

CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2



NEW QUESTION 1

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

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

Answer: A

Explanation:

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

NEW QUESTION 2

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

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

Answer: C

Explanation:

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

NEW QUESTION 3

A technician is troubleshooting a lack of outgoing audio on a third-party Windows 10 VoIP application. The PC uses a USB microphone connected to a powered hub. The technician verifies the microphone works on the PC using Voice Recorder. Which of the following should the technician do to solve the issue?

- A. Remove the microphone from the USB hub and plug it directly into a USB port on the PC.
- B. Enable the microphone under Windows Privacy settings to allow desktop applications to access it.
- C. Delete the microphone from Device Manager and scan for new hardware.
- D. Replace the USB microphone with one that uses a traditional 3.5mm plug.

Answer: B

Explanation:

In Windows 10, there are privacy settings that control access to certain devices, such as microphones, cameras, and other input devices. If the microphone is not enabled under these privacy settings, the VoIP application may not have access to it, causing a lack of outgoing audio. The technician can go to the Windows 10 Settings menu, select the Privacy submenu, and under App permissions, select Microphone. The technician should then turn on the toggle switch for the VoIP application to allow it to access the microphone. Removing the microphone from the USB hub and plugging it directly into a USB port on the PC may or may not solve the issue, as the issue could be related to the privacy settings. Deleting the microphone from Device Manager and scanning for new hardware may also not solve the issue, as the issue could be related to the privacy settings. Replacing the USB microphone with one that uses a traditional 3.5mm plug is not recommended, as it would require purchasing a new microphone and may not solve the issue.

NEW QUESTION 4

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: C

Explanation:

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 source.

NEW QUESTION 5

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

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

Answer: B

Explanation:

The user should install and run Linux and the required application as a virtual machine installed under the Windows OS. This solution would allow for parallel execution of the Linux application and Windows applications2.

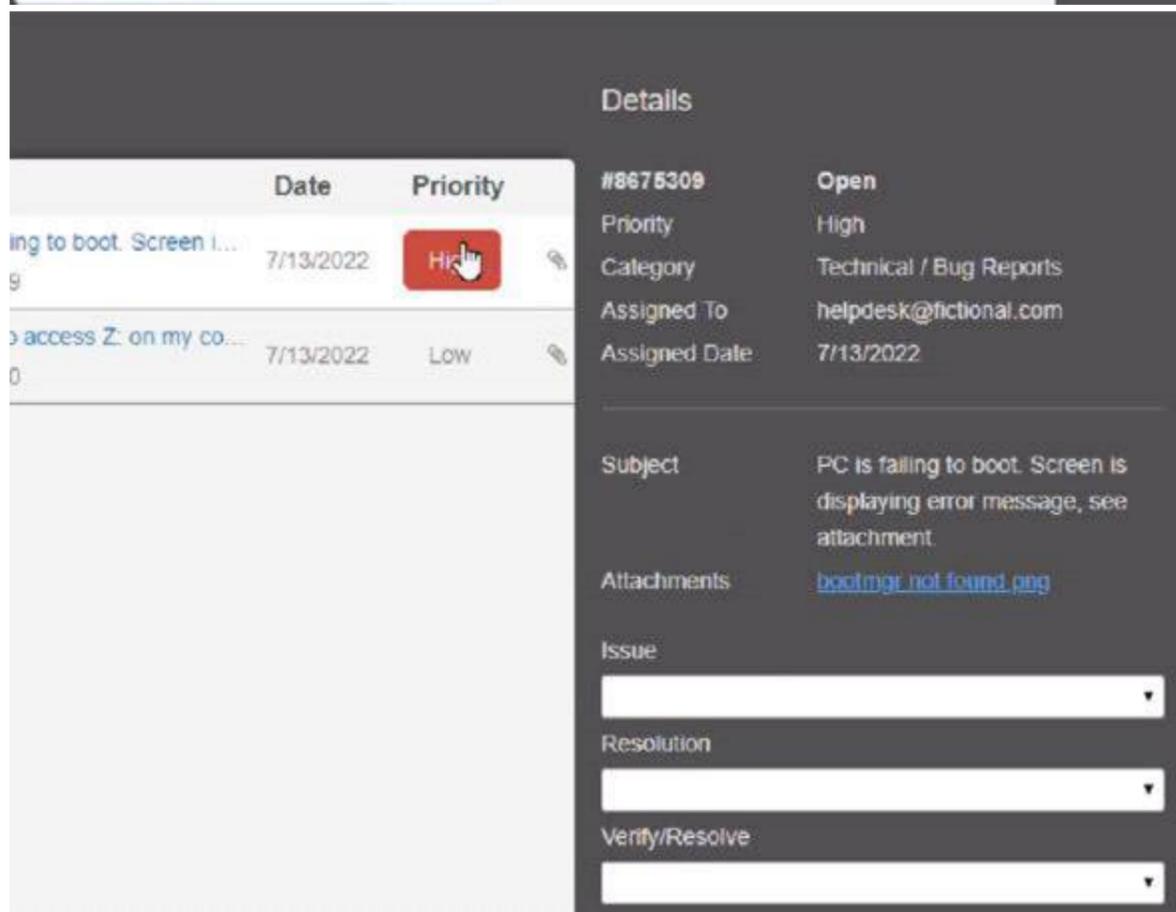
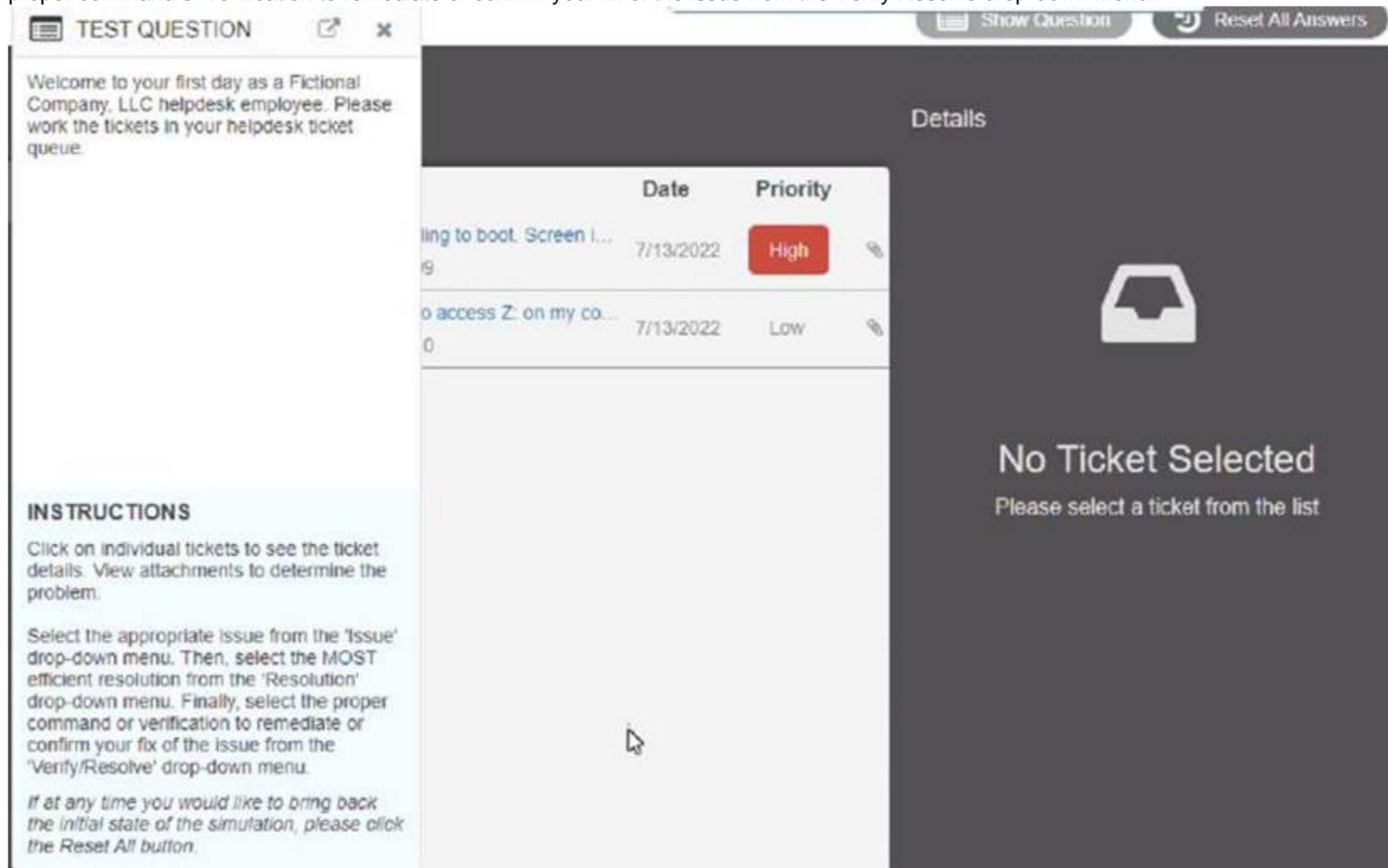
The MOST efficient solution that allows for parallel execution of the Linux application and Windows applications is to install and run Linux and the required application as a virtual machine installed under the Windows OS. This is because it allows you to run both Linux and Windows together without the need to keep the Linux portion confined to a VM window3.

NEW QUESTION 6

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

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

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



The screenshot displays a helpdesk interface. On the left, a table lists tickets with columns for 'Date' and 'Priority'. The first ticket is titled 'ing to boot. Screen i...' with a date of 7/13/2022 and a priority of 'High'. The second ticket is 'x access Z: on my co...' with a date of 7/13/2022 and a priority of 'Low'. A 'Details' panel for ticket #8675309 is open, showing it is 'Open' with a 'High' priority, assigned to 'helpdesk@fictional.com' on 7/13/2022. The subject is 'PC is failing to boot. Screen is displaying error message, see attachment.' An attachment 'bootmgr not found.png' is listed. Below the details, an 'Issue' dropdown menu is open, showing a list of technical categories such as 'Corrupt OS', 'Recent Windows Updates', 'Graphics Drive Updates', 'BSOD', 'Printing Issues', 'Limited Network Connectivity', 'Services Failed to Start', 'User Profile is Corrupted', 'Application Crash', 'User cannot access shared resource', 'URL contains typo', 'Reinstall Operating System', 'Rollback Updates', 'Rollback Drivers', 'Repair Application', 'Restart Print Spooler', 'Disable Network Adapter', 'Update Network Drivers', 'Refresh DHCP', 'Rebuild Windows Profile', 'Apply Updates', 'Repair Installation', 'Restore from Recovery Partition', 'Remap network drive', 'Verify integrity of disk drive', 'Initiate screen share session with user', 'Windows recovery environment', and 'Inform user of AUP violation'. At the bottom, a 'Verify/Resolve' dropdown menu is open, showing a list of commands: 'chkdsk', 'dism', 'diskpart', 'sfc', 'dd', 'ctrl + alt + del', 'net use', 'net user', 'netstat', 'netsh', and 'bootrec'.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Details

#8675309 **Open**

Priority High

Category Technical / Bug Reports

Assigned To helpdesk@fictional.com

Assigned Date 7/13/2022

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

Attachments [bootmgr not found.png](#)

Issue

Corrupt OS

Resolution

Reinstall Operating System

Verify/Resolve

chkdsk

[Close Ticket](#)

NEW QUESTION 7

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

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

Answer: A

Explanation:

Multifactor authentication will be forced for Wi-Fi after deploying a client certificate to be used for Wi-Fi access for all devices in an organization.

References:

➤ [CompTIA Security+ \(Plus\) Practice Test Questions | CompTIA](https://www.comptia.org/training/resources/comptia-security-practice-tests). Retrieved from <https://www.comptia.org/training/resources/comptia-security-practice-tests>

NEW QUESTION 8

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

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

Answer: C

Explanation:

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

NEW QUESTION 9

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

- A. FreeBSD
- B. Chrome OS
- C. macOS
- D. Windows

Answer: B

Explanation:

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

NEW QUESTION 10

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

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

Answer: D

Explanation:

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

NEW QUESTION 10

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

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

Answer: C

Explanation:

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

NEW QUESTION 13

Which of the following is the STRONGEST wireless configuration?

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

Answer: B

Explanation:

The strongest wireless configuration is B. WPA3. WPA3 is the most up-to-date wireless encryption protocol and is the most secure choice. It replaces PSK with SAE, a more secure way to do the initial key exchange. At the same time, the session key size of WPA3 increases to 128-bit in WPA3-Personal mode and 192-bit in WPA3-Enterprise, which makes the password harder to crack than the previous Wi-Fi security standards
<https://www.makeuseof.com/tag/wep-wpa-wpa2-wpa3-explained/>

NEW QUESTION 14

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

Explanation:

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 17

An analyst needs GUI access to server software running on a macOS server. Which of the following options provides the BEST way for the analyst to access the macOS server from the Windows workstation?

- A. RDP through RD Gateway
- B. Apple Remote Desktop
- C. SSH access with SSH keys
- D. VNC with username and password

Answer: B

Explanation:

Apple Remote Desktop is a remote access solution that allows a user to access and control another macOS computer from their Windows workstation. It provides a graphical user interface so that the analyst can easily access the server software running on the macOS server. Apple Remote Desktop also supports file transfers, so the analyst can easily transfer files between the two computers. Additionally, Apple Remote Desktop supports encryption, so data is secure during

transmission.

NEW QUESTION 21

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

Explanation:

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 25

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

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

Answer: A

Explanation:

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

NEW QUESTION 28

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 32

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

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

Answer: B

Explanation:

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

NEW QUESTION 36

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

Explanation:

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 40

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: CE

Explanation:

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 43

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

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

Answer: B

Explanation:

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

NEW QUESTION 46

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

Explanation:

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 desktop.

NEW QUESTION 50

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: B

Explanation:

The technician would most likely use the Task Manager tool to safely make this change. 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 53

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

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

Answer:

C

Explanation:

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

NEW QUESTION 58

Which of the following Wi-Fi protocols is the MOST secure?

- A. WPA3
- B. WPA-AES
- C. WEP
- D. WPA-TKIP

Answer: A

Explanation:

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

NEW QUESTION 63

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

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

Answer: D

Explanation:

This is the most effective way to selectively prevent programs from loading on a Windows 10 machine. The Startup tab can be accessed by opening Task Manager and then selecting the Startup tab. From there, the technician can methodically disable items that are currently listed as enabled, reboot the machine, and check for issue resolution at each startup. If the issue persists, the technician can then move on to disabling the next item on the list.

NEW QUESTION 65

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

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

Answer: D

Explanation:

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

NEW QUESTION 70

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

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

Answer: D

Explanation:

The CompTIA A+ Core 2 220-1102 exam covers this topic in the following domains: 1.2 Given a scenario, use appropriate resources to support users and 1.3 Explain the importance of security awareness.

NEW QUESTION 75

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

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

Answer: D

Explanation:

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

NEW QUESTION 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: B

Explanation:

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 environment.

NEW QUESTION 82

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

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

Answer: B

Explanation:

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

NEW QUESTION 84

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

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

Answer: C

Explanation:

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

NEW QUESTION 86

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

Explanation:

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

NEW QUESTION 90

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

Explanation:

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 95

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

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

Answer: C

Explanation:

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

NEW QUESTION 97

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

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

Answer: B

Explanation:

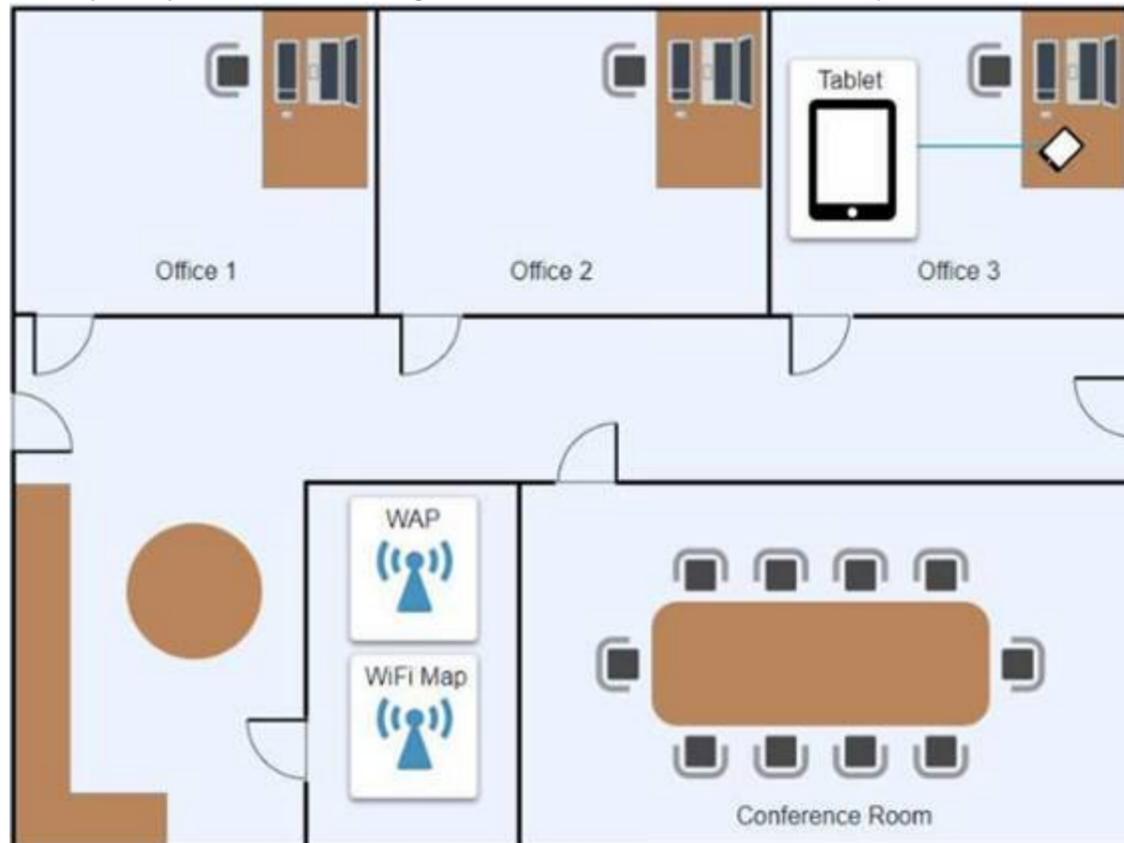
This is because remote wipe allows the data on the smartphone to be erased remotely, which helps to ensure that sensitive data does not fall into the wrong hands.

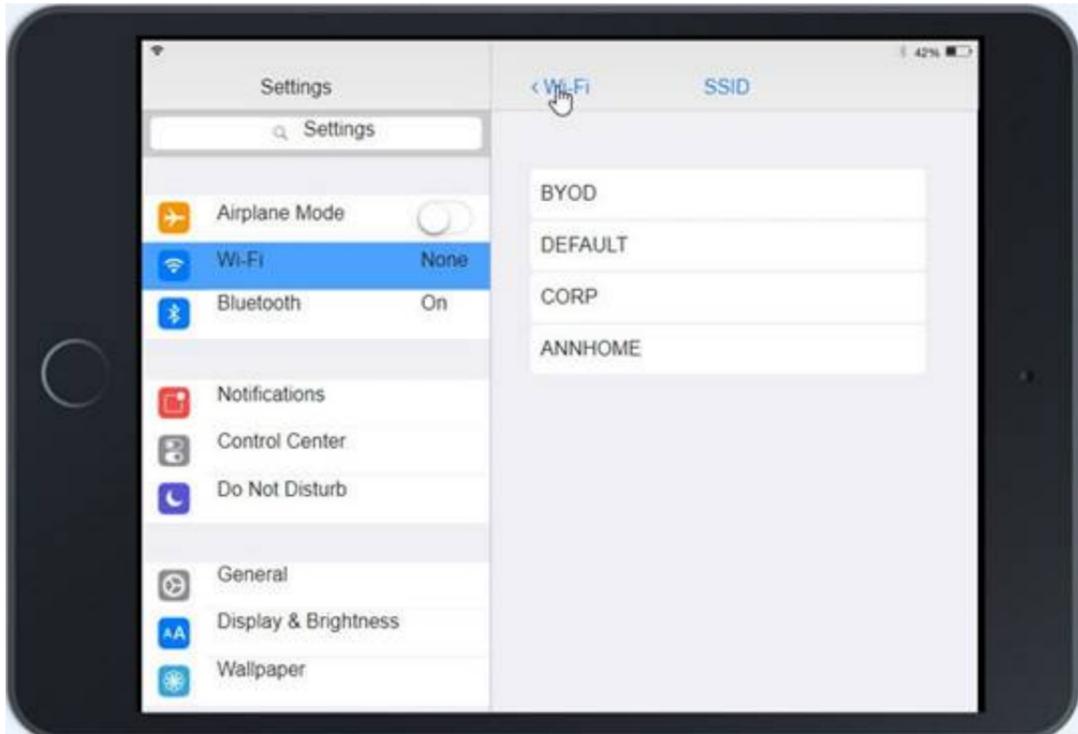
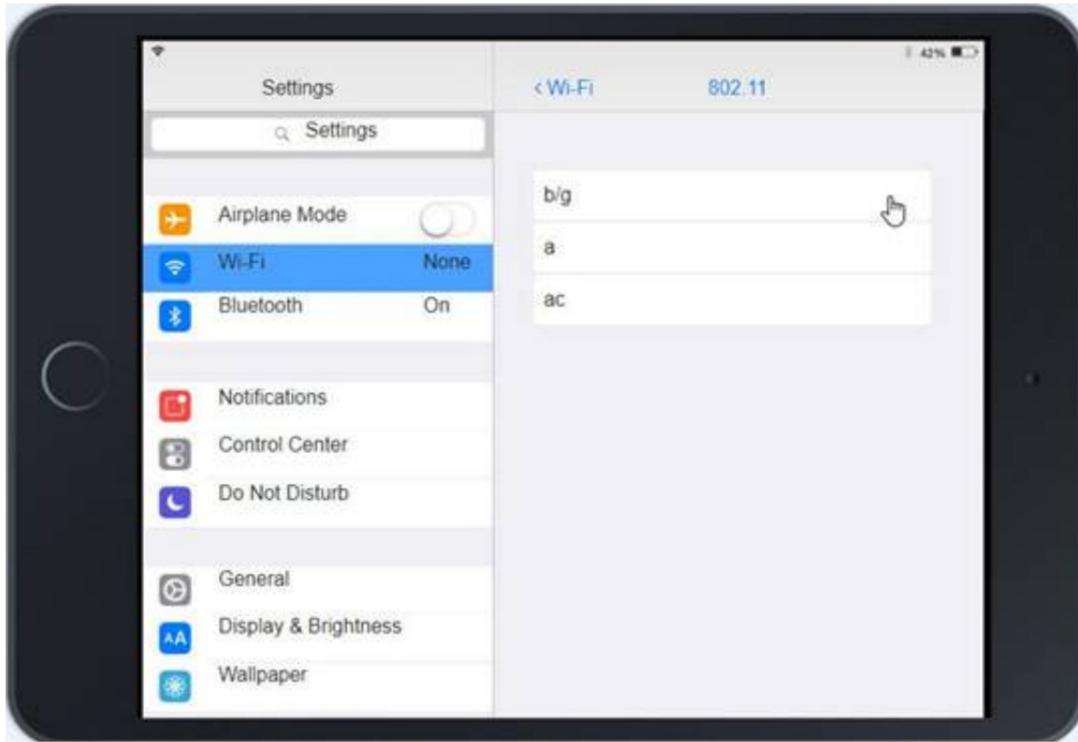
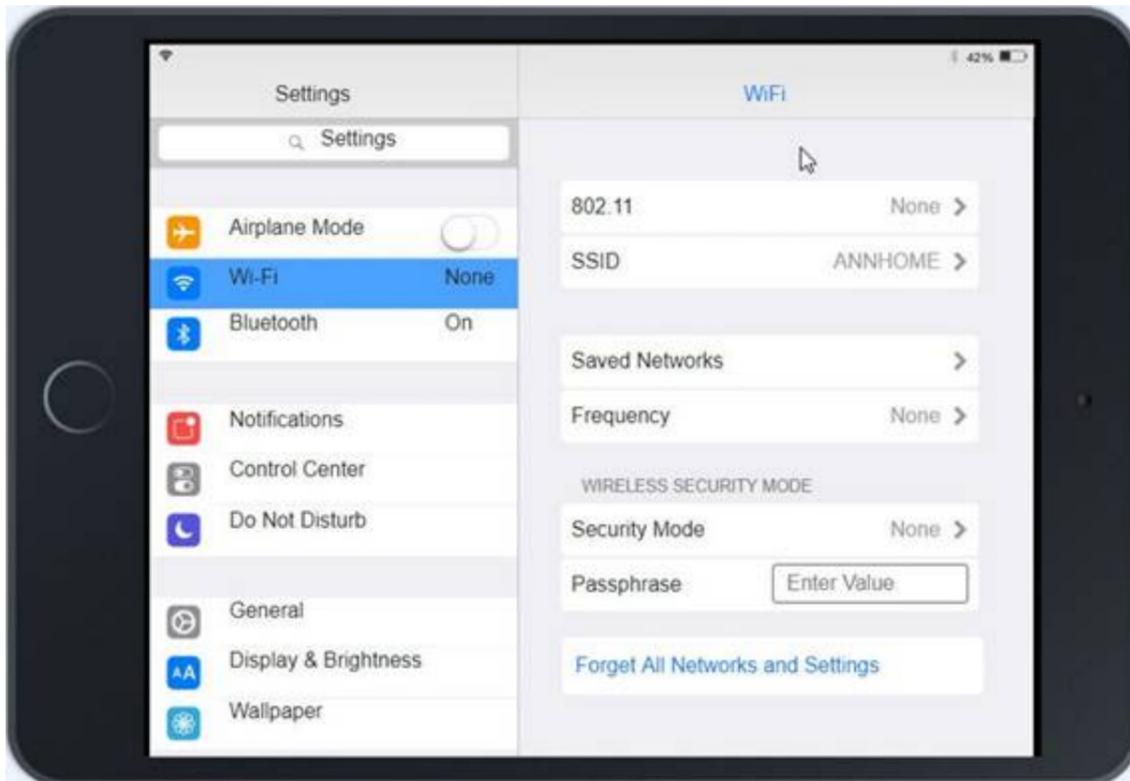
NEW QUESTION 98

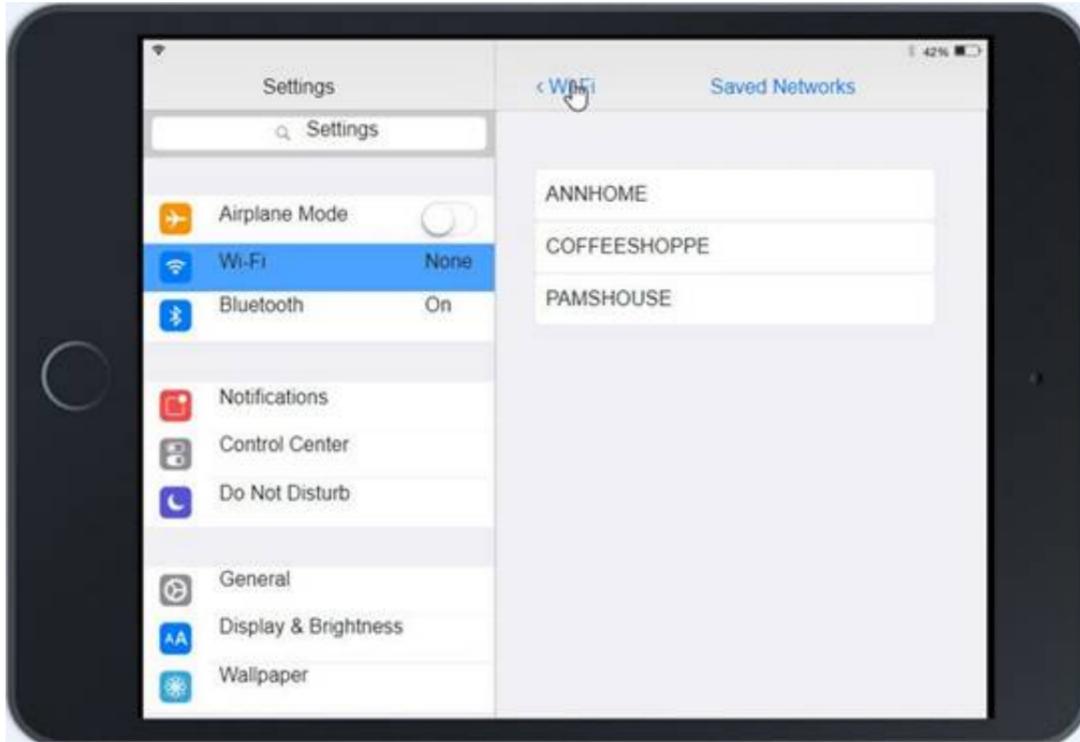
Ann, a CEO, has purchased a new consumer-class tablet for personal use, but she is unable to connect it to the company’s wireless network. All the corporate laptops are connecting without issue. She has asked you to assist with getting the device online.

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

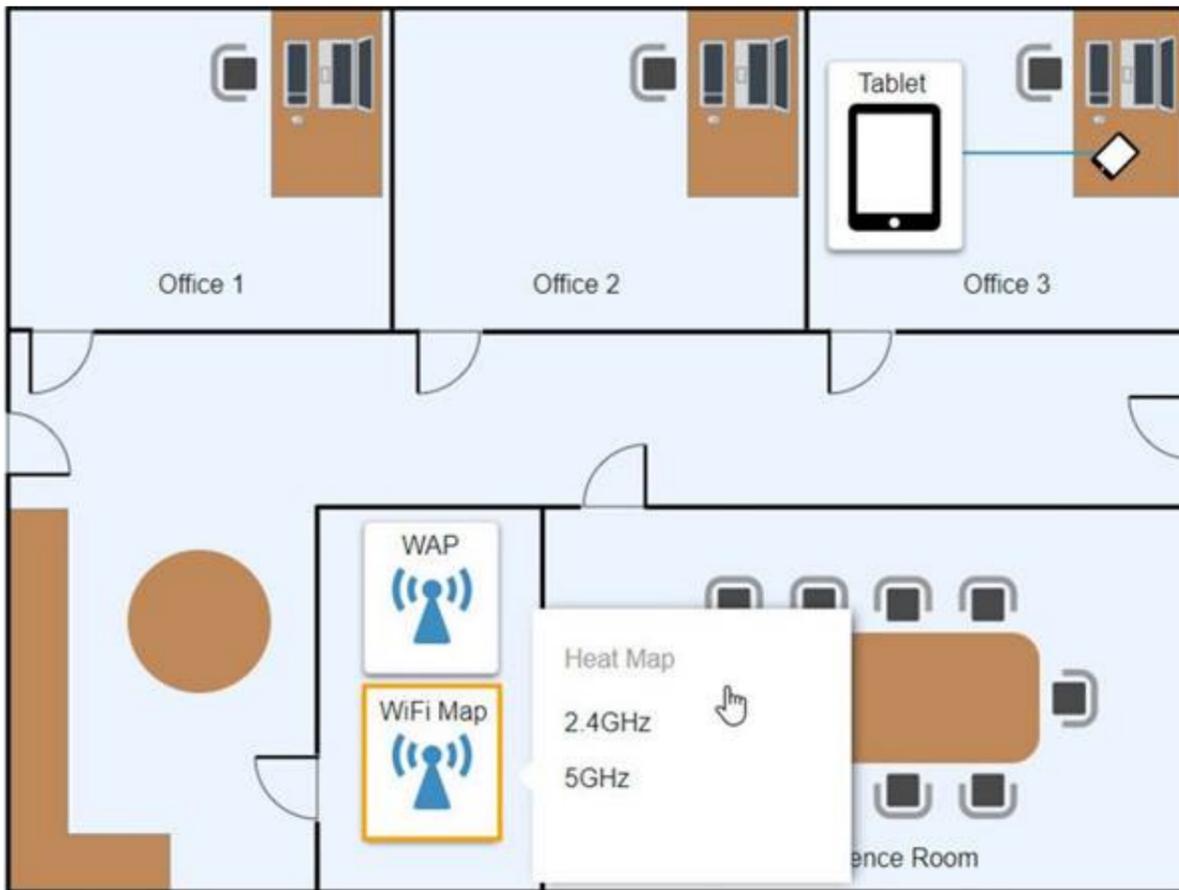
- VOIP

- Controller
- Cloud Access
- Maintenance

Wireless Networks

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

Create New Wireless Network

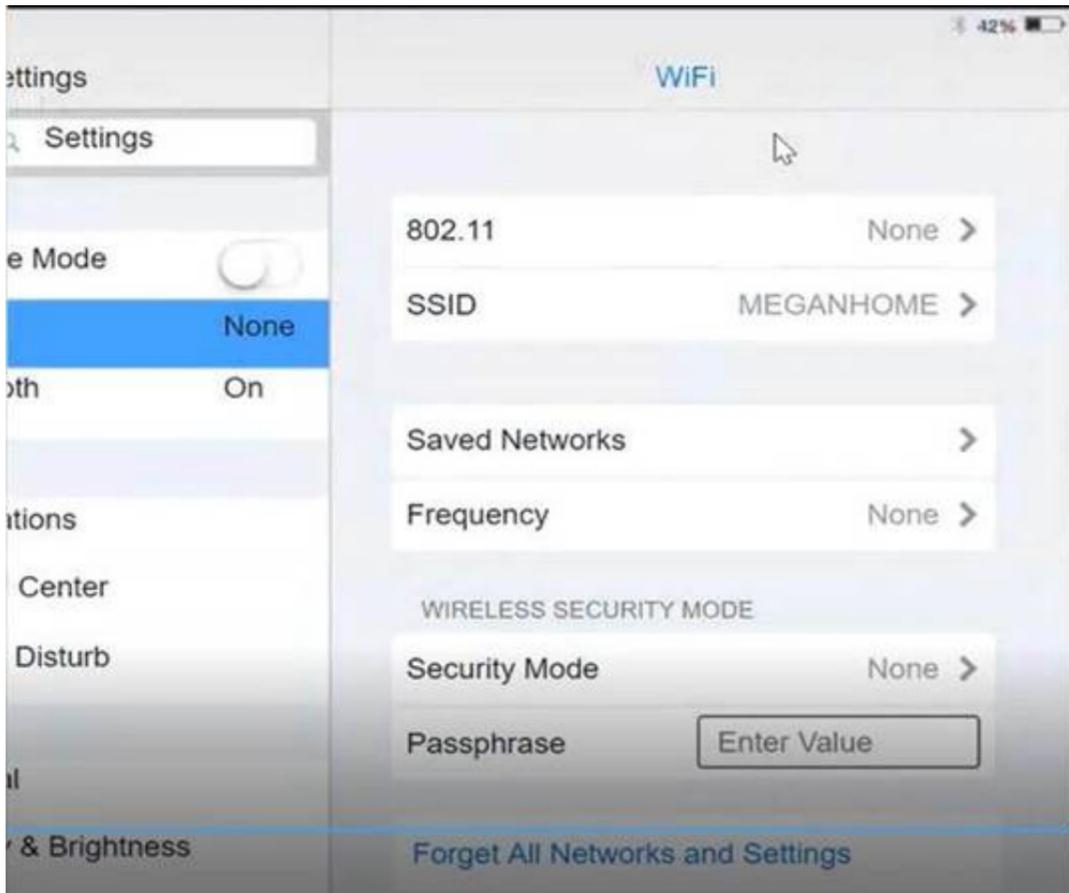


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

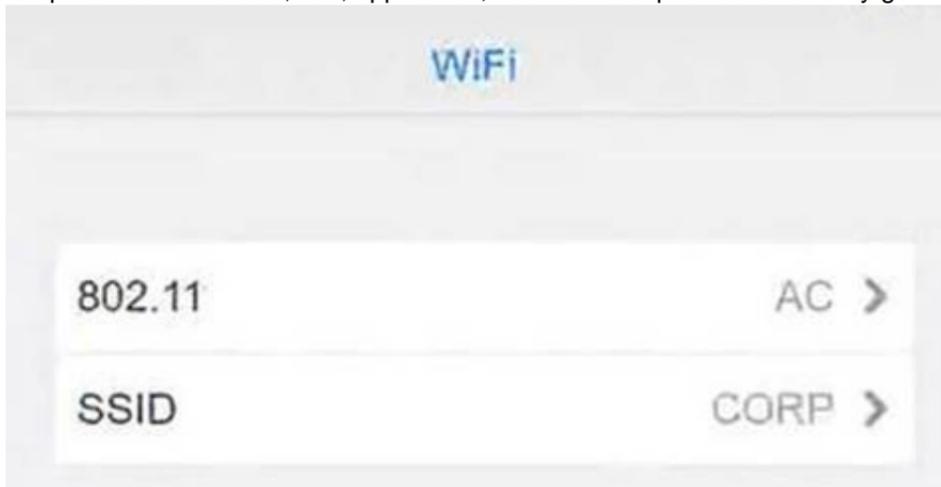
Graphical user interface, application Description automatically generated



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



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



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



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



Select the WPA2

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



Ann needs to connect to the BYOD SSID, using 2.4GHZ. The selected security method chose should be WPA PSK, and the password should be set to TotallySecret.

Graphical user interface, application Description automatically generated



NEW QUESTION 102

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

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

Answer: C

Explanation:

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

NEW QUESTION 107

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

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

Answer: B

Explanation:

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

NEW QUESTION 110

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

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

Answer: A

Explanation:

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

NEW QUESTION 115

Which of the following is an example of MFA?

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

Answer: D

Explanation:

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

NEW QUESTION 118

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

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

Answer: C

Explanation:

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

NEW QUESTION 120

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

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

Answer: A

Explanation:

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

NEW QUESTION 125

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

Explanation:

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 129

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

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

Answer: A

Explanation:

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

NEW QUESTION 134

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

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

Answer: C

Explanation:

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

NEW QUESTION 136

A user corrects a laptop that is running Windows 10 to a docking station with external monitors when working at a desk. The user would like to close the laptop when it is docked, but the user reports it goes to sleep when it is closed. Which of the following is the BEST solution to prevent the laptop from going to sleep when it is closed and on the docking station?

- A. Within the Power Options of the Control Panel utility click the Change Plan Settings button for the enabled power plan and select Put the Computer to Sleep under the Plugged In category to Never
- B. Within the Power Options of the Control Panel utility, click the Change Plan Settings button for the enabled power plan and select Put the Computer to Sleep under the On Battery category to Never
- C. Within the Power Options of the Control Panel utility select the option Choose When to Turn Off the Display and select Turn Off the Display under the Plugged In category to Never
- D. Within the Power Options of the Control Panel utility, select the option Choose What Closing the Lid Does and select When I Close the Lid under the Plugged in category to Do Nothing

Answer: D

Explanation:

The laptop has an additional option under power and sleep settings that desktops do not have. Switching to do nothing prevents the screen from turning off when closed.

NEW QUESTION 139

A technician is installing a new business application on a user's desktop computer. The machine is running Windows 10 Enterprise 32-bit operating system. Which of the following files should the technician execute in order to complete the installation?

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

Answer: D

Explanation:

The 32-bit operating system can only run 32-bit applications, so the technician should execute the 32-bit installer. The "x86" in the file name refers to the 32-bit architecture.

<https://www.digitaltrends.com/computing/32-bit-vs-64-bit-operating-systems/>

NEW QUESTION 142

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

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

Answer: C

Explanation:

The technician should quarantine the system first.

NEW QUESTION 146

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

Explanation:

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.

NEW QUESTION 151

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

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 156

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

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

Answer: D

Explanation:

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

NEW QUESTION 159

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

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

Answer: D

Explanation:

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

NEW QUESTION 162

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

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

Answer: AE

Explanation:

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

NEW QUESTION 166

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

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

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

Details

#8675310	Open
Priority	Low
Category	Technical / Bug Reports
Assigned To	helpdesk@fictional.com
Assigned Date	7/13/2022

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

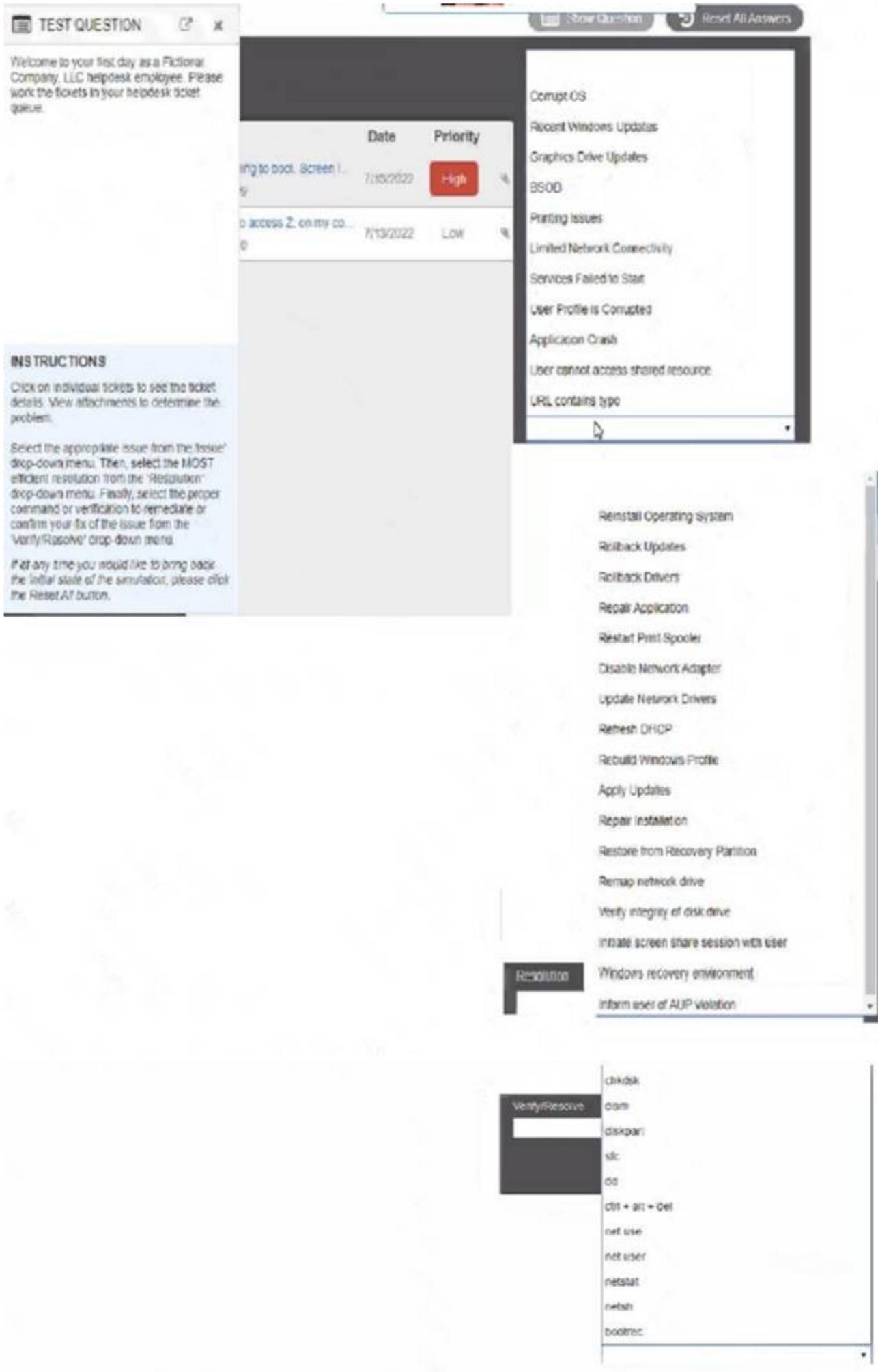
Attachments [File Explorer.jpg](#)

Issue

Resolution

Verify/Resolve

[Close Ticket](#)



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Details

#8675310 **Open**

Priority Low

Category Technical / Bug Reports

Assigned To helpdesk@fictional.com

Assigned Date 7/13/2022

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

Attachments [File Explorer.jpg](#)

Issue

Resolution

Verify/Resolve

[Close Ticket](#)

NEW QUESTION 169

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

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

Answer: B

Explanation:

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

NEW QUESTION 170

A user reports that a PC seems to be running more slowly than usual. A technician checks system resources, but disk, CPU, and memory usage seem to be fine. The technician sees that GPU temperature is extremely high. Which of the following types of malware is MOST likely to blame?

- A. Spyware
- B. Cryptominer
- C. Ransomware
- D. Boot sector virus

Answer: B

Explanation:

The type of malware that is most likely to blame for a PC running more slowly than usual and having an extremely high GPU temperature is a "cryptominer". Cryptominers are a type of malware that use the resources of a computer to mine cryptocurrency. This can cause the computer to run more slowly than usual and can cause the GPU temperature to rise. Spyware is a type of malware that is used to spy on a user's activities, but it does not typically cause high GPU temperatures. Ransomware is a type of malware that encrypts a user's files and demands payment to unlock them, but it does not typically cause high GPU temperatures. Boot sector viruses are a type of malware that infects the boot sector of a hard drive, but they do not typically cause high GPU temperatures

NEW QUESTION 172

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

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

Answer: B

Explanation:

Bollards are the best solution to enhance building security in order to prevent vehicles from driving into the building while also maintaining easy access for customers⁴

References: 2. Bollards. Retrieved from <https://en.wikipedia.org/wiki/Bollard>

NEW QUESTION 173

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

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

Answer: C

Explanation:

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

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

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

NEW QUESTION 178

A user receives a notification indicating the antivirus protection on a company laptop is out of date. A technician is able to ping the user's laptop. The technician checks the antivirus parent servers and sees the latest signatures have been installed. The technician then checks the user's laptop and finds the antivirus engine and definitions are current. Which of the following has MOST likely occurred?

- A. Ransomware
- B. Failed OS updates
- C. Adware
- D. Missing system files

Answer: B

Explanation:

The most likely reason for the antivirus protection on a company laptop being out of date is failed OS updates¹. Antivirus software relies on the operating system to function properly. If the operating system is not up-to-date, the antivirus software may not function properly and may not be able to receive the latest virus definitions and updates². Therefore, it is important to keep the operating system up-to-date to ensure the antivirus software is functioning properly².

NEW QUESTION 180

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

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

Answer: C

Explanation:

The OS utility used to change the color of the cursor in Windows is Ease of Access Center¹²

The user can change the cursor color by opening the Settings app, selecting Accessibility in the left sidebar selecting Mouse pointer and touch under Vision, and choosing one of the cursor options. The user can

select Custom to pick a color and use the Size slider to make the cursor larger or smaller²

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

NEW QUESTION 182

A systems administrator needs to reset a user's 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 the user from changing the password.
- C. Disable the account
- D. Choose a password that never expires.

Answer: A

Explanation:

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 2 220-1102 exam covers this topic in the domain 1.4 Given a scenario, use appropriate data destruction and disposal methods.

NEW QUESTION 183

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

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

Answer: B

Explanation:

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

NEW QUESTION 188

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 189

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

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

Answer: B

Explanation:

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

NEW QUESTION 193

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: A

Explanation:

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

NEW QUESTION 197

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

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

Answer: D

Explanation:

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

NEW QUESTION 201

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

Explanation:

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 203

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

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

Answer: C

Explanation:

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

NEW QUESTION 204

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

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

Answer: C

Explanation:

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

NEW QUESTION 205

A technician is setting up a new laptop. The company's security policy states that users cannot install virtual machines. Which of the following should the technician implement to prevent users from enabling virtual technology on their laptops?

- A. UEFI password
- B. Secure boot
- C. Account lockout
- D. Restricted user permissions

Answer: B

Explanation:

A technician setting up a new laptop must ensure that users cannot install virtual machines as the company's security policy states. One way to prevent users from enabling virtual technology is by implementing Secure Boot. Secure Boot is a feature of UEFI firmware that ensures the system only boots using firmware that is trusted by the manufacturer. It verifies the signature of all bootloaders, operating systems, and drivers before running them, preventing any unauthorized modifications to the boot process. This will help prevent users from installing virtual machines on the laptop without authorization.

NEW QUESTION 206

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 210

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

- The device is hot even when it is not in use.
 - Applications crash, especially when others are launched
 - Certain applications, such as GPS, are in portrait mode when they should be in landscape mode
- Which of the following can the technician do to MOST likely resolve these issues with minimal impact? (Select TWO).

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

Answer: AC

Explanation:

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

NEW QUESTION 212

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

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

Answer: C

Explanation:

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

NEW QUESTION 216

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

220-1102 Practice Exam Features:

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

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