D. Device Manager

Answer: B

Explanation:

To exclude an application folder from being cataloged by a Windows 10 search, the technician should use the Indexing Options utility

NEW QUESTION 122

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 126

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

220-1102 Practice Exam Features:

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

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