CompTIA.220-1102.v2023-09-12.q129

Exam Code:	220-1102
Exam Name:	CompTIA A+ Certification Exam: Core 2
Certification Provider:	CompTIA
Free Question Number:	129
Version:	v2023-09-12
# of views:	1488
# of Questions views:	1290
https://www.freepdfdumps.com/CompTIA.220-1102.v2023-09-12.q129.html	

NEW QUESTION: 1
Which of the following Linux commands would be used to install an application?
A. yum
B. grep
C. ls
D. sudo
Answer: D (LEAVE A REPLY)
The Linux command used to install an application is sudo. The sudo command allows users to run programs with the security privileges of another user, such as the root user. This is necessary to install applications because it requires administrative privileges1

NEW QUESTION: 2
A help desk technician is troubleshooting a workstation in a SOHO environment that is running above normal system baselines. The technician discovers an unknown executable with a random string name running on the system. The technician terminates the process, and the system returns to normal operation. The technician thinks the issue was an infected file, but the antivirus is not detecting a threat. The technician is concerned other machines may be infected with this unknown virus. Which of the following is the MOST effective way to check other machines on the network for this unknown threat?
A. Run a startup script that removes files by name.
B. Provide a sample to the antivirus vendor.
C. Manually check each machine.
D. Monitor outbound network traffic.
Answer: C (LEAVE A REPLY)
The most effective way to check other machines on the network for this unknown threat is to manually check each machine. This can help to identify any other machines that may be infected with the unknown virus and allow them to be cleaned.

NEW QUESTION: 3
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 (LEAVE A REPLY)
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: 4
A user calls the help desk to report potential malware on a computer. The anomalous activity began after the user clicked a link to a free gift card in a recent email The technician asks the user to describe any unusual activity, such as slow performance, excessive pop-ups, and browser redirections. Which of the following should the technician do NEXT?
A. Advise the user to run a complete system scan using the OS anti-malware application
B. Guide the user to reboot the machine into safe mode and verify whether the anomalous activities are still present
C. Have the user check for recently installed applications and outline those installed since the link in the email was clicked
D. Instruct the user to disconnect the Ethernet connection to the corporate network.
Answer: D (LEAVE A REPLY)
First thing you want to do is quarantine/disconnect the affected system from the network so whatever malicious software doesn't spread.

NEW QUESTION: 5
A user installed a new application that automatically starts each time the user logs in to a Windows 10 system. The user does not want this to happen and has asked for this setting to be changed. Which of the following tools would the technician MOST likely use to safely make this change?
A. Registry Editor
B. Task Manager
C. Event Viewer
D. Local Users and Groups
Answer: (SHOW ANSWER)

The technician would most likely use the Task Manager tool to safely make this change12 The Task Manager tool can be used to disable applications from starting automatically on Windows 10 The tool that a technician would most likely use to stop an application from automatically starting when a user logs in to a Windows 10 system is the Task Manager. The Task Manager can be used to view and manage processes, including those that are set to automatically start when a user logs in to the system.

NEW QUESTION: 6
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 (LEAVE A REPLY)
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: 7
Which of the following is used to integrate Linux servers and desktops into Windows Active Directory environments?
A. apt-get
B. CIFS
C. Samba
D. greP
Answer: C (LEAVE A REPLY)
Samba is a software suite that allows Linux servers and desktops to integrate with Windows Active Directory environments. Samba can act as a domain controller, a file server, a print server, or a client for Windows networks. Samba can also provide authentication and authorization services for Linux users and devices using Active Directory.

NEW QUESTION: 8
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 (LEAVE A REPLY)
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: 9
A technician is preparing to remediate a Trojan virus that was found on a workstation. Which of the following steps should the technician complete BEFORE removing the virus?
A. Disable System Restore.
B. Schedule a malware scan.
C. Educate the end user.
D. Run Windows Update.
Answer: (SHOW ANSWER)
Before removing a Trojan virus from a workstation, a technician should disable System Restore. System Restore is a feature that allows users to restore their system to a previous state in case of problems or errors. However, System Restore can also restore infected files or registry entries that were removed by antivirus software or manual actions. By disabling System Restore, a technician can ensure that the Trojan virus is completely removed and does not reappear after a system restore operation. Scheduling a malware scan may help detect and remove some malware but may not be effective against all types of Trojan viruses. Educating the end user may help prevent future infections but does not address the current issue of removing the Trojan virus. Running Windows Update may help patch some security vulnerabilities but does not guarantee that the Trojan virus will be removed. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.3

NEW QUESTION: 10
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 (LEAVE A REPLY)
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: 11
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 (LEAVE A REPLY)
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: 12
An Android user contacts the help desk because a company smartphone failed to complete a tethered OS update A technician determines there are no error messages on the device Which of the following should the technician do NEXT?
A. Verify all third-party applications are disabled
B. Determine if the device has adequate storage available.
C. Check if the battery is sufficiently charged
D. Confirm a strong internet connection is available using Wi-Fi or cellular data
Answer: (SHOW ANSWER)
Since there are no error messages on the device, the technician should check if the battery is sufficiently charged1 If the battery is low, the device may not have enough power to complete the update2 In this scenario, the technician has already determined that there are no error messages on the device. The next best step would be to check if the battery is sufficiently charged. If the battery is low, it could be preventing the device from completing the update process.
Verifying that third-party applications are disabled, determining if the device has adequate storage available, and confirming a strong internet connection are all important steps in troubleshooting issues with mobile devices. However, since the problem in this scenario is related to a failed OS update, it is important to first check the battery level before proceeding with further troubleshooting steps.

NEW QUESTION: 13
Which of the following is a consequence of end-of-lite operating systems?
A. Operating systems void the hardware warranty.

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

NEW QUESTION: 14
An incident handler needs to preserve evidence for possible litigation. Which of the following will the incident handler MOST likely do to preserve the evidence?
A. Encrypt the files
B. Clone any impacted hard drives
C. Contact the cyber insurance company
D. Inform law enforcement
Answer: B (LEAVE A REPLY)
The incident handler should clone any impacted hard drives to preserve evidence for possible litigation1

NEW QUESTION: 15
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 (LEAVE A REPLY)
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: 16
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 (LEAVE A REPLY)
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: 17
A technician installed Windows 10 on a workstation. The workstation only has 3.5GB of usable RAM, even though the technician installed 8GB. Which of the following is the MOST likely reason this system is not utilizing all the available RAM?
A. The system is missing updates.
B. The systems utilizing a 32-bit OS.
C. The system's memory is failing.
D. The system requires BIOS updates.
Answer: B (LEAVE A REPLY)
The most likely reason that the system is not utilizing all the available RAM is that it is running a 32-bit OS. A 32-bit OS can only address up to 4GB of RAM, and some of that is reserved for hardware and system use1. Therefore, even if the technician installed 8GB of RAM, the system can only use around 3.5GB of usable RAM. To use the full 8GB of RAM, the technician would need to install a 64-bit OS, which can address much more memory2. The system missing updates, the system's memory failing, or the system requiring BIOS updates are not likely to cause this issue.

NEW QUESTION: 18

Which of the following is the proper way for a technician to dispose of used printer consumables?
A. Proceed with the custom manufacturer's procedure.
B. Proceed with the disposal of consumables in standard trash receptacles.
C. Empty any residual ink or toner from consumables before disposing of them in a standard recycling bin.
D. Proceed with the disposal of consumables in standard recycling bins.
Answer: A (LEAVE A REPLY)
When it comes to disposing of used printer consumables , it is important to follow the manufacturer's instructions or guidelines for proper disposal, as different types of consumables may require different disposal procedures. Some manufacturers provide specific instructions for proper disposal, such as sending the used consumables back to the manufacturer or using special recycling programs.
Therefore, the proper way for a technician to dispose of used printer consumables is to proceed with the custom manufacturer's procedure , if provided. This option ensures that the disposal is handled in an environmentally friendly and safe manner.

NEW QUESTION: 19
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: (SHOW ANSWER)
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: 20
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 12
D. Check the computer's date and time.
Answer: (SHOW ANSWER)

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: 21
A technician installed Windows 10 on a workstation. The workstation only has 3.5GB of usable RAM, even though the technician installed 8GB. Which of the following is the MOST likely reason this system is not utilizing all the available RAM?
A. The system is missing updates.
B. The system is utilizing a 32-bit OS.
C. The system's memory is failing.
D. The system requires BIOS updates
Answer: B (LEAVE A REPLY)
The most likely reason that the system is not utilizing all the available RAM is that the system is utilizing a 32-bit OS. A 32-bit OS is an operating system that uses 32 bits to address memory locations and perform calculations. A 32-bit OS can only support up to 4GB of RAM, and some of that RAM may be reserved for hardware devices or system functions, leaving less than 4GB of usable RAM for applications and processes. A 32-bit OS cannot recognize or utilize more than 4GB of RAM, even if more RAM is installed on the system. To utilize all the available RAM, the system needs to use a 64-bit OS, which can support much more RAM than a 32-bit OS. The system missing updates may cause some performance or compatibility issues, but it does not affect the amount of usable RAM on the system. The system's memory failing may cause some errors or crashes, but it does not affect the amount of usable RAM on the system. The system requiring BIOS updates may cause some configuration or compatibility issues, but it does not affect the amount of usable RAM on the system. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.1

NEW QUESTION: 22
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 lor 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 (LEAVE A REPLY)
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: 23
While staying at a hotel, a user attempts to connect to the hotel Wi-Fi but notices that multiple SSIDs have very similar names. Which of the following social-engineering attacks is being attempted?
A. Evil twin
B. Impersonation
C. Insider threat
D. Whaling
Answer: (SHOW ANSWER)
An evil twin is a type of social-engineering attack that involves setting up a rogue wireless access point that mimics a legitimate one. The attacker can then intercept or modify the traffic of the users who connect to the fake SSID. The attacker may also use phishing or malware to steal credentials or personal information from the users

NEW QUESTION: 24
An employee calls the help desk regarding an issue with a laptop PC. After a Windows update, the user can no longer use certain locally attached devices, and a reboot has not fixed the issue. Which of the following should the technician perform to fix the issue?
A. Disable the Windows Update service.
B. Check for updates.
C. Restore hidden updates.
D. Rollback updates.
Answer: D (LEAVE A REPLY)
The technician should perform a rollback of the Windows update that caused the issue with the locally attached devices. A rollback is a process of uninstalling an update and restoring the previous version of the system. This can help to fix any compatibility or performance issues caused by the update1. To rollback an update, the technician can use the Settings app, the Control Panel, or the System Restore feature. The technician should also check for any device driver updates that might be needed after rolling back the update. Disabling the Windows Update service is not a good practice, as it can prevent the system from receiving important security and feature updates. Checking for updates might not fix the issue, as the update that caused the issue might still be installed. Restoring hidden updates is not relevant, as it only applies to updates that have been hidden by the user to prevent them from being installed2.

NEW QUESTION: 25
A technician needs to provide recommendations about how to upgrade backup solutions for a site in an area that has frequent hurricanes and an unstable power grid. Which of the following should the technician recommend implementing?

A. High availability
B. Regionally diverse backups
C. On-site backups
D. Incremental backups
Answer: B (LEAVE A REPLY)
Regionally diverse backups are backups that are stored in different geographic locations, preferably far away from the primary site1. This way, if a disaster such as a hurricane or a power outage affects one location, the backups in another location will still be available and accessible2. Regionally diverse backups can help ensure business continuity and data recovery in case of a disaster3. The other options are not the best backup solutions for a site in an area that has frequent hurricanes and an unstable power grid. High availability is a feature that allows a system to remain operational and accessible even if one or more components fail, but it does not protect against data loss or corruption4. On-site backups are backups that are stored in the same location as the primary site, which means they are vulnerable to the same disasters that can affect the primary site. Incremental backups are backups that only store the changes made since the last backup, which means they require less storage space and bandwidth, but they also depend on previous backups to restore data and may not be sufficient for disaster recovery.

NEW QUESTION: 26
The network was breached over the weekend System logs indicate that a single user's account was successfully breached after 500 attempts with a dictionary attack. Which of the following would BEST mitigate this threat?
A. Encryption at rest
B. Account lockout
C. Automatic screen lock
D. Antivirus
Answer: B (LEAVE A REPLY)
Account lockout would best mitigate the threat of a dictionary attack1

NEW QUESTION: 27
A user is setting up a computer for the first time and would like to create a secondary login with permissions that are different than the primary login. The secondary login will need to be protected from certain content such as games and websites. Which of the following Windows settings should the user utilize to create the secondary login?
A. Privacy
B. Accounts
C. Personalization
D. Shared resources
Answer: B (LEAVE A REPLY)
To create a secondary login with different permissions in Windows 10, the user should utilize the Accounts setting. Here are the steps to create a new user account with different permissions:

Right-click the Windows Start menu button.
Select Control Panel.
Select User Accounts.
Select Manage another account.
Select Add a new user in PC settings.
Use the Accounts dialog box to configure a new account.1

NEW QUESTION: 28
A kiosk, which is running Microsoft Windows 10, relies exclusively on a numeric keypad to allow customers to enter their ticket numbers but no other information. If the kiosk is idle for four hours, the login screen locks. Which of the following sign-on options would allow any employee the ability to unlock the kiosk?
A. Requiring employees to enter their usernames and passwords
B. Setting up facial recognition for each employee
C. Using a PIN and providing it to employees
D. Requiring employees to use their fingerprints
Answer: C (LEAVE A REPLY)
The best sign-on option that would allow any employee the ability to unlock the kiosk that relies exclusively on a numeric keypad is to use a PIN and provide it to employees. A PIN is a Personal Identification Number that is a numeric code that can be used as part of authentication or access control. A PIN can be entered using only a numeric keypad and can be easily shared with employees who need to unlock the kiosk. Requiring employees to enter their usernames and passwords may not be feasible or convenient if the kiosk only has a numeric keypad and no other input devices. Setting up facial recognition for each employee may not be possible or secure if the kiosk does not have a camera or biometric sensor. Requiring employees to use their fingerprints may not be possible or secure if the kiosk does not have a fingerprint scanner or biometric sensor. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

NEW QUESTION: 29
A user is attempting to make a purchase at a store using a phone. The user places the phone on the payment pad, but the device does not recognize the phone. The user attempts to restart the phone but still has the same results. Which of the following should the user do to resolve the issue?
A. Turn off airplane mode while at the register.
B. Verify that NFC is enabled.
C. Connect to the store's Wi-Fi network.
D. Enable Bluetooth on the phone.
Answer: (SHOW ANSWER)
The user should verify that NFC is enabled on their phone. NFC is a technology that allows two devices to communicate with each other when they are in close proximity2.

NFC (Near Field Communication) technology allows a phone to wirelessly communicate with a payment terminal or other compatible device. In order to use NFC to make a payment or transfer information, the feature must be enabled on the phone. Therefore, the user should verify that NFC is enabled on their phone before attempting to make a payment with it. The other options, such as turning off airplane mode, connecting to Wi-Fi, or enabling Bluetooth, do not pertain to the NFC feature and are unlikely to resolve the issue. This information is covered in the Comptia A+ Core2 documents/guide under the Mobile Devices section.

NEW QUESTION: 30
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 (LEAVE A REPLY)
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 applications2.
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 window3.

NEW QUESTION: 31
Upon downloading a new ISO, an administrator is presented with the following string:
59d15a16ce90cBcc97fa7c211b767aB
Which of the following BEST describes the purpose of this string?
A. XSS verification
B. AES-256 verification
C. Hash verification
D. Digital signature verification
Answer: (SHOW ANSWER)
Hash verification is a process that verifies the integrity of a file by comparing the hash value of the downloaded file to the hash value provided by the source1

NEW QUESTION: 32
A user reports a computer is running slow. Which of the following tools will help a technician identity the issued
A. Disk Cleanup
B. Group Policy Editor
C. Disk Management
D. Resource Monitor
Answer: (SHOW ANSWER)
Resource Monitor will help a technician identify the issue when a user reports a computer is running slow1

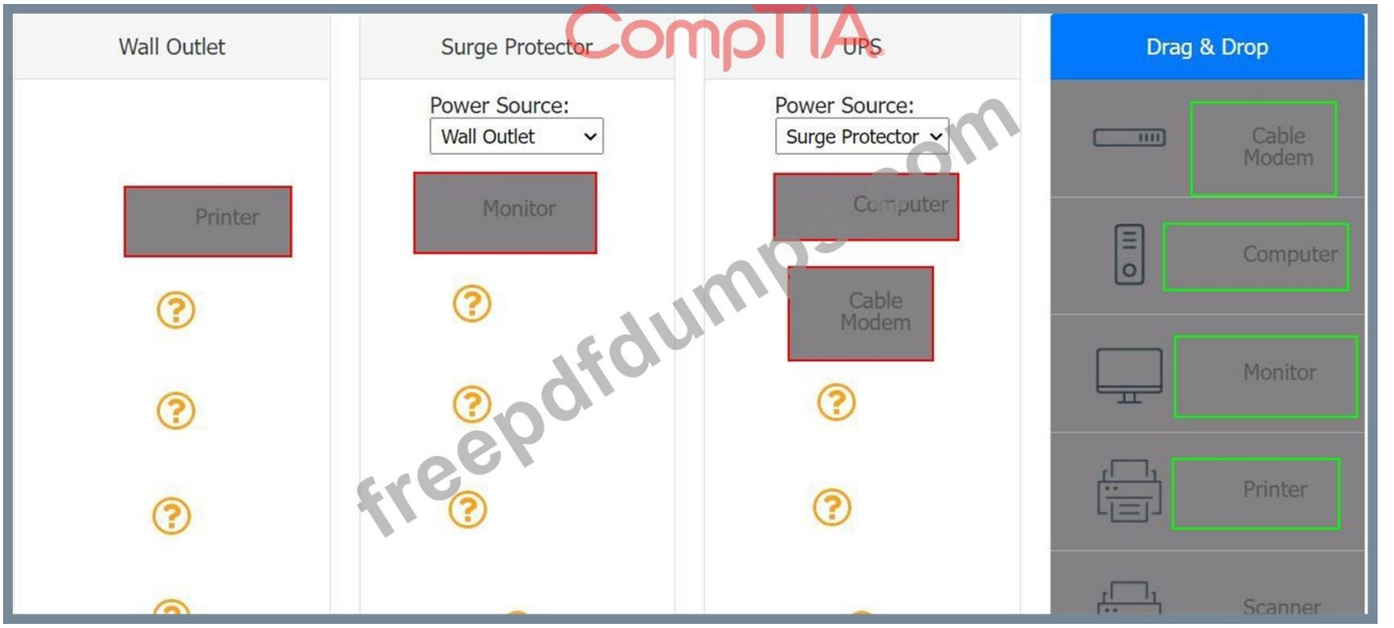
NEW QUESTION: 33
A technician downloads a validated security tool and notes the vendor hash of a58e87a2. When the download is complete, the technician again validates the hash, but the value returns as 2a876a7d3. Which of the following is the MOST likely cause of the issue?
A. Private-browsing mode
B. Invalid certificate
C. Modified file
D. Browser cache
Answer: C (LEAVE A REPLY)
The most likely cause of the issue of having different hash values for a downloaded security tool is a modified file. A hash value is a unique and fixed-length string that is generated from an algorithm that processes data or files. A hash value can be used to verify the integrity and authenticity of data or files by comparing it with a known or expected value. If the hash values do not match, it means that the data or file has been altered or corrupted in some way. A modified file may result from intentional or unintentional changes, such as editing, encryption, compression or malware infection. Private-browsing mode is a feature that allows users to browse the web without storing any browsing history, cookies or cache on their browser. Private-browsing mode does not affect the hash value of a downloaded file but only how the browser handles user data. Invalid certificate is an error that occurs when a website or a server does not have a valid or trusted digital certificate that proves its identity and secures its communication. Invalid certificate does not affect the hash value of a downloaded file but only how the browser verifies the website

or server's credibility. Browser cache is a temporary storage that stores copies of web pages, images and other content that users have visited on their browser.

NEW QUESTION: 34

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.

Answer:



NEW QUESTION: 35

A computer on a corporate network has a malware infection. Which of the following would be the BEST method for returning the computer to service?

A. Scanning the system with a Linux live disc, flashing the BIOS, and then returning the computer to service

B. Flashing the BIOS, reformatting the drive, and then reinstalling the OS

C. Degaussing the hard drive, flashing the BIOS, and then reinstalling the OS

D. Reinstalling the OS. flashing the BIOS, and then scanning with on-premises antivirus

Answer: (SHOW ANSWER)

Flashing the BIOS, reformatting the drive, and then reinstalling the OS is the best method for returning a computer with a malware infection to service. Flashing the BIOS updates the firmware of the motherboard and can remove any malware that may have infected it. Reformatting the drive erases all data on it and can remove any malware that may have infected it. Reinstalling the OS restores the system files and settings to their original state and can remove any malware that may have modified them. Scanning the system with a Linux live disc may not detect or remove all malware infections. Degaussing the hard drive is an extreme method of destroying data that may damage the drive beyond repair. Reinstalling the OS before flashing the BIOS or scanning with antivirus may not remove malware infections that persist in the BIOS or other files.

NEW QUESTION: 36

Following the latest Windows update PDF files are opening in Microsoft Edge instead of Adobe Reader. Which of the following utilities should be used to ensure all PDF files open in Adobe Reader?

A. Network and Sharing Center

B. Programs and Features

C. Default Apps

D. Add or Remove Programs

Answer: C (LEAVE A REPLY)

Default Apps should be used to ensure all PDF files open in Adobe Reader1

NEW QUESTION: 37

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

A. incineration

B. Resale

C. Physical destruction

D. Dumpster for recycling plastics

Answer: (SHOW ANSWER)

When disposing of non-compliant Ethernet cards, the most environmentally friendly option is to use a dumpster for recycling plastics. This method is the most effective way to reduce the amount of waste that is sent to landfills, and it also helps to reduce the amount of energy used in the

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

NEW QUESTION: 38
A new service desk is having a difficult time managing the volume of requests. Which of the following is the BEST solution for the department?
A. Implementing a support portal
B. Creating a ticketing system
C. Commissioning an automated callback system
D. Submitting tickets through email
Answer: A (LEAVE A REPLY)
A support portal is an online system that allows customers to access customer service tools, submit requests and view status updates, as well as access information such as how-to guides, FAQs, and other self-service resources. This would be the best solution for the service desk, as it would allow them to easily manage the volume of requests by allowing customers to submit their own requests and view the status of their requests. Additionally, the portal would provide customers with self-service resources that can help them resolve their own issues, reducing the amount of tickets that need to be handled by the service desk.

NEW QUESTION: 39
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 (LEAVE A REPLY)
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: 40

A technician is installing a program from an ISO file. Which of the following steps should the technician take?

A. Mount the ISO and run the installation file.

B. Copy the ISO and execute on the server.

C. Copy the ISO file to a backup location and run the ISO file.

D. Unzip the ISO and execute the setup.exe file.

Answer: A (LEAVE A REPLY)

Mounting the ISO and running the installation file is the correct way to install a program from an ISO file. An ISO file is an image of a disc that contains all the files and folders of a program. Mounting the ISO means creating a virtual drive that can access the ISO file as if it were a physical disc. Running the installation file means executing the setup program that will install the program on the computer

NEW QUESTION: 41

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 clearnmgr 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 (LEAVE A REPLY)

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: 42

A Microsoft Windows PC needs to be set up for a user at a targe corporation. The user will need access to the corporate domain to access email and shared drives. Which of the following versions of Windows would a technician MOST likely deploy for the user?

A. Windows Enterprise Edition

B. Windows Professional Edition

C. Windows Server Standard Edition

D. Windows Home Edition

Answer: B (LEAVE A REPLY)

The Windows Professional Edition is the most likely version that a technician would deploy for a user at a target corporation. This version of Windows is designed for business use and provides the necessary features and capabilities that a user would need to access the corporate domain, such as email and shared drives.

NEW QUESTION: 43

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

NEW QUESTION: 44
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: A,E (LEAVE A REPLY)
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: 45
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 (LEAVE A REPLY)

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: 46

A Windows workstation that was recently updated with approved system patches shut down instead of restarting. Upon reboot, the technician notices an alert stating the workstation has malware in the root OS folder. The technician promptly performs a System Restore and reboots the workstation, but the malware is still detected. Which of the following BEST describes why the system still has malware?

A. A system patch disabled the antivirus protection and host firewall.

B. The system updates did not include the latest anti-malware definitions.

C. The system restore process was compromised by the malware.

D. The malware was installed before the system restore point was created.

Answer: D (LEAVE A REPLY)

The best explanation for why the system still has malware after performing a System Restore is that the malware was installed before the system restore point was created. A system restore point is a snapshot of the system settings and configuration at a certain point in time. A System Restore is a feature that allows users to restore their system to a previous state in case of problems or errors. However, a System Restore does not affect personal files or folders, and it may not remove malware that was already present on the system before the restore point was created. A system patch disabling the antivirus protection and host firewall may increase the risk of malware infection, but it does not explain why the malware persists after a System Restore. The system updates not including the latest anti-malware definitions may reduce the effectiveness of malware detection and removal, but it does not explain why the malware persists after a System Restore. The system restore process being compromised by the malware may prevent a successful System Restore, but it does not explain why the malware persists after a System Restore. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.3

NEW QUESTION: 47
While assisting a customer with an issue, a support representative realizes the appointment is taking longer than expected and will cause the next customer meeting to be delayed by five minutes. Which of the following should the support representative do NEXT?
A. Send a quick message regarding the delay to the next customer.
B. Cut the current customer's lime short and rush to the next customer.
C. Apologize to the next customer when arriving late.
D. Arrive late to the next meeting without acknowledging the lime.
Answer: A (LEAVE A REPLY)
The support representative should send a quick message regarding the delay to the next customer. This will help the next customer understand the situation and adjust their schedule accordingly.

NEW QUESTION: 48
A user updates a mobile device's OS. A frequently used application becomes consistently unresponsive immediately after the device is launched. Which of the following troubleshooting steps should the user perform FIRST?
A. Delete the application's cache.
B. Check for application updates.
C. Roll back the OS update.
D. Uninstall and reinstall the application.
Answer: B (LEAVE A REPLY)
Sometimes, an OS update can cause compatibility issues with some applications that are not optimized for the new version of the OS. To fix this, the user should check if there are any updates available for the application that can resolve the issue. The user can check for application updates by following these steps:
On an Android device, open the Google Play Store app and tap on the menu icon in the top left corner. Then tap on My apps & games and look for any updates available for the application. If there is an update, tap on Update to install it.
On an iOS device, open the App Store app and tap on the Updates tab at the bottom. Then look for any updates available for the application. If there is an update, tap on Update to install it.

NEW QUESTION: 49

A user reports that a workstation is operating sluggishly Several other users operate on the same workstation and have reported that the workstation is operating normally. The systems administrator has validated that the workstation functions normally. Which of the following steps should the systems administrator most likely attempt NEXT?

A. Increase the paging file size

B. Run the chkdsk command

C. Rebuild the user's profile

D. Add more system memory.

E. Defragment the hard drive.

Answer: C (LEAVE A REPLY)

Since the systems administrator has validated that the workstation functions normally and other users operate on the same workstation without any issues, the next step should be to rebuild the user's profile. This will ensure that any corrupted files or settings are removed and the user's profile is restored to its default state.

NEW QUESTION: 50

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 (LEAVE A REPLY)

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 scenario1

NEW QUESTION: 51

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

A. VNC

B. MFA

C. MSRA

D. RDP

Answer: (SHOW ANSWER)

The tool that the technician will most likely use to remotely connect to a Linux desktop is VNC. VNC stands for Virtual Network Computing and is a protocol that allows remote access and control of a graphical desktop environment over a network. VNC is natively designed for Linux and can also support other operating systems, such as Windows and Mac OS. VNC can be used to assist users with troubleshooting by viewing and interacting with their desktops remotely. MFA stands for Multi-Factor Authentication and is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. MFA is not a tool that can be used to remotely connect to a Linux desktop but a technique that can be used to enhance security for systems or services. MSRA stands for Microsoft Remote Assistance and is a feature that allows remote access and control of a Windows desktop environment over a network. MSRA is not natively designed for Linux and may not be compatible or supported by Linux systems. RDP stands for Remote Desktop Protocol and is a protocol that allows remote access and control of a Windows desktop environment over a network. RDP is not natively designed for Linux and may not be compatible or supported by Linux systems. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

NEW QUESTION: 52

Which of the following is a proprietary Cisco AAA protocol?

A. TKIP

B. AES

C. RADIUS

D. TACACS+

Answer: D (LEAVE A REPLY)

TACACS+ is a proprietary Cisco AAA protocol

NEW QUESTION: 53

A BSOD appears on a user's workstation monitor. The user immediately presses the power button to shut down the PC, hoping to repair the issue. The user then restarts the PC, and the BSOD reappears, so the user contacts the help desk. Which of the following should the technician use to determine the cause?

A. Stop code

B. Event Mewer

C. Services

D. System Configuration

Answer: A (LEAVE A REPLY)

When a Blue Screen of Death (BSOD) appears on a Windows workstation, it indicates that there is a serious problem with the operating system. The stop code displayed on the BSOD can provide valuable information to help determine the cause of the issue. The stop code is a specific

error code that is associated with the BSOD, and it can help identify the root cause of the problem.
In this scenario, the user has encountered a BSOD and has restarted the PC, only to see the BSOD reappear. This suggests that the problem is persistent and requires further investigation. By analyzing the stop code displayed on the BSOD, a technician can begin to identify the underlying issue and take appropriate actions to resolve it.

NEW QUESTION: 54
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: (SHOW ANSWER)
https://www.educba.com/shell-scripting-in-linux/

NEW QUESTION: 55
A technician is in the process of installing a new hard drive on a server but is called away to another task. The drive has been unpackaged and left on a desk. Which of the following should the technician perform before leaving?
A. Ask coworkers to make sure no one touches the hard drive.
B. Leave the hard drive on the table; it will be okay while the other task is completed.
C. Place the hard drive in an antistatic bag and secure the area containing the hard drive.
D. Connect an electrostatic discharge strap to the drive.
Answer: C (LEAVE A REPLY)
The technician should place the hard drive in an antistatic bag and secure the area containing the hard drive before leaving. This will protect the hard drive from electrostatic discharge (ESD), dust, moisture, and physical damage. Asking coworkers to make sure no one touches the hard drive is not a reliable or secure way to prevent damage. Leaving the hard drive on the table exposes it to ESD and other environmental hazards. Connecting an electrostatic discharge strap to the drive is not enough to protect it from dust, moisture, and physical damage.

NEW QUESTION: 56
A user reports a computer is running slow. Which of the following tools will help a technician identify the issue?
A. Disk Cleanup
B. Disk Management
C. Group Policy Editor
D. Resource Monitor
Answer: D (LEAVE A REPLY)

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: 57
A team of support agents will be using their workstations to store credit card dat a. Which of the following should the IT department enable on the workstations in order to remain compliant with common regulatory controls? (Select TWO).
A. Encryption
B. Antivirus
C. AutoRun
D. Guest accounts
E. Default passwords
F. Backups
Answer: (SHOW ANSWER)
Encryption is a way of protecting cardholder data by transforming it into an unreadable format that can only be decrypted with a secret key1. Backups are a way of ensuring that cardholder data is not lost or corrupted in case of a disaster or system failure2. Both encryption and backups are part of the PCI DSS requirements that apply to any entity that stores, processes, or transmits cardholder data1. The other options are not directly related to credit card data security or compliance.

NEW QUESTION: 58
The audio on a user's mobile device is inconsistent when the user uses wireless headphones and moves around. Which of the following should a technician perform to troubleshoot the issue?
A. Verify the Wi-Fi connection status.
B. Enable the NFC setting on the device.
C. Bring the device within Bluetooth range.
D. Turn on device tethering.
Answer: (SHOW ANSWER)
Bringing the device within Bluetooth range is the best way to troubleshoot the issue of inconsistent audio when using wireless headphones and moving around. Bluetooth is a wireless technology that allows devices to communicate over short distances, typically up to 10 meters or 33 feet. If the device is too far from the headphones, the Bluetooth signal may be weak or interrupted, resulting in poor audio quality or loss of connection.

NEW QUESTION: 59
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 (LEAVE A REPLY)
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: 60
A new employee was hired recently. Which of the following documents will the new employee need to sign before being granted login access to the network?
A. MSDS
B. EULA
C. UAC
D. AUP
Answer: D (LEAVE A REPLY)
A new employee will need to sign an AUP before being granted login access to the network. An AUP is an Acceptable Use Policy that defines the rules and guidelines for using network resources and services in an organization. An AUP typically covers topics such as security, privacy, ethics, compliance and liability issues related to network usage. An AUP helps protect the organization and its users from legal, regulatory and reputational risks associated with network activities. An MSDS is a Material Safety Data Sheet that provides information about hazardous substances and how to handle them safely. An MSDS is not related to network access or usage. A EULA is an End User License Agreement that specifies the terms and conditions for using a software product or service. A EULA is usually provided by software vendors or developers and does not apply to network access or usage in general. A UAC is a User Account Control that is a security feature that prompts users for permission or confirmation before performing certain actions that require elevated privileges or affect system settings. A UAC is not a document that needs to be signed by users but a mechanism that helps prevent unauthorized changes or malware infections on a system. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.1

NEW QUESTION: 61
A systems administrator needs to reset a users password because the user forgot it. The systems administrator creates the new password and wants to further protect the user's account Which of the following should the systems administrator do?
A. Require the user to change the password at the next log-in.
B. Disallow tie user from changing the password.
C. Disable the account
D. Choose a password that never expires.
Answer: A (LEAVE A REPLY)

This will ensure that the user is the only one who knows their password, and that the new password is secure.
The CompTIA A+ Core 2 220-1002 exam covers this topic in the domain 1.4 Given a scenario, use appropriate data destruction and disposal methods.

NEW QUESTION: 62
A customer called the help desk to report that a machine that was recently updated is no longer working. The support technician checks the latest logs to see what updates were deployed, but nothing was deployed in more than three weeks. Which of the following should the support technician do to BEST resolve the situation?
A. Offer to wipe and reset the device for the customer.
B. Advise that the help desk will investigate and follow up at a later date.
C. Put the customer on hold and escalate the call to a manager.
D. Use open-ended questions to further diagnose the issue.
Answer: D (LEAVE A REPLY)
Open-ended questions are questions that require more than a yes or no answer and encourage the customer to provide more details and information. Using open-ended questions can help the support technician to understand the problem better, identify the root cause, and find a suitable solution. Some examples of open-ended questions are:
What exactly is not working on your machine?
When did you notice the problem?
How often does the problem occur?
What were you doing when the problem happened?
What have you tried to fix the problem?
Offering to wipe and reset the device for the customer is not a good option, as it may result in data loss and inconvenience for the customer. It should be used as a last resort only if other troubleshooting steps fail. Advising that the help desk will investigate and follow up at a later date is not a good option, as it may leave the customer unsatisfied and frustrated. It should be used only if the problem requires further research or escalation and cannot be resolved on the first call. Putting the customer on hold and escalating the call to a manager is not a good option, as it may waste time and resources. It should be used only if the problem is beyond the support technician's scope or authority and requires managerial intervention.

NEW QUESTION: 63
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: A,C (LEAVE A REPLY)
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.skillsoft.com/course/comptia-a-core-2-safety-procedures-environmental-impacts-cbdf0f2c-61c0-4f4a-a659-dc98f1f00158

NEW QUESTION: 64
A user receives the following error while attempting to boot a computer.
BOOTMGR is missing
press Ctrl+Alt+Del to restart
Which of the following should a desktop engineer attempt FIRST to address this issue?
A. Repair Windows.
B. Partition the hard disk.
C. Reimage the workstation.
D. Roll back the updates.
Answer: A (LEAVE A REPLY)
The error "BOOTMGR is missing" indicates that the boot sector is damaged or missing1. The boot sector is a part of the hard disk that contains the code and information needed to start Windows1. To fix this error, one of the possible methods is to run Startup Repair from Windows Recovery Environment (WinRE)1. Startup Repair is a tool that can automatically diagnose and repair problems with the boot process2.

NEW QUESTION: 65
A technician is working on a way to register all employee badges and associated computer IDs. Which of the following options should the technician use in order to achieve this objective?
A. Database system
B. Software management
C. Active Directory description

D. Infrastructure as a Service

Answer: A (LEAVE A REPLY)

A database system is a software application that allows storing, organizing, and managing data in a structured way. A database system can be used to register all employee badges and associated computer IDs by creating a table or a record for each employee that contains their badge number, computer ID, name, and other relevant information. A database system can also facilitate searching, updating, and deleting data as needed. Software management is a general term that refers to the process of planning, developing, testing, deploying, and maintaining software applications. It does not directly address the issue of registering employee badges and computer IDs. Active Directory description is a field in Active Directory that can be used to store additional information about an object, such as a user or a computer. It is not a software application that can be used to register employee badges and computer IDs by itself. Infrastructure as a Service (IaaS) is a cloud computing model that provides servers, storage, networking, and software over the internet. It does not directly address the issue of registering employee badges and computer IDs either.

https://www.idcreator.com/

https://www.alphacard.com/photo-id-systems/card-type/employee-badges

NEW QUESTION: 66

The command cac cor.pti

a. 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 comptia. txt would be displayed.

C. The contents of the text comptia.txt would be categorized in alphabetical order.

D. The contents of the text comptia. txt would be copied to another comptia. txt file

Answer: B (LEAVE A REPLY)

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: 67

A technician has just used an anti-malware removal tool to resolve a user's malware issue on a corporate laptop. Which of the following BEST describes what the technician should do before returning the laptop to the user?

A. Educate the user on malware removal.

B. Educate the user on how to reinstall the laptop OS.

C. Educate the user on how to access recovery mode.

D. Educate the user on common threats and how to avoid them.

Answer: D (LEAVE A REPLY)

educating the user on common threats and how to avoid them (D) would be a good step before returning the laptop to the user. This can help prevent similar issues from happening again.

NEW QUESTION: 68
A user requires local administrative access to a workstation. Which of the following Control Panel utilities allows the technician to grant access to the user?
A. System
B. Network and Sharing Center
C. User Accounts
D. Security and Maintenance
Answer: C (LEAVE A REPLY)
User Accounts is a Control Panel utility that allows the technician to manage user accounts and groups on a workstation1. The technician can use User Accounts to grant local administrative access to a user by adding the user to the Administrators group1. The Administrators group has full control over the workstation and can perform tasks such as installing software, changing system settings, and accessing all files.

NEW QUESTION: 69
A user rotates a cell phone horizontally to read emails, but the display remains vertical, even though the settings indicate autorotate is on. VT1ich of the following will MOST likely resolve the issue?
A. Recalibrating the magnetometer
B. Recalibrating the compass
C. Recalibrating the digitizer
D. Recalibrating the accelerometer
Answer: D (LEAVE A REPLY)
When a user rotates a cell phone horizontally to read emails and the display remains vertical, even though the settings indicate autorotate is on, this is typically due to a problem with the phone's accelerometer. The accelerometer is the sensor that detects changes in the phone's orientation and adjusts the display accordingly. If the accelerometer is not calibrated correctly, the display may not rotate as expected.
Recalibrating the accelerometer is the most likely solution to this issue. The process for recalibrating the accelerometer can vary depending on the specific device and operating system, but it typically involves going to the device's settings and finding the option to calibrate or reset the sensor. Users may need to search their device's documentation or online resources to find specific instructions for their device.

NEW QUESTION: 70
A technician installed a new application on a workstation. For the program to function properly, it needs to be listed in the Path Environment Variable. Which of the following Control Panel utilities should the technician use?
A. System
B. Indexing Options
C. Device Manager

D. Programs and Features

Answer: (SHOW ANSWER)

System is the Control Panel utility that should be used to change the Path Environment Variable. The Path Environment Variable is a system variable that specifies the directories where executable files are located. To edit the Path Environment Variable, the technician should go to System > Advanced system settings > Environment Variables and then select Path from the list of system variables and click Edit.

NEW QUESTION: 71

A technician installed a known-good, compatible motherboard on a new laptop. However, the motherboard is not working on the laptop. Which of the following should the technician MOST likely have done to prevent damage?

A. Removed all jewelry

B. Completed an inventory of tools before use

C. Practiced electrical fire safety

D. Connected a proper ESD strap

Answer: D (LEAVE A REPLY)

The technician should have connected a proper ESD strap to prevent damage to the motherboard. ESD (electrostatic discharge) can cause damage to electronic components, and an ESD strap helps to prevent this by grounding the technician and preventing the buildup of static electricity. Removing all jewelry is also a good practice, but it is not the most likely solution to this problem.

NEW QUESTION: 72

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

A. Pretexting

B. Spoofing

C. Vishing

D. Scareware

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 73

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. ehkdsk

C. git clone

D. zobocopy

Answer: (SHOW ANSWER)

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: 74

A technician is configuring a SOHO device Company policy dictates that static IP addresses cannot be used. The company wants the server to maintain the same IP address at all times. Which of the following should the technician use?

A. DHCP reservation

B. Port forwarding

C. DNS A record

D. NAT

Answer: A (LEAVE A REPLY)

The technician should use DHCP reservation to maintain the same IP address for the server at all times. DHCP reservation allows the server to obtain an IP address dynamically from the DHCP server, while ensuring that the same IP address is assigned to the server each time it requests an IP address.

NEW QUESTION: 75

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: (SHOW ANSWER)

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

NEW QUESTION: 76

A technician at a customer site is troubleshooting a laptop A software update needs to be downloaded but the company's proxy is blocking traffic to the update site. Which of the following should the technician perform?

A. Change the DNS address to 1.1.1.1

B. Update Group Policy

C. Add the site to the client's exceptions list
D. Verity the software license is current.
Answer: C (LEAVE A REPLY)
The technician should add the update site to the client's exceptions list to bypass the proxy. This can be done through the client's web browser settings, where the proxy settings can be configured. By adding the update site to the exceptions list, the client will be able to access the site and download the software update.

NEW QUESTION: 77
A help desk team lead contacts a systems administrator because the technicians are unable to log in to a Linux server that is used to access tools. When the administrator tries to use remote desktop to log in to the server, the administrator sees the GUI is crashing. Which of the following methods can the administrator use to troubleshoot the server effectively?
A. SFTP
B. SSH
C. VNC
D. MSRA
Answer: (SHOW ANSWER)
The administrator can use Virtual Network Computing (VNC) to troubleshoot the server effectively. VNC is a graphical desktop sharing system that allows the administrator to remotely control the desktop of a Linux server.

NEW QUESTION: 78
Which of the following is MOST likely used to run .vbs files on Windows devices?
A. winmgmt.exe
B. powershell.exe
C. cscript.exe
D. explorer.exe
Answer: (SHOW ANSWER)
A .vbs file is a Virtual Basic script written in the VBScript scripting language. It contains code that can be executed within Windows via the Windows-based script host (Wscript.exe), to perform certain admin and processing functions1. Cscript.exe is a command-line version of the Windows

Script Host that provides command-line options for setting script properties. Therefore, cscript.exe is most likely used to run .vbs files on Windows devices. Reference: 1: https://fileinfo.com/extension/vbs : https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/cscript

NEW QUESTION: 79
A user is unable to log in to the network. The network uses 802.1X with EAP-TLS to authenticate on the wired network. The user has been on an extended leave and has not logged in to the computer in several months. Which of the following is causing the login issue?
A. Expired certificate
B. OS update failure
C. Service not started
D. Application crash
E. Profile rebuild needed
Answer: (SHOW ANSWER)
EAP-TLS is a method of authentication that uses certificates to establish a secure tunnel between the client and the server3. The certificates have a validity period and must be renewed before they expire1. If the user has been on an extended leave and has not logged in to the computer in several months, it is possible that the certificate on the client or the server has expired and needs to be renewed2. The other options are not directly related to EAP-TLS authentication or 802.1X network access.

NEW QUESTION: 80
A systems administrator is setting up a Windows computer for a new user Corporate policy requires a least privilege environment. The user will need to access advanced features and configuration settings for several applications. Which of the following BEST describes the account access level the user will need?
A. Power user account
B. Standard account
C. Guest account
D. Administrator account
Answer: (SHOW ANSWER)
The account access level the user will need to access advanced features and configuration settings for several applications while adhering to corporate policy requiring a least privilege environment is a standard account. This is because a standard account allows the user to access advanced features and configuration settings for several applications while adhering to corporate policy requiring a least privilege environment1.

NEW QUESTION: 81

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 (LEAVE A REPLY)

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: 82

A user is trying to use a third-party USB adapter but is experiencing connection issues. Which of the following tools should the technician use to resolve this issue?

A. taskschd.msc

B. eventvwr.msc

C. de vmgmt. msc

D. diskmgmt.msc

Answer: C (LEAVE A REPLY)

The tool that the technician should use to resolve the connection issues with the third-party USB adapter is devmgmt.msc. Devmgmt.msc is a command that opens the Device Manager, which is a utility that allows users to view and manage the hardware devices and drivers installed on a computer. The technician can use the Device Manager to check the status, properties and compatibility of the USB adapter and its driver, and perform actions such as updating, uninstalling or reinstalling the driver, enabling or disabling the device, or scanning for hardware changes. Taskschd.msc is a command that opens the Task Scheduler, which is a utility that allows users to create and manage tasks that run automatically at specified times or events. The Task Scheduler is not relevant or useful for resolving connection issues with the USB adapter. Eventvwr.msc is a command that opens the Event Viewer, which is a utility that allows users to view and monitor the system logs and events. The Event Viewer may provide some information or clues about the connection issues with the USB adapter, but it does not allow users to manage or troubleshoot the device or its driver directly. Diskmgmt.msc is a command that opens the Disk Management, which is a utility that allows users to view and manage the disk drives and partitions on a computer. The Disk Management is not relevant or useful for resolving connection issues with the USB adapter. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

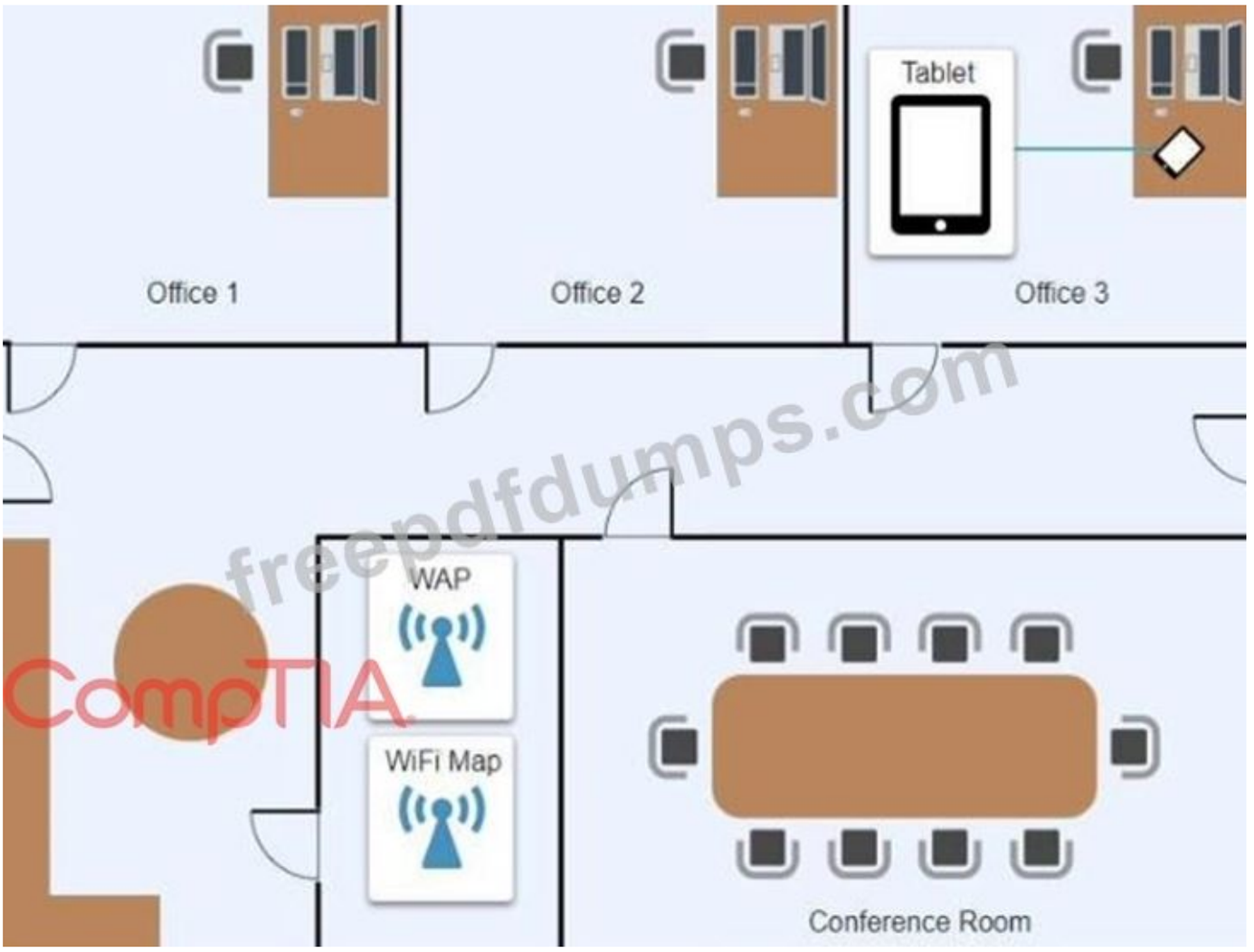
NEW QUESTION: 83

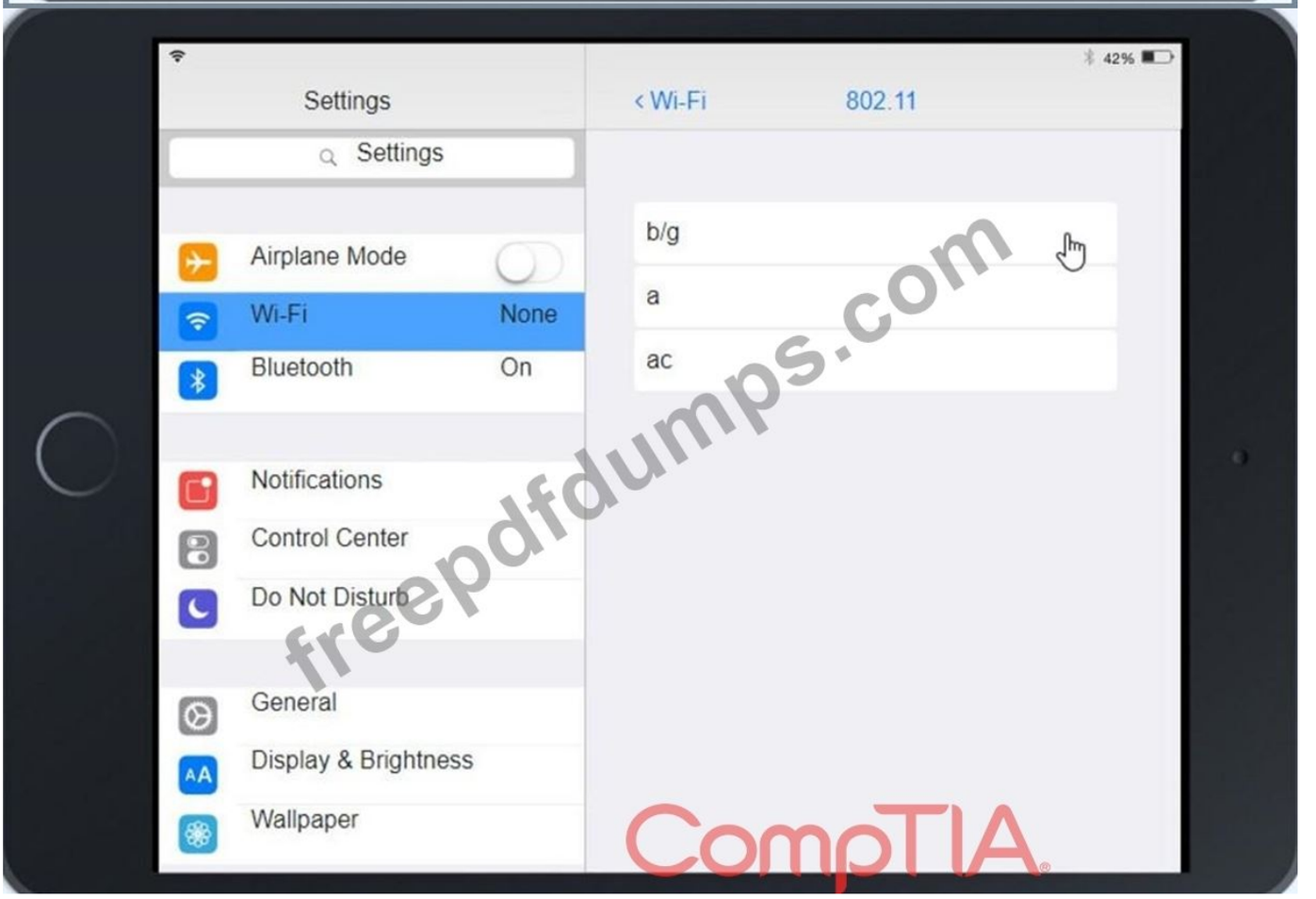
Ann, a CEO, has purchased a new consumer-class tablet for personal use, but she is unable to connect it to the company's wireless network. All the corporate laptops are connecting without issue. She has asked you to assist with getting the device online.

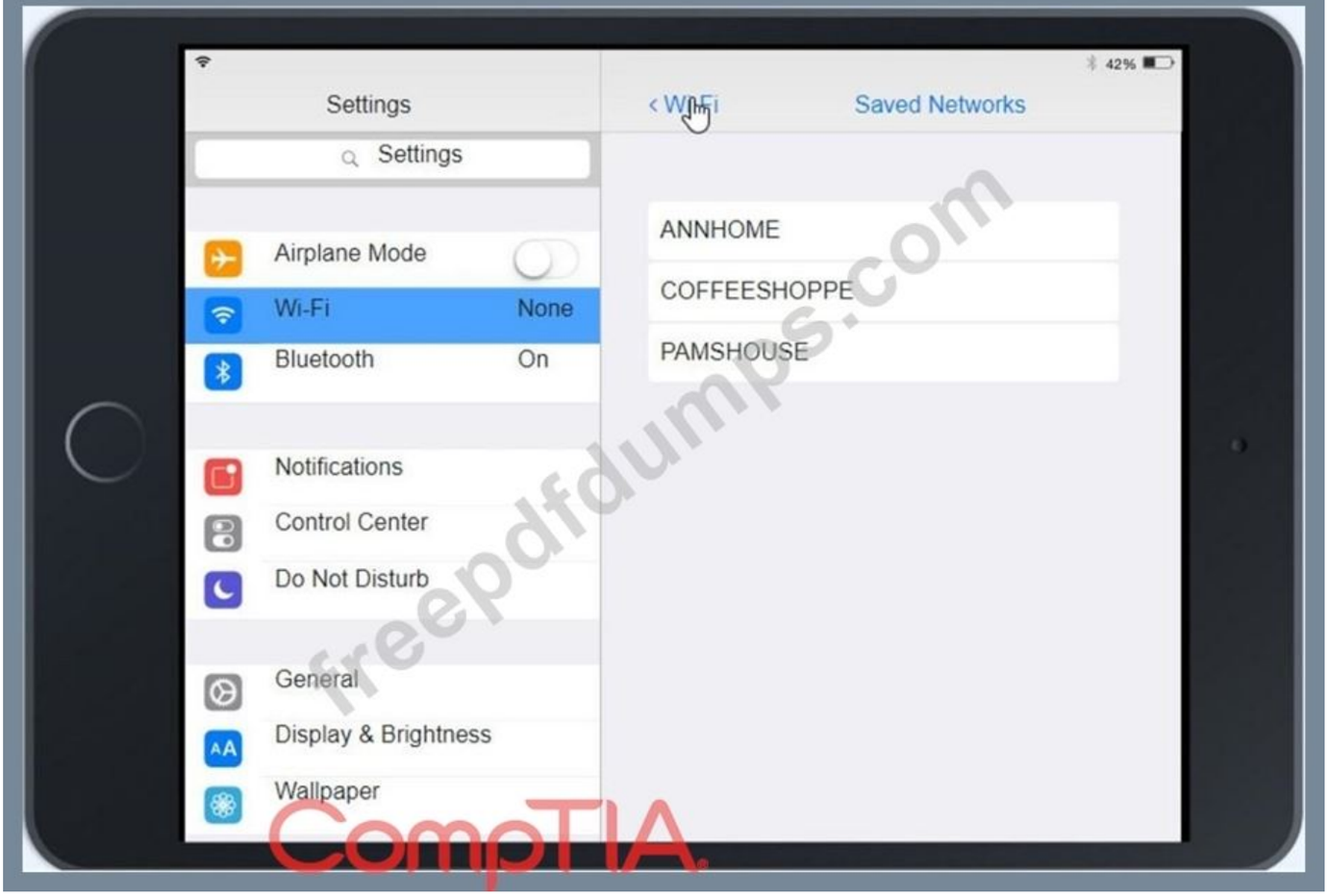
INSTRUCTIONS

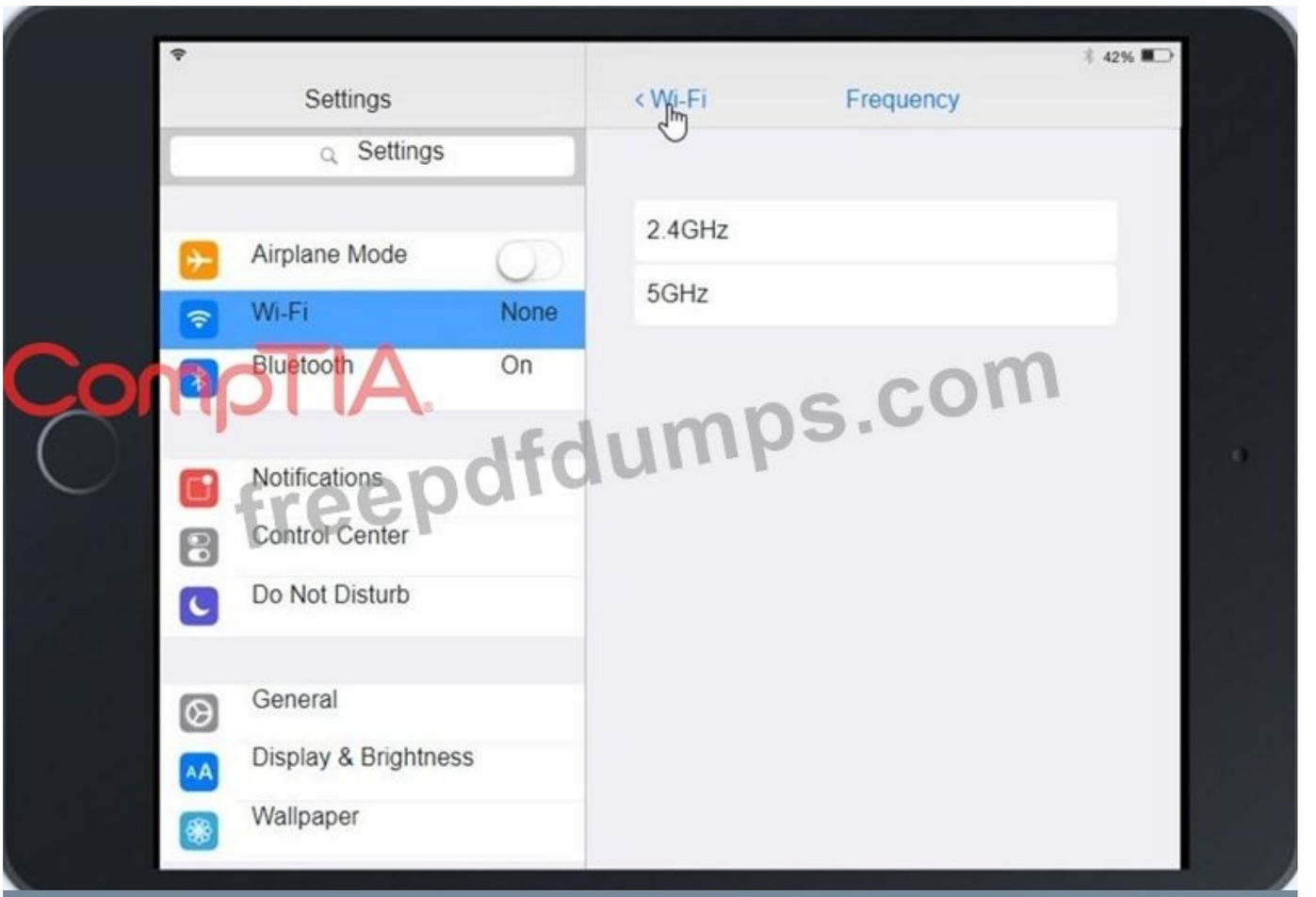
Review the network diagrams and device configurations to determine the cause of the problem and resolve any discovered issues.

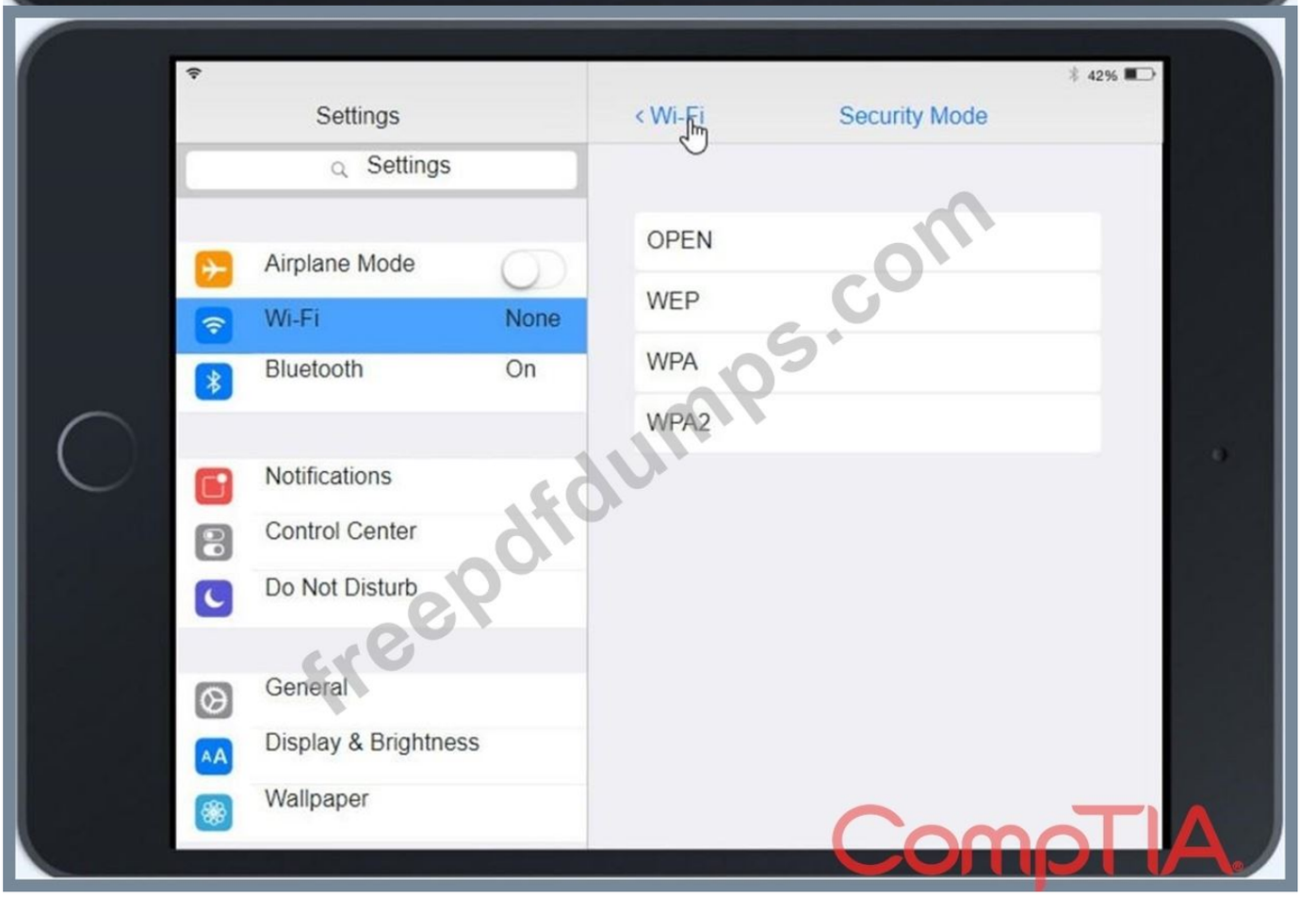
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

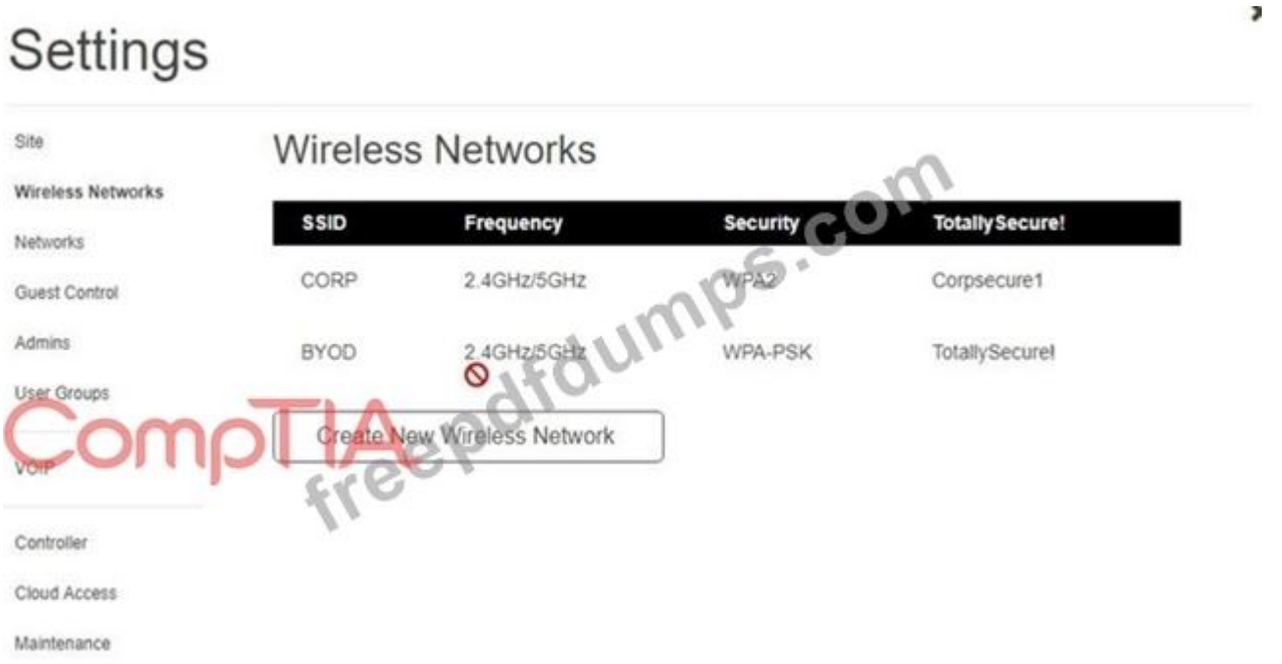


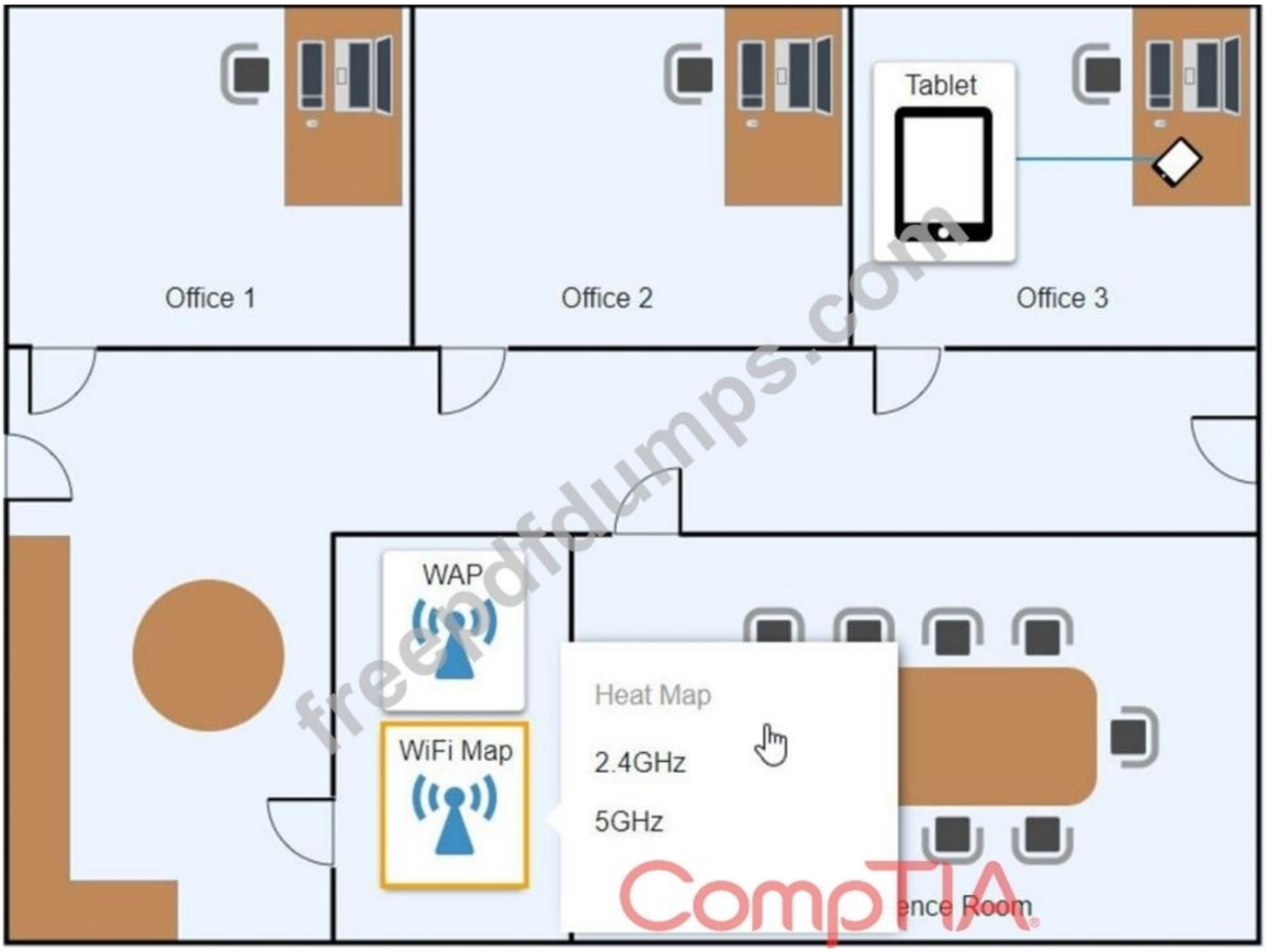









Settings
Site
Wireless Networks
Networks
Guest Control
Admins
User Groups
VOIP
Controller
Cloud Access
Maintenance
Wireless Networks
SSID
Frequency
Security
Totally Secure!
CORP
2.4GHz/5GHz
WPA2
Corpsecure1
BYOD
2.4GHz/5GHz
WPA-PSK
TotallySecure!
Create New Wireless Network

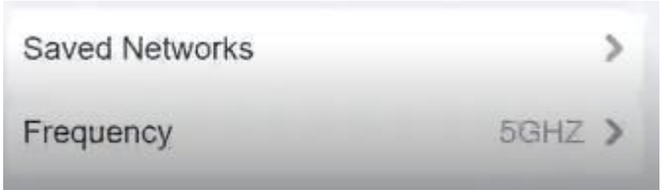

Tablet
Office 1
Office 2
Office 3
WAP
WiFi Map
Heat Map
2.4GHz
5GHz
ence Room

Answer:

Click on 802.11 and Select ac

Click on SSID and select CORP

Click on Frequency and select 5GHz



At Wireless Security Mode, Click on Security Mode

Select the WPA2

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.

NEW QUESTION: 84
A desktop specialist needs to prepare a laptop running Windows 10 for a newly hired employee. Which of the following methods should the technician use to refresh the laptop?
A. Internet-based upgrade
B. Repair installation
C. Clean install
D. USB repair
E. In place upgrade
Answer: C (LEAVE A REPLY)
The desktop specialist should use a clean install to refresh the laptop. A clean install will remove all data and applications from the laptop and install a fresh copy of Windows 10, ensuring that the laptop is ready for the newly hired employee.

NEW QUESTION: 85
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 (LEAVE A REPLY)
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 macOS1.

NEW QUESTION: 86
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 (LEAVE A REPLY)
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: 87
Which of the following Wi-Fi protocols is the MOST secure?
A. WPA3
B. WPA-AES
C. WEP
D. WPA-TKIP
Answer: A (LEAVE A REPLY)
https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0)

NEW QUESTION: 88
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 (LEAVE A REPLY)
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: 89
A systems administrator is creating a new document with a list of the websites that users are allowed to access. Which of the following types of documents is the administrator MOST likely creating?
A. Access control list
B. Acceptable use policy
C. Incident report
D. Standard operating procedure
Answer: A (LEAVE A REPLY)
An access control list (ACL) is a list of permissions associated with a system resource (object), such as a website. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects1. A systems administrator can create an ACL to define the list of websites that users are allowed to access.

NEW QUESTION: 90
A junior administrator is responsible for deploying software to a large group of computers in an organization. The administrator finds a script on a popular coding website to automate this distribution but does not understand the scripting language. Which of the following BEST describes the risks in running this script?
A. The instructions from the software company are not being followed.
B. Security controls will treat automated deployments as malware.
C. The deployment script is performing unknown actions.
D. Copying scripts off the internet is considered plagiarism.
Answer: C (LEAVE A REPLY)
The risks in running this script are that the deployment script is performing unknown actions. Running the script blindly could cause unintended actions, such as deploying malware or deleting important files, which could negatively impact the organization's network and data1.

NEW QUESTION: 91
A macOS user needs to create another virtual desktop space. Which of the following applications will allow the user to accomplish this task?
A. Dock
B. Spotlight
C. Mission Control
D. Launchpad
Answer: (SHOW ANSWER)
application that will allow a macOS user to create another virtual desktop space is Mission Control Mission Control lets you create additional desktops, called spaces, to organize the windows of your apps. You can create a space by entering Mission Control and clicking the Add

button in the Spaces bar1. You can also assign apps to specific spaces and move between them easily1.

NEW QUESTION: 92
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: (SHOW ANSWER)
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: 93
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 (LEAVE A REPLY)
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: 94
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 (LEAVE A REPLY)
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: 95
A network technician installed a SOHO router for a home office user. The user has read reports about home routers being targeted by malicious actors and then used in DDoS attacks. Which of the following can the technician MOST likely do to defend against this threat?
A. Add network content filtering.
B. Disable the SSID broadcast.
C. Configure port forwarding.
D. Change the default credentials.
Answer: D (LEAVE A REPLY)
One of the most effective ways to defend against malicious actors targeting home routers for DDoS attacks is to change the default credentials of the router. The default credentials are often well-known or easily guessed by attackers, who can then access and compromise the router settings and firmware. By changing the default credentials to strong and unique ones, a technician can prevent unauthorized access and configuration changes to the router. Adding network content filtering may help block some malicious or unwanted websites but may not prevent attackers from exploiting router vulnerabilities or backdoors. Disabling the SSID broadcast may help reduce the visibility of the wireless network but may not prevent attackers from scanning or detecting it. Configuring port forwarding may help direct incoming traffic to specific devices or services but may not prevent attackers from sending malicious packets or requests to the router. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

NEW QUESTION: 96

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: (SHOW ANSWER)

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: 97

While browsing a website, a staff member received a message that the website could not be trusted. Shortly afterward, several other colleagues reported the same issue across numerous other websites. Remote users who were not connected to corporate resources did not have any issues. Which of the following is MOST likely the cause of this issue?

A. A bad antivirus signature update was installed.

B. A router was misconfigured and was blocking traffic.

C. An upstream internet service provider was flapping.

D. The time or date was not in sync with the website.

Answer: (SHOW ANSWER)

The most likely cause of this issue is that a router was misconfigured and was blocking traffic. This would explain why remote users who were not connected to corporate resources did not have any issues.

NEW QUESTION: 98

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: (SHOW ANSWER)

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

NEW QUESTION: 99
A technician is working to resolve a Wi-Fi network issue at a doctor's office that is located next to an apartment complex. The technician discovers that employees and patients are not the only people on the network. Which of the following should the technician do to BEST minimize this issue?
A. Disable unused ports.
B. Remove the guest network
C. Add a password to the guest network
D. Change the network channel.
Answer: D (LEAVE A REPLY)
Changing the network channel is the best solution to minimize the issue of employees and patients not being the only people on the Wi-Fi network5

NEW QUESTION: 100
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 (LEAVE A REPLY)
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 authorized2.
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: 101
A user lost a company tablet that was used for customer intake at a doctor's office. Which of the following actions would BEST protect against unauthorized access of the data?
A. Changing the office's Wi-Fi SSID and password
B. Performing a remote wipe on the device
C. Changing the user's password
D. Enabling remote drive encryption
Answer: (SHOW ANSWER)

The best action to protect against unauthorized access of the data on the lost company tablet is to perform a remote wipe on the device. A remote wipe is a feature that allows an administrator or a user to erase all the data and settings on a device remotely, usually through a web portal or an email command. A remote wipe can help prevent the data from being accessed or compromised by anyone who finds or steals the device. Changing the office's Wi-Fi SSID and password may prevent the device from connecting to the office network but may not prevent the data from being accessed locally or through other networks. Changing the user's password may prevent the device from logging in to the user's account but may not prevent the data from being accessed by other means or accounts. Enabling remote drive encryption may protect the data from being read by unauthorized parties but may not be possible if the device is already lost or turned off.
Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.1

NEW QUESTION: 102
A user connected a laptop to a wireless network and was tricked into providing login credentials for a website. Which of the following threats was used to carry out the attack?
A. Zero day
B. Vishing
C. DDoS
D. Evil twin
Answer: B (LEAVE A REPLY)
Vishing, also known as voice phishing, is a type of social engineering attack where the attacker tricks the victim into divulging sensitive information over the phone. In this case, the attacker tricked the user into providing login credentials for a website.

NEW QUESTION: 103
A wireless network is set up, but it is experiencing some interference from other nearby SSIDs. Which of the following can BEST resolve the interference?
A. Changing channels
B. Modifying the wireless security
C. Disabling the SSIO broadcast
D. Changing the access point name
Answer: A (LEAVE A REPLY)
Changing channels can best resolve interference from other nearby SSIDs. Wireless networks operate on different channels, and changing the channel can help to avoid interference from other nearby networks.

NEW QUESTION: 104
A technician needs to interconnect two offices to the main branch while complying with good practices and security standards. Which of the following should the technician implement?
A. MSRA

B. VNC
C. VPN
D. SSH
Answer: C (LEAVE A REPLY)
A technician needs to interconnect two offices to the main branch while complying with good practices and security standards. The technician should implement VPN

NEW QUESTION: 105
A technician, who is working at a local office, has found multiple copies of home edition software installed on computers. Which of the following does this MOST likely violate?
A. EULA
B. PII
C. DRM
D. Open-source agreement
Answer: (SHOW ANSWER)
The installation of home edition software on computers at a local office most likely violates the EULA. EULA stands for End User License Agreement and is a legal contract that specifies the terms and conditions for using a software product or service. EULA typically covers topics such as license scope, duration and limitations, rights and obligations of the parties, warranties and disclaimers, liability and indemnity clauses, and termination procedures. EULA may also restrict the use of home edition software to personal or non-commercial purposes only, and prohibit the use of home edition software in business or professional settings. Violating EULA may result in legal actions or penalties from the software vendor or developer. PII stands for Personally Identifiable Information and is any information that can be used to identify or locate an individual, such as name, address, phone number, email address, social security number or credit card number. PII is not related to software installation or licensing but to data protection and privacy. DRM stands for Digital Rights Management and is a technology that controls or restricts the access and use of digital content, such as music, movies, books or games. DRM is not related to software installation or licensing but to content distribution and piracy prevention. Open-source agreement is a type of license that allows users to access, modify and distribute the source code of a software product or service freely and openly. Open-source agreement does not restrict the use of software to home edition only but encourages collaboration and innovation among developers and users. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.1

NEW QUESTION: 106
A user reports that after a recent software deployment to upgrade applications, the user can no longer use the Testing program.
However, other employees can successfully use the Testing program.
INSTRUCTIONS

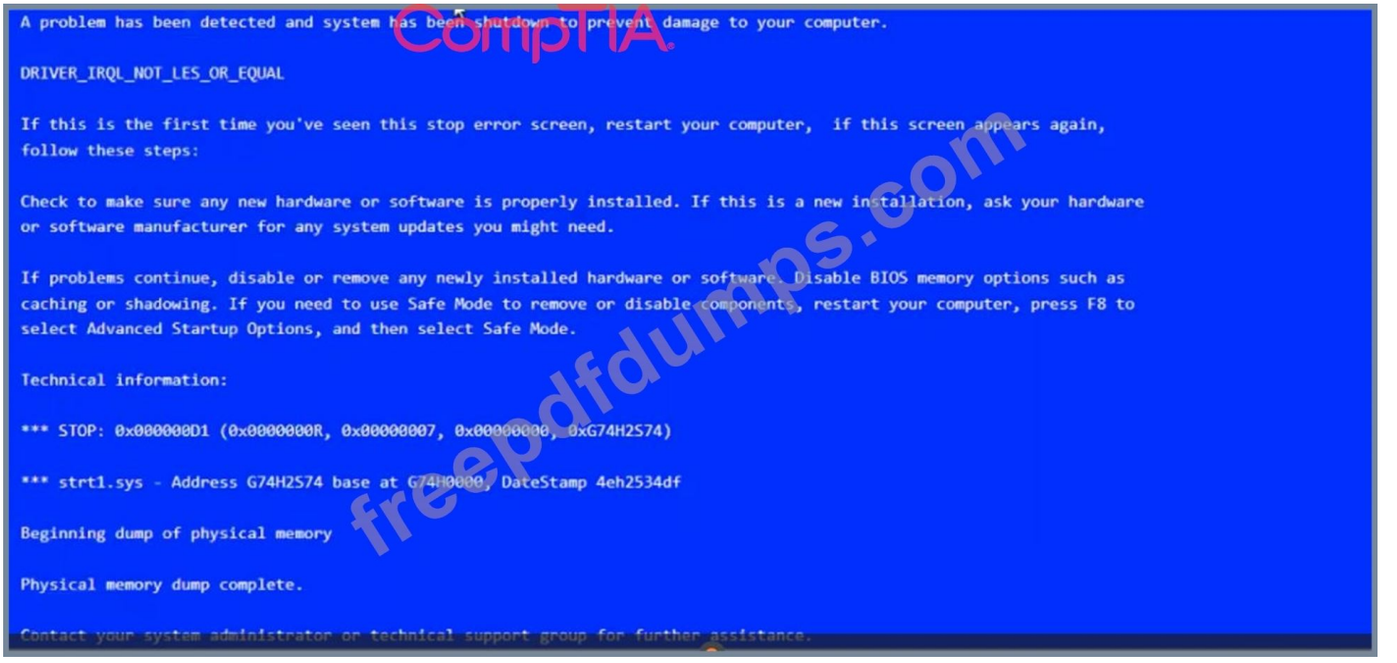
Review the information in each tab to verify the results of the deployment and resolve any issues discovered by selecting the:

Index number of the Event Viewer issue

First command to resolve the issue

Second command to resolve the issue

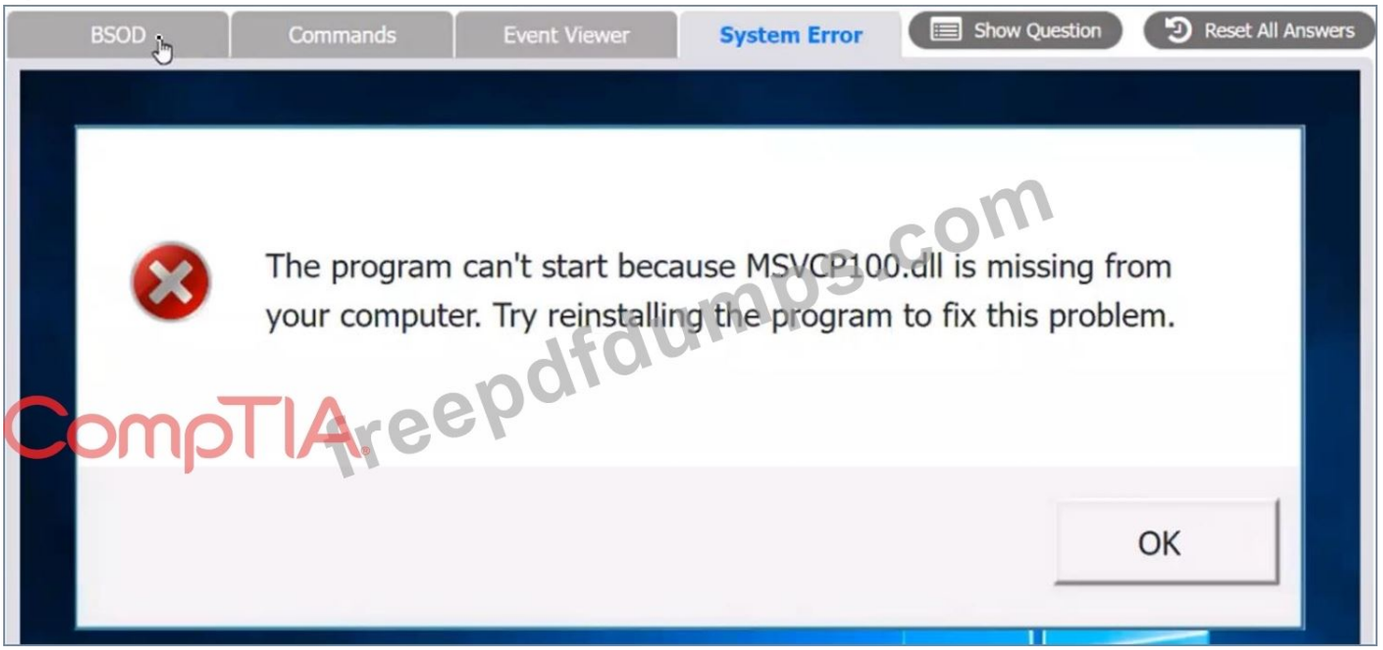
BSOD



Commands:

Event Viewer:

System Error:



A. Pending

Answer: A (LEAVE A REPLY)

Valid 220-1102 Dumps shared by Actual4test.com for Helping Passing 220-1102 Exam! Actual4test.com now offer the **newest 220-1102 exam dumps**, the Actual4test.com 220-1102 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 220-1102 dumps with Test Engine here: https://www.actual4test.com/220-1102_examcollection.html (**845** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 107

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 file server is offline.

B. The user is not connected to the VPN.

C. A low battery is preventing the connection.

D. The log-in script failed.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 108

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

A. acceptable use policy.

B. regulatory compliance requirements.

C. non-disclosure agreement

D. incident response procedures

Answer: A (LEAVE A REPLY)

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: 109

A user's mobile phone has become sluggish A systems administrator discovered several malicious applications on the device and reset the phone. The administrator installed MDM software. Which of the following should the administrator do to help secure the device against this threat in the future? (Select TWO).

A. Prevent a device root

B. Disable biometric authentication

C. Require a PIN on the unlock screen

D. Enable developer mode

E. Block a third-party application installation

F. Prevent GPS spoofing

Answer: C,E (LEAVE A REPLY)

To help secure the device against this threat in the future, the administrator should require a PIN on the unlock screen and block a third-party application installation. Requiring a PIN on the unlock screen can help to prevent unauthorized access to the device, while blocking third-party application installation can help to prevent malicious applications from being installed on the device.

NEW QUESTION: 110
A user is attempting to browse the internet using Internet Explorer. When trying to load a familiar web page, the user is unexpectedly redirected to an unfamiliar website. Which of the following would MOST likely solve the issue?
A. Updating the operating system
B. Changing proxy settings
C. Reinstalling the browser
D. Enabling port forwarding
Answer: C (LEAVE A REPLY)
Reinstalling the browser would most likely solve the issue. This would remove any malicious software or add-ons that may be causing the issue and restore the browser to its default settings.

NEW QUESTION: 111
A user is unable to log in to the domain with a desktop PC, but a laptop PC is working properly on the same network. A technician logs in lo the desktop PC with a local account but is unable to browse to the secure intranet site to get troubleshooting tools. Which of the following is the MOST likely cause of the issue?
A. Time drift
B. Dual in-line memory module failure
C. Application crash
D. Filesystem errors
Answer: A (LEAVE A REPLY)
The most likely cause of the issue is a "time drift". Time drift occurs when the clock on a computer is not synchronized with the clock on the domain controller. This can cause authentication problems when a user tries to log in to the domain. The fact that the technician is unable to browse to the secure intranet site to get troubleshooting tools suggests that there may be a problem with the network connection or the firewall settings on the desktop PC12

NEW QUESTION: 112
A technician is troubleshooting a PC that has been performing poorly. Looking at the Task Manager, the technician sees that CPU and memory resources seem fine, but disk throughput is at 100%.
Which of the following types of malware is the system MOST likely infected with?
A. Keylogger
B. Rootkit
C. Ransomware
D. Trojan
Answer: C (LEAVE A REPLY)

Ransomware is a type of malware that encrypts the files on the victim's computer and demands a ransom for their decryption. Ransomware can cause high disk throughput by encrypting large amounts of data in a short time.

NEW QUESTION: 113
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 (LEAVE A REPLY)
Shredding is the most effective method to securely dispose of data stored on optical discs12

NEW QUESTION: 114
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 (LEAVE A REPLY)
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: 115
A manager called the help desk to ask for assistance with creating a more secure environment for the finance department- which resides in a non-domain environment. Which of the following would be the BEST method to protect against unauthorized use?
A. Implementing password expiration
B. Restricting user permissions
C. Using screen locks
D. Disabling unnecessary services
Answer: B (LEAVE A REPLY)

Restricting user permissions is a method of creating a more secure environment for the finance department in a non-domain environment. This means that users will only have access to the files and resources that they need to perform their tasks and will not be able to modify or delete other files or settings that could compromise security or functionality.

NEW QUESTION: 116
A user receives a call from someone who claims to be from the user's bank and requests information to ensure the user's account is safe. Which of the following social-engineering attacks is the user experiencing?
A. Phishing
B. Smishing
C. Whaling
D. Vishing
Answer: D (LEAVE A REPLY)
The user is experiencing a vishing attack. Vishing stands for voice phishing and is a type of social-engineering attack that uses phone calls or voice messages to trick users into revealing personal or financial information. Vishing attackers often pretend to be from legitimate organizations, such as banks, government agencies or service providers, and use various tactics, such as urgency, fear or reward, to persuade users to comply with their requests. Phishing is a type of social-engineering attack that uses fraudulent emails or websites to trick users into revealing personal or financial information. Phishing does not involve phone calls or voice messages. Smishing is a type of social-engineering attack that uses text messages or SMS to trick users into revealing personal or financial information. Smishing does not involve phone calls or voice messages. Whaling is a type of social-engineering attack that targets high-profile individuals, such as executives, celebrities or politicians, to trick them into revealing personal or financial information. Whaling does not necessarily involve phone calls or voice messages.
Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.1

NEW QUESTION: 117
A company discovered that numerous computers from multiple geographic locations are sending a very high number of connection requests which is causing the company's web server to become unavailable to the general public. Which of the following attacks is occurring?
A. Zero day
B. SOL injection
C. Cross-site scripting
D. Distributed denial of service
Answer: (SHOW ANSWER)
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: 118
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: (SHOW ANSWER)
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: 119
Which of the following data is MOST likely to be regulated?
A. Name in a Phone book
B. Name on a medical diagnosis
C. Name on a job application
D. Name on a employer's website
Answer: (SHOW ANSWER)
A name on a medical diagnosis (B) is most likely to be regulated. This is because it falls under the category of protected health information (PHI), which is subject to regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. These regulations aim to protect the privacy and security of individuals' health information.

NEW QUESTION: 120

An organization is centralizing support functions and requires the ability to support a remote user's desktop. Which of the following technologies will allow a technician to see the issue along with the user?

A. RDP

B. VNC

C. SSH

D. VPN

Answer: B (LEAVE A REPLY)

VNC will allow a technician to see the issue along with the user when an organization is centralizing support functions and requires the ability to support a remote user's desktop1

NEW QUESTION: 121

Which of the following OS types provides a lightweight option for workstations thai need an easy-to-use browser-based interface?

A. FreeBSD

B. Chrome OS

C. macOS

D. Windows

Answer: (SHOW ANSWER)

Chrome OS provides a lightweight option for workstations that need an easy-to-use browser-based interface1

NEW QUESTION: 122

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

A. Battery disposal

B. Electrostatic discharge mats

C. Toner disposal

D. Humidity levels

Answer: D (LEAVE A REPLY)

One of the most important environmental concerns inside a data center is the level of humidity. High levels of humidity can cause condensation, which can result in corrosion of components and other equipment. Low levels of humidity can cause static electricity to build up, potentially leading

to electrostatic discharge (ESD) and damage to components. Therefore, it is crucial to maintain a relative humidity range of 40-60% in a data center to protect the equipment and ensure proper operation.

NEW QUESTION: 123
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 (LEAVE A REPLY)
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: 124
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: (SHOW ANSWER)
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: 125
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 (LEAVE A REPLY)
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: 126
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 (LEAVE A REPLY)
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: 127
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. msinf032exe
D. msconfig_exe
Answer: A (LEAVE A REPLY)
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/O1. Resource Monitor provides detailed information about the system's resource usage, including disk I/O1. The technician can use this information to identify the process that is causing the high disk I/O and take appropriate action1.

NEW QUESTION: 128
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 (LEAVE A REPLY)
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: 129
A user is configuring a new SOHO Wi-Fi router for the first time. Which of the following settings should the user change FIRST?
A. Encryption
B. Wi-Fi channel
C. Default passwords
D. Service set identifier
Answer: C (LEAVE A REPLY)
the user should change the default passwords first when configuring a new SOHO Wi-Fi router1