CompTIA.220-1102.v2026-04-30.q382

Exam Code:	220-1102
Exam Name:	CompTIA A+ Certification Exam: Core 2
Certification Provider:	CompTIA
Free Question Number:	382
Version:	v2026-04-30
# of views:	442
# of Questions views:	3820
https://www.freepdfdumps.com/CompTIA.220-1102.v2026-04-30.q382.html	

NEW QUESTION: 1
While testing a new computer, a technician hears a loud buzzing sound, smells smoke, and sees a flame inside the power supply. Which of the following actions should the technician take first?
A. Extinguish the fire with water.
B. Smother the fire by replacing the system case.
C. Disconnect the power cord from the wall outlet.
D. Turn off the power supply switch.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 2
A technician is troubleshooting a user's PC that is running slowly and displaying frequent pop-ups. The technician thinks malware may be causing the issues, but before the issues began the user installed anti-malware software in response to a pop-up window Which of the following is the most likely cause of these issues'?
A. Expired certificate
B. False alert
C. Missing system files
D. OS update failure
Answer: B (LEAVE A REPLY)
The scenario described is characteristic of a malware tactic known as scareware, where users are tricked into installing malware through false alerts claiming that their system is infected. The anti-malware software installed in response to a pop-up is likely malicious, causing the system to run slowly and display frequent pop-ups.

NEW QUESTION: 3
Which of the following attacks can a hacker use to execute code on a user's computer when the user visits a specially prepared, malicious website?
A. DoS
B. Spoofing

C. XSS
D. SQL injection
Answer: (SHOW ANSWER)
Cross-site scripting (XSS) (Option C) allows attackers to inject malicious scripts into web pages viewed by users. When the user visits the compromised site, the script runs in the user's browser, potentially allowing the attacker to steal data or perform unauthorized actions. XSS is a common vulnerability in web applications that allows code execution.
DoS (Option A) disrupts services but doesn't involve executing code on a user's device.
Spoofing (Option B) involves impersonating another device or user but doesn't execute code.
SQL injection (Option D) attacks a database and is unrelated to executing code on the user's computer.
CompTIA A+ Core 2 Reference:
2.4 - Explain common social engineering attacks, including XSS.

NEW QUESTION: 4
Which of the following editions of Windows 10 requires reactivation every 180 days?
A. Enterprise
B. Pro for Workstation
C. Home
D. Pro
Answer: A (LEAVE A REPLY)
Windows 10 Enterprise is an edition of Windows 10 that is designed for large organizations that need advanced security and management features. Windows 10 Enterprise can be activated using different methods, such as Multiple Activation Key (MAK), Active Directory-based Activation (ADBA), or Key Management Service (KMS)1. KMS is a method of activation that uses a local server to activate multiple devices on a network. KMS activations are valid for 180 days and need to be renewed periodically by connecting to the KMS server2. If a device does not renew its activation within 180 days, it will enter a grace period of 30 days, after which it will display a warning message and lose some functionality until it is reactivated3. The other editions of Windows 10 do not require reactivation every 180 days. Windows 10 Pro for Workstation is an edition of Windows 10 that is designed for high-performance devices that need advanced features such as ReFS file system, persistent memory, and faster file sharing. Windows 10 Pro for Workstation can be activated using a digital license or a product key. Windows 10 Home is an edition of Windows 10 that is designed for personal or home use. Windows 10 Home can be activated using a digital license or a product key. Windows 10 Pro is an edition of Windows 10 that is designed for business or professional use. Windows 10 Pro can be activated using a digital license or a product key. None of these editions require reactivation every 180 days unless there are significant hardware changes or other issues that affect the activation status.

NEW QUESTION: 5
A technician is concerned about a large increase in the number of whaling attacks happening in the industry. The technician wants to limit the company's risk to avoid any issues. Which of the following items should the technician implement?
A. Screened subnet
B. Firewall
C. Anti-phishing training

D. Antivirus

Answer: C (LEAVE A REPLY)

Anti-phishing training is a method of educating users on how to identify and avoid phishing attacks, which are attempts to trick users into revealing sensitive information or performing malicious actions by impersonating legitimate entities or persons. Whaling attacks are a specific type of phishing attack that target high-level executives or influential individuals within an organization. Anti-phishing training can help users recognize the signs of whaling attacks and prevent them from falling victim to them. Screened subnet, firewall, and antivirus are not items that can directly address the issue of whaling attacks.

NEW QUESTION: 6

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: 7

A user is setting up backups on a workstation. The user wants to ensure that the restore process is as simple as possible. Which of the following backup types should the user select?

A. Full

B. Incremental

C. Differential

D. Synthetic

Answer: (SHOW ANSWER)

Full backup is the best option to ensure that the restore process is as simple as possible. A full backup is a backup type that copies all the data from the source to the destination, regardless of whether the data has changed or not. A full backup provides the most complete and consistent backup of the data, and it allows the user to restore the data from a single backup set without relying on any previous or subsequent backups. Incremental, differential, and synthetic backups are not as simple as full backups for restoring data. An incremental backup is a backup type that copies only the data that has changed since the last backup, whether it was full or incremental. An incremental backup requires less time and space than a full backup, but it also requires multiple backup sets to restore the data completely. A differential backup is a backup type that copies only the data that has changed since the last full backup. A differential backup requires more time and space than an incremental backup, but it also requires fewer backup sets to restore the data than an incremental backup. A synthetic backup is a backup type that combines a full backup with one or more incremental or differential backups to create a consolidated backup set. A synthetic backup requires less time and bandwidth than a full backup, but it also requires more processing power and storage space than an incremental or differential backup. Reference:

Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15 CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 458

NEW QUESTION: 8
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: 9
A technician needs to formal 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)
Since Windows systems support FAT32 and NTFS "out of the box" and Linux supports a whole range of them including FAT32 and NTFS, it is highly recommended to format the partition or disk you want to share in either FAT32 or NTFS, but since FAT32 has a file size limit of 4.2 GB, if you happen to work with huge files, then it is better you use NTFS

NEW QUESTION: 10
Which of the following scripting languages is the most commonly used for system administration on Windows operating systems?
A. JavaScript
B. PowerShell
C. Bash
D. Python
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
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: 12
Which of the following protects a mobile device against unwanted access when it is left unattended?
A. PIN code
B. OS updates
C. Antivirus software
D. BYOD policy
Answer: A (LEAVE A REPLY)

A PIN code is a numeric password that protects a mobile device against unwanted access when it is left unattended. It requires the user to enter the correct code before unlocking the device. OS updates, antivirus software and BYOD policy are other security measures for mobile devices, but they do not prevent unauthorized access when the device is left unattended. Verified Reference: https://www.comptia.org/blog/mobile-device-security
https://www.comptia.org/certifications/a

NEW QUESTION: 13
A technician is tasked with configuring a computer for a visually impaired user. Which of the following utilities should the technician use?
A. Device Manager
B. System
C. Ease of Access Center
D. Programs and Features
Answer: C (LEAVE A REPLY)
The Ease of Access Center is a built-in utility in Windows that provides tools and options for making a computer easier to use for individuals with disabilities, including the visually impaired. In the Ease of Access Center, the technician can turn on options like high contrast display, screen magnification, and screen reader software to help the user better interact with the computer.

NEW QUESTION: 14
SIMULATION
You have been contacted through the help desk chat application. A user is setting up a replacement SOHO router. Assist the user with setting up the router.
INSTRUCTIONS
Select the most appropriate statement for each response. Click the send button after each response to continue the chat. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Answer:
See the solution below in Explanation
Explanation:

NEW QUESTION: 15

Which of the following commands should a technician use to change user permissions?

A. sudo

B. pwd

C. chmod

D. mv
Answer: C (LEAVE A REPLY)

NEW QUESTION: 16
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.

Answer:

TEST QUESTION

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

INSTRUCTIONS

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

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

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

Show Question | Reset All Answers

	Date	Priority
ling to boot. Screen i... /9	7/13/2022	High
o access Z: on my co... 0	7/13/2022	Low

Issue:
- Corrupt OS
- Recent Windows Updates
- Graphics Drive Updates
- BSOD
- Printing Issues
- Limited Network Connectivity
- Services Failed to Start
- User Profile is Corrupted
- Application Crash
- User cannot access shared resource
- URL contains typo

Resolution:
- Reinstall Operating System
- Rollback Updates
- Rollback Drivers
- Repair Application
- Restart Print Spooler
- Disable Network Adapter
- Update Network Drivers
- Refresh DHCP
- Rebuild Windows Profile
- Apply Updates
- Repair Installation
- Restore from Recovery Partition
- Remap network drive
- Verify integrity of disk drive
- Initiate screen share session with user
- Windows recovery environment
- Inform user of AUP violation

Verify/Resolve:
- chkdsk
- dism
- diskpart
- sfc
- dd
- ctrl + alt + del
- net use
- net user
- netstat
- netsh
- bootrec

NEW QUESTION: 17
Which of the following commands should a technician use to change user permissions?
A. sudo
B. chxod
C. xv
D. pwd
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth
The sudo (SuperUser DO) command is used in Linux-based systems to execute administrative tasks, such as changing permissions or accessing root-level files and directories. When a technician needs to change file or user permissions, they often use chmod or chown with sudo to gain the required privileges.
Option B (chxod): This is a typo. The correct command is chmod, used to change file permissions.
Option C (xv): Not a valid command in Linux related to permissions.
Option D (pwd): Stands for "print working directory," used to display the current directory, not manage permissions.
? Reference:
CompTIA A+ 220-1102 Exam Objective 1.4 - "Given a scenario, use features and tools of the Mac OS and Linux client/desktop operating systems."

NEW QUESTION: 18
A technician is configuring a workstation's security settings, and the following options are available:
Account lockout policy
Group policy
Two-factor authentication
Password complexity requirements
Firewalls
User accounts
Access control lists
Antivirus software
Which of the following settings should the technician configure to deploy strong password enforcement across the enterprise?
A. Account lockout policy
B. Group policy
C. Two-factor authentication

D. Access control lists

Answer: B (LEAVE A REPLY)

The technician should configure "Group Policy" (Option B) to enforce password complexity across the enterprise. Group Policy in a Windows environment allows administrators to manage various settings, including password policies, at a domain level. This can include enforcing complexity requirements (such as minimum length, use of uppercase, lowercase, and special characters), expiration times, and other security measures.

Account lockout policy (Option A) controls how many failed login attempts trigger a lockout but does not handle password complexity.

Two-factor authentication (Option C) is an additional security measure requiring a second form of authentication, but it does not enforce password policies.

Access control lists (Option D) define which users or systems have access to resources, not how passwords are managed.

CompTIA A+ Core 2 Reference:

2.6 - Configure workstation security best practices, including password complexity and group policies.

NEW QUESTION: 19

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: 20

An organization's critical database files were attacked with ransomware. The company refuses to pay the ransom for a decryption key. All traces of the infection have been removed from the underlying servers. Which of the following should the company do next?

A. Scan all of the infected files with up-to-date, anti-malware cleaning software.

B. Fully patch the server operating systems hosting the fileshares.

C. Change the files to be read-only.

D. Restore critical data from backup.

Answer: D (LEAVE A REPLY)
When an organization refuses to pay the ransom for a decryption key after a ransomware attack, and all traces of the infection have been removed, the next critical step is:
Restore critical data from backup: This is the most effective way to recover from a ransomware attack without paying the ransom. Assuming the organization has good backup practices, the backups should be free from infection and can be restored to get the systems operational again.
Scan all of the infected files with up-to-date, anti-malware cleaning software: This step is important during the infection removal process but does not address restoring the encrypted files.
Fully patch the server operating systems hosting the fileshares: While this is necessary to prevent future attacks, it does not recover the encrypted files.
Change the files to be read-only: This will not help recover the encrypted data.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 2.8: Given a scenario use common data destruction and disposal methods.
Best practices for ransomware recovery.

NEW QUESTION: 21
A user's computer was infected with a Trojan. The user thinks the Trojan was introduced when clicking on a malicious link in an email. Which of the following actions should the technician take to prevent further damage to the computer?
A. Review the proxy settings.
B. Scan the system with a rootkit scanner.
C. Enable the firewall.
D. Ensure anti-malware signatures are up to date.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
A technician is upgrading the Microsoft Windows 10 OS. Which of the following are required for the technician to safely upgrade the OS? (Select two).
A. Release notes
B. Antivirus software
C. Backup of critical data
D. Device drivers
E. Word processing software
F. Safe boot mode
Answer: (SHOW ANSWER)
To safely upgrade the Microsoft Windows 10 OS, it is essential to backup critical data (C) and ensure that you have the necessary device drivers (D). Backing up critical data protects against potential data loss during the upgrade process. Having the correct device drivers ensures that the hardware components function properly with the new OS version, preventing issues like loss of functionality or compatibility problems.

NEW QUESTION: 23

Which of the following is the Windows OS that only recognizes 4GB of RAM?
A. The 32-bit OS
B. The trial version OS
C. The Home version OS
D. The 64-bit OS
Answer: (SHOW ANSWER)

NEW QUESTION: 24
A customer wants to make sure the data is protected and secure on a Windows laptop's hard drive. Which of the following is the best solution?
A. Windows Backup
B. BitLocker
C. Shadow Copy
D. Trusted PlatformModule
Answer: B (LEAVE A REPLY)
BitLocker is a full-disk encryption feature included with Windows Vista and later. It is designed to protect data by providing encryption for entire volumes. By encrypting the hard drive, BitLocker prevents unauthorized access to the data stored on the drive, securing it in case the laptop is lost or stolen. BitLocker is preferable over options like Windows Backup (which is for data recovery, not encryption), Shadow Copy (used for backup and does not encrypt data), and Trusted Platform Module (TPM, which is a hardware component used alongside BitLocker for securing encryption keys).

NEW QUESTION: 25
A technician connects an additional monitor to a PC using a USB port. The original HDMI monitor is mounted to the left of the new monitor. When moving the mouse to the right from the original monitor to the new monitor, the mouse stops at the end of the screen on the original monitor. Which of the following will allow the mouse to correctly move to the new monitor?
A. Rearranging the monitor's position in display settings
B. Swapping the cables for the monitors
C. Using the Ctrl+AIt+> to correct the display orientation
D. Updating the display drivers for the video card
Answer: (SHOW ANSWER)
The correct answer is B. Swapping the cables for the monitors. When the second monitor is connected with the HDMI port, it is necessary to swap the cables for the monitors so that the mouse can move from the original monitor to the new monitor. This is because the HDMI port is designed to only support one monitor, and the mouse will not be able to move from one to the other without the cables being swapped.
According to CompTIA A+ Core 2 documents, "When connecting multiple displays to a system, the cables used to connect the displays must be swapped between the displays. For example, if a monitor is connected to a system using a VGA cable, the VGA cable must be moved to the next display to allow the mouse to move between the two displays."

NEW QUESTION: 26
A user is unable to use any internet-related functions on a smartphone when it is not connected to Wi-Fi When the smartphone is connected to Wi-Fi the user can browse the internet and send and receive email. The user is also able to

send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi. Which of the following is the MOST likely reason the user is unable to use the internet on the smartphone when it is not connected to Wi-Fi?

A. The smartphone's line was not provisioned with a data plan

B. The smartphone's SIM card has failed

C. The smartphone's Bluetooth radio is disabled.

D. The smartphone has too many applications open

Answer: A (LEAVE A REPLY)

The smartphone's line was not provisioned with a data plan. The user is unable to use any internet-related functions on the smartphone when it is not connected to Wi-Fi because the smartphone's line was not provisioned with a data plan. The user can send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi because these functions do not require an internet connection1

NEW QUESTION: 27

A user is unable to access the company's network. A technician learns the user's account became inaccessible after multiple unsuccessful login attempts. The user also changed their password before the issue started. Which of the following steps should the technician take to resolve the issue?

A. Escalate the user's issue to the network team.

B. Reset the user's password.

C. Unlock the user's account.

D. Verify the user's login and password.

Answer: C (LEAVE A REPLY)

Detailed Explanation with Core 2 Reference:If multiple unsuccessful attempts led to the account being locked, the technician should unlock the account. Core 2 covers user account management practices, including unlocking accounts and managing failed login attempts (Core 2 Objective 2.5).

NEW QUESTION: 28

An organization implemented a method of wireless security that requires both a user and the user's computer to be in specific managed groups on the server in order to connect to Wi-Fi. Which of the following wireless security methods BEST describes what this organization implemented?

A. TKIP

B. RADIUS

C. WPA2

D. AES

Answer: (SHOW ANSWER)

RADIUS stands for Remote Authentication Dial-In User Service and it is a protocol that provides centralized authentication, authorization, and accounting for network access. RADIUS can be used to implement a method of wireless security that requires both a user and the user's computer to be in specific managed groups on the server in order to connect to Wi-Fi. This is also known as 802.1X authentication or EAP-TLS authentication

NEW QUESTION: 29

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

A. Navigate to the Control Panel utility, select the Security and Maintenance submenu, select Change Security and Maintenance settings, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete

B. Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign in options, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.

C. Navigate to the Windows 10 Settings menu, select the Update & Security submenu select Windows Security, select Windows Hello Fingerprint and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete

D. Navigate to the Control Panel utility, select the Administrative Tools submenu, select the user account in the list, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.

Answer: B (LEAVE A REPLY)

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: 30

A technician wants to securely dispose of storage drives. Which of the following is the best way to eliminate data on SSDs?

A. Degaussing

B. Shredding

C. Erasing

D. Drilling

Answer: (SHOW ANSWER)

For securely disposing of SSDs, physical destruction methods like shredding are considered most effective: Shredding:This method involves physically breaking the SSD into small pieces, making data recovery practically impossible. It's a recommended practice for ensuring that sensitive data on SSDs is irretrievably destroyed.

NEW QUESTION: 31

A company wants to remove information from past users' hard drives in order to reuse the hard drives Witch of the following is the MOST secure method

A. Reinstalling Windows

B. Performing a quick format

C. Using disk-wiping software

D. Deleting all files from command-line interface

Answer: C (LEAVE A REPLY)

Using disk-wiping software is the most secure method for removing information from past users' hard drives in order to reuse the hard drives. Disk-wiping software can help to ensure that all data on the hard drive is completely erased and cannot be recovered.

NEW QUESTION: 32

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: 33

Which of the following is natively used with Active Directory?

A. Windows 10

B. macOS

C. Linux

D. Chrome OS

Answer: A (LEAVE A REPLY)

Windows 10 is natively compatible with Active Directory. Active Directory is a Windows-based directory service that manages domain-based networks. It allows for centralized management of users, groups, and resources, which is a key feature in enterprise environments using Windows OS, such as Windows 10. Other operating systems like macOS, Linux, and Chrome OS may require additional software or configurations to interact with Active Directory, but they do not natively support it.

NEW QUESTION: 34
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 (LEAVE A REPLY)
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: 35
A technician is assisting a customer who is having difficulty accessing the company's website. Which of the following should the technician do first?
A. Ask the customer for their log-in credentials.
B. Check the company's internal knowledge base for solutions.
C. Refer the customer to a more experienced technician.
D. Record the details of the issue in the company's ticketing system.
Answer: D (LEAVE A REPLY)
When a customer is having difficulty accessing the company's website, the technician should first document the issue in the company's ticketing system. This step ensures that the problem is officially logged, which allows for proper tracking, prioritization, and assignment to the appropriate personnel if needed. Recording the details helps in maintaining a record of the issue and the troubleshooting steps taken, which is useful for future reference and analysis.
A . Ask the customer for their log-in credentials. This is not appropriate as it breaches security protocols and is not the first step in troubleshooting.
B . Check the company's internal knowledge base for solutions. While useful, this step comes after the issue has been documented.
C . Refer the customer to a more experienced technician. This might be necessary later, but initially, the issue should be documented.
Reference:
CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 4.1: Documentation and support systems, including the use of ticketing systems for tracking incidents.

NEW QUESTION: 36
A technician is securing a new Windows 10 workstation and wants to enable a Screensaver lock. Which of the following options in the Windows settings should the technician use?

A. Ease of Access
B. Privacy
C. Personalization
D. Update and Security
Answer: (SHOW ANSWER)
The technician should use the Personalization option in the Windows settings to enable a Screensaver lock. The Personalization option allows users to customize the appearance and behavior of their desktop, such as themes, colors, backgrounds, lock screen and screensaver. The technician can enable a Screensaver lock by choosing a screensaver from the drop-down menu, setting a wait time in minutes and checking the box that says "On resume, display logon screen". This will lock the computer and require a password or PIN to log back in after the screensaver is activated. Ease of Access is an option in the Windows settings that allows users to adjust accessibility features and settings, such as narrator, magnifier, high contrast and keyboard shortcuts. Ease of Access is not related to enabling a Screensaver lock. Privacy is an option in the Windows settings that allows users to manage privacy and security settings, such as location, camera, microphone and app permissions. Privacy is not related to enabling a Screensaver lock. Update and Security is an option in the Windows settings that allows users to check and install updates, troubleshoot problems, backup files and restore system. Update and Security is not related to enabling a Screensaver lock. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.7

NEW QUESTION: 37
A systems administrator receives notification about unauthorized access to company resources outside normal business hours. Which of the following security measures should the systems administrator implement to prevent further unauthorized use?
A. SSL-enabled DNS
B. Anonymizing VPNs
C. Perimeter firewalls
D. Multifactor authentication
Answer: D (LEAVE A REPLY)

NEW QUESTION: 38
A company is looking lot a solution that provides a backup for all data on the system while providing the lowest impact to the network. Which of the following backup types will the company MOST likely select?
A. Off-site
B. Synthetic
C. Full
D. Differential
Answer: B (LEAVE A REPLY)
A synthetic backup is a backup type that provides a backup for all data on the system while providing the lowest impact to the network. It combines a full backup with one or more incremental backups to create a single backup set, without requiring access to the original data source. Off-site is a backup location, not a backup type. Full and differential are backup types, but they have a higher impact on the network than synthetic. Verified Reference: https://www.comptia.org/blog/what-is-a-synthetic-backup https://www.comptia.org/certifications/a

NEW QUESTION: 39
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: 40
A user is unable to access the internet but can still print to network printers. Other users are not experiencing this issue. Which of the following steps should the technician take first to diagnose the issue?
A. Validate physical connectivity.
B. Reboot the router.
C. Disable IPv6.
D. Check the DNS settings.
Answer: D (LEAVE A REPLY)
When a user can access the local network (as evidenced by printing to network printers) but not the internet, the issue is often related to Domain Name System (DNS) resolution. DNS is responsible for translating domain names (like google.com) into IP addresses that computers use to communicate. If the DNS settings are incorrect or the DNS server is unreachable, the computer won't be able to find the IP addresses of websites and other internet resources.

NEW QUESTION: 41
A system drive is nearly full, and a technician needs lo tree up some space. Which of the following tools should the technician use?
A. Disk Cleanup
B. Resource Monitor
C. Disk Defragment
D. Disk Management
Answer: A (LEAVE A REPLY)
Disk Cleanup is a tool that can free up some space on a system drive that is nearly full. It can delete temporary files, cached files, recycle bin files, old system files and other unnecessary data. Resource Monitor is a tool that shows the network activity of each process on a Windows machine. Disk Defragment is a tool that optimizes the performance of a hard drive by rearranging the data into contiguous blocks. Disk Management is a tool that allows creating, formatting,

resizing and deleting partitions on a hard drive. Verified Reference: https://www.comptia.org/blog/how-to-use-disk-cleanup https://www.comptia.org/certifications/a

NEW QUESTION: 42
Internet speeds on a user's Windows 10 device are slow, but other devices on the same network are running at normal speeds. A technician thinks the issue may be related to the proxy settings. Which of the following should the technician check to verify the proxy configuration?
A. Network and Sharing Center
B. Internet Options
C. Firewall settings
D. System settings
Answer: (SHOW ANSWER)
The correct place to check proxy settings in Windows 10 is under Internet Options (Option B), specifically in the "Connections" tab. Proxy configurations can affect internet speeds if misconfigured or if a proxy is being used unnecessarily.
Network and Sharing Center (Option A) provides information on network connections but doesn't handle proxy settings.
Firewall settings (Option C) manage network traffic rules but don't directly affect proxy settings.
System settings (Option D) contain general system configurations, not specific to proxy settings.
CompTIA A+ Core 2 Reference:
1.6 - Configure networking features in Windows, including proxy settings

NEW QUESTION: 43
The Chief Executive Officer at a bark recently saw a news report about a high-profile cybercrime where a remote-access tool that the bank uses for support was also used in this crime. The report stated that attackers were able to brute force passwords to access systems. Which of the following would BEST limit the bark's risk? (Select TWO)
A. Enable multifactor authentication for each support account
B. Limit remote access to destinations inside the corporate network
C. Block all support accounts from logging in from foreign countries
D. Configure a replacement remote-access tool for support cases.
E. Purchase a password manager for remote-access tool users
F. Enforce account lockouts after five bad password attempts
Answer: A,F (LEAVE A REPLY)
The best ways to limit the bank's risk are to enable multifactor authentication for each support account and enforce account lockouts after five bad password attempts. Multifactor authentication adds an extra layer of security to the login process, making it more difficult for attackers to gain access to systems. Account lockouts after five bad password attempts can help to prevent brute force attacks by locking out accounts after a certain number of failed login attempts.

NEW QUESTION: 44
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: 45
Every time a user tries to open the organization's proprietary application on an Android tablet, the application immediately closes. Other applications are operating normally. Which of the following troubleshooting actions would MOST likely resolve the Issue? (Select TWO).
A. Uninstalling the application
B. Gaining root access to the tablet
C. Resetting the web browser cache
D. Deleting the application cache
E. Clearing the application storage
F. Disabling mobile device management
Answer: A,E (LEAVE A REPLY)
Uninstalling and reinstalling the application can resolve the issue of it crashing immediately on an Android tablet, as it can fix any corrupted or missing files or settings. Clearing the application storage can also resolve the issue, as it can free up space and remove any conflicting data. Gaining root access to the tablet, resetting the web browser cache, deleting the application cache and disabling mobile device management are not likely to resolve the issue, as they do not affect how the application runs. Verified Reference: https://www.comptia.org/blog/how-to-fix-android-apps-crashing https://www.comptia.org/certifications/a

NEW QUESTION: 46
A technician needs to strengthen security controls against brute-force attacks. Which of the following options best meets this requirement?
A. Multifactor authentication
B. Encryption
C. Increased password complexity
D. Secure password vault
Answer: (SHOW ANSWER)
Multifactor authentication (MFA) significantly enhances security by requiring two or more forms of verification before granting access to an account or system. This method is highly effective against brute-force attacks, where attackers attempt to guess a user's password through repeated trials. By implementing MFA, even if a password is compromised, unauthorized access is still prevented without the additional authentication factor(s), such as a code from a smartphone app, a fingerprint, or a physical security token.

* Multifactor authentication: Provides an additional layer of security beyond just the password, making it much harder for attackers to gain unauthorized access through brute-force methods, as they would need to compromise more than one authentication factor.
Encryption (B) is crucial for protecting data at rest and in transit, but it does not directly prevent brute-force login attempts. Increased password complexity (C) can deter brute-force attacks by making passwords harder to guess, but it is not as effective as MFA in preventing access when passwords are compromised. A secure password vault (D) helps users manage and store their passwords securely, which can indirectly contribute to security by allowing users to keep more complex passwords, but it does not directly prevent brute-force attacks on accounts.

NEW QUESTION: 47
Which of the following filesystem types does macOS use?
A. ext4
B. exFAT
C. NTFS
D. APFS
Answer: D (LEAVE A REPLY)
APFS stands for Apple File System and it is the default filesystem type for macOS since High Sierra (10.13) version1. APFS is optimized for flash storage and supports features such as encryption, snapshots, cloning, and space sharing1.

NEW QUESTION: 48
A SOHO client is having trouble navigating to a corporate website. Which of the following should a technician do to allow access?
A. Adjust the content filtering.
B. Unmap port forwarding.
C. Disable unused ports.
D. Reduce the encryption strength
Answer: (SHOW ANSWER)
Content filtering is a process that manages or screens access to specific emails or webpages based on their content categories1. Content filtering can be used by organizations to control content access through their firewalls and enforce corporate policies around information system management2. A SOHO client may have content filtering enabled on their network and may need to adjust it to allow access to a corporate website that is blocked by default. The client can use a software program, a hardware device, or a subscription service to configure the content filtering settings and whitelist the desired website2.

NEW QUESTION: 49
A customer is configuring on an old desktop an inexpensive file server to share photos and videos and wants to avoid complicated licensing. Which of the following operating systems should the technician most likely recommend?
A. Chrome OS
B. Linux
C. macOS
D. Windows
Answer: (SHOW ANSWER)
For an inexpensive file server to share photos and videos while avoiding complicated licensing, the technician should recommend:
* Linux: Linux is a free and open-source operating system that is ideal for setting up a file server. It offers robust file-sharing capabilities with minimal licensing complications.
* Chrome OS: Designed primarily for lightweight, web-based tasks and not ideal for a file server.
* macOS: Requires Apple hardware and involves more complex licensing compared to Linux.
* Windows: While capable of being a file server, Windows may involve licensing fees, particularly for server editions.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 1.8: Explain common OS types and their purposes.
Linux documentation and its use in setting up file servers.

NEW QUESTION: 50
Which of the following best describes XFS?
A. A filesystem used by the Linux OS
B. A filesystem used by iOS
C. A filesystem used by the Windows OS
D. A filesystem used by macOS
Answer: A (LEAVE A REPLY)
XFS is a high-performance filesystem created by Silicon Graphics in 1994 and is commonly used by Linux operating systems. It supports large files and directories and is known for its robustness and scalability. Other filesystems like NTFS (Windows), APFS (macOS), and HFS (macOS) are used on different platforms.

NEW QUESTION: 51
A user created a file on a shared drive and wants to prevent its data from being accidentally deleted by others. Which of the following applications should the technician use to assist the user with hiding the file?
A. Device Manager
B. Indexing Options
C. File Explorer
D. Administrative Tools
Answer: C (LEAVE A REPLY)
The technician should use the File Explorer application to assist the user with hiding the file 1. The user can right-click the file and select Properties. In the Properties dialog box, select the Hidden check box, and then click OK 1.

NEW QUESTION: 52
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: 53
A technician is working with a company to determine the best way to transfer sensitive personal information between offices when conducting business. The company currently uses USB drives and is resistant to change. The company's compliance officer states that all media at rest must be encrypted. Which of the following would be the BEST way to secure the current workflow?
A. Deploy a secondary hard drive with encryption on the appropriate workstation
B. Configure a hardened SFTP portal for file transfers between file servers
C. Require files to be individually password protected with unique passwords
D. Enable BitLocker To Go with a password that meets corporate requirements
Answer: D (LEAVE A REPLY)
The BEST way to secure the current workflow of transferring sensitive personal information between offices when conducting business is to enable BitLocker To Go with a password that meets corporate requirements. This is because BitLocker To Go is a full-disk encryption feature that encrypts all data on a USB drive, which is what the company currently uses, and requires a password to access the data.

NEW QUESTION: 54
A user is unable to see transaction details on a website, and nothing happens when the user clicks the details button. Which of the following should the user do to fix this issue?
A. Clear the browser cache.
B. Disable the pop-up blocker.
C. Configure private browsing.
D. Verify valid certificates.
Answer: B (LEAVE A REPLY)
Pop-up blockers can sometimes prevent essential pop-up windows required by websites to display transaction details.

Clear the browser cache: Helps with loading issues but not specific to pop-ups.
Disable the pop-up blocker: The correct solution, as it allows the blocked pop-up to be displayed.
Configure private browsing: Prevents storing browsing data but does not affect pop-ups.
Verify valid certificates: Ensures secure connections but does not resolve pop-up issues.

NEW QUESTION: 55
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: 56
A technician has been tasked with troubleshooting audiovisual issues in a conference room. The meeting presenters are unable to play a video with sound. The following error is received:
The Audio Driver is not running.
Which of the following will MOST likely resolve the issue?
A. compmgmt.msc
B. regedit.exe
C. explorer.exe
D. taskmgt.exe
E. gpmc.msc
F. services.msc

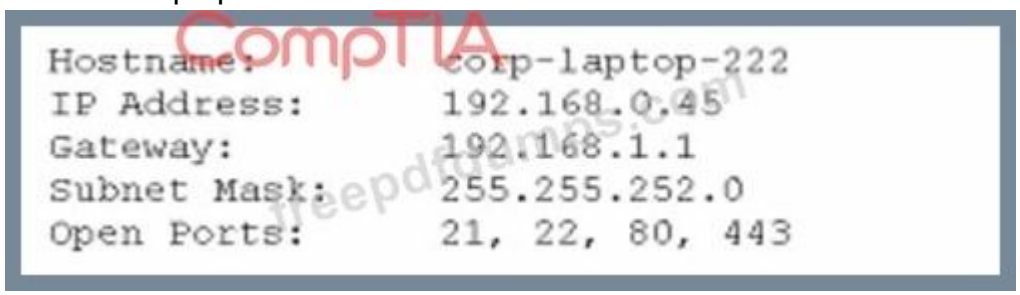
Answer: F (LEAVE A REPLY)
services.msc is a tool that can be used to resolve the issue of "The Audio Driver is not running" on a Windows machine. It allows a technician to view, start, stop and configure the services that run on the system, such as the Windows Audio service. compmgmt.msc, regedit.exe, explorer.exe, taskmgt.exe and gpmc.msc are other tools that can be used for different purposes on a Windows machine, but they are not related to audio drivers or services. Verified Reference: https://www.comptia.org/blog/what-is-services-msc https://www.comptia.org/certifications/a

NEW QUESTION: 57
A workstation does not recognize a printer. However, the previous day. the printer successfully received a job from the workstation. Which of the following tools should a technician use to see what happened before the failure?
A. Performance Monitor
B. Devices and Printers
C. Task Scheduler
D. Event Viewer
Answer: D (LEAVE A REPLY)
When troubleshooting a printer that was previously working but is no longer recognized by a workstation, Event Viewer is the most appropriate tool to check for historical logs and events related to the printer and the system.
Option A: Performance MonitorPerformance Monitor is used for monitoring system performance and resources in real-time and does not provide specific historical event logs related to device failures.
Option B: Devices and PrintersDevices and Printers show the status and properties of connected devices but do not provide a historical log of events or errors.
Option C: Task SchedulerTask Scheduler manages and monitors scheduled tasks but does not log hardware events or errors.
Option D: Event ViewerEvent Viewer logs system events, including errors, warnings, and information related to hardware and software. It is ideal for checking what happened prior to the printer failure.
Reference:
CompTIA A+ 220-1102 Objective 3.1 (Troubleshoot common Windows OS problems), particularly using Event Viewer for diagnosing issues.

NEW QUESTION: 58
A user's application is unresponsive. Which of the following Task Manager tabs will allow the user to address the situation?
A. Startup
B. Performance
C. Application history
D. Processes
Answer: (SHOW ANSWER)
The Processes tab in the Task Manager shows all the running processes on the computer, including applications and background services. The user can use this tab to identify the unresponsive application and end its process by right-clicking on it and selecting End task. This will free up the system resources and close the application. The other tabs in the Task Manager do not allow the user to address the situation. The Startup tab shows the programs that run when the

computer starts, the Performance tab shows the system resource usage and statistics, and the Application history tab shows the resource usage of the applications over time

NEW QUESTION: 59
A technician is trying to connect to a user's laptop in order to securely install updates. Given the following information about the laptop:



Which of the following should the technician do to connect via RDP?
A. Confirm the user can ping the default gateway.
B. Change the IP address on the user's laptop.
C. Change the subnet mask on the user's laptop.
D. Open port 3389 on the Windows firewall.
Answer: D (LEAVE A REPLY)
In order to connect to a user's laptop via RDP, the technician should open port 3389 on the Windows firewall. This is because RDP uses port 3389 for communication12. The other options are not necessary or relevant for establishing an RDP connection.
Confirming the user can ping the default gateway is not required for RDP, as it only tests the network connectivity between the user's laptop and the router. RDP works over the internet, so the technician should be able to ping the user's laptop directly using its IP address3.
Changing the IP address on the user's laptop is not needed for RDP, as long as the IP address is valid and not conflicting with another device on the network. The user's laptop has a valid IP address of 192.168.0.45, which belongs to the same subnet as the gateway (192.168.0.1) and the subnet mask (255.255.255.0)4.
Changing the subnet mask on the user's laptop is not required for RDP, as long as the subnet mask matches the network configuration. The user's laptop has a correct subnet mask of 255.255.255.0, which defines a network with 254 possible hosts4.
Reference:
1: [What is RDP and How Does It Work? - CompTIA] 2: CompTIA A+ Certification Exam Core 2 Objectives - CompTIA 3: [Ping (networking utility) - Wikipedia] 4: [IP address - Wikipedia] : What is RDP and How Does It Work? - CompTIA : CompTIA A+ Certification Exam Core 2 Objectives - CompTIA : Ping (networking utility) - Wikipedia) : IP address - Wikipedia

NEW QUESTION: 60
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: 61
A user's corporate iPhone had issues and was repaired while the user was on vacation. The mobile phone has compared to an identical phone. Which of the following best describes what is happening to the phone?
A. APK Source
B. Connectivity issues
C. Developer Mode
D. Jailbreak
Answer: (SHOW ANSWER)
A jailbroken iPhone (Option D) allows users to bypass Apple's restrictions to install unauthorized apps and modify system settings. This situation suggests the phone may have been compromised or tampered with, potentially voiding warranties and exposing the device to security vulnerabilities.
APK Source (Option A) refers to Android packages, not applicable to iPhones.
Connectivity issues (Option B) doesn't explain the comparison to an identical phone.
Developer Mode (Option C) is typically used for app development, not indicative of the situation.
CompTIA A+ Core 2 Reference:
2.7 - Explain mobile device security, including risks of jailbreaking

NEW QUESTION: 62
Which of the following protocols supports fast roaming between networks?
A. WEP
B. WPA
C. WPA2
D. LEAP

E. PEAP

Answer: C (LEAVE A REPLY)

WPA2 is the only protocol among the options that supports fast roaming between networks. Fast roaming, also known as IEEE 802.11r or Fast BSS Transition (FT), enables a client device to roam quickly in environments implementing WPA2 Enterprise security, by ensuring that the client device does not need to re-authenticate to the RADIUS server every time it roams from one access point to another1. WEP, WPA, LEAP, and PEAP do not support fast roaming and require the client device to perform the full authentication process every time it roams, which can cause delays and interruptions in the network service.

Reference:

The Official CompTIA A+ Core 2 Study Guide2, page 263.

WiFi Fast Roaming, Simplified3

NEW QUESTION: 63

A user reports a hardware issue to the help desk. Which of the following should the help desk technician do first when responding to the user?

A. Ask the user for the model number of the hardware.

B. Offer a temporary replacement device to the user.

C. Submit the issue to the manufacturer.

D. Remotely install updates to the device driver.

Answer: A (LEAVE A REPLY)

The first step in troubleshooting a hardware issue is to identify the hardware device that is causing the problem. Asking the user for the model number of the hardware can help the help desk technician to find the specifications, manuals, drivers, and other relevant information for the device. This can also help the technician to determine if the device is compatible with the user's system, if it has any known issues or defects, and if it is covered by warranty or support contract. Asking the user for the model number of the hardware is a help desk best practice that can save time and effort in resolving the issue

NEW QUESTION: 64

Which of the following technologies is proprietary and can be configured to use MFA?

A. WPA2

B. MS-CHAPv2

C. Kerberos

D. RADIUS

Answer: (SHOW ANSWER)

NEW QUESTION: 65

A technician has verified that a user's computer has a virus and the antivirus software is out of date. Which of the following steps should the technician take next?

A. Quarantine the computer.

B. Use a previous restore point.

C. Educate the end user about viruses.

D. Download the latest virus definitions.

Answer: D (LEAVE A REPLY)
The first step in removing a virus from a computer is to update the antivirus software with the latest virus definitions. Virus definitions are files that contain information about the characteristics and behavior of known viruses and malware. They help the antivirus software to identify and remove the malicious threats from the computer. Without the latest virus definitions, the antivirus software may not be able to detect or remove the virus that infected the user's computer. Therefore, the technician should download the latest virus definitions from the antivirus vendor's website or use the update feature in the antivirus program before scanning the computer for viruses.
Reference:
How to remove malware or viruses from my Windows 10 PC, section 21
How to Remove a Virus From a Computer in 2023, section 32
The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2193

NEW QUESTION: 66
A client's device was recently used by multiple other users. The client reports their device is now running slower than usual. Which of the following steps should a technician take first? (Select two.)
A. Perform a virus scan
B. Check the startup programs
C. Back up the data
D. Disable the guest account
E. Update the firmware
F. Reinstall the operating system
Answer: A,B (LEAVE A REPLY)
Comprehensive and Detailed In-Depth
The two best first steps are:
Perform a virus scan - Multiple users on a device increase the risk of malware, which can cause performance issues.
Check the startup programs - Unnecessary programs running at startup can slow down the system.
C . Back up the data - Important but not the first step for performance troubleshooting.
D . Disable the guest account - May prevent future unauthorized use but does not immediately fix the current issue.
E . Update the firmware - Firmware updates improve hardware stability but are unlikely to fix a sudden performance drop.
F . Reinstall the operating system - A last resort, as it erases data and takes significant time.
Reference:
CompTIA A+ 220-1102, Objective 2.4 - Malware and Security Threat Removal

NEW QUESTION: 67
Which of the following is used to detect and record access to restricted areas?
A. Bollards
B. Video surveillance
C. Badge readers
D. Fence
Answer: (SHOW ANSWER)

Badge readers are devices that scan employee or visitor credentials, logging entries and exits from restricted areas. Video surveillance (B) provides a visual record but does not directly control access. Bollards (A) and fences (D) provide physical security but cannot detect or record access events.

NEW QUESTION: 68
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: 69
A Linux technician needs a filesystem type that meets the following requirements:
. All changes are tracked.
. The possibility of file corruption is reduced.
* Data recovery is easy.
Which of the following filesystem types best meets these requirements?
ext3
A. FAT32
B. exFAT
C. NTFS
Answer: A (LEAVE A REPLY)
The ext3 file system is a Linux native file system that meets the requirements of the question. It has the following features:
All changes are tracked. The ext3 file system uses a journaling mechanism that records all changes to the file system metadata in a special log called the journal before applying them to the actual file system. This ensures that the file system can be restored to a consistent state in case of a power failure or system crash12.
The possibility of file corruption is reduced. The journaling feature of ext3 also reduces the possibility of file corruption, as it avoids the need for a full file system check after an unclean shutdown. The file system can be quickly replayed from the journal and any inconsistencies can be fixed12.
Data recovery is easy. The ext3 file system supports undeletion of files using tools such as ext3grep or extundelete, which can scan the file system for deleted inodes and attempt to recover the data blocks associated with them34.
Reference:
1: Introduction to Linux File System [Structure and Types] - MiniTool1 2: 7 Ways to Determine the File System Type in Linux (Ext2, Ext3 or Ext4) - Tecmint3 3: How to Recover Deleted Files in Linux with ext3grep 4: How to Recover Deleted Files from ext3 Partitions

NEW QUESTION: 70
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 (LEAVE A REPLY)
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: 71
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: 72
A technician installs specialized software on a workstation. The technician then attempts to run the software. The workstation displays a message indicating the software is not authorized to run. Which of the following should the technician do to most likely resolve the issue?
A. Install the software in safe mode.
B. Attach the external hardware token.
C. Install OS updates.
D. Restart the workstation after installation.
Answer: B (LEAVE A REPLY)
A hardware token is a physical device that provides an additional layer of security for software authorization. Some specialized software may require a hardware token to be attached to the workstation in order to run. A hardware token may contain a cryptographic key, a password, or a one-time code that verifies the user's identity or permission. Installing the software in safe mode, installing OS updates, and restarting the workstation after installation are not likely to resolve the issue of software authorization.

NEW QUESTION: 73

A corporate smartphone was stored for five months after setup. During this time, the company did not have any system updates. When the phone is turned on, an application runs, but it crashes intermittently. Which of the following should a technician do next?
Restart the phone.
A. Reimage the OS.
B. Reinstall the application.
C. Clear the cache.
Answer: C (LEAVE A REPLY)
Reinstalling the application is the best option to fix the intermittent crashing of the application on the corporate smartphone. Reinstalling the application will ensure that the latest version of the app is installed, which may have bug fixes and compatibility updates that can resolve the crashing issue. Reinstalling the app will also clear any corrupted or outdated data or cache that may cause the app to malfunction.
The other options are not as effective or appropriate as reinstalling the app. Restarting the phone may temporarily fix the issue, but it will not address the root cause of the app crashing, which may be related to the app itself or its data. Reimaging the OS is a drastic and unnecessary measure that will erase all the data and settings on the phone and restore it to its factory state. This will also remove all the other apps and files that may be important for the corporate use of the phone. Clearing the cache may help to free up some space and improve the performance of the app, but it will not update the app or fix any bugs that may cause the app to crash.
Reference:
Top 5 Reasons Behind Your App Crash and Solutions To Fix Them1
How to Stop Apps From Crashing on Android2
Why are my Android phone apps crashing or closing & how to fix the issue3

NEW QUESTION: 74
A technician is troubleshooting an issue with a computer that contains sensitive information. The technician determines the computer needs to be taken off site for repair. Which of the following should the technician do NEXT?
A. Remove the HDD and then send the computer for repair.
B. Check corporate polices for guidance.
C. Delete the sensitive information before the computer leaves the building.
D. Get authorization from the manager.
Answer: D (LEAVE A REPLY)
The next step that the technician should do before taking the computer off site for repair is to get authorization from the manager. Getting authorization from the manager is important because it ensures that the technician has permission and approval to remove the computer from the premises and perform the repair work off site. Getting authorization from the manager can also help document and communicate the reason and duration of the repair and avoid any misunderstanding or conflict with the user or the organization. Removing the HDD and then sending the computer for repair may not be feasible or necessary if the issue is not related to the HDD or if the HDD contains essential data or software for the repair. Checking corporate policies for guidance may be a good step but it does not replace getting authorization from the manager who is responsible for the computer and its data. Deleting the sensitive information before the computer leaves the building may not be possible or advisable if the issue prevents access to the data or if the data is needed for

troubleshooting or recovery purposes. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.1

NEW QUESTION: 75
A corporation purchased new computers for a school. The computers are the same make and model and need to have the standard image loaded. Which of the following orchestration tools should a desktop administrator use tor wide-scale deployment?
A. USB drive
B. DVD Installation media
C. PXE boot
D. Recovery partition
Answer: C (LEAVE A REPLY)
PXE (Preboot eXecution Environment) boot is an orchestration tool that allows a desktop administrator to deploy a standard image to multiple computers over a network. It requires a PXE server that hosts the image and a PXE client that boots from the network interface card (NIC). USB drive and DVD installation media are not orchestration tools, but manual methods of installing an image on each computer individually. Recovery partition is not an orchestration tool, but a hidden partition on the hard drive that contains an image of the factory settings. Verified Reference: https://www.comptia.org/blog/what-is-pxe-boot https://www.comptia.org/certifications/a

NEW QUESTION: 76
A customer needs to verify an executable file that the customer downloaded from a website. Which of the following should the customer use to verify the file?
A. Password manager
B. BitLocker
C. FileVault
D. Checksum
E. Secure site
Answer: D (LEAVE A REPLY)
A checksum is a cryptographic hash function (like MD5 or SHA-256) used to verify the integrity of files. When downloading files from the internet, websites often provide the checksum value of the file so that users can ensure the file was not altered during download or corrupted. The user can generate the checksum on their local system and compare it to the one provided by the site. If they match, the file is intact and safe to use. Other options like BitLocker or FileVault are encryption tools, and a password manager is irrelevant to file verification.
Reference:
CompTIA A+ 220-1102 Domain 3.5: File Integrity Checking (CompTIA) (ProfMesser)

NEW QUESTION: 77
A user sent a large amount of money to a supplier's bank account and claims that the Chief Executive Officer instructed the user to do so. A technician informs the user that the request was fraudulent and contacts the authorities. Which of the following types of attack took place?
A. Whaling attack
B. Phishing
C. Insider threat
D. Spoofing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 78
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: A (LEAVE A REPLY)
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: 79
A customer needs to purchase a desktop capable of rendering video. Which of the following should the customer prioritize?
A. NIC
B. USB
C. GPU
D. HDMI
Answer: C (LEAVE A REPLY)
For rendering video, the most critical component a customer should prioritize in a desktop is:
* GPU (Graphics Processing Unit):The GPU is specifically designed to handle complex graphics and video rendering tasks. A powerful GPU will significantly improve performance in video rendering applications.
* NIC (Network Interface Card):Important for network connectivity but irrelevant for video rendering.

* USB:Useful for peripherals but does not impact video rendering capabilities.
* HDMI:An important output interface for connecting monitors but not crucial for the rendering process itself.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 1.8: Explain common OS types and their purposes, including hardware components for specific tasks.
GPU importance in video rendering documentation.

NEW QUESTION: 80
A technician suspects a rootkit has been installed and needs to be removed. Which of the following would BEST resolve the issue?
A. Application updates
B. Anti-malware software
C. OS reinstallation
D. File restore
Answer: C (LEAVE A REPLY)
If a rootkit has caused a deep infection, then the only way to remove the rootkit is to reinstall the operating system. This is because rootkits are designed to be difficult to detect and remove, and they can hide in the operating system's kernel, making it difficult to remove them without reinstalling the operating system
https://www.minitool.com/backup-tips/how-to-get-rid-of-rootkit-windows-10.html

NEW QUESTION: 81
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: (SHOW ANSWER)
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: 82
A company wants to take advantage of modern technology and transition away from face-to-face meetings. Which of the following types of software would benefit the company the most? (Select two).
A. Videoconferencing
B. File transfer
C. Screen-sharing
D. Financial
E. Remote access

F. Record-keeping

Answer: A,C (LEAVE A REPLY)

For a company looking to transition away from face-to-face meetings, videoconferencing and screen-sharing software would be most beneficial.

Videoconferencing software allows participants to conduct virtual meetings with audio and video capabilities, effectively simulating a face-to-face interaction without the need for physical presence. This can greatly reduce travel costs and time while maintaining the personal touch of meetings.

Screen-sharing enables participants in a virtual meeting to view one another's computer screens in real time. This is particularly useful for presentations, collaborative work, and troubleshooting, as it allows for a more interactive and engaging meeting experience.

Both technologies support the company's goal of leveraging modern technology to enhance communication and collaboration while reducing reliance on physical meetings.

NEW QUESTION: 83

A technician needs to add an individual as a local administrator on a Windows home PC. Which of the following utilities would the technician MOST likely use?

A. Settings > Personalization

B. Control Panel > Credential Manager

C. Settings > Accounts > Family and Other Users

D. Control Panel > Network and Sharing Center

Answer: C (LEAVE A REPLY)

The technician would most likely use Settings > Accounts > Family and Other Users to add an individual as a local administrator on a Windows home PC. Settings > Accounts > Family and Other Users allows users to add and manage other user accounts on their Windows PC. The technician can add an individual as a local administrator by selecting Add someone else to this PC under Other users and following the steps to create a new user account with administrator privileges. Settings > Personalization allows users to customize the appearance and behavior of their desktop, such as themes, colors, backgrounds, lock screen and screensaver. Settings > Personalization is not related to adding an individual as a local administrator on a Windows home PC but to configuring desktop settings and preferences. Control Panel > Credential Manager allows users to view and manage their web credentials and Windows credentials stored on their Windows PC. Control Panel > Credential Manager is not related to adding

NEW QUESTION: 84

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

A. Shut down the infected computer and swap it with another computer

B. Investigate what the interface is and what triggered it to pop up

C. Proceed with initiating a full scan and removal of the viruses using the presented interface

D. Call the phone number displayed in the interface of the antivirus removal tool

Answer: C (LEAVE A REPLY)

The technician should not proceed with initiating a full scan and removal of the viruses using the presented interface or call the phone number displayed in the interface of the antivirus removal tool12 Shutting down the infected computer and swapping it with another computer is not necessary at this point12 The technician should not immediately assume that the message is legitimate or perform any actions without knowing what the interface is and what triggered it to pop up. It is important to investigate the issue further, including checking the legitimacy of the antivirus program and the message it is displaying.

NEW QUESTION: 85
A customer installed a new web browser from an unsolicited USB drive that the customer received in the mail. The browser is not working as expected, and internet searches are redirected to another site. Which of the following should the user do next after uninstalling the browser?
A. Delete the browser cookies and history.
B. Reset all browser settings.
C. Change the browser default search engine.
D. Install a trusted browser.
Answer: D (LEAVE A REPLY)
The customer's web browser is likely infected by a browser hijacker, which is a type of malware that changes the browser's settings and redirects the user to malicious websites. A browser hijacker can also steal the user's personal data, display unwanted ads, and install more malware on the device. To remove a browser hijacker, the user should first uninstall the browser from the Control Panel, then scan the device with an antivirus or anti-malware program, and finally install a trusted browser from a legitimate source. Deleting the browser cookies and history, resetting the browser settings, or changing the browser default search engine may not be enough to get rid of the browser hijacker, as it may have embedded itself into the system or other browser components.

NEW QUESTION: 86
A technician is building a new desktop machine for a user who will be using the workstation to render 3-D promotional movies. Which of the following is the most important component?
A. Dedicated GPU
B. DDR5 SODIMM
C. NVMe disk
D. 64-bit CPU
Answer: (SHOW ANSWER)
A dedicated GPU (graphics processing unit) is the most important component for rendering 3-D promotional movies, as it can handle the complex calculations and graphics operations required for creating realistic and high-quality images. A dedicated GPU has its own memory and processor, which are optimized for graphics tasks. A dedicated GPU can also support multiple monitors, high resolutions, and advanced features such as ray tracing12.

NEW QUESTION: 87
Which of the following is the best way to limit the loss of confidential data if an employee's company smartphone is lost or stolen?
A. Installing a VPN

B. Implementing location tracking
C. Configuring remote wipe
D. Enabling backups
Answer: C (LEAVE A REPLY)
Configuring remote wipe allows the device owner or administrator to erase all the data on the device remotely, in case it is lost or stolen. This prevents unauthorized access to confidential data and reduces the risk of data breaches. Installing a VPN, implementing location tracking, and enabling backups are useful features, but they do not directly limit the loss of data if the device is compromised. Reference: CompTIA A+ Certification Exam Core 2 Objectives, Domain 2.0: Security, Objective 2.5: Given a scenario, use methods to secure mobile devices.

NEW QUESTION: 88
A user attempts to open some files, but a message appears stating that the files are encrypted. The user was able to access these files before without receiving this message and no changes have been made within the company. Which of the following has infected the computer?
A. Cryptominer
B. Phishing
C. Ransomware
D. Keylogger
Answer: C (LEAVE A REPLY)
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: 89
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: 90
A user asks a technician for recommendations to back up desktop data from a Windows OS. The technician recommends implementing daily full backups, but the user is concerned about having enough space. Which of the following additional backup methods should the technician recommend?
A. Transaction log
B. Incremental
C. Synthetic
D. Differential
Answer: (SHOW ANSWER)
Detailed Explanation with Core 2 Reference:Incremental backups only save changes made since the last backup, significantly reducing storage space requirements compared to full backups. This approach is consistent with the Core 2 objective of understanding various backup methods and their space requirements (Core 2 Objective 4.3).

NEW QUESTION: 91
Which of the following defines the extent of a change?
A. Scope
B. Purpose
C. Analysis
D. Impact
Answer: A (LEAVE A REPLY)
The term that defines the extent of a change is scope. Scope is a measure of the size, scale and boundaries of a project or an activity. Scope defines what is included and excluded in the project or activity, such as goals, requirements, deliverables, tasks and resources. Scope helps determine the feasibility, duration and cost of the project or activity. Scope also helps manage the expectations and needs of the stakeholders involved in the project or activity. Purpose is the reason or objective for doing a project or an activity. Purpose defines why the project or activity is important or necessary, such as solving a problem, meeting a need or achieving a goal. Purpose helps provide direction, motivation and justification for the project or activity. Analysis is the process of examining, evaluating and interpreting data or information related to a project or an activity. Analysis helps identify, understand and prioritize issues, risks, opportunities and solutions for the project or activity. Impact is the effect or outcome of a project or an activity on something or someone else. Impact defines how the project or activity affects or influences other factors, such as performance, quality, satisfaction or value. Impact helps measure the success and effectiveness of the project or activity. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 5.2

NEW QUESTION: 92
A user requested that the file permissions on a Linux device be changed to only allow access to a certain group of users. Which of the following commands should be used to complete the user's request?
A. cat
B. chmod
C. pwd
D. cacls
Answer: B (LEAVE A REPLY)
The chmod command is used to change the permissions of files and directories in Linux. It can grant or revoke read, write, and execute permissions for the owner, the group, and others. To change the file permissions to only allow access to a certain group of users, the chmod command can use either the symbolic or the numeric mode. For example, to give read and write permissions to the group and no permissions to others, the command can be:
chmod g+rw,o-rwx filename
or
chmod 660 filename

NEW QUESTION: 93
A technician is setting up a network printer for a customer who has a SOHO router. The technician wants to make sure the printer stays connected in the future and is available on all the computers in the house. Which of the following should the technician configure on the printer?
A. DNS settings
B. Static IP
C. WWAN
D. Meteredconnection
Answer: B (LEAVE A REPLY)
Configuring a static IP address for a network printer in a SOHO (Small Office/Home Office) environment ensures that the printer maintains the same IP address over time. This consistency is crucial for networked devices like printers, as computers and other devices rely on this specific address to connect to the printer. If the printer's IP address were to change (as it might with DHCP), devices would no longer be able to communicate with it without reconfiguration.
* Static IP: Assigning a static IP address to the printer ensures it always uses the same IP, making it reliably accessible to all computers in the house regardless of network changes or router reboots.
DNS settings (A) are generally not necessary to configure directly on most network printers unless you're dealing with advanced network configurations or using the printer for scanning to email functions. WWAN (C) stands for Wireless Wide Area Network, which is not typically relevant for a standard network printer setup in a home or small office. Metered connection (D) is a Windows feature that helps reduce data usage on a connection, it's not relevant to configuring a printer's network settings.

NEW QUESTION: 94

A technician is setting up a printer on a Linux workstation. Which of the following commands should the technician use to set the default printer?

A. ipr

B. lspool

C. lpstat

D. lpoptions

Answer: A (LEAVE A REPLY)

In Linux, thelpcommand is used to manage print jobs, including setting the default printer. Thelpcommand allows users to send print jobs to a printer queue, check the status of print jobs, and cancel print jobs, among other functionalities. By using options and parameters with thelpcommand, a technician can specify a particular printer as the default for future print jobs, ensuring that documents are routed to the correct printer without needing to specify it each time.

NEW QUESTION: 95

A technician was assigned a help desk ticket and resolved the issue. Which of the following should the technician update to assist other technicians in resolving similar issues?

End user training

A. Progress notes

B. Knowledge base

C. Acceptable use policy document

Answer: (SHOW ANSWER)

A knowledge base is a centralized repository of information that can be used by technicians to find solutions to common problems, best practices, troubleshooting guides, and other useful resources12. Updating the knowledge base with the details of the issue and the resolution can help other technicians who encounter similar issues in the future. It can also reduce the number of tickets and improve customer satisfaction3.

Reference1: The Official CompTIA A+ Core 2 Student Guide (Exam 220-1102), page 10-11 2: CompTIA A+ Certification Exam Core 2 Objectives, page 13 3: CompTIA A+ Core 2 (220-1102) Certification Study Guide, page 10-12

NEW QUESTION: 96

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

A. Encrypting File System

B. FileVault

C. BitLocker

D. Encrypted LVM

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 97

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: B (LEAVE A REPLY)
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: 98
When visiting a particular website, a user receives a message stating, "Your connection is not private." Which of the following describes this issue?
A. Certificate warning
B. Malware
C. JavaScript error
D. Missing OS update
Answer: A (LEAVE A REPLY)
A certificate warning is a message that appears when a web browser cannot verify the identity or security of a website. It usually means that there is a problem with the website's SSL certificate, such as expiration, invalidity, or mismatch. A certificate warning can indicate that the website is unsafe or compromised, and that the user's connection is not private123.

NEW QUESTION: 99
A technician requires graphical remote access to various Windows, Linux, and macOS desktops on the company LAN. The security administrator asks the technician to utilize a single software solution that does not require an external internet connection. Which of the following remote access tools is the technician most likely to install?
A. VNC
B. RMM
C. RDP
D. SSH
Answer: (SHOW ANSWER)
VNC (Virtual Network Computing) is a remote access tool that allows the technician to access and control various Windows, Linux, and macOS desktops on the company LAN using a graphical user interface. VNC does not require an external internet connection, as it works over a local network or a VPN. VNC uses a client-server model, where the server runs on the remote desktop and the client connects to it from another device. VNC can transmit the keyboard and mouse events from the client to the server, and the screen updates from the server to the client, enabling the technician to interact with the remote desktop as if it were local12.
VNC is a better option than the other choices because:
RMM (Remote Monitoring and Management) (B) is not a single software solution, but a category of software solutions that enable IT professionals to remotely monitor, manage, and troubleshoot multiple devices and networks. RMM software may include remote access tools, but also other features such as patch management, backup and recovery, security, reporting,

and automation. RMM software may require an external internet connection, as it often relies on cloud-based services or web-based consoles34.
RDP (Remote Desktop Protocol) is a remote access tool that allows the technician to access and control Windows desktops on the company LAN using a graphical user interface. However, RDP is not compatible with Linux or macOS desktops, unless they have third-party software installed that can emulate or translate the RDP protocol. RDP also has some security and performance issues, such as encryption vulnerabilities, bandwidth consumption, and latency problems56.
SSH (Secure Shell) (D) is a remote access tool that allows the technician to access and control various Windows, Linux, and macOS desktops on the company LAN using a command-line interface. SSH does not require an external internet connection, as it works over a local network or a VPN. SSH uses encryption and authentication to secure the communication between the client and the server. However, SSH does not provide a graphical user interface, which may limit the functionality and usability of the remote desktop7 .
Reference:
1: What is VNC? - Definition from Techopedia1 2: How VNC Works - RealVNC2 3: What is Remote Monitoring and Management (RMM)? - Definition from Techopedia3 4: What is RMM Software? - NinjaRMM4 5: What is Remote Desktop Protocol (RDP)? - Definition from Techopedia5 6: Remote Desktop Protocol: What it is and how to secure it - CSO Online6 7: What is Secure Shell (SSH)? - Definition from Techopedia7 : How to Use SSH to Access a Remote Server in Linux or Windows - Hostinger Tutorials

NEW QUESTION: 100
Which of the following should be documented to ensure that the change management plan is followed?
A. Scope of the change
B. Purpose of the change
C. Change rollback plan
D. Change risk analysis
Answer: A (LEAVE A REPLY)
The scope of the change is one of the elements that should be documented to ensure that the change management plan is followed. The scope of the change defines the boundaries and limitations of the change, such as what is included and excluded, what are the deliverables and outcomes, what are the assumptions and constraints, and what are the dependencies and risks. The scope of the change helps to clarify the expectations and objectives of the change, as well as to prevent scope creep or deviation from the original plan. The scope of the change also helps to measure the progress and success of the change, as well as to communicate the change to the stakeholders and the team

NEW QUESTION: 101
A customer, whose smartphone's screen was recently repaired, reports that the device has no internet access through Wi-Fi. The device shows that it is connected to Wi-Fi, has an address of 192.168.1.42. and has no subnet mask. Which of the following should the technician check next?
A. Internal antenna connections
B. Static IP settings
C. Airplane mode
D. Digitizer calibration

Answer: (SHOW ANSWER)
Given that the smartphone's screen was recently repaired and now experiences issues with Wi-Fi connectivity, despite showing that it is connected to a network, the problem could be related to the internal antenna connections that might have been disturbed or disconnected during the repair process.
* Internal Antenna Connections: Smartphones use internal antennas for Wi-Fi and cellular connections. If these antennas are not properly connected, the device may show as connected to a Wi-Fi network but fail to transmit data effectively, resulting in no internet access.
Checking static IP settings (B) would be relevant if the device were not obtaining an IP address at all, but the device does have an IP address. Airplane mode (C) would prevent the device from connecting to Wi-Fi networks entirely. Digitizer calibration (D) is related to the touchscreen functionality and would not affect Wi- Fi connectivity.

NEW QUESTION: 102
After a failed update, an application no longer launches and generates the following error message: Application needs to be repaired. Which of the following Windows 10 utilities should a technician use to address this concern?
A. Device Manager
B. Administrator Tools
C. Programs and Features
D. Recovery
Answer: D (LEAVE A REPLY)
Recovery is a Windows 10 utility that can be used to address the concern of a failed update that prevents an application from launching. Recovery allows the user to reset the PC, go back to a previous version of Windows, or use advanced startup options to troubleshoot and repair the system2. Device Manager, Administrator Tools, and Programs and Features are not Windows 10 utilities that can fix a failed update.

NEW QUESTION: 103
Which of the following security threats requires a phone call to launch the attack?
A. XSS
B. DDoS
C. Spoofing
D. Vishing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 104
Which of the following script file types is typically used to install Windows packages?
A. .py
B. .sh
C. .js
D. .ps1
Answer: D (LEAVE A REPLY)

NEW QUESTION: 105

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 (LEAVE A REPLY)
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: 106
An Android user reports that when attempting to open the company's proprietary mobile application it immediately doses. The user states that the issue persists, even after rebooting the phone. The application contains critical information that cannot be lost. Which of the following steps should a systems administrator attempt FIRST?
A. Uninstall and reinstall the application
B. Reset the phone to factory settings
C. Install an alternative application with similar functionality
D. Clear the application cache.
Answer: (SHOW ANSWER)
The systems administrator should clear the application cache12
If clearing the application cache does not work, the systems administrator should uninstall and reinstall the application12
Resetting the phone to factory settings is not necessary at this point12 Installing an alternative application with similar functionality is not necessary at this point12

NEW QUESTION: 107
A user identified that a program installed in a workstation does not have optional features enabled. Which of the following must the technician do to install the optional features?
A. Goto Programs andFeatures, uninstall the program, and reinstallit.

B. Goto AdministrativeTools and edit System Configuration.
C. Goto AdministrativeTools and run Disk Cleanup.
D. Goto Programs andFeatures, select the program, and click onChange.
Answer: (SHOW ANSWER)
When a user needs to install optional features for a program that is already installed, the technician should:
* Go to Programs and Features: Access this via the Control Panel.
* Select the program: Find the installed program in the list.
* Click on Change: The "Change" option allows modifications to the installed program, such as adding or removing features, without completely uninstalling and reinstalling the program.
This method is the most efficient and avoids unnecessary reinstallation of the software, which could lead to data loss or require reconfiguration.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 1.4: Given a scenario use the appropriate Microsoft Windows 10 Control Panel utility.
Windows application management documentation.

NEW QUESTION: 108
A user downloaded a 64-bit version of a new software program, but the installation failed due to an error. Which of the following most likely caused the error?
A. The OS version is incompatible.
B. The user needs to enable ActiveX.
C. The .NET Framework needs to be updated.
D. The user needs administrator privileges.
Answer: (SHOW ANSWER)
The most likely reason for the installation failure of a 64-bit software is that the operating system is incompatible, specifically if the system is running a 32-bit version of the OS. A 64-bit program requires a 64-bit operating system to run, and if the user's OS is a 32-bit version, the software will fail to install. Other reasons, like needing administrator privileges or updating .NET, are valid but less likely since the error message would be different.
Reference:
Microsoft Support: 32-bit and 64-bit Windows: Frequently Asked Questions CompTIA A+ 220-1102 Study Guide (CompTIA) (ProfMesser)

NEW QUESTION: 109
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: 110
A student is setting up a new Windows 10 laptop for the upcoming semester. The student is interested in customizing the wallpaper. Which of the following should the student use to change the wallpaper?
A. Apps and Features
B. Personalization
C. File Explorer
D. Task Manager

Answer: B (LEAVE A REPLY)
To change the wallpaper on a Windows 10 laptop, the "Personalization" settings should be used. These settings allow users to customize themes, which include various aspects of the desktop environment such as the desktop wallpaper, screen saver, color scheme, and more. This makes "Personalization" the correct option for customizing the wallpaper.Reference: Official CompTIA A+ Core 1 and Core 2 Student Guide.

NEW QUESTION: 111
A user received an alert from a Windows computer indicating low storage space. Which of the following will best resolve this issue?
A. Reviewing System Information
B. Running Disk Cleanup
C. Editing the Registry
D. Checking the Performance Monitor
E. Increasing the memory
Answer: (SHOW ANSWER)
To resolve an issue of low storage space on a Windows computer, the best approach is to Run Disk Cleanup (B). Disk Cleanup is a built-in utility that helps users free up space on their hard drives by deleting temporary files, system files, and other unnecessary files that are no longer needed, thereby resolving low storage space issues

NEW QUESTION: 112
A user reports a computer is running slow. Which of the following tools will help a technician identify the issue?

A. Disk Cleanup
B. Group Policy Editor
C. Disk Management
D. Resource Monitor
Answer: D (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: 113
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: A,C (LEAVE A REPLY)
The technician can close unnecessary applications and turn on autorotation to resolve these issues with minimal impact. Autorotation can help the device to switch between portrait and landscape modes automatically. Closing unnecessary applications can help to free up the device's memory and reduce the device's temperature1 Reference:
CompTIA A+ Certification Exam: Core 2 (220-1102) Exam Objectives Version 4.0. Retrieved from https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0)

NEW QUESTION: 114
A user is experiencing the following issues with Bluetooth on a smartphone:
* The user cannot hear any sound from a speaker paired with the smartphone.
* The user is having issues synchronizing data from their smart watch, which is also connected via Bluetooth.
A technician checked the Bluetooth settings, confirmed it is successfully paired with a speaker, and adjusted the volume levels, but still could not hear anything. Which of the following steps should the technician take next to troubleshoot the Bluetooth issues?
A. Restart the smartphone.
B. Reset the network settings.
C. Unpair the Bluetooth speaker.
D. Check for system updates.
Answer: A (LEAVE A REPLY)

Restarting the smartphone can resolve a wide range of technical issues, including those related to Bluetooth connectivity. This simple step can refresh the system and eliminate temporary software glitches that might be interfering with Bluetooth functions like audio output and data synchronization.
Restart the smartphone: This action clears the system's RAM and can resolve conflicts between the Bluetooth service and other processes running on the smartphone, potentially fixing both the audio and synchronization issues.
Resetting network settings (B) could also potentially fix the issue but is a more drastic step that also clears Wi-Fi networks and passwords, cellular settings, and VPN configurations, which might not be necessary. Unpairing the Bluetooth speaker (C) could help if the issue is specific to the speaker, but since there are also synchronization issues with the smartwatch, the problem seems broader. Checking for system updates (D) is a good general maintenance step, but it's more likely to help with ongoing or known issues rather than immediate connectivity problems.

NEW QUESTION: 115
Which of The following refers to the steps to be taken if an Issue occurs during a change Implementation?
A. Testing
B. Rollback
C. Risk
D. Acceptance
Answer: (SHOW ANSWER)
Rollback refers to the steps to be taken if an issue occurs during a change implementation. It means restoring the system to its previous state before the change was applied, using backup data or configuration files. It can minimize the impact and downtime caused by a failed change. Testing refers to the steps to be taken before a change implementation, to verify that the change works as expected and does not cause any errors or conflicts. Risk refers to the potential negative consequences of a change implementation, such as data loss, security breach, performance degradation, etc. Acceptance refers to the steps to be taken after a change implementation, to confirm that the change meets the requirements and expectations of the stakeholders. Verified Reference: https://www.comptia.org/blog/change-management-process https://www.comptia.org/certifications/a

NEW QUESTION: 116
Which of the following filesystems is most likely to be used for the boot volume on a Linux desktop?
A. APFS
B. HFS
C. NTFS
D. ext4
Answer: D (LEAVE A REPLY)

NEW QUESTION: 117
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: (SHOW ANSWER)
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/sc40crsbook_chapter1.html

NEW QUESTION: 118
Which of the following macOS features provides the user with a high-level view of all open windows?
A. Mission Control
B. Finder
C. Multiple Desktops
D. Spotlight
Answer: (SHOW ANSWER)
Mission Control is the macOS feature that provides the user with a high-level view of all open windows. Mission Control allows the user to see and switch between multiple desktops, full-screen apps, and windows in a single screen. Mission Control can be accessed by swiping up with three or four fingers on the trackpad, pressing F3 on the keyboard, or moving the cursor to a hot corner

NEW QUESTION: 119
A small company has an office in a multitenant building. The company has implemented a wireless network for its employees to use. However, the network speeds are slow, and many employees have had intermittent access to the Internet. The network consists of a single wireless router with default settings in place. Which of the following should a technician do to improve the network speed and Internet access?
A. Enable WPA3 security.
B. Implement MAC filtering.
C. Change the wireless channel.
D. Create a guest network.
Answer: (SHOW ANSWER)

NEW QUESTION: 120
A technician needs to open a port on a firewall in order to connect to a Linux server via a terminal interface. Which of the following ports should the technician open?
A. 22
B. 21
C. 53
D. 443
E. 3389
Answer: (SHOW ANSWER)

NEW QUESTION: 121

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: 122

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 (LEAVE A REPLY)

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: 123

A company has experienced a ransomware attack. Which of the following is the best way to recover from ransomware?

A. Antivirus

B. Backups

C. Anti-malware

D. Recovery mode

Answer: B (LEAVE A REPLY)
Comprehensive and Detailed In-Depth
The best way to recover from a ransomware attack is by restoring clean backups of the affected files. Ransomware encrypts files and demands a ransom for decryption, but paying the ransom is not recommended because it does not guarantee file recovery.
A . Antivirus - Incorrect. Antivirus software may detect and remove the ransomware, but it cannot decrypt the files.
C . Anti-malware - Incorrect. Anti-malware software helps prevent infection but cannot recover encrypted files.
D . Recovery mode - Incorrect. Recovery mode restores system files but does not recover user data from ransomware.
Best Practice:
Regularly back up critical data and store backups in offline or cloud-based solutions to prevent ransomware from encrypting them.
Reference:
CompTIA A+ 220-1102, Objective 2.4 - Removing Malware and Security Threats

NEW QUESTION: 124
A technician is troubleshooting an issue that requires a user profile to be rebuilt. The technician is unable to locate Local Users and Groups in the Mtv1C console. Which of the following is the NEXT step the technician should take to resolve the issue?
A. Run the antivirus scan.
B. Add the required snap-in.
C. Restore the system backup
D. use the administrator console.
Answer: B (LEAVE A REPLY)
Local Users and Groups is a Microsoft Management Console (MMC) snap-in that allows you to manage user accounts or groups on your computer1. If you cannot find it in the MMC console, you can add it manually by following these steps2:
Press Windows key + R to open the Run dialog box, or open the Command Prompt.
Type mmc and hit Enter. This will open a blank MMC console.
Click File and then Add/Remove Snap-in.
In the Add or Remove Snap-ins window, select Local Users and Groups from the Available snap-ins list, and click Add.
In the Select Computer window, choose Local computer or Another computer, depending on which computer you want to manage, and click Finish.
Click OK to close the Add or Remove Snap-ins window. You should now see Local Users and Groups in the MMC console.

NEW QUESTION: 125
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 (LEAVE A REPLY)
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: 126
A technician is on-site dealing with an angry customer. The customer thinks the issues have not been addressed, while the technician thinks that the issue has been correctly resolved. Which of the following should the technician do to handle the situation?
A. Insist that the customer is correct and document the concern.
B. Listen to the customer and do not speak at all.
C. Escalate the issue to the next tier.
D. Apologize and ask what would help resolve the issue.
Answer: (SHOW ANSWER)
When dealing with an angry customer, active listening and empathy are crucial. Even if the technician believes the issue has been resolved, the customer's concerns must be acknowledged professionally.
* Option A (Incorrect): Insisting that the customer is correct and simply documenting the concern does not resolve the issue. The technician should aim to engage with the customer constructively.
* Option B (Incorrect): While listening is important, completely staying silent without engaging in a discussion does not help in resolving the issue.
* Option C (Incorrect): Escalating the issue immediately without attempting to resolve it first is not the best approach unless all other options fail.
* Option D (Correct): Apologizing and asking what would help resolve the issue demonstrates empathy and professionalism. It helps defuse the situation and allows for an opportunity to find a mutually acceptable solution.
CompTIA A+ Core 2 Reference:
* 220-1102 Exam Objective 4.3 - Explain the importance of professionalism, including empathy, active listening, and proper documentation.

NEW QUESTION: 127
A user is trying to use proprietary software, but it crashes intermittently. The user notices that the desktop is displaying a "low memory" warning message. Upon restarting the desktop, the issue persists. Which of the following should a technician do next to troubleshoot the issue?
A. Reimage the computer.
B. Replace the system RAM.
C. Reinstall and update the failing software.
D. Decrease the page file size.
Answer: C (LEAVE A REPLY)
The most likely cause of the intermittent crashes is that the proprietary software is incompatible, outdated, or corrupted. Reinstalling and updating the software can fix these issues and ensure the software runs smoothly. Reimaging the computer or replacing the system RAM are too drastic and unnecessary steps. Decreasing the page file size can worsen the low memory problem and affect the performance of other applications.

NEW QUESTION: 128
Users report that they can log in to the web application during business hours, but none of the application's functions are working properly. Company policy does not allow for the server to be rebooted during business hours. Which of the following should a technician do to fix the web application and follow company policy?
A. Restart services.
B. Roll back Windows updates.
C. Perform a Windows repair.
D. Add RAM to the server.
Answer: A (LEAVE A REPLY)
Restarting services can resolve issues with web applications without requiring a full server reboot, which aligns with the company policy.
Restart services: Likely to resolve issues with the web application by refreshing the necessary services.
Roll back Windows updates: Unnecessary if the issue is with the application services.
Perform a Windows repair: More disruptive and not typically needed for application service issues.
Add RAM to the server: Would require a reboot and is not immediately necessary for troubleshooting application issues.

NEW QUESTION: 129
Which of the following helps ensure that a piece of evidence extracted from a PC is admissible in a court of law?
A. Data integrity form
B. Valid operating system license
C. Documentation of an incident
D. Chain of custody
Answer: D (LEAVE A REPLY)
Chain of custody is a process that helps ensure that a piece of evidence extracted from a PC is admissible in a court of law. Chain of custody refers to the documentation and tracking of who handled, accessed, modified, or transferred the evidence, when, where, why, and how. Chain of custody can help establish the authenticity, integrity, and reliability of the evidence, as well as prevent tampering, alteration, or loss of the evidence. Data integrity form, valid operating system license, and documentation of an incident are not processes that can ensure that a piece of evidence extracted from a PC is admissible in a court of law.

NEW QUESTION: 130
Which of the following environmental effects can be the result of using virtualization?
A. Greater energy consumption
B. Noise pollution
C. Reduced space requirements
D. Fewer maintenance needs
Answer: (SHOW ANSWER)
One of the key environmental benefits of using virtualization is the reduction in physical space requirements. Virtualization allows multiple virtual machines to run on a single physical server, reducing the need for multiple physical servers. This consolidation leads to fewer physical machines, saving space in data centers and reducing the overall physical footprint.

A . Greater energy consumption is incorrect as virtualization typically leads to reduced energy consumption due to the consolidation of hardware.
B . Noise pollution can be reduced because fewer physical machines often mean less overall noise.
D . Fewer maintenance needs is a possible benefit but not directly related to environmental effects like reduced space requirements.
Reference:
CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 4.5: Summarizing environmental impacts and local environmental controls, including the benefits of virtualization.

NEW QUESTION: 131
A user is unable to access a remote server from a corporate desktop computer using the appropriate terminal emulation program. The user contacts the help desk to report the issue. Which of the following clarifying questions would be most effective for the help desk technician to ask the user in order to understand the issue?
A. What is the error message?
B. Does the program work on another computer?
C. Did the program ever work?
D. Is anyone else having this issue?
Answer: A (LEAVE A REPLY)
The most effective clarifying question for the help desk technician to ask the user in order to understand the issue is A. What is the error message? This question will help the technician to identify the possible cause and solution of the problem, as the error message will provide specific information about the nature and location of the error, such as the server name, the port number, the protocol, the authentication method, or the network status. The error message will also help the technician to troubleshoot the issue by following the suggested steps or searching for the error code online.
This question is more effective than the other choices because:
B . Does the program work on another computer? is not a very helpful question, as it will not reveal the source of the error or how to fix it. The program may work on another computer for various reasons, such as different network settings, firewall rules, permissions, or software versions. However, this question will not tell the technician what is wrong with the user's computer or the remote server, or what needs to be changed or updated to make the program work.
C . Did the program ever work? is not a very relevant question, as it will not address the current issue or how to resolve it. The program may have worked in the past, but it may have stopped working due to changes in the network configuration, the server status, the software updates, or the user credentials. However, this question will not tell the technician what has changed or how to restore the program functionality.
D . Is anyone else having this issue? is not a very useful question, as it will not explain the reason or the solution for the error. The issue may affect only the user, or multiple users, depending on the scope and the impact of the error. However, this question will not tell the technician what is causing the error or how to fix it for the user or the others.
Reference:
How to Troubleshoot Terminal Emulation Problems - Techwalla : How to Read and Understand Windows Error Messages - Lifewire : How to Troubleshoot Network Connectivity Problems - How-To Geek : How to Troubleshoot Software Problems - dummies : How to Troubleshoot Common PC Issues For Users - MakeUseOf

NEW QUESTION: 132

Which of the following Is used to identify potential issues with a proposed change poor lo implementation?

A. Request form

B. Rollback plan

C. End-user acceptance

D. Sandbox testing

Answer: D (LEAVE A REPLY)

Sandbox testing is a method of identifying potential issues with a proposed change prior to implementation. It involves creating a simulated or isolated environment that mimics the real system and applying the change to it. This can help to verify that the change works as expected and does not cause any errors or conflicts. Request form, rollback plan and end-user acceptance are other components of a change management process, but they do not involve identifying issues with a change. Verified Reference: https://www.comptia.org/blog/what-is-sandbox-testing https://www.comptia.org/certifications/a

NEW QUESTION: 133

A technician is adding some Windows 10 workstations to the corporate domain. A script was able to add the majority of the workstations, but failed on a couple. Which of the following menus should the technician check in order to complete the task manually?

A. User Accounts

B. System Properties

C. Windows Firewall

D. Network and Sharing

Answer: (SHOW ANSWER)

To manually add a workstation to a domain, the technician needs to access the System Properties menu where domain settings are configured.

User Accounts: Manages user accounts but does not handle domain membership.

System Properties: The correct place to add or change domain membership settings.

Windows Firewall: Manages firewall settings but not domain membership.

Network and Sharing: Manages network connections and sharing but not domain settings.

NEW QUESTION: 134

A technician finds that a new company security policy has broken an application in use at a branch office. Which of the following should the technician do to ensure that the application is fixed and prevent the issue from reoccurring?

A. Request a policy exception be put in place while the application requirements are addressed

B. Reinstall the affected software using local administrative rights for each computer

C. Remove the new security settings and change the administrative accounts on the branch office computers to prevent the settings from being reapplied

D. Research and procure a replacement application that is not adversely affected by the new policy

Answer: A (LEAVE A REPLY)

Comprehensive and Detailed In-Depth

If a new security policy disrupts an essential application, the best course of action is to request a policy exception while a permanent solution is developed. This allows the application to function while ensuring compliance with company security policies.

B . Reinstall the affected software using local administrative rights for each computer - Incorrect. If the security policy is blocking the application, reinstalling it will not resolve the issue.
C . Remove the new security settings and change administrative accounts - Incorrect. Altering security settings without approval could violate company policies and create security risks.
D . Research and procure a replacement application - Incorrect. While replacing the application may be an option, it is not an immediate solution to restoring functionality.
Reference:
CompTIA A+ 220-1102, Objective 2.2 - Security Best Practices

NEW QUESTION: 135
An engineer is configuring a new server that requires a bare-metal installation. Which of the following installation methods should the engineer use if installation media is not available on site?
A. Image deployment
B. Recovery partition installation
C. Remote network installation
D. Repair installation
Answer: D (LEAVE A REPLY)
Remote network installation is the best option for configuring a new server that requires a bare-metal installation without installation media on site. A remote network installation is a method of installing an operating system or an application over a network connection, such as LAN, WAN, or Internet. A remote network installation can use various protocols, such as PXE, HTTP, FTP, or SMB, to access the installation files from a server or a cloud service. A remote network installation can also use various tools, such as Windows Deployment Services, Microsoft Deployment Toolkit, or Red Hat Kickstart, to automate and customize the installation process. A remote network installation can save time and resources by eliminating the need for physical media and allowing centralized management of multiple installations. Image deployment, recovery partition installation, and repair installation are not correct answers for this question. Image deployment is a method of installing an operating system or an application by copying a preconfigured image file to a target device. Image deployment requires an existing image file and a compatible device. Recovery partition installation is a method of restoring an operating system or an application from a hidden partition on the hard disk that contains the original factory settings. Recovery partition installation requires an existing recovery partition and a functional hard disk. Repair installation is a method of fixing an operating system or an application that is corrupted or damaged by replacing or repairing the system files without affecting the user data or settings. Repair installation requires an existing operating system or application and a working device. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 16 CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 106

NEW QUESTION: 136
A company's help desk receives numerous calls from employees reporting issues related to a current security breach. Which of the following steps should the help desk team take to document the breach?
A. Record the details in the ticketing system.
B. Take screenshots and attach them to the root cause analysis.
C. Discuss the incident with the company's legal team.

D. List the details in the company's knowledge base.

Answer: (SHOW ANSWER)

In the event of a security breach, documenting the incident is crucial for tracking, analysis, and resolution. The appropriate steps should ensure thorough documentation and communication:

Option A: Record the details in the ticketing system.Correct Answer. The ticketing system is the primary tool for IT support to track incidents. Recording the details in the ticketing system ensures that all relevant information is documented systematically, can be easily accessed, and tracked through the resolution process.

This aligns with best practices in incident documentation and support systems information management as outlined in the CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 4.1.

Option B: Take screenshots and attach them to the root cause analysis.While screenshots can be useful, the first step should be to record the details in the ticketing system. Screenshots may be added later as supplementary information.

Option C: Discuss the incident with the company's legal team.Involving the legal team is important for certain aspects of a security breach, but the initial step should still be to document the incident in the ticketing system.

NEW QUESTION: 137

A remote user is experiencing issues with Outlook settings and asks a technician to review the settings. Which of the following can the technician use to access the user's computer remotely?

A. VPN

B. RDP

C. RMM

D. SSH

Answer: C (LEAVE A REPLY)

One of the possible ways to access the user's computer remotely is to use RDP, which stands for Remote Desktop Protocol. RDP is a protocol that allows a user to connect to another computer over a network and use its graphical interface. RDP is commonly used for remote desktop software, such as Microsoft Remote Desktop Connection1. To use RDP, the user's computer must run RDP server software, and the technician must run RDP client software. The technician can then enter the user's IP address or hostname, and provide the appropriate credentials to log in to the user's computer. Once connected, the technician can view and control the user's desktop, and review the Outlook settings.

NEW QUESTION: 138

Which of the following is the most significant drawback of using the WEP protocol for wireless security?

A. Complex configuration process

B. Slow data transfer speed

C. Vulnerability to key-cracking attacks
D. Incompatibility with older devices
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth
WEP (Wired Equivalent Privacy) is highly vulnerable to key-cracking attacks, as its encryption key can be easily broken with freely available tools.
A . Complex configuration process - Incorrect. WEP is actually easy to configure.
B . Slow data transfer speed - Incorrect. WEP does not significantly impact speed.
D . Incompatibility with older devices - Incorrect. WEP is compatible with older devices but is insecure.

NEW QUESTION: 139
A company is opening several remote offices and would like to have the capability for its systems administrator to automate patch management and software deployment. Which of the following would meet this requirement?
A. MSRA
B. SSH
C. RMM
D. VNC
Answer: C (LEAVE A REPLY)

NEW QUESTION: 140
A user's home system has been infected with malware. A technician has isolated the system from the network and disabled System Restore. Which of the following should the technician do next?
A. Perform an antivirus scan.
B. Run Windows updates.
C. Reimage the system.
D. Enable System Restore.
Answer: A (LEAVE A REPLY)
When dealing with a malware-infected system, isolating the system from the network and disabling System Restore are critical initial steps. The next step in the malware removal process should be:
* Perform an antivirus scan: This helps to identify and remove the malware from the system. Running a thorough scan using updated antivirus software is essential to detect and clean any malicious files.
* Run Windows updates: This is important for system security but should be done after the malware is removed to avoid further issues.
* Reimage the system: This is a more drastic measure and should be considered if the antivirus scan cannot fully clean the system.
* Enable System Restore: This should only be done after the system is confirmed to be clean.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 3.3: Given a scenario use best practice procedures for malware removal.
Malware removal best practices documentation.

NEW QUESTION: 141
Given the following information:
jdoe pizza
jdoe rock
jdoe guitar
Which of the following types of attacks is occurring?
A. DDoS
B. Spoofing
C. SQL injection
D. Dictionary
Answer: (SHOW ANSWER)

NEW QUESTION: 142
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: 143
A user reports that the hard drive activity light on a Windows 10 desktop computer has been steadily lit for more than an hour, and performance is severely degraded. Which of the following tabs in Task Manager would contain the information a technician would use to identify the cause of this issue?
A. Services
B. Processes
C. Performance
D. Startup
Answer: (SHOW ANSWER)
Processes tab in Task Manager would contain the information a technician would use to identify the cause of this issue. The Processes tab in Task Manager displays all the processes running on the computer, including the CPU and memory usage of each process. The technician can use this tab to identify the process that is causing the hard drive activity light to remain lit and the performance degradation1

NEW QUESTION: 144
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: 145
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: (SHOW ANSWER)
The user can enable speech recognition on a PC in the Ease of Access settings tool. To set up Speech Recognition on a Windows PC, the user should open Control Panel, click on Ease of Access, click on Speech Recognition, and click the Start Speech Recognition link. Language settings can be used to change the language of the speech recognition feature, but they will not enable the feature. System settings can be used to configure the hardware and software of the PC, but they will not enable the speech recognition feature. Personalization settings can be used to customize the appearance and behavior of the PC, but they will not enable the speech recognition feature1 Open up ease of access, click on speech, then there is an on and off button for speech recognition.

NEW QUESTION: 146
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: 147
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 log-in script failed.
B. The file server is offline.
C. The user is not connected to the VPN.
D. A low battery is preventing the connection.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 148
A technician wants to install Developer Mode on a Windows laptop but is receiving a "failed to install package" message. Which of the following should the technician do first?
A. Enable SSH.
B. Check for Windows updates.
C. Reboot computer.
D. Ensure internet connectivity.
Answer: (SHOW ANSWER)
Developer Mode on Windows 10 is a feature that allows developers to test and debug their applications on their devices, as well as sideload apps and access other developer tools12. To enable Developer Mode, the user needs to go to the Settings app, select Update & Security, choose For Developers, and switch to Developer Mode123. However, enabling Developer Mode requires internet connectivity, as Windows will download and install a package of features, such as Windows Device Portal and SSH services, that are necessary for Developer Mode124. If the user does not have internet connectivity, they will receive a "failed to install package" message when trying to enable Developer Mode4. Therefore, the first thing that the technician should do is to ensure that the laptop has internet access, either through Wi-Fi or Ethernet, and then try to enable Developer Mode again4

NEW QUESTION: 149
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: (SHOW ANSWER)

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: 150

A technician sees a file that is requesting payment to a cryptocurrency address. Which of the following should the technician do first?

A. Quarantine the computer.

B. Disable System Restore.

C. Update the antivirus software definitions.

D. Boot to safe mode.

Answer: A (LEAVE A REPLY)

Quarantining the computer means isolating it from the network and other devices to prevent the spread of malware or ransomware. Ransomware is a type of malware that encrypts the files on a computer and demands payment (usually in cryptocurrency) to restore them. If a technician sees a file that is requesting payment to a cryptocurrency address, it is likely that the computer has been infected by ransomware. Quarantining the computer should be the first step to contain the infection and prevent further damage. Disabling System Restore, updating the antivirus software definitions, and booting to safe mode are not steps that should be done before quarantining the computer.

NEW QUESTION: 151

A company installed WAPs and deployed new laptops and docking stations to all employees. The docking stations are connected via LAN cables. Users are now reporting degraded network service. The IT department has determined that the WAP mesh network is experiencing a higher than anticipated amount of traffic. Which of the following would be the most efficient way to ensure the wireless network can support the expected number of wireless users?

A. Replacing non-mobile users' laptops with wired desktop systems

B. Increasing the wireless network adapter metric

C. Adding wireless repeaters throughout the building

D. Upgrading the current mesh network to support the 802.11 n specification

Answer: D (LEAVE A REPLY)

When a WAP (Wireless Access Point) mesh network is experiencing a higher than anticipated amount of traffic, leading to degraded network service, upgrading the network to a more advanced wireless standard can help alleviate the problem. The 802.11n specification, also known as Wireless-N, offers significant improvements over earlier standards like 802.11b/g

in terms of speed, range, and reliability. It allows for increased data throughput and better coverage, which can support a higher number of wireless users effectively.
* Upgrading to 802.11n: This involves replacing existing WAPs with those that support the 802.11n standard or higher. The upgrade can result in improved network performance by accommodating more wireless connections with higher data rates, reducing congestion and improving overall network efficiency.
Replacing non-mobile users' laptops with wired desktop systems (A) could reduce wireless traffic but may not be feasible or desirable for all users. Increasing the wireless network adapter metric (B) would affect route priority but not overall network capacity. Adding wireless repeaters (C) can extend the range but might also introduce additional latency and does not necessarily increase the network's capacity to handle more users efficiently.

NEW QUESTION: 152
The calendar application on an employee's smartphone is experiencing frequent crashes, and the smartphone has become unresponsive. Which of the following should a technician do first to resolve the issue?
A. Reinstall the application on the smartphone.
B. Update the smartphone's OS.
C. Reset the smartphone to factory settings.
D. Reboot the smartphone.
Answer: D (LEAVE A REPLY)
Rebooting the smartphone is the first and simplest step to resolve the issue of frequent crashes and unresponsiveness. Rebooting clears the memory, closes the background apps, and refreshes the system. It can also fix minor glitches and bugs that may cause the calendar app or the smartphone to malfunction12. The other options are either too drastic or unnecessary. Reinstalling the application may not solve the problem if the issue is with the smartphone itself. Updating the smartphone's OS may not be possible or helpful if the device is unresponsive or incompatible. Resetting the smartphone to factory settings will erase all the data and settings on the device, which should be the last resort.

NEW QUESTION: 153
A large university wants to equip all classrooms with high-definition IP videoconferencing equipment. Which of the following would most likely be impacted in this situation?
A. SAN
B. LAN
C. GPU
D. PAN
Answer: (SHOW ANSWER)

LAN is the most likely option to be impacted in this situation. LAN stands for Local Area Network, and it is a network that connects devices within a limited area, such as a building or a campus. Installing high-definition IP videoconferencing equipment in all classrooms would require a high bandwidth and reliable LAN infrastructure to support the video and audio transmission. The LAN would also need to be configured with proper security, quality of service, and multicast protocols to ensure the optimal performance of the videoconferencing system. SAN, GPU, and PAN are not directly related to this scenario. SAN stands for Storage Area Network, and it is a network that provides access to consolidated storage devices. GPU stands for Graphics Processing Unit, and it is a hardware component that handles graphics rendering and computation. PAN stands for Personal Area Network, and it is a network that connects devices within a short range, such as Bluetooth or infrared. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 20 CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 104

NEW QUESTION: 154
A technician needs to disable guest log-ins on domain-joined desktop machines. Which of the following should the technician use?
A. Group Policy
B. Firewall
C. Microsoft Management Control
D. MSConfig
Answer: A (LEAVE A REPLY)
Disabling guest accounts on domain-joined machines is done through Group Policy. Group Policy allows centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment. By using the Group Policy Editor (gpedit.msc), administrators can enforce policies such as disabling the guest account across all machines within the domain. The other options (Firewall, Microsoft Management Console, MSConfig) do not provide functionality specific to managing user accounts in this context.

NEW QUESTION: 155
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: 156

A technician needs to configure laptops so that only administrators can enable virtualization technology if needed. Which of the following should the technician configure?

A. Guest account

B. Screen lock

C. AutoRun setting

D. BIOS password

Answer: (SHOW ANSWER)

NEW QUESTION: 157

A user's personal computer was infected with malware that had a known remediation. Which of the following should the user have done to prevent this issue?

A. Maintained a preinstallation environment

B. Kept endpoint protection software updated

C. Disabled System Restore

D. Created a restore point

Answer: B (LEAVE A REPLY)

NEW QUESTION: 158

Which of the following threats will the use of a privacy screen on a computer help prevent?

A. Impersonation

B. Shoulder surfing

C. Whaling

D. Tailgating

Answer: (SHOW ANSWER)

Shoulder surfing is a threat that involves someone looking over another person's shoulder to observe their screen, keyboard, or other sensitive information. Shoulder surfing can be used to steal passwords, personal identification numbers (PINs), credit card numbers, or other confidential data. The use of a privacy screen on a computer can help prevent shoulder surfing by limiting the viewing angle of the screen and making it harder for someone to see the screen from the side or behind. Impersonation, whaling, and tailgating are not threats that can be prevented by using a privacy screen on a computer.

NEW QUESTION: 159

Which of the following Linux commands would help to identify which directory the user is currently operating in?

A. pwd

B. dig

C. find

D. cat

Answer: (SHOW ANSWER)

The pwd command, which stands for "print working directory," is used in Linux and Unix-like operating systems to display the current directory in which the user is operating. This command outputs the full pathname of the current working directory, helping users to understand their current location in the filesystem hierarchy.

* pwd: When executed, it provides the absolute path of the directory you're currently in, which is useful for navigation and scripting purposes.
Other options listed:
* dig: This command is used for querying DNS name servers for information about host addresses, mail exchanges, name servers, and related information.
* find: This command is used to search for files in a directory hierarchy based on specified criteria (such as name, modification date, size, etc.).
* cat: Short for "concatenate," this command is used to read the contents of files and output them to the terminal.

NEW QUESTION: 160
A technician is installing RAM in a new workstation and needs to protect against electrostatic discharge. Which of the following will best resolve this concern?
A. Battery backup
B. Thermal paste
C. ESD strap
D. Consistent power
Answer: C (LEAVE A REPLY)
An ESD strap, also known as an antistatic wrist strap, is a device that prevents electrostatic discharge (ESD) from damaging sensitive electronic components such as RAM. ESD is the sudden flow of electricity between two objects with different electrical charges, which can cause permanent damage or malfunction to electronic devices. An ESD strap connects the technician's wrist to a grounded surface, such as a metal case or a mat, and equalizes the electrical potential between the technician and the device. Battery backup, thermal paste, and consistent power are not devices that can protect against ESD.

NEW QUESTION: 161
A technician installs a Bluetooth headset for a user. During testing, the sound is still coming from the speaker on the computer. The technician verifies the headset shows up in Device Manager. Which of the following would the technician most likely do to fix this issue?
A. Replace the battery on the headset, and try again later.
B. Update the drivers for the wireless headset.
C. Verify that the sound is not muted in the control panel.
D. Change the headset as the default device in sound settings.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 162
During a network outage, a technician discovers a new network switch that was not listed in the support documentation. The switch was installed during a recent change window when a new office was added to the environment. Which of the following would most likely prevent this type of mismatch after next month's change window?
A. Performing annual network topology reviews
B. Requiring all network changes include updating the network diagrams
C. Allowing network changes once per year

D. Routinely backing up switch configuration files

Answer: (SHOW ANSWER)

This would ensure that the support documentation reflects the current state of the network and prevents any confusion or mismatch during a network outage. Updating the network diagrams is also one of the best practices for network documentation, as stated in the Official CompTIA A+ Core 2 Study Guide1. The other options are not as effective or feasible as option B. Performing annual network topology reviews is too infrequent and may not capture recent changes. Allowing network changes once per year is too restrictive and may not meet the business needs. Routinely backing up switch configuration files is important, but it does not help with identifying new switches or devices on the network.

NEW QUESTION: 163

A technician needs to configure a backup solution that will have the least additional expenses and impact on users. Which of the following steps should the technician complete? (Select two.)

A. Configure the backup to run when the user logs in

B. Configure the backup to run after peak hours

C. Use third-party licensed backup software

D. Use the built-in OS backup utility

E. Configure the backup job to run every hour

F. Use an external storage device for the backup

Answer: B,D (LEAVE A REPLY)

Comprehensive and Detailed In-Depth

To minimize costs and user disruption, the technician should:

B . Configure the backup to run after peak hours - This prevents slowdowns during working hours.

D . Use the built-in OS backup utility - This avoids additional licensing costs.

A . Configure the backup to run when the user logs in - Incorrect. This could slow down startup and affect productivity.

C . Use third-party licensed backup software - Incorrect. This would increase expenses.

E . Configure the backup job to run every hour - Incorrect. Frequent backups may slow down the system unnecessarily.

F . Use an external storage device - Incorrect. While useful, it may require additional costs and maintenance.

Reference:

CompTIA A+ 220-1102, Objective 4.1 - Backup and Recovery Concepts

NEW QUESTION: 164

A technician needs to configure a computer for a user to work from home so the user can still securely access the user's shared files and corporate email. Which of the following tools would best accomplish this task*?

A. MSRA

B. FTP

C. RMM

D. VPN

Answer: D (LEAVE A REPLY)

A Virtual Private Network (VPN) creates a secure connection over the internet to a network, allowing a user to access shared files and corporate email as if they were directly connected to the network. This makes VPN the best tool for secure remote work access, compared to the other options which do not offer the same level of secure, remote network access.

NEW QUESTION: 165
Which of the following script types is used with the Python language by default?
A. .ps1
B. .vbs
C. .bat
D. .py
Answer: D (LEAVE A REPLY)
The script type that is used with the Python language by default is .py. .py is a file extension that indicates a Python script file that contains Python code that can be executed by a Python interpreter or compiler. Python is a high-level, general-purpose and interpreted programming language that can be used for various applications, such as web development, data analysis, machine learning and automation. .ps1 is a file extension that indicates a PowerShell script file that contains PowerShell code that can be executed by a PowerShell interpreter or compiler. PowerShell is a task-based, command-line and scripting language that can be used for system administration and automation on Windows systems. .vbs is a file extension that indicates a VBScript file that contains VBScript code that can be executed by a VBScript interpreter or compiler. VBScript is an Active Scripting language that can be used for web development and automation on Windows systems. .bat is a file extension that indicates a batch file that contains a series of commands that can be executed by a command-line interpreter or shell on Windows systems. Batch files can be used for system administration and automation on Windows systems. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 4.3

NEW QUESTION: 166
A technician, who is completing hardware upgrades at a company, is approached by a user who submitted a computer upgrade request. After checking the list of offices to upgrade, the technician finds that the user's office is not listed for an upgrade. Which of the following actions should the technician take next?
A. Ask the company's human resources department to address the issue.
B. Notify the project manager about the user's concern.
C. Tell the user that this request is not on the list to be upgraded.
D. Ask the user's supervisor if the technician should upgrade the computer.
Answer: B (LEAVE A REPLY)
When a technician finds that a user's office is not listed for an upgrade but the user has submitted a request, the appropriate action is to:
* Notify the project manager about the user's concern: The project manager oversees the upgrade process and can address any discrepancies or omissions in the upgrade list.
* Ask the company's human resources department to address the issue: HR typically handles personnel matters, not hardware upgrades.
* Tell the user that this request is not on the list to be upgraded: This does not resolve the user's concern and could cause frustration.
* Ask the user's supervisor if the technician should upgrade the computer: The supervisor may not have the authority or information to make decisions about the upgrade list.
Reference:

CompTIA A+ 220-1102 Exam Objectives, Section 4.1: Given a scenario implement best practices associated with documentation and support systems information management.
Best practices for handling user requests and project management documentation.

NEW QUESTION: 167
A user's laptop is shutting down every time the laptop lid is closed, which is leading to frequent work interruptions. Which of the following should a help desk specialist do to remediate the issue?
A. Configure the sleep settings.
B. Disablehibernation.
C. Edit thepower plan.
D. Turn onfast startup.
Answer: C (LEAVE A REPLY)
When a user's laptop shuts down every time the lid is closed, it typically means that the power settings are configured to put the laptop into a shutdown state when the lid is closed. To remediate this issue:
Edit the power plan: This involves changing the settings for what happens when the laptop lid is closed.
Go to Control Panel > Hardware and Sound > Power Options.
Click on "Choose what closing the lid does."
Change the settings for "When I close the lid" to either "Sleep" or "Do nothing" instead of "Shut down." Configure the sleep settings: While similar to editing the power plan, this option specifically adjusts the sleep settings rather than the overall power plan settings.
Disable hibernation: This is a less direct solution but could be considered if the laptop was set to hibernate and then experiencing issues.
Turn on fast startup: This setting affects how quickly the computer starts up from a shutdown, but it does not directly address the issue of what happens when the lid is closed.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 1.5: Given a scenario, use the appropriate Microsoft Windows settings.
Windows power management documentation.

NEW QUESTION: 168
A user contacted the help desk to report pop-ups on a company workstation indicating the computer has been infected with 137 viruses and payment is needed to remove them. The user thought the company-provided antivirus software would prevent this issue. The help desk ticket states that the user only receives these messages when first opening the web browser. Which of the following steps would MOST likely resolve the issue? (Select TWO)

A. Scan the computer with the company-provided antivirus software
B. Install a new hard drive and clone the user's drive to it
C. Deploy an ad-blocking extension to the browser.
D. Uninstall the company-provided antivirus software
E. Click the link in the messages to pay for virus removal
F. Perform a reset on the user's web browser
Answer: C,F (LEAVE A REPLY)
"The user thought the company-provided antivirus software would prevent this issue." The most likely steps to resolve the issue are to deploy an ad-blocking extension to the browser and perform a reset on the user's web browser. Ad-blocking extensions can help to prevent pop-ups and other unwanted content from appearing in the browser, and resetting the browser can help to remove any malicious extensions or settings that may be causing the issue.

NEW QUESTION: 169
Employees at comptia.org are reporting getting an usual amount of emails from a coworker. A technician discovers the emails were sent from the following address:
john@cOmptia.org
Which of the following social engineering attacks is this an example of?
A. Whaling
B. Insider threat
C. Phishing
D. Vishing
E. Evil twin
Answer: C (LEAVE A REPLY)
Phishing involves tricking individuals into disclosing sensitive information or installing malware through deceptive emails.
Whaling: A specific type of phishing targeting high-profile individuals.
Insider threat: Malicious activities by someone within the organization.
Phishing: General deceptive emails to trick users into compromising information or installing malware.
Vishing: Voice phishing, conducted over the phone.
Evil twin: A rogue Wi-Fi access point mimicking a legitimate one to intercept data.

NEW QUESTION: 170
A technician is trying to encrypt a single folder on a PC. Which of the following should the technician use to accomplish this task?
A. FAT32
B. exFAT
C. BitLocker
D. EFS
Answer: D (LEAVE A REPLY)
EFS (Encrypting File System) is a feature that allows a user to encrypt a single folder or file on a Windows PC. It uses a public key encryption system to protect the data from unauthorized access. FAT32 and exFAT are file system formats that

do not support encryption. BitLocker is a feature that encrypts the entire drive, not a single folder or file. Verified Reference: https://www.comptia.org/blog/what-is-efs https://www.comptia.org/certifications/a

NEW QUESTION: 171
A change advisory board just approved a change request. Which of the following is the MOST likely next step in the change process?
A. End user acceptance
B. Perform risk analysis
C. Communicate to stakeholders
D. Sandbox testing
Answer: (SHOW ANSWER)
The risk analysis should be performed before it's taken to the board. The step after the board approves the change is End User Agreenment Reference: https://www.youtube.com/watch?v=Ru77iZxuElA&list=PLG49S3nxzAnna96gzhJrzkii4hH_mgW4b&index=59

NEW QUESTION: 172
An application's performance is degrading over time. The application is slowing but never gives an error and does not crash. Which of the following tools should a technician use to start troubleshooting?
A. Reliability history
B. Computer management
C. Resource monitor
D. Disk defragment
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth
The Resource Monitor provides real-time data on CPU, memory, disk, and network usage, making it the best tool to identify performance degradation over time. It allows technicians to check which processes are consuming excessive system resources.
A . Reliability history - Incorrect. Reliability Monitor tracks system errors and crashes, but it does not help diagnose ongoing performance issues.
B . Computer management - Incorrect. Computer Management provides system utilities but does not offer real-time monitoring of resource usage.
D . Disk defragment - Incorrect. Disk defragmentation improves disk access times but is unrelated to an application gradually slowing down.
Reference:
CompTIA A+ 220-1102, Objective 1.4 - Windows System Utilities for Troubleshooting

NEW QUESTION: 173
The camera and microphone on an iPhone user's device are activating without any user input. The user's friend recently modified the device to allow applications to be installed outside the normal App Store. Which of the following is the issue?
A. The user connected a counterfeit Lightning cable to the iPhone.
B. The device is unenrolled from Mobile Device Management.

C. The device was jailbroken to remove internal security protections.
D. The iPhone has an out-of-date operating system.
Answer: C (LEAVE A REPLY)
The camera and microphone on an iPhone activating without user input, especially after allowing applications to be installed outside the normal App Store, is a classic sign of the device being jailbroken. Jailbreaking an iPhone removes many of the built-in security features and restrictions, allowing the installation of apps from third-party sources. These third-party apps can be malicious and can gain unauthorized access to system resources like the camera and microphone.
A . The user connected a counterfeit Lightning cable to the iPhone. While counterfeit cables can be harmful, they typically cause charging or connectivity issues rather than security vulnerabilities that would enable camera and microphone activation without user input.
B . The device is unenrolled from Mobile Device Management. Unenrolling from MDM removes organizational controls but does not directly cause unauthorized camera and microphone activation.
D . The iPhone has an out-of-date operating system. An outdated OS can have vulnerabilities, but the scenario specifically mentions modifications to allow third-party app installations, pointing to jailbreaking as the primary cause.
Reference:
CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 2.3: Security measures and their purposes including mobile device security.

NEW QUESTION: 174
A technician is setting up a newly built computer. Which of the following is the fastest way for the technician to install Windows 10?
A. Factory reset
B. System Restore
C. In-place upgrade
D. Unattended installation
Answer: D (LEAVE A REPLY)
The correct answer is D. Unattended installation. An unattended installation is a way of installing Windows 10 without requiring any user input or interaction. It uses a configuration file called answer file that contains the settings and preferences for the installation, such as the product key, language, partition, and network settings. An unattended installation can be performed by using a bootable USB flash drive or DVD that contains the Windows 10 installation files and the answer file1. This is the fastest way for the technician to install Windows 10 on a newly built computer, as it automates the whole process and saves time.
A factory reset is a way of restoring a computer to its original state by deleting all the data and applications and reinstalling the operating system. A factory reset can be performed by using the recovery partition or media that came with the computer, or by using the Reset this PC option in Windows 10 settings2. A factory reset is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system to be present.
A system restore is a way of undoing changes to a computer's system files and settings by using a restore point that was created earlier. A system restore can be performed by using the System Restore option in Windows 10 settings or by using the Advanced Startup Options menu3. A system restore is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system and restore points to be present.

An in-place upgrade is a way of upgrading an existing operating system to a newer version without losing any data or applications. An in-place upgrade can be performed by using the Windows 10 Media Creation Tool or by running the Setup.exe file from the Windows 10 installation media. An in-place upgrade is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system to be present.

NEW QUESTION: 175
A technician needs to perform after-hours service starting at 10:00 p.m. The technician is currently 20 minutes late. The customer will also be late. Which of the following should the technician do considering proper communication techniques and professionalism?
Do not notify the customer if arriving before the customer.
A. Dismiss the customer and proceed with the after-hours work.
B. Contact the customer if the technician is arriving late.
C. Disclose the experience via social media.
Answer: C (LEAVE A REPLY)
The best option for the technician to demonstrate proper communication techniques and professionalism is to contact the customer if the technician is arriving late. This shows respect for the customer's time and expectations, and allows the customer to adjust their schedule accordingly. It also helps to maintain a positive relationship and trust between the technician and the customer. The technician should apologize for the delay and provide a realistic estimate of their arrival time. The technician should also thank the customer for their patience and understanding.
The other options are not appropriate or professional. Do not notify the customer if arriving before the customer is not a good practice, as it may cause confusion or frustration for the customer. The customer may have made other plans or arrangements based on the technician's original schedule, and may not be available or prepared for the service. Dismiss the customer and proceed with the after-hours work is rude and disrespectful, as it ignores the customer's needs and preferences. The customer may have questions or concerns about the service, or may want to supervise or verify the work. The technician should always communicate with the customer before, during, and after the service. Disclose the experience via social media is unethical and unprofessional, as it may violate the customer's privacy and the company's policies. The technician should not share any confidential or sensitive information about the customer or the service on social media, or make any negative or inappropriate comments about the customer or the situation.
Reference:
CompTIA A+ Certification Exam Core 2 Objectives1
CompTIA A+ Core 2 (220-1102) Certification Study Guide2
8 Ways You Can Improve Your Communication Skills3
Professionalism in Communication | How To Do It And How It Pays4

NEW QUESTION: 176
A technician needs to track evidence for a forensic investigation on a Windows computer. Which of the following describes this process?
A. Valid license
B. Data retention requirements
C. Material safety data sheet
D. Chain of custody

Answer: D (LEAVE A REPLY)
Chain of custody is a legal term that refers to the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence1. It is important in forensic investigations to establish that the evidence is in fact related to the case, and that it has not been tampered with or contaminated. A technician needs to track evidence for a forensic investigation on a Windows computer by following the proper procedures for collecting, handling, storing, and analyzing the evidence, and documenting every step of the process on a chain of custody form23

NEW QUESTION: 177
Which of the following default system tools can be used in macOS to allow the technician to view the screen simultaneously with the user?
A. Remote Assistance
B. Remote Desktop Protocol
C. Screen Sharing
D. Virtual Network Computing
Answer: C (LEAVE A REPLY)
Screen Sharing is the default system tool that can be used in macOS to allow the technician to view the screen simultaneously with the user. Screen Sharing is a built-in app that lets users share their Mac screen with another Mac on the network. The user can enable screen sharing in the System Preferences > Sharing pane, and then allow other users to request or enter a password to access their screen1. The technician can launch the Screen Sharing app from the Spotlight search or the Finder sidebar, and then enter the user's name, address, or Apple ID to connect to their screen2. Remote Assistance is a Windows feature that allows users to invite someone to help them with a problem on their PC3. Remote Desktop Protocol (RDP) is a protocol that allows users to connect to a remote computer over a network4. Virtual Network Computing (VNC) is a technology that allows users to share their screen with other devices using a VNC viewer app1. These are not default system tools in macOS, although they can be used with third-party software or settings.

NEW QUESTION: 178
An MDM report shows that a user's company cell phone has unauthorized applications installed. The device has recently checked into the MDM server, and the company still has access to remotely wipe the device. Which of the following describes the action the user has performed?
A. Obtained root access
B. Upgraded the OS
C. Installed a VPN
D. Uninstalled the MDM software
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth
If an MDM (Mobile Device Management) solution detects unauthorized applications, it is likely that the user has rooted (Android) or jailbroken (iOS) the device to bypass security restrictions. Root access allows the user to install unauthorized applications that MDM policies would normally block.
B . Upgraded the OS - Incorrect. Upgrading the OS does not bypass security policies or allow unauthorized apps.
C . Installed a VPN - Incorrect. A VPN does not affect the MDM system or allow unauthorized apps.

D . Uninstalled the MDM software - Incorrect. If the MDM software was removed, the device would not still be reporting to the MDM server.
Reference:
CompTIA A+ 220-1102, Objective 2.7 - Mobile Device Security and MDM

NEW QUESTION: 179
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: 180
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: 181
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: (SHOW ANSWER)

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: 182
A client recently upgraded their Windows 10 machine to Windows 11. The client reports the following message displays when turning the computer on: "Error loading operating system." Which of the following should a technician do first to troubleshoot this issue?
A. Disable the Secure Boot feature.
B. Use the automated startup recovery.
C. Format the drive.
D. Resize the boot partition.
Answer: B (LEAVE A REPLY)
The "Error loading operating system" message in Windows typically indicates a problem with the boot process. This could be due to corrupted system files, boot configuration data (BCD) errors, or issues with the hard drive.
Windows has a built-in automated startup recovery tool designed to diagnose and fix these types of problems. It attempts to automatically find and repair issues that are preventing Windows from starting correctly.
Here's why the other options are not the best first step:
A . Disable the Secure Boot feature: Secure Boot is a security feature that helps prevent malware from loading during startup. While it can sometimes cause issues with incompatible hardware or software, it's unlikely to be the primary cause of this error after a Windows upgrade.
C . Format the drive: Formatting the drive should be a last resort as it will erase all data on the hard drive.
D . Resize the boot partition: Resizing the boot partition is a complex task and not usually necessary to fix a boot error.
Troubleshooting Steps:
Use the automated startup recovery:
This is usually attempted automatically when Windows fails to boot.
If it doesn't start automatically, you might need to access the Advanced Startup Options menu (usually by repeatedly pressing F8 or Shift+F8 during startup).
If automated repair fails, try other options from the Advanced Startup Options menu:
System Restore: Restore the system to a point before the upgrade.
Startup Repair: This tool can fix more complex boot errors.

Command Prompt: Use the command prompt to run commands like bootrec /fixmbr, bootrec /fixboot, and bootrec /rebuildbcd to repair the boot configuration.

NEW QUESTION: 183
Malware is installed on a device after a user clicks on a link in a suspicious email. Which of the following is the best way to remove the malware?
A. Run System Restore.
B. Place in recovery mode.
C. Schedule a scan.
D. Restart the PC.
Answer: (SHOW ANSWER)
Recovery mode is a special boot option that allows the user to access advanced tools and features to troubleshoot and remove malware from the device. Recovery mode can also restore the system to a previous state or reset the device to factory settings. Running System Restore, scheduling a scan, or restarting the PC may not be effective in removing the malware, as it may still be active or hidden in the system files.

NEW QUESTION: 184
A user clicks a link in an email. A warning message in the user's browser states the site's certificate cannot be verified. Which of the following is the most appropriate action for a technician to take?
A. Click proceed.
B. Report the employee to the human resources department for violating company policy.
C. Restore the computer from the last known backup.
D. Close the browser window and report the email to IT security.
Answer: (SHOW ANSWER)
A warning message in the user's browser stating the site's certificate cannot be verified indicates that the site may be insecure, fraudulent, or malicious. This could be a sign of a phishing attempt, where the sender of the email tries to trick the user into clicking a link that leads to a fake website that mimics a legitimate one, in order to steal the user's personal or financial information. The most appropriate action for a technician to take in this situation is to close the browser window and report the email to IT security, who can investigate the source and content of the email, and take the necessary steps to protect the user and the network from potential harm. Clicking proceed could expose the user to malware, identity theft, or data breach. Reporting the employee to the human resources department for violating company policy is unnecessary and harsh, as the user may not have been aware of the phishing attempt or the company policy. Restoring the computer from the last known backup is premature and ineffective, as the user may not have been infected by anything, and the backup may not remove the email or the link from the user's inbox

NEW QUESTION: 185
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: (SHOW ANSWER)
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: 186
During a recent flight an executive unexpectedly received several dog and cat pictures while trying to watch a movie via in-flight Wi-Fi on an iPhone. The executive has no records of any contacts sending pictures like these and has not seen these pictures before. To BEST resolve this issue, the executive should:
A. set AirDrop so that transfers are only accepted from known contacts
B. completely disable all wireless systems during the flight
C. discontinue using iMessage and only use secure communication applications
D. only allow messages and calls from saved contacts
Answer: A (LEAVE A REPLY)
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: 187
A user is having issues with document-processing software on a Windows workstation. Other users that log in to the same device do not have the same issue.
Which of the following should a technician do to remediate the issue?
A. Roll back the updates.
B. Increase the page file.
C. Update the drivers.
D. Rebuild the profile.
Answer: D (LEAVE A REPLY)
The issue is specific to the user's profile, so the technician should rebuild the profile. Rebuilding the profile will create a new profile and transfer the user's data to the new profile1

NEW QUESTION: 188
A technician needs administrator access on a Windows workstation to facilitate system changes without elevating permissions. Which of the following would best accomplish this task?
A. Group Policy Editor
B. Local Users and Groups

C. Device Manager
D. System Configuration
Answer: B (LEAVE A REPLY)
Local Users and Groups is the best option to accomplish this task. Local Users and Groups is a tool that allows managing the local user accounts and groups on a Windows workstation. The technician can use this tool to create a new user account with administrator privileges or add an existing user account to the Administrators group. This way, the technician can log in with the administrator account and make system changes without elevating permissions. Group Policy Editor, Device Manager, and System Configuration are not correct answers for this question. Group Policy Editor is a tool that allows configuring policies and settings for users and computers in a domain environment. Device Manager is a tool that allows managing the hardware devices and drivers on a Windows workstation. System Configuration is a tool that allows modifying the startup options and services on a Windows workstation. None of these tools can directly grant administrator access to a user account. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 13 CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 103

NEW QUESTION: 189
Which of the following is used to ensure users have the appropriate level of access to perform their job functions?
A. Access control list
B. Multifactor authentication
C. Least privilege
D. Mobile device management
Answer: C (LEAVE A REPLY)
Least privilege is the principle that is used to ensure users have the appropriate level of access to perform their job functions. Least privilege means granting users only the minimum amount of access rights and permissions they need to perform their tasks, and nothing more. Least privilege reduces the risk of unauthorized access, data leakage, malware infection, or accidental damage by limiting what users can do on the system or network. Access control list, multifactor authentication, and mobile device management are not principles, but rather mechanisms or methods that can implement least privilege. Access control list is a list that specifies the users or groups that are allowed or denied access to a resource, such as a file, folder, or printer. Multifactor authentication is a method that requires users to provide two or more pieces of evidence to prove their identity, such as a password, a token, or a biometric factor. Mobile device management is a tool that allows managing and securing mobile devices, such as smartphones or tablets, that are used by employees to access corporate data or applications. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25
[CompTIA Security+ SY0-601 Certification Study Guide], page 1003

NEW QUESTION: 190
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: 191
Which of the following is a situation in which a surge suppressor is considered critical?
A. A device is being turned on for the first time.
B. The electrical source is near high humidity.
C. A device requires 220V or higher.
D. The electrical source is not grounded.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 192
A user reports that a VPN connection is not working. A technician does not find any internal documentation about this issue. Which of the following should the technician do once the issue is resolved? (Select two).
A. Report the error to the user's supervisor.
B. Create a KB article about the error and share it with the team.
C. Note the resolution in the ticket closure message.
D. Replace the user's computer to avoid future issues.
E. Escalate the ticket to the engineering team for investigation.
F. Update local digital certificates on the user's workstation.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 193
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: C (LEAVE A REPLY)
https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0)

NEW QUESTION: 194
A large company is changing its password length requirements. The Chief Information Officer is mandating that passwords now be at least 12 characters long, instead of 10. Which of the following should be used to adjust this setting?
Group Policy
A. User accounts
B. Access control lists
C. Authenticator applications

Answer: A (LEAVE A REPLY)
Group Policy is a feature of Windows that allows administrators to manage and configure settings for computers and users on a network12. One of the settings that can be controlled by Group Policy is the password policy, which defines the rules for creating and changing passwords, such as minimum length, complexity, expiration, and history34. By using Group Policy, the Chief Information Officer can enforce the new password length requirement for all users and computers in the company's domain, without having to manually adjust each user account or device.
Reference1: The Official CompTIA A+ Core 2 Student Guide (Exam 220-1102), page 10-11 2: CompTIA A+ Certification Exam Core 2 Objectives, page 13 3: The Official CompTIA A+ Core 2 Instructor Guide (Exam 220-1102), page 10-12 4: CompTIA A+ Certification Exam: Core 2 (220-1102) Exam Objectives

NEW QUESTION: 195
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 (LEAVE A REPLY)
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: 196
A technician successfully removed malicious software from an infected computer after running updates and scheduled scans to mitigate future risks. Which of the following should the technician do next?
A. Educate the end user on best practices for security.
B. Quarantine the host in the antivirus system.
C. Investigate how the system was infected with malware.
D. Create a system restore point.
Answer: (SHOW ANSWER)
Educating the end user on best practices for security is the next step that the technician should take after successfully removing malicious software from an infected computer. Educating the end user on best practices for security is an important part of preventing future infections and mitigating risks. The technician should explain to the end user how to avoid common sources of malware, such as phishing emails, malicious websites, or removable media. The technician should also advise the end user to use strong passwords, update software regularly, enable antivirus and firewall protection, and backup data frequently. Educating the end user on best practices for security can help the end user become more aware and responsible for their own security and reduce the likelihood of recurrence of malware infections.
Quarantining the host in the antivirus system, investigating how the system was infected with malware, and creating a

system restore point are not the next steps that the technician should take after successfully removing malicious software from an infected computer. Quarantining the host in the antivirus system is a step that the technician should take before removing malicious software from an infected computer. Quarantining the host in the antivirus system means isolating the infected computer from the network or other devices to prevent the spread of malware. Investigating how the system was infected with malware is a step that the technician should take during or after removing malicious software from an infected computer. Investigating how the system was infected with malware means identifying the source, type, and impact of malware on the system and documenting the findings and actions taken. Creating a system restore point is a step that the technician should take before removing malicious software from an infected computer. Creating a system restore point means saving a snapshot of the system's configuration and settings at a certain point in time, which can be used to restore the system in case of failure or corruption. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15 CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 458

NEW QUESTION: 197
A technician is setting up a new PC in a SOHO. Which of the following should the technician most likely configure on the PC?
A. VDI
B. Mapped drives
C. Wireless WAN
D. Domain
Answer: (SHOW ANSWER)
In a Small Office/Home Office (SOHO) setup, the technician is most likely to configure mapped drives on a new PC. Mapped drives allow for easy access to shared resources such as files and printers on the network. This setup facilitates file sharing and collaboration within a small network, making it an essential configuration for SOHO environments.

NEW QUESTION: 198
When a user is in the office, web pages are loading slowly on the user's phone. Which of the following best explains this issue?
A. Exceeded the data usage limit
B. Sluggish response time
C. Degraded network service
D. High network traffic
Answer: (SHOW ANSWER)

When a user experiences slow web page loading on their phone while in the office, the most likely cause is:
* High network traffic:In an office environment, many devices are often connected to the network simultaneously, which can lead to congestion and slow internet speeds. High network traffic means more devices are competing for the same bandwidth, causing delays.
* Exceeded the data usage limit:This typically applies to cellular data plans, not Wi-Fi in an office setting.
* Sluggish response time:This is a symptom rather than a cause and can result from high network traffic.
* Degraded network service:While this could be a factor, it is broader and less specific than high network traffic, which is more directly related to the user's experience.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 2.7: Given a scenario troubleshoot problems with wired and wireless networks.
Network performance troubleshooting documentation.

NEW QUESTION: 199
A user with a disability needs to be able to press the Ctrl+Alt+Del keyboard sequence one key at a time. Which of the following turns on this Ease of Access feature?
A. Press the Shift key five times in a row.
B. Press Ctrl+Alt+Esc simultaneously.
C. Press Ctrl+Alt+Tab simultaneously.
D. Press the Windows key+Tab.
Answer: A (LEAVE A REPLY)
The Ease of Access feature in Windows that allows a user to press keyboard shortcuts one key at a time is called "Sticky Keys." Sticky Keys is designed to assist users with disabilities who have difficulty pressing multiple keys simultaneously.
To enable Sticky Keys:
Press the Shift key five times in a row: This is the quickest method to activate Sticky Keys. When you press the Shift key five times, a dialog box appears, asking if you want to turn on Sticky Keys. This method is widely documented as the default shortcut for enabling this feature.
Confirmation dialog: A confirmation dialog will appear asking if you want to turn on Sticky Keys. Click "Yes" to enable it.
Control Panel or Settings: Alternatively, you can enable Sticky Keys through the Control Panel or the Settings app. Go to "Ease of Access" settings, find the "Keyboard" section, and turn on Sticky Keys from there.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 1.4: Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.
Windows Ease of Access documentation.

NEW QUESTION: 200
A hard drive that previously contained PII needs to be repurposed for a public access workstation. Which of the following data destruction methods should a technician use to ensure data is completely removed from the hard drive?
A. Recycling
B. Shredding
C. Degaussing

D. Low-level formatting
Answer: D (LEAVE A REPLY)

NEW QUESTION: 201
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: 202
A technician is investigating a workstation that has not received the latest policy changes. Which of the following commands should the technician use to apply the latest domain policy changes?
A. sfc /scannow
B. gpupdare /force
C. chkdsk /y
D. xcopy Zp
Answer: B (LEAVE A REPLY)
When a workstation has not received the latest policy changes, the gpupdate command is used to manually apply the latest group policies from the domain controller.
Option A: sfc /scannowThis command is used to scan and repair corrupted system files, not to update group policies.
Option B: gpupdate /forceThis command forces the workstation to reapply all group policies, ensuring that the latest policies are applied immediately.
Option C: chkdsk /yThis command checks the integrity of the file system and fixes logical file system errors, not to update group policies.
Option D: xcopy /ZpThis command is used for copying files and directories, not for updating group policies.
Reference:
CompTIA A+ 220-1102 Objective 1.6 (Configure Microsoft Windows networking features on a client/desktop), particularly managing and applying group policies.

NEW QUESTION: 203
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: 204
Multiple users routinely record log-in information in readily accessible areas. Which of the following is the best way to mitigate this issue?
A. Trusted sources
B. Valid certificates
C. User training
D. Password manager
Answer: D (LEAVE A REPLY)
Using a password manager is the best way to mitigate the issue of users recording their login information in accessible areas. Password managers securely store and encrypt passwords and login details, reducing the need for users to write down or remember multiple complex passwords. This approach enhances security by encouraging the use of strong, unique passwords for different accounts without the risk of forgetting them or the unsafe practice of writing them down. Trusted sources, valid certificates, and user training are important security measures but do not directly address the problem of managing multiple secure passwords as effectively as a password manager does.

NEW QUESTION: 205
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: 206
A user recently accessed several websites that required log-in credentials. During subsequent visits, the user noticed that the log-in credential fields were already filled in. Which of the following is a way to prevent the browser from remembering the credentials for future visits?
A. Clearing the browser cache

B. Deleting the trusted sources
C. Disabling the password manager
D. Removing the secure connections
Answer: (SHOW ANSWER)

NEW QUESTION: 207
Which of the following documents in criminal proceedings must be updated every time a piece of evidence is touched or transferred in order for the evidence to be considered valid?
A. Licensing agreement
B. Regulatory compliance
C. Incident documentation
D. Chain of custody
Answer: D (LEAVE A REPLY)
In criminal proceedings, maintaining the integrity of evidence is crucial. The document that must be updated every time evidence is handled or transferred is:
* Chain of custody: This document tracks the history of the evidence, detailing every person who has handled it and every transfer that has occurred. It ensures that the evidence has not been tampered with and maintains its validity in court.
* Licensing agreement: Pertains to software usage rights and has no relation to evidence handling.
* Regulatory compliance: Refers to adherence to laws and regulations, not evidence tracking.
* Incident documentation: Details the incident but does not specifically track evidence handling.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 4.6: Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.
Legal documentation and evidence handling procedures.

NEW QUESTION: 208
A homeowner recently moved and requires a new router for the new ISP to function correctly. The internet service has been installed and has been confirmed as functional. Which of the following is the FIRST step the homeowner should take after installation of all relevant cabling and hardware?
A. Convert the PC from a DHCP assignment to a static IP address.
B. Run a speed test to ensure the advertised speeds are met.
C. Test all network sharing and printing functionality the customer uses.
D. Change the default passwords on new network devices.
Answer: (SHOW ANSWER)
When a homeowner moves and sets up a new router for the new ISP it is important to take appropriate security measures to protect their network from potential security threats. The FIRST step that the homeowner should take after installation of all relevant cabling and hardware is to change the default passwords on new network devices.
Most modern routers come with default usernames and passwords that are widely known to potential attackers. If these defaults are not changed, it could make it easier for external attackers to gain unauthorized access to the network.
Changing the passwords on new network devices is a simple but effective way to improve the security posture of the network.

NEW QUESTION: 209
Which of the following types of malware is designed to enable administrative access to a computer?
A. Rootkit
B. Trojan
C. Worm
D. Ransomware
Answer: A (LEAVE A REPLY)
A rootkit (Option A) is a type of malware designed to gain administrative (root) access to a system while hiding its presence. Rootkits can manipulate system processes and files to remain undetected, making them particularly dangerous.
Trojan (Option B) is malware disguised as legitimate software but doesn't necessarily provide administrative access.
Worm (Option C) spreads across networks but doesn't grant administrative access.
Ransomware (Option D) encrypts data and demands a ransom but doesn't typically provide ongoing administrative access.
CompTIA A+ Core 2 Reference:
2.3 - Explain malware types, including rootkits and their purpose .

NEW QUESTION: 210
Which of the following would typically require the most computing resources from the host computer?
Chrome OS
A. Windows
B. Android
C. macOS
D. Linux
Answer: B (LEAVE A REPLY)
Windows is the operating system that typically requires the most computing resources from the host computer, compared to the other options. Computing resources include hardware components such as CPU, RAM, disk space, graphics card, and network adapter. The minimum system requirements for an operating system indicate the minimum amount of computing resources needed to install and run the operating system on a computer. The higher the minimum system requirements, the more computing resources the operating system consumes.
According to the web search results, the minimum system requirements for Windows 10 and Windows 11 are as follows12: CPU: 1 GHz or faster with two or more cores (Windows 10); 1 GHz or faster with two or more cores on a compatible 64-bit processor (Windows 11) RAM: 1 GB for 32-bit or 2 GB for 64-bit (Windows 10); 4 GB (Windows 11) Disk space: 16 GB for 32-bit or 32 GB for 64-bit (Windows 10); 64 GB (Windows 11) Graphics card: DirectX 9 or later with WDDM 1.0 driver (Windows 10); DirectX 12 compatible with WDDM 2.0 driver (Windows 11) Network adapter: Ethernet or Wi-Fi (Windows 10); Ethernet or Wi-Fi that supports 5 GHz (Windows 11) The minimum system requirements for macOS Ventura are as follows:
CPU: Intel Core i3 or higher, or Apple M1 chip
RAM: 4 GB
Disk space: 35.5 GB
Graphics card: Metal-capable
Network adapter: Ethernet or Wi-Fi

The minimum system requirements for Chrome OS are as follows:
CPU: Intel Celeron or higher
RAM: 2 GB
Disk space: 16 GB
Graphics card: Integrated
Network adapter: Ethernet or Wi-Fi
The minimum system requirements for Android are as follows:
CPU: 1 GHz or higher
RAM: 512 MB
Disk space: 8 GB
Graphics card: OpenGL ES 2.0
Network adapter: Ethernet or Wi-Fi
The minimum system requirements for Linux vary depending on the distribution, but a common example is Ubuntu, which has the following minimum system requirements:
CPU: 2 GHz dual core processor or better
RAM: 4 GB
Disk space: 25 GB
Graphics card: 1024 x 768 screen resolution
Network adapter: Ethernet or Wi-Fi
Based on the comparison of the minimum system requirements, Windows has the highest requirements for CPU, RAM, disk space, and graphics card, while Chrome OS and Android have the lowest requirements. macOS and Linux have moderate requirements, depending on the hardware and software configuration. Therefore, Windows is the operating system that typically requires the most computing resources from the host computer.
Reference:
Windows, macOS, Chrome OS, or Linux: Which Operating System Is Right for You?1 Comparison of operating systems3 Windows 10 vs 11 Minimum System Requirements: Why Need a New One?2 macOS Monterey - Technical Specifications Chrome OS - Wikipedia Android - Wikipedia Installation/SystemRequirements - Community Help Wiki

NEW QUESTION: 211
A home office user wants to ensure a PC is backed up and protected against local natural disasters and hardware failures. Which of the following would meet the user's requirements?
A. Using an agent-based cloud backup solution
B. Implementing a grandfather-father-son backup rotation
C. Automating backups to a local network share
D. Saving files manually to an external drive
Answer: A (LEAVE A REPLY)
For ensuring data protection against local natural disasters and hardware failures, the best approach is to use an off-site solution that provides redundancy and is resilient to local disruptions.
Using an agent-based cloud backup solution: This method involves backing up data to a remote cloud server, providing protection against local disasters like floods, fires, or hardware failures since the data is stored off-site and can be accessed from anywhere.

Implementing a grandfather-father-son backup rotation: While effective for managing local backups, this method typically involves physical media which could still be vulnerable to local disasters.
Automating backups to a local network share: This keeps the backups within the same physical location, making them susceptible to local disasters.
Saving files manually to an external drive: This method is prone to human error and doesn't provide automated or off-site protection.

NEW QUESTION: 212
A technician is troubleshooting a user's PC that is displaying pop-up windows, which are advertising free software downloads. When the technician tries to open a document, the system displays an error message that reads: Not enough memory to perform this operation. Which of the following should be the technician's next step to resolve this issue?
A. Install antispyware
B. Reimage the system
C. Disable the pop-up blocker
D. Upgrade the browser
E. Install antivirus software
Answer: (SHOW ANSWER)
The presence of pop-up windows advertising free software and the error message about memory are indicative of spyware infection. Installing and running antispyware software is a practical first step to remove the unwanted software and resolve the issue without resorting to more drastic measures like re-imaging the system.

NEW QUESTION: 213
A user is attempting to access a shared drive from a company-issued laptop while working from home. The user is unable to access any files and notices a red X next to each shared drive. Which of the following needs to be configured in order to restore the user's access to the shared drives?
A. IPv6
B. VPN
C. IPS
D. DNS
Answer: B (LEAVE A REPLY)
When a user is unable to access shared drives from a company-issued laptop while working from home, the likely requirement is:

* VPN (Virtual Private Network): A VPN allows secure access to the company's network from a remote location. Without a VPN connection, the user cannot access network resources such as shared drives.
* IPv6: Involves IP addressing and is not directly related to accessing shared drives.
* IPS (Intrusion Prevention System): Provides network security but does not facilitate access to shared drives.
* DNS: Manages domain name resolution and is not typically the issue when specific shared drives are inaccessible.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 2.7: Explain common methods for securing mobile and embedded devices.
VPN configuration and remote access documentation.

NEW QUESTION: 214
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

NEW QUESTION: 215
A user's workstation was infected with a newly discovered virus that the AV system detected. After a full virus scan and a workstation reboot, the virus is still present in the OS. Which of the following actions should the user take to remove the virus?
A. Enable the system firewall.
B. Use bootable antivirus media to scan the system.
C. Download software designed to specifically target the virus.
D. Run the operating system update process.
Answer: (SHOW ANSWER)
Using bootable antivirus media to scan the system is an effective method for removing a persistent virus. Booting from external antivirus media allows the system to scan for and remove malware without the infected operating system running, which can prevent the virus from hiding or resisting removal efforts that might occur within the active OS environment.

NEW QUESTION: 216
Which of the following macOS file types requires mounting before installation?
A. .pkg
B. .zip
C. .app
D. .dmg
Answer: D (LEAVE A REPLY)

The .dmg file type in macOS requires mounting before installation. .dmg files are disk image files used to distribute software on macOS. When opened, they mount a virtual disk on the desktop, from which the application can be installed. Other file types like .pkg, .zip, and .app have different processes for installation and do not require mounting in the same way.

NEW QUESTION: 217
Which of the following would most likely be used to extend the life of a device?
A. Battery backup
B. Electrostatic discharge mat
C. Proper ventilation
D. Green disposal
Answer: C (LEAVE A REPLY)
Proper ventilation is a factor that can extend the life of a device by preventing overheating and thermal damage to the device's components. Proper ventilation means ensuring that there is enough airflow around and inside the device to dissipate heat and maintain a suitable temperature for optimal performance. Proper ventilation can be achieved by using fans, heat sinks, vents, or liquid cooling systems, as well as avoiding placing the device near heat sources or in enclosed spaces. Battery backup, electrostatic discharge mat, and green disposal are not factors that can extend the life of a device.

NEW QUESTION: 218
A company would like to implement multifactor authentication for all employees at a minimal cost. Which of the following best meets the company's requirements?
A. Biometrics
B. Soft token
C. Access control lists
D. Smart card
Answer: (SHOW ANSWER)
A soft token, also known as a software token or an OTP (one-time password) app, is a type of multifactor authentication that generates a temporary code or password on a user's device, such as a smartphone or a tablet. The user must enter this code or password along with their username and password to access their account or service. A soft token can help improve security by adding an extra layer of verification and preventing unauthorized access even if the user's credentials are compromised. A soft token can also be implemented at a minimal cost, as it does not require any additional hardware or infrastructure. Biometrics, access control lists, and smart card are not types of multifactor authentication that can be implemented at a minimal cost.

NEW QUESTION: 219
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: (SHOW ANSWER)

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: 220

A technician is troubleshooting a Windows 10 PC that has experienced a BSOD. The user recently installed optional Windows updates. Which of the following is best way to resolve the issue?

A. Enable System Restore.

B. Roll back the device drivers.

C. Reinstall the OS.

D. Update the BIOS.

Answer: B (LEAVE A REPLY)

To resolve a BSOD issue on a Windows 10 PC after installing optional Windows updates, the best approach is to Roll back the device drivers (B). BSODs can often be caused by incompatible or faulty drivers introduced during an update. Rolling back the drivers to a previous version can restore system stability and resolve the BSOD issue.

NEW QUESTION: 221

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: A (LEAVE A REPLY)

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: 222

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: 223

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)

Explore

The correct answer is D. Internet Options. The Internet Options utility in Windows allows you to configure various settings related to your internet connection, including the proxy server settings. To access the Internet Options utility, you can either open the Control Panel and click on Internet Options, or open any web browser and click on the Tools menu and then on Internet Options. In the Internet Options window, go to the Connections tab and click on the LAN settings button. Here, you can enable or disable the use of a proxy server, as well as enter the address and port number of the proxy server you want to use12.

Security and Maintenance is a utility in Windows that allows you to view and manage the security and maintenance status of your computer, such as firewall, antivirus, backup, troubleshooting, and recovery settings. It does not have any option to configure proxy server settings.

Network and Sharing Center is a utility in Windows that allows you to view and manage your network connections, such as Wi-Fi, Ethernet, VPN, or dial-up. It also allows you to change network settings, such as network discovery, file and printer sharing, homegroup, and adapter settings. It does not have any option to configure proxy server settings.

Windows Defender Firewall is a utility in Windows that allows you to enable or disable the firewall protection for your computer, as well as configure firewall rules for inbound and outbound traffic. It does not have any option to configure proxy server settings.

NEW QUESTION: 224

A technician needs to access a Windows 10 desktop on the network in a SOHO using RDP. Although the connection is unsuccessful, the technician is able to ping the computer successfully. Which of the following is MOST likely preventing the connection?

A. The Windows 10 desktop has Windows 10 Home installed.

B. The Windows 10 desktop does not have DHCP configured.

C. The Windows 10 desktop is connected via Wi-Fi.

D. The Windows 10 desktop is hibernating.

Answer: A (LEAVE A REPLY)

The Windows 10 desktop has Windows 10 Home installed, which does not support RDP (Remote Desktop Protocol) as a host. Only Windows 10 Pro, Enterprise, and Education editions can act as RDP hosts and allow remote access to their desktops1. The Windows 10 desktop does not have DHCP configured, is connected via Wi-Fi, or is hibernating are not likely to prevent the RDP connection if the technician is able to ping the computer successfully.

NEW QUESTION: 225

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: D (LEAVE A REPLY)

Resource Monitor will help a technician identify the issue when a user reports a computer is running slow1

NEW QUESTION: 226

A hotel's Wi-Fi was used to steal information on a corporate laptop. A technician notes the following security log:

SRC: 192.168.1.1/secrets.zip Protocol SMB >> DST: 192.168.1.50/capture

The technician analyses the following Windows firewall information:

Port	Status	Direction
1	Open	In/Out
445	Open	In/Out
25	Open	Out
110	Open	In/Out
53	Open	In/Out

Which of the following protocols most likely allowed the data theft to occur?

A. 1

B. 53

C. 110

D. 445

Answer: D (LEAVE A REPLY)

The protocol that most likely allowed the data theft to occur is SMB over TCP port 445. SMB is a network file sharing protocol that enables access to files, printers, and other resources on a network. Port 445 is used by SMB to communicate directly over TCP without the need for NetBIOS, which is an older and less secure protocol. The security log shows that the source IP address 192.168.1.1 sent a file named secrets.zip using SMB protocol to the destination IP address 192.168.1.50, which captured the file. The Windows firewall information shows that port 445 is enabled for inbound and outbound traffic, which means that it is not blocked by the firewall. Therefore, port 445 is the most likely port that was exploited by the attacker to steal the data from the corporate laptop.

Reference:

SMB port number: Ports 445, 139, 138, and 137 explained1

What is an SMB Port + Ports 445 and 139 Explained2

CompTIA A+ Certification Exam Core 2 Objectives3

NEW QUESTION: 227

Which of the following often uses an SMS or third-party application as a secondary method to access a system?

A. MFA

B. WPA2

C. AES

D. RADIUS

Answer: A (LEAVE A REPLY)

MFA (Multi-Factor Authentication) is a security measure that often uses an SMS or third-party application as a secondary method to access a system. MFA requires the user to provide two or more pieces of evidence to prove their identity, such as something they know (e.g., password), something they have (e.g., phone), or something they are (e.g., fingerprint)2. WPA2 (Wi-Fi Protected Access 2) is a security protocol for wireless networks that does not use SMS or third-party applications. AES (Advanced Encryption Standard) is a symmetric encryption algorithm that does not use SMS or third-party applications. RADIUS (Remote Authentication Dial-In User Service) is a network protocol that provides centralized authentication and authorization for remote access clients, but does not use SMS or third-party applications.

NEW QUESTION: 228

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: 229
After clicking on a link in an email a Chief Financial Officer (CFO) received the following error:

The CFO then reported the incident to a technician. The link is purportedly to the organization's bank. Which of the following should the technician perform FIRST?
A. Update the browser's CRLs
B. File a trouble ticket with the bank.
C. Contact the ISP to report the CFCs concern
D. Instruct the CFO to exit the browser
Answer: A (LEAVE A REPLY)
The technician should update the browser's CRLs first. The error message indicates that the certificate revocation list (CRL) is not up to date. Updating the CRLs will ensure that the browser can verify the authenticity of the bank's website.

NEW QUESTION: 230

A user is unable to start a computer following a failed Windows 10 update. When trying to start the computer, the user sees a blue screen of death. Which of the following steps should a technician take to diagnose the issue?
A. Perform a safe mode boot.
B. Run the System Restore wizard.
C. Start the computer in the last known-good configuration.
D. Reset the BIOS settinqs.
Answer: A (LEAVE A REPLY)
Booting in safe mode is the initial step to diagnose a computer experiencing a blue screen of death (BSOD) following a failed Windows 10 update. Safe mode starts the computer with a minimal set of drivers and services, allowing troubleshooting and identification of the problematic software or driver causing the BSOD. This mode provides a safer environment to uninstall recent updates or drivers, perform system scans, and restore the system if necessary. Other options like System Restore wizard, last known-good configuration, and resetting BIOS settings may be subsequent steps but do not directly diagnose the issue as effectively as booting in safe mode.

NEW QUESTION: 231
A desktop technician has received reports that a user's PC is slow to load programs and saved files. The technician investigates and discovers an older HDD with adequate free space. Which of the following should the technician use to alleviate the issue first?
A. Disk Management
B. Disk Defragment
C. Disk Cleanup
D. Device Manager
Answer: (SHOW ANSWER)
Disk Defragment is a tool that can be used to improve the performance of a hard disk drive (HDD). HDDs store data in sectors and clusters on spinning platters. Over time, as data is written, deleted, and moved, the data may become fragmented, meaning that it is spread across different locations on the disk. This causes the HDD to take longer to access and load data, resulting in slower performance. Disk Defragment consolidates the fragmented data and rearranges it in a contiguous manner, which reduces the seek time and increases the speed of the HDD. Disk Management, Disk Cleanup, and Device Manager are not tools that can alleviate the issue of slow HDD performance.

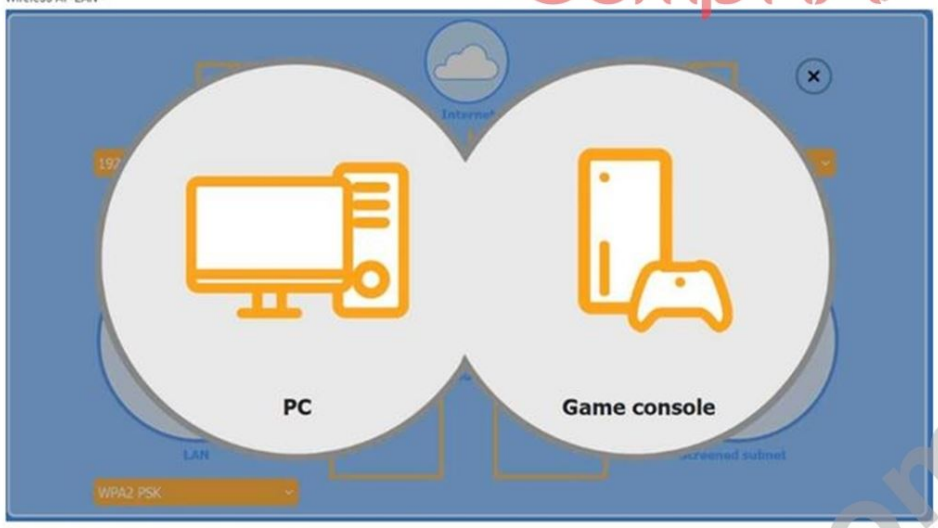
NEW QUESTION: 232
Which of the following is used to explain issues that may occur during a change implementation?
A. Scope change
B. End-user acceptance
C. Risk analysis
D. Rollback plan
Answer: (SHOW ANSWER)
Risk analysis is used to explain issues that may occur during a change implementation. Risk 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

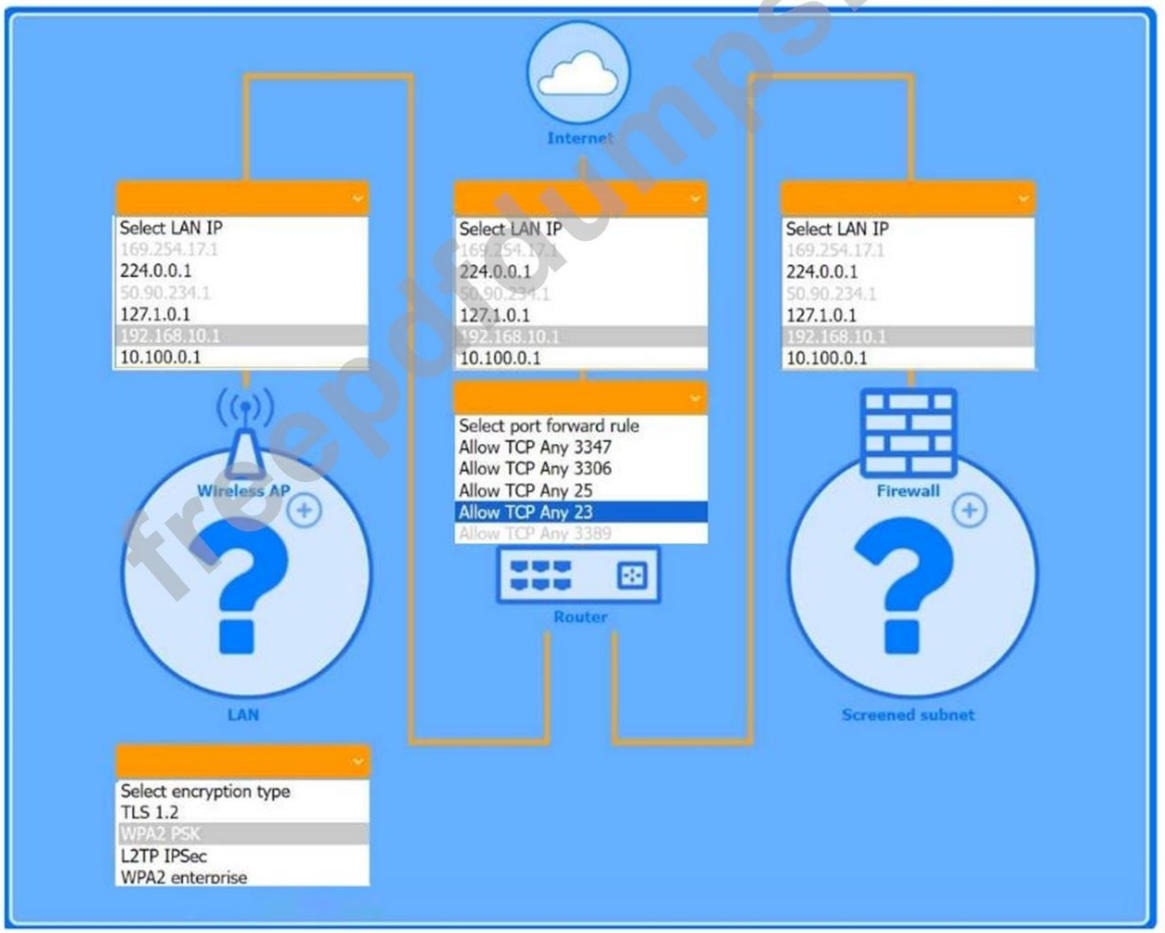
NEW QUESTION: 233
A user has a license for an application that is in use on a personal home laptop. The user approaches a systems administrator about using the same license on multiple computers on the corporate network. Which of the following BEST describes what the systems administrator should tell the user?
A. Use the application only on the home laptop because it contains the initial license.
B. Use the application at home and contact the vendor regarding a corporate license.
C. Use the application on any computer since the user has a license.
D. Use the application only on corporate computers.
Answer: B (LEAVE A REPLY)
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: 234
You are configuring a home network for a customer. The customer has requested the ability to access a Windows PC remotely, and needs all chat and optional functions to work in their game console.
INSTRUCTIONS
Use the drop-down menus to complete the network configuration for the customer. Each option may only be used once, and not all options will be used. Then, click the + sign to place each device in its appropriate location. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Wireless AP LAN -

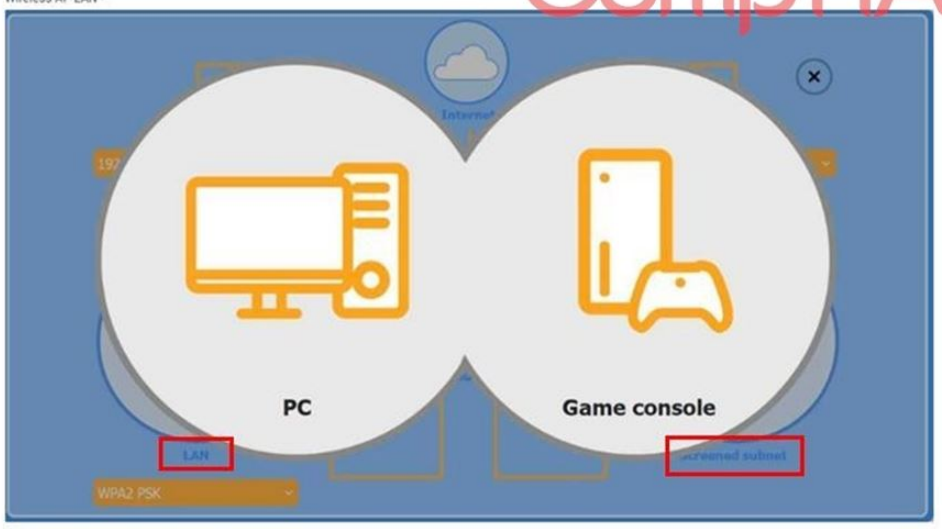


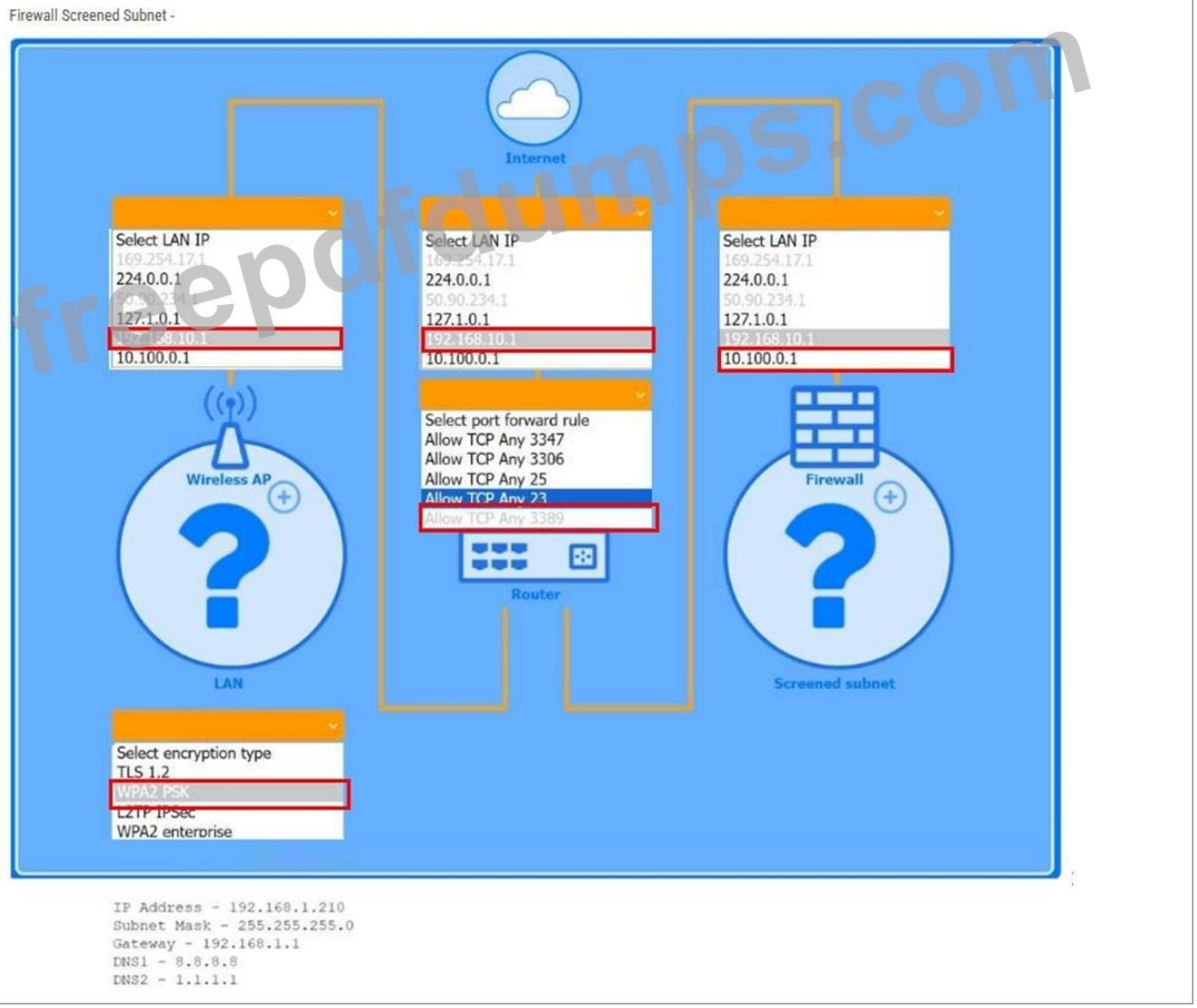
Firewall Screened Subnet -




```
IP Address - 192.168.1.210
Subnet Mask - 255.255.255.0
Gateway - 192.168.1.1
DNS1 - 8.8.8.8
DNS2 - 1.1.1.1
```

Answer:





NEW QUESTION: 235

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 (LEAVE A REPLY)
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: 236
A user's PC is performing slowly after the user clicked on a suspicious email attachment. The technician notices that a single process is taking 100% of RAM, CPU, and network resources. Which of the following should the technician do first?
A. Disconnect the computer from the network
B. Run an antivirus scan
C. Reboot the computer
D. Educate the user about cybersecurity best practices
Answer: A (LEAVE A REPLY)
The technician should disconnect the computer from the network (Option A) first to prevent any further spread of the infection or data loss. Once the machine is isolated from the network, the technician can safely investigate the malware without risking infection to other systems.
Running an antivirus scan (Option B) comes after isolating the system.
Rebooting the computer (Option C) could lead to the loss of critical information or make it harder to diagnose the issue.
Educating the user (Option D) is important but should happen after resolving the immediate issue.
CompTIA A+ Core 2 Reference:
3.3 - Best practices for malware removal, including isolating the system first.

NEW QUESTION: 237
A change advisory board authorized a setting change so a technician is permitted to implement the change. The technician successfully implemented the change. Which of the following should be done NEXT?
A. Document the date and time of change.
B. Document the purpose of the change.
C. Document the risk level.
D. Document findings of the sandbox test.
Answer: (SHOW ANSWER)
After implementing a change authorized by the change advisory board (CAB), the technician should document the date and time of change as part of the post-implementation review. This helps to track the change history, verify the success of the change, and identify any issues or incidents caused by the change1. Documenting the purpose of the change, the risk level, and the findings of the sandbox test are all part of the pre-implementation activities that should be done before submitting the change request to the CAB2.

NEW QUESTION: 238

A user receives an error message on a Windows 10 device when trying to access a mapped drive from a Windows XP machine in the office. Other Windows XP devices in the office can access the drive. Which of the following Control Panel utilities should the user select to enable connectivity to the device?

A. Devices and Printers

B. Administrative Tools

C. Network and Sharing Center

D. Programs and Features

Answer: C (LEAVE A REPLY)

The Network and Sharing Center in the Control Panel is the central place to manage network connections and settings in Windows. When facing issues with accessing a mapped drive, this utility allows users to review and adjust network settings, making it possible to resolve connectivity problems. It provides options to view network status, set up new connections, change adapter settings, and troubleshoot network problems, which can help in enabling connectivity to the mapped drive on the Windows XP machine.

NEW QUESTION: 239

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 (LEAVE A REPLY)

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: 240

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: 241
A payroll workstation has data on it that needs to be readily available and can be recovered quickly if something is accidentally removed. Which of the following backup methods should be used to provide fast data recovery in this situation?
A. Full
B. Differential
C. Synthetic
D. Incremental
Answer: A (LEAVE A REPLY)
A full backup does not depend on any previous backups, unlike differential or incremental backups, which only save the changes made since the last backup. A synthetic backup is a type of full backup that combines an existing full backup with incremental backups to create a new full backup, but it still requires multiple backup sets to recover dat a. Therefore, a full backup is the most suitable for the payroll workstation that needs to have its data readily available and recoverable. You can learn more about the differences between full, differential, incremental, and synthetic backups from this article.

NEW QUESTION: 242
A user calls the help desk to report that mapped drives are no longer accessible. The technician verifies that clicking on any of the drives on the user's machine results in an error message. Other users in the office are not having any issues. As a first step, the technician would like to remove and attempt to reconnect the drives. Which of the following command-line tools should the technician use?
A. net use
B. set
C. mkdir
D. rename
Answer: A (LEAVE A REPLY)
The technician should use net use command-line tool to remove and reconnect mapped drives. Net use is a command that allows users to manage network connections and resources, such as shared folders or printers. Net use can be used to map or unmap network drives by specifying their drive letters and network paths. For example, net use Z: \server\share maps drive Z: to \server\share folder, and net use Z: /delete unmaps drive Z:. Set is a command that displays or modifies

environment variables for the current user or process. Set is not related to managing mapped drives. Mkdir is a command that creates a new directory or folder in the current or specified location. Mkdir is not related to managing mapped drives. Rename is a command that renames a file or folder in the current or specified location. Rename is not related to managing mapped drives. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

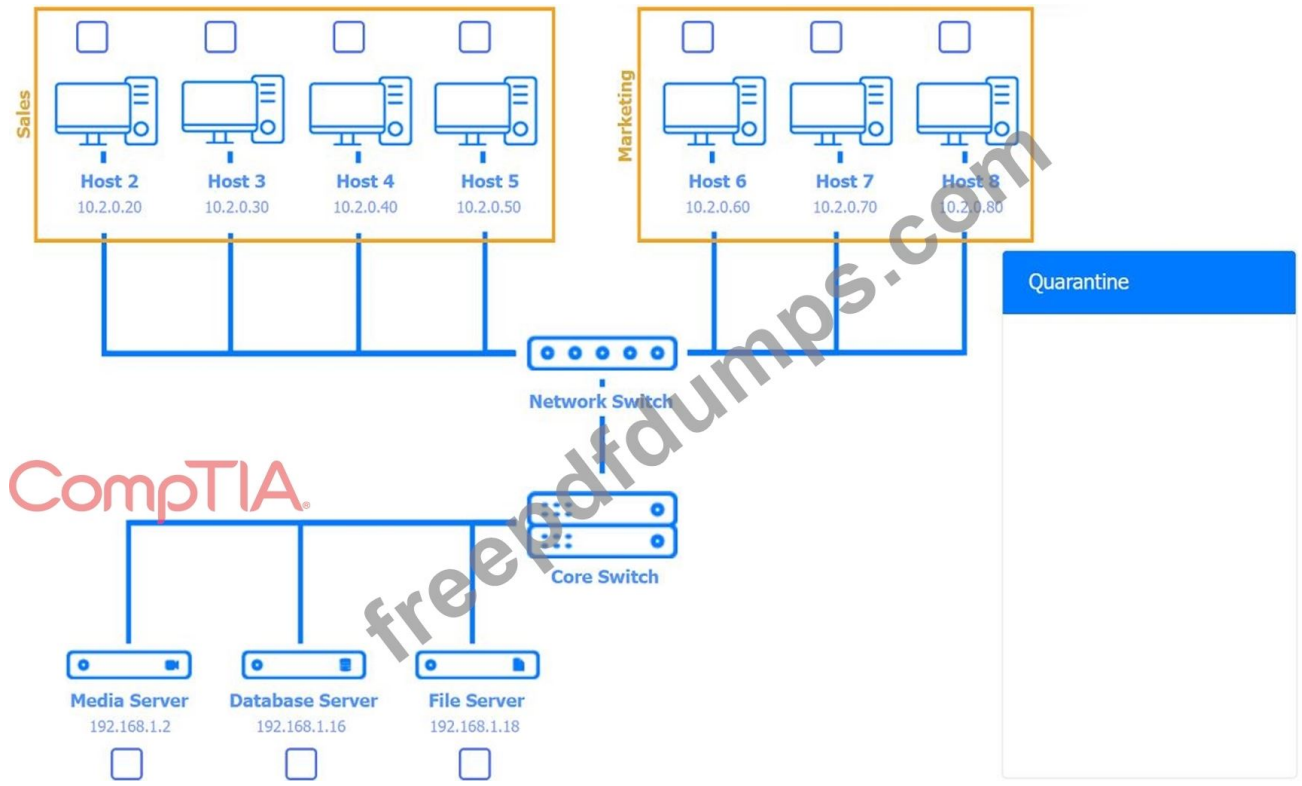
NEW QUESTION: 243
Which of the following is the most secure method of preventing someone from accessing a cell phone?
A. PIN
B. Swipe
C. Passphrase
D. Pattern
Answer: C (LEAVE A REPLY)
A passphrase is the most secure method among the options listed for preventing unauthorized access to a cell phone. Unlike a simple PIN or pattern, a passphrase is typically longer and can include a combination of letters, numbers, and special characters, making it harder to guess or brute force. Swipe and pattern locks are generally easier to bypass or observe due to smudge traces or pattern predictability. CompTIA A+ Core 2 security domain stresses using strong authentication methods to protect mobile devices, and passphrases are recommended for their complexity and strength. This aligns with mobile device security best practices covered in the official study guide, emphasizing strong, complex authentication mechanisms to secure sensitive data on mobile devices.

NEW QUESTION: 244
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: C (LEAVE A REPLY)
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: 245
A company is transitioning to a new firewall and discovers that one of the servers is still sending traffic to the old firewall. Which of the following IP address settings should a technician change to resolve this issue?
A. Dynamic

B. Gateway
C. NAT
D. DNS server
Answer: B (LEAVE A REPLY)
Detailed Explanation with Core 2 Reference:The default gateway directs network traffic to external networks. If the traffic is still going to the old firewall, updating the gateway setting will redirect it to the new firewall. This task is part of network configuration management covered in Core 2 (Core 2 Objective 2.5).

NEW QUESTION: 246
SIMULATION
Multiple users are reporting audio issues as well as performance issues after downloading unauthorized software. You have been dispatched to identify and resolve any issues on the network using best practice procedures.
INSTRUCTIONS
Quarantine and configure the appropriate device(s) so that the users' audio issues are resolved using best practice procedures.
Multiple devices may be selected for quarantine.
Click on a host or server to configure services.



Host 2 Services

Name	Status
Application Information	
Background Intelligent Transfer Service	Started
Bluetooth Support Service	
DHCP Client	Started
DNS Client	Started
Extensible Authentication Protocol	Started
Network Connections	Started
Netlogon	
Offline Files	
Parental Controls	
Persistance.j1zpxn Installer Service	Started

Host 2 Services

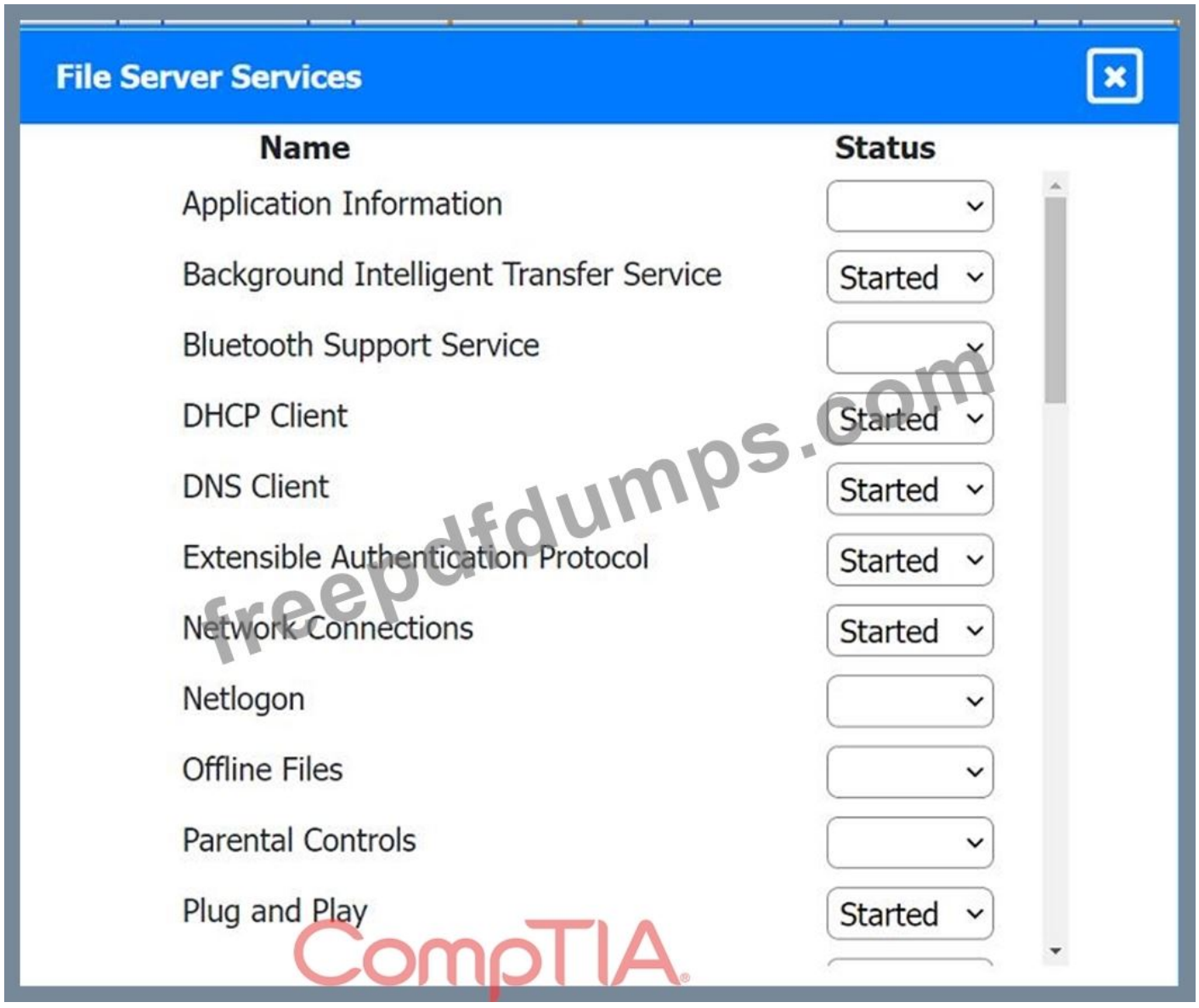
Name	Status
Volume Shadow Copy	
Windows Audio	
Windows Backup	
Windows CardSpace	
Windows Defender	
Windows Event Log	Started
Windows Firewall	
Windows Installer	
Windows Search	Started
Windows Time	
Windows Update	Started

Media Server Services

Name	Status
Application Information	
Background Intelligent Transfer Service	Started
Bluetooth Support Service	
DHCP Client	Started
DNS Client	Started
Extensible Authentication Protocol	Started
Network Connections	Started
Netlogon	
Offline Files	
Parental Controls	
Plug and Play	Started

Database Server Services

Name	Status
Application Information	
Background Intelligent Transfer Service	Started
Bluetooth Support Service	
DHCP Client	Started
DNS Client	Started
Extensible Authentication Protocol	Started
Network Connections	Started
Netlogon	
Offline Files	
Parental Controls	
Plug and Play	Started



Answer:

See the Explanation for the solution

Explanation:

Host 2 and Media Server put them to Quarantine.

NEW QUESTION: 247

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: 248
A technician receives a call (rom a user who is having issues with an application. To best understand the issue, the technician simultaneously views the user's screen with the user. Which of the following would BEST accomplish this task?
A. SSH
B. VPN
C. VNC
D. RDP
Answer: C (LEAVE A REPLY)
VNC (Virtual Network Computing) is a protocol that allows a technician to simultaneously view and control a user's screen remotely. VNC uses a server-client model, where the user's computer runs a VNC server and the technician's computer runs a VNC client. VNC can work across different platforms and operating systems3. SSH (Secure Shell) is a protocol that allows a technician to access a user's command-line interface remotely, but not their graphical user interface. VPN (Virtual Private Network) is a technology that creates a secure and encrypted connection over a public network, but does not allow screen sharing. RDP (Remote Desktop Protocol) is a protocol that allows a technician to access a user's desktop remotely, but not simultaneously with the user.

NEW QUESTION: 249
A user needs assistance installing software on a Windows PC but will not be in the office. Which of the following solutions would a technician MOST likely use to assist the user without having to install additional software?
A. VPN
B. MSRA
C. SSH
D. RDP
Answer: B (LEAVE A REPLY)
MSRA stands for Microsoft Remote Assistance, and it is a feature that allows a technician to remotely view and control another user's Windows PC with their permission. MSRA is built-in to Windows and does not require any additional software installation. To use MSRA, the technician and the user need to follow these steps:
On the user's PC, type msra in the search box on the taskbar and select Invite someone to connect to your PC and help you, or offer to help someone else.
Select Save this invitation as a file and choose a location to save the file. This file contains a password that the technician will need to connect to the user's PC.
Send the file and the password to the technician via email or another secure method.
On the technician's PC, type msra in the search box on the taskbar and select Help someone who has invited you.
Select Use an invitation file and browse to the location where the file from the user is saved. Enter the password when prompted.
The user will see a message asking if they want to allow the technician to connect to their PC. The user should select Yes.
The technician will see the user's desktop and can request control of their PC by clicking Request control on the top bar.
The user should allow this request by clicking Yes.

The technician can now view and control the user's PC and assist them with installing software.

NEW QUESTION: 250
A technician is setting up a desktop computer in a small office. The user will need to access files on a drive shared from another desktop on the network. Which of the following configurations should the technician employ to achieve this goal?
A. Configure the network as private
B. Enable a proxy server
C. Grant the network administrator role to the user
D. Create a shortcut to public documents
Answer: A (LEAVE A REPLY)
The technician should configure the network as private to allow the user to access files on a drive shared from another desktop on the network1

NEW QUESTION: 251
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: 252
A user's iPhone was permanently locked after several failed log-in attempts. Which of the following authentication methods are needed to restore access, applications, and data to the device?
A. Fingerprint and pattern
B. Facial recognition and PIN code
C. Primary account and password
D. Recovery contact and recovery key
Answer: D (LEAVE A REPLY)
If a user's iPhone is permanently locked after several failed log-in attempts, the user will need to use the recovery contact and recovery key to restore access, applications, and data to the device. The recovery contact is a trusted person who can receive a verification code from Apple and share it with the user. The recovery key is a 28-character code that the user created when setting up two-factor authentication for their Apple ID. The user will need to enter both the verification code and the recovery key on another device or computer to unlock their iPhone. This method will erase the iPhone and restore it from the iCloud backup

NEW QUESTION: 253
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: (SHOW ANSWER)
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: 254
A Windows user wants a filesystem that protects confidential data from attackers who have physical access to the system. Which of the following should the user choose?
A. ext
B. APFS
C. FAT
D. EFS
Answer: D (LEAVE A REPLY)
EFS (Encrypting File System) is a feature of Windows that provides filesystem-level encryption. It is designed to encrypt files and folders to protect them from unauthorized access, even if an attacker has physical access to the computer.
ext: A filesystem type used primarily in Linux, without native encryption features for Windows.
APFS: Apple's filesystem, used in macOS and iOS.
FAT: A simple filesystem type with no encryption features.
EFS: The correct choice for a Windows user needing to encrypt data at the filesystem level to protect against unauthorized physical access.

NEW QUESTION: 255
Which of the following file types would be used in the Windows Startup folder to automate copying a personal storage table (.pst file) to a network drive at log-in?
A. .bat
B. .dll
C. .ps1
D. .txt
Answer: A (LEAVE A REPLY)
The .bat file type would be used in the Windows Startup folder to automate copying a personal storage table (.pst) file to a network drive at log-in. A .bat file is a batch file that contains a series of commands that can be executed by the command interpreter. A .bat file can be used to perform various tasks, such as copying, moving, deleting, or renaming files or directories. A .bat file can be placed in the Windows Startup folder to run automatically when a user logs in to the system.

A .bat file can use the copy command to copy a .pst file from a local drive to a network drive. A .pst file is a personal storage table file that contains email messages, contacts, calendars, and other data from Microsoft Outlook. A .pst file can be backed up to a network drive for security or recovery purposes. The .dll, .ps1, and .txt file types are not used in the Windows Startup folder to automate copying a .pst file to a network drive at log-in. A .dll file is a dynamic link library file that contains code or data that can be shared by multiple programs. A .dll file cannot be executed directly by the user or the system. A .ps1 file is a PowerShell script file that contains commands or expressions that can be executed by the PowerShell interpreter. A .ps1 file can also perform various tasks, such as copying files or directories, but it requires PowerShell to be installed and configured on the system. A .txt file is a plain text file that contains unformatted text that can be read by any text editor or word processor. A .txt file cannot contain commands or expressions that can be executed by the system. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 18 CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 459

NEW QUESTION: 256
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: 257

A technician is setting up a wireless network in a small, crowded office and wants to minimize Wi-Fi access. Which of the following security settings should the technician enable?

A. Port forwarding

B. Unused ports

C. SSID broadcast

D. Allow list

Answer: D (LEAVE A REPLY)

Enabling an allow list (Option D) will limit access to the wireless network by only allowing devices with specified MAC addresses to connect. This is an effective method for minimizing Wi-Fi access in a crowded environment.

Port forwarding (Option A) controls traffic through specific ports but doesn't minimize wireless access.

Unused ports (Option B) could refer to physical network ports or firewall settings, unrelated to controlling Wi-Fi access.

Disabling SSID broadcast (Option C) might hide the network name but doesn't secure access.

CompTIA A+ Core 2 Reference:

2.9 - Configure security settings for SOHO networks, including MAC filtering .

NEW QUESTION: 258

A user connected a smartphone to a coffee shop's public Wi-Fi and noticed the smartphone started sending unusual SMS messages and registering strange network activity. A technician thinks a virus or other malware has infected the device. Which of the following should the technician suggest the user do immediately to best address these security and privacy concerns? (Select two).

A. Install all application updates.

B. Reboot the device.

C. Schedule an antivirus scan.

D. Uninstall recently installed applications.

E. Stay offline when in public places.

F. Enable airplane mode.

Answer: (SHOW ANSWER)

NEW QUESTION: 259

A technician is finalizing a new workstation for a user. The user's PC will be connected to the internet but will not require the same private address each time. Which of the following protocols will the technician MOST likely utilize?

A. DHCP

B. SMTP

C. DNS

D. RDP

Answer: A (LEAVE A REPLY)

DHCP stands for Dynamic Host Configuration Protocol and it is used to assign IP addresses and other network configuration parameters to devices on a network automatically. This is useful for devices that do not require the same private address each time they connect to the internet.

NEW QUESTION: 260

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

A. Lock all devices in a closet.

B. Ensure all devices are from the same manufacturer.

C. Change the default administrative password.

D. Install the latest operating system and patches

Answer: C (LEAVE A REPLY)

The technician should change the default administrative password FIRST to ensure the network equipment is secured against external threats on the Internet. Changing the default administrative password is a basic security measure that can help prevent unauthorized access to the network equipment. Locking all devices in a closet is a physical security measure that can help prevent theft or damage to the devices, but it does not address external threats on the Internet. Ensuring all devices are from the same manufacturer is not a security measure and does not address external threats on the Internet. Installing the latest operating system and patches is important for maintaining the security of the network equipment, but it is not the first action the technician should take1

NEW QUESTION: 261

Remote employees need access to information that is hosted on local servers at the company. The IT department needs to find a solution that gives employees secure access to the company's resources as if the employees were on premises. Which of the following remote connection services should the IT team implement?

A. SSH

B. VNC

C. VPN

D. RDP

Answer: C (LEAVE A REPLY)

A VPN (Virtual Private Network) is a service that allows remote employees to access the company's network resources securely over the internet as if they were on premises. A VPN encrypts the data traffic between the employee's device and the VPN server, and assigns the employee a virtual IP address that belongs to the company's network. This way, the employee can access the local servers, files, printers, and other resources without exposing them to the public internet. A VPN also protects the employee's privacy and identity by masking their real IP address and location.

NEW QUESTION: 262

An administrator is designing and implementing a server backup system that minimizes the capacity of storage used. Which of the following is the BEST backup approach to use in conjunction with synthetic full backups?

A. Differential

B. Open file

C. Archive

D. Incremental

Answer: D (LEAVE A REPLY)

Incremental backups are backups that only include the changes made since the last backup, whether it was a full or an incremental backup. Incremental backups minimize the capacity of storage used and are often used in conjunction with

synthetic full backups, which are backups that combine a full backup and subsequent incremental backups into a single backup set.

NEW QUESTION: 263
A user needs to test several software replacement possibilities. Part of the process involves installing the different software options on a corporate-imaged sandboxed PC. Which of the following is the best option to allow the user to install the required software?
A. Make the user a member of Domain Admins.
B. Add the user to the local Administrators group.
C. Let the user use credentials from another user who has rights.
D. Give the user the local, high-privileged account password.
E. Give the user the local, high-privileged account password - Incorrect. This could allow unauthorized configuration changes.
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed In-Depth
The best practice is to add the user to the local Administrators group, allowing them to install software on their own machine without giving them excessive permissions across the entire network.
A . Make the user a member of Domain Admins - Incorrect. This would give too much control over the network, creating a major security risk.
C . Let the user use credentials from another user who has rights - Incorrect. Sharing credentials violates security best practices.

NEW QUESTION: 264
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: (SHOW ANSWER)
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: 265
A technician has been unable to remediate a persistent malware infection on a user's workstation. After the technician reinstalled the OS. the malware infection returned later that day. Which of the following is the most likely source?
A. Trojan
B. Boot sector virus
C. Spyware

D. Rootkit

Answer: B (LEAVE A REPLY)

A boot sector virus infects the master boot record (MBR) of a hard drive, the sector that contains information required to start the operating system after the computer is turned on. This type of virus is particularly insidious because it loads into memory immediately upon booting and before most antivirus programs start. This makes it possible for the virus to evade detection and removal, and can easily reinfect a system even after the operating system is reinstalled if the boot sector is not cleaned.

Boot sector virus: Given that the malware infection returned after the OS reinstallation, it's likely that the virus was not removed from the boot sector during the reinstallation process. Reinstalling the OS without cleaning the boot sector won't remove the infection, allowing the virus to continue to affect the system.

Other options:

Trojan: A Trojan is a type of malware that disguises itself as legitimate software. While Trojans can be persistent, the reinstallation of the OS should remove any Trojans unless they are reintroduced after installation.

Spyware: Spyware is designed to gather information about a person or organization without their knowledge. Like Trojans, spyware should be removed with an OS reinstallation unless it is reintroduced in some way.

Rootkit: Rootkits are designed to enable continued privileged access to a computer while actively hiding their presence. While a rootkit could potentially survive an OS reinstall if it infects the firmware or certain areas outside the OS, the scenario described points more specifically to a boot sector virus, especially considering the immediate return of the infection after OS reinstallation.

NEW QUESTION: 266

A technician is creating a location on a Windows workstation for a customer to store meeting minutes. Which of the following commands should the technician use?

A. c: \minutes

B. dir

C. rmdir

D. md

Answer: (SHOW ANSWER)

The command md stands for make directory and is used to create a new directory or folder in the current location. In this case, the technician can use md minutes to create a folder named minutes in the C: drive. The other commands are not relevant for this task. c: \minutes is not a command but a path to a folder. dir is used to display a list of files and folders in the current directory. rmdir is used to remove or delete an existing directory or folder.

NEW QUESTION: 267

SIMULATION

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

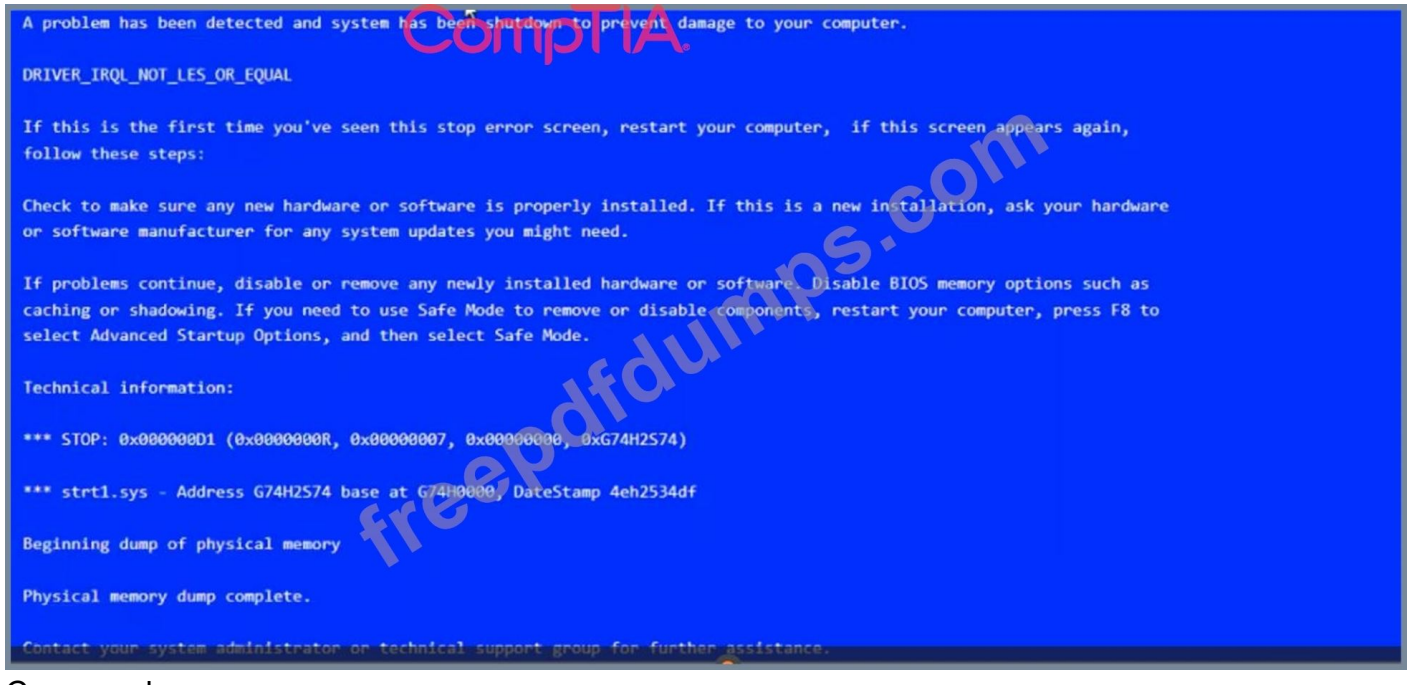
Review the information in each tab to verify the results of the deployment and resolve any issues discovered by selecting the:

Index number of the Event Viewer issue

First command to resolve the issue

Second command to resolve the issue

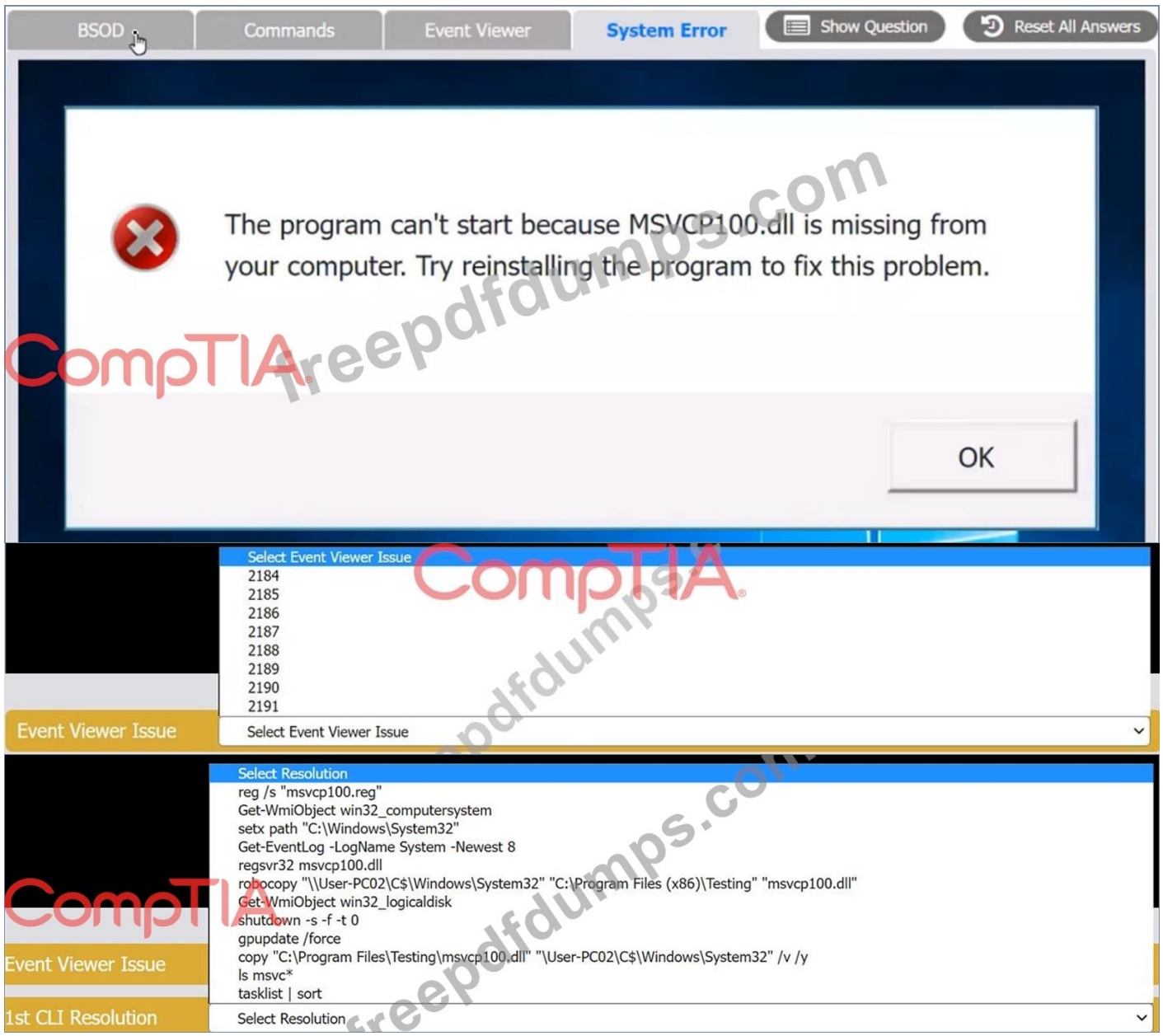
BSOD



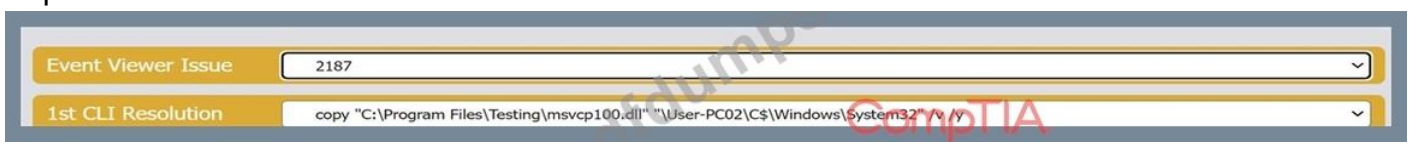
Commands:

Event Viewer:

System Error:



Answer:
see the answer below in explanation
Explanation:



The user is experiencing a system error that prevents them from using the Testing program. The error message indicates that the file MSVCP100.dll is missing from the computer. This file is part of the Microsoft Visual C++ 2010 Redistributable Package, which is required by some applications to run properly. The error may have occurred due to a corrupted or incomplete software deployment.
To resolve this issue, the user needs to restore the missing file and register it in the system. One possible way to do this is to copy the file from another computer that has the Testing program installed and working, and then use the regsvr32 command to register it. The steps are as follows:
On another computer (User-PC02) that has the Testing program installed and working, locate the file MSVCP100.dll in the folder C:\Program Files\Testing.
Share the folder C:\Windows\System32 on User-PC02 by right-clicking on it, selecting Properties, then Sharing, then Advanced Sharing, then checking Share this folder, then clicking OK.
On the user's computer (User-PC01), open a command prompt as an administrator by clicking Start, typing cmd, right-clicking on Command Prompt, and selecting Run as administrator.
In the command prompt, type the following command to copy the file MSVCP100.dll from User-PC02 to User-PC01: copy "C:\Program Files\Testing\msvcp100.dll" "\\User-PC02\C$\Windows\System32" After the file is copied, type the following command to register it in the system: regsvr32 msvcp100.dll Restart the user's computer and try to run the Testing program again.
Therefore, based on the instructions given by the user, the correct answers are:
Select Event Viewer Issue: 2187
Select First Command: copy "C:\Program Files\Testing\msvcp100.dll" "\\User-PC02\C$\Windows\System32" Select Second Command: regsvr32 msvcp100.dll

NEW QUESTION: 268
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: 269
Which of the following are mobile operating systems used on smartphones? (Select two).
A. macOS
B. Windows
C. Chrome OS
D. Linux
E. iOS
F. Android
Answer: (SHOW ANSWER)
iOS and Android are the two most popular and widely used mobile operating systems for smartphones. They are both based on Unix-like kernels and provide a variety of features and applications for users and developers. iOS is developed by Apple and runs exclusively on Apple devices, such as iPhones and iPads. Android is developed by Google and runs on a range of devices from different manufacturers, such as Samsung, Huawei, and Motorola. The other options are not mobile operating systems for smartphones, but rather for other types of devices or platforms. macOS is a desktop operating system for Apple computers, such as MacBooks and iMacs. Windows is a desktop operating system for Microsoft computers, such as Surface and Dell. Chrome OS is a web-based operating system for Google devices, such as Chromebooks and Chromecast. Linux is a family of open-source operating systems for various devices and platforms, such as Ubuntu, Fedora, and Raspberry Pi.

NEW QUESTION: 270
A technician is asked to resize a partition on the internal storage drive of a computer running macOS. Which of the followings tools should the technician use to accomplish this task?
A. Consoltf
B. Disk Utility
C. Time Machine
D. FileVault
Answer: B (LEAVE A REPLY)
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: 271
In an organization with a standardized set of installed software, a developer submits a request to have new software installed. The company does not currently have a license for this software, but the developer already downloaded the installation file and is requesting that the technician install it. The developer states that the management team approved the business use of this software. Which of the following is the best action for the technician to take?

A. Contact the software vendor to obtain the license for the user, and assist the user with installation once the license is purchased.
B. Run a scan on the downloaded installation file to confirm that it is free of malicious software, install the software, and document the software installation process.
C. Indicate to the developer that formal approval is needed; then, the IT team should investigate the software and the impact it will have on the organization before installing the software.
D. Install the software and run a full system scan with antivirus software to confirm that the operating system is free of malicious software.
Answer: (SHOW ANSWER)
Installing new software on an organization's system or device can have various implications, such as compatibility, security, performance, licensing, and compliance issues. Therefore, it is important to follow the best practices for software installation, such as doing research on the software, checking the system requirements, scanning the installation file for malware, and obtaining the proper license345. The technician should not install the software without formal approval from the management team, as this could violate the organization's policies or regulations. The technician should also not install the software without investigating the software and its impact on the organization, as this could introduce potential risks or problems to the system or device. The technician should indicate to the developer that formal approval is needed, and then work with the IT team to evaluate the software and its suitability for the organization before installing it

NEW QUESTION: 272
A technician needs to join a Windows client to a domain. Which of the following is required?
A. Local access
B. Internet connection
C. Enterprise administrative permissions
D. Computer MAC address
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed In-Depth
Joining a Windows client to a domain requires Enterprise administrative permissions because only domain administrators or authorized users can add computers to an Active Directory (AD) domain.
A . Local access - Incorrect. A user does not need to be physically near the computer; the action can be performed remotely.
B . Internet connection - Incorrect. A domain join occurs over a local network, not the internet.
D . Computer MAC address - Incorrect. MAC addresses are used for network identification but are not required to join a domain.

Steps to Join a Domain:
Open Settings > System > About > Domain or Workgroup Settings
Click Change settings > Change
Enter the domain name and provide admin credentials
Restart the computer

NEW QUESTION: 273
An employee has been using the same password for multiple applications and websites for the past several years. Which of the following would be best to prevent security issues?
A. Configuring firewall settings
B. Implementing expiration policies
C. Defining complexity requirements
D. Updating antivirus definitions
Answer: B (LEAVE A REPLY)
To prevent security issues related to an employee using the same password for multiple applications and websites, implementing expiration policies (B) is best. Password expiration policies require users to change their passwords at regular intervals, which helps to mitigate the risks associated with password reuse. Regularly changing passwords reduces the chances of unauthorized access from compromised credentials.

NEW QUESTION: 274
A customer's workstation cannot connect to the internet. A technician runs a command on the workstation to view the network settings. The following is a partial readout of the response:

```
Physical Address.....: 7C-B2-7D-73-2E-63
IPv4 Address.....: 172.16.1.10
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 172.32.11.157
DNS Servers.....: 8.8.8.8
                  4.2.2.1
```

Which of the following is the most likely cause of the issue?
A. The subnet mask is incorrect.
B. The DNS servers are incorrect.
C. The physical address is spoofed.
D. The gateway setting is incorrect.
E. The IP address is incorrect.
Answer: (SHOW ANSWER)

NEW QUESTION: 275
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 (LEAVE A REPLY)
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

NEW QUESTION: 276
A user's work PC has been the target of multiple phishing attacks. Which of the following is a way for the user to prevent further attacks?
A. Enabling Windows Firewall
B. Activating the email spam filter
C. Using a secure VPN connection
D. Running vulnerability scans on a schedule
Answer: B (LEAVE A REPLY)
Phishing attacks are typically delivered via email, so the most effective immediate measure is to filter out these malicious emails.
Enabling Windows Firewall: Helps protect against network threats but does not specifically address phishing emails.
Activating the email spam filter: Directly targets phishing attempts by filtering and blocking suspicious emails before they reach the user.
Using a secure VPN connection: Enhances secure communications but does not prevent phishing attacks.
Running vulnerability scans on a schedule: Identifies and mitigates vulnerabilities but does not address phishing emails directly.

NEW QUESTION: 277
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: A (LEAVE A REPLY)
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: 278
Which of the following features allows a user to install software from a DVD even when the laptop running macOS does not have an optical drive?
A. Multiple Desktops
B. Target Disk
C. Remote Disc
D. Disk Utility
Answer: C (LEAVE A REPLY)

NEW QUESTION: 279

A technician needs to recommend a way to keep company devices for field and home-based staff up to date. The users live in various places across the country and the company has several national offices that staff can go to for technical support Which of the following methods is most appropriate for the users?

A. Make office attendance mandatory for one day per week so that updates can be installed.

B. Ask users to ensure that they run updates on devices and reboot computers on a regular basis.

C. Push updates out via VPN on a weekly basis in a staggered manner so that the network is not affected.

D. Configure cloud-based endpoint management software to automatically manage computer updates.

Answer: (SHOW ANSWER)

For a company with geographically dispersed staff and the need to keep devices updated, using cloud-based endpoint management software is the most efficient method. This type of software allows IT administrators to remotely manage and push updates to company devices, regardless of their location. It ensures that all devices remain up to date with the latest security patches and software updates without requiring physical access or user intervention. This approach is scalable, reduces the risk of unpatched vulnerabilities, and is convenient for both the IT department and the end-users.

NEW QUESTION: 280

Antivirus software indicates that a workstation is infected with ransomware that cannot be quarantined. Which of the following should be performed first to prevent further damage to the host and other systems?

Turn off the machine.

A. Run a full antivirus scan.

B. Remove the LAN card.

C. Install a different endpoint solution.

Answer: A (LEAVE A REPLY)

Turning off the machine is the first and most urgent step to prevent further damage to the host and other systems. Ransomware can encrypt files, steal data, and spread to other devices on the network if the infected machine remains online. Turning off the machine will stop the ransomware process and isolate the machine from the network12. The other options are either ineffective or risky. Running a full antivirus scan may not detect or remove the ransomware, especially if it is a new or unknown variant. Removing the LAN card may disconnect the machine from the network, but it will not stop the ransomware from encrypting or deleting files on the local drive. Installing a different endpoint solution may not be possible or helpful if the ransomware has already compromised the system or blocked the installation.

NEW QUESTION: 281

Which of the following file types allows a user to easily uninstall software from macOS by simply placing it in the trash bin?

.exe

A. .dmg

B. . app

C. . rpm

D. .pkg

Answer: (SHOW ANSWER)

app files are application bundles that contain all the necessary files and resources for a Mac app. They can be easily deleted by dragging them to the Trash or using Launchpad12. Other file types, such as .exe, .dmg, .rpm, and .pkg, are either not compatible with macOS or require additional steps to uninstall34.

NEW QUESTION: 282
A new spam gateway was recently deployed at a small business However; users still occasionally receive spam. The management team is concerned that users will open the messages and potentially infect the network systems. Which of the following is the MOST effective method for dealing with this Issue?
A. Adjusting the spam gateway
B. Updating firmware for the spam appliance
C. Adjusting AV settings
D. Providing user training
Answer: D (LEAVE A REPLY)
The most effective method for dealing with spam messages in a small business is to provide user training1. Users should be trained to recognize spam messages and avoid opening them1. They should also be trained to report spam messages to the IT department so that appropriate action can be taken1. In addition, users should be trained to avoid clicking on links or downloading attachments from unknown sources1. By providing user training, the management team can reduce the risk of users opening spam messages and potentially infecting the network systems1.

NEW QUESTION: 283
A user reports that an air-gapped computer may have been infected with a virus after the user transferred files from a USB drive. The technician runs a computer scan with Windows Defender but does not find an infection. Which of the following actions should the technician take next? (Select two).
A. Examine the event logs.
B. Connect to the network.
C. Document the findings.
D. Update the definitions.
E. Reimage the computer.
F. Enable the firewall.
Answer: (SHOW ANSWER)
When dealing with a suspected virus infection on an air-gapped computer, after an initial scan with Windows Defender shows no infection, the next steps should include examining the event logs to look for suspicious activity and updating the virus definitions for a more thorough scan. Event logs can provide insights into system changes and potential malicious activities, while updated definitions ensure the antivirus software can detect the latest threats. Connecting to the network or enabling the firewall might not be appropriate due to the risk of spreading the infection, and re-imaging the computer or documenting the findings would be subsequent steps if the initial actions don't resolve the issue.Reference: Official CompTIA A+ Core 1 and Core 2 Student Guide.

NEW QUESTION: 284
Which of the following is a reason why PII is regulated?
A. To protect privacy rights
B. To increase efficiency of databases
C. To stop information leaks
D. To establish a chain-of-custody

E. To discourage anonymity
Answer: A (LEAVE A REPLY)

NEW QUESTION: 285
Which of the following is the STRONGEST wireless configuration?
A. WPS
B. WPA3
C. WEP
D. WMN
Answer: B (LEAVE A REPLY)
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: 286
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: 287
The screen on a user's mobile device is not autorotating even after the feature has been enabled and the device has been restarted. Which of the following should the technician do next to troubleshoot the issue?
A. Calibrate the phone sensors.

B. Enable the touch screen.
C. Reinstall the operating system.
D. Replace the screen.
Answer: (SHOW ANSWER)
Calibrating the phone sensors is a step that can troubleshoot the issue of screen not autorotating on a mobile device. Screen autorotation is a feature that automatically adjusts the screen orientation based on the device's position and movement. Screen autorotation relies on sensors such as accelerometer and gyroscope to detect the device's tilt and rotation. Calibrating the phone sensors can help fix any errors or inaccuracies in the sensor readings that may prevent screen autorotation from working properly. Enabling the touch screen, reinstalling the operating system, and replacing the screen are not steps that should be done next to troubleshoot this issue.

NEW QUESTION: 288
A company would like to deploy baseline images to new computers as they are started up on the network. Which of the following boot processes should the company use for this task?
A. ISO
B. Secure
C. USB
D. PXE
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed In-Depth
PXE (Preboot Execution Environment) allows a computer to boot from a network server and install a system image remotely. It is commonly used for large-scale deployments because it eliminates the need for physical installation media.
A . ISO - Incorrect. ISO files are used for manual installations, but they do not automate network deployments.
B . Secure - Incorrect. There is no "secure boot process" option for automated deployments. Secure Boot is a security feature.
C . USB - Incorrect. USB boot requires manual installation on each device, making it inefficient for mass deployment.

NEW QUESTION: 289
A technician receives an invalid certificate error when visiting a website. Other workstations on the same local network are unable to replicate this issue. Which of the following is most likely causing the issue?
A. Date and time
B. User access control
C. UEFI boot mode
D. Log-on times
Answer: A (LEAVE A REPLY)
Date and time is the most likely cause of the issue. The date and time settings on a workstation affect the validity of the certificates used by websites to establish secure connections. If the date and time are incorrect, the workstation may not recognize the certificate as valid and display an invalid certificate error. Other workstations on the same local network may not have this issue if their date and time are correct. User access control, UEFI boot mode, and log-on times are not likely causes of the issue. User access control is a feature that prevents unauthorized changes to the system by prompting for confirmation or credentials. UEFI boot mode is a firmware interface that controls the boot process of the workstation. Log-

on times are settings that restrict when a user can log in to the workstation. None of these factors affect the validity of the certificates used by websites. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 14 CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 456

NEW QUESTION: 290
An office is experiencing constant connection attempts to the corporate Wi-Fi. Which of the following should be disabled to mitigate connection attempts?
SSID
A. DHCP
B. Firewall
C. SSD
Answer: (SHOW ANSWER)
The SSID (Service Set Identifier) is the name of a wireless network that is broadcasted by the router or the Wi-Fi base station. The SSID helps nearby devices to identify and connect to the available networks. However, broadcasting the SSID also exposes the network to potential connection attempts from unauthorized or malicious users. Therefore, disabling the SSID can mitigate connection attempts by making the network invisible or hidden to the devices that are not already connected to it. To connect to a hidden network, the user would need to know the exact SSID and enter it manually.
The other options are not related to mitigating connection attempts to the corporate Wi-Fi. DHCP (Dynamic Host Configuration Protocol) is a protocol that assigns IP addresses to the devices on a network. Firewall is a software or hardware device that filters the incoming and outgoing network traffic based on predefined rules. SSD (Solid State Drive) is a type of storage device that uses flash memory to store data. Disabling any of these options would not prevent connection attempts to the Wi-Fi network, and may cause other problems or issues for the network functionality and performance.
Reference:
What is SSID + how to find (and change) it1
Choosing an SSID2
SSID Meaning: Finding Your Network's Name3

NEW QUESTION: 291
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 (LEAVE A REPLY)
Erasing/wiping the hard drives is the best method to dispose of the drives containing PII

NEW QUESTION: 292

A user clicked a link in an email, and now the cursor is moving around on its own. A technician notices that File Explorer is open and data is being copied from the local drive to an unknown cloud storage location. Which of the following should the technician do first?

A. Investigate the reported symptoms.

B. Run anti-malware software.

C. Educate the user about dangerous links.

D. Quarantine the workstation.

Answer: D (LEAVE A REPLY)

When a user's cursor is moving on its own and unauthorized data transfer is occurring, the first step a technician should take is to Quarantine the workstation. This involves isolating the affected system from the network to prevent the spread of malware or unauthorized access to other parts of the network. Quarantining helps in containing the threat and provides a safe environment to investigate and remediate the issue without risking further contamination or data loss.

NEW QUESTION: 293

A computer is restarting automatically and displaying the following error message: "Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you. (0% complete)." Which of the following should the technician do first to diagnose the issue?

A. Check the system event logs.

B. Verify the hardware driver versions.

C. Install Windows updates.

D. Perform a RAM diagnostic.

Answer: A (LEAVE A REPLY)

The first step is to check the system event logs using tools like Event Viewer. This will allow the technician to identify any critical errors or warnings that occurred before the restart. Based on these logs, further troubleshooting can be done. Verifying driver versions and performing diagnostics can follow once the root cause is identified.

NEW QUESTION: 294

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)

Risk analysis is the process of identifying and evaluating the potential threats and impacts of a change on the system, network, or service. It is an essential step before approving a change request, as it helps to determine the level of risk, the mitigation strategies, and the contingency plans. Risk analysis also helps to prioritize the change requests based on their urgency and importance12.

NEW QUESTION: 295

A company is experiencing a DDoS attack. Several internal workstations are the source of the traffic. Which of the following types of infections are the workstations most likely experiencing? (Select two).
A. Zombies
B. Keylogger
C. Adware
D. Botnet
E. Ransomware
F. Spyware
Answer: A,D (LEAVE A REPLY)
Zombies and botnets are terms that describe the types of infections that can cause internal workstations to participate in a DDoS (distributed denial-of-service) attack. A DDoS attack is a malicious attempt to disrupt the normal functioning of a website or a network by overwhelming it with a large amount of traffic from multiple sources. Zombies are infected computers that are remotely controlled by hackers without the owners' knowledge or consent. Botnets are networks of zombies that are coordinated by hackers to launch DDoS attacks or other malicious activities. Keylogger, adware, ransomware, and spyware are not types of infections that can cause internal workstations to participate in a DDoS attack.

NEW QUESTION: 296
A vendor provided installation software on a DVD-ROM. The software is not available to download on the vendor's website. The technician needs to install the software on several laptops that do not have an optical disc drive. The laptops are connected to the corporate network but are physically located at remote sites. Which of the following is the best installation method for the technician to use?
A. Use a computer that has an optical disc drive to create an ISO file from the DVD-ROM, store the ISO file on the file server, connect remotely to each laptop, and install the software on each laptop using the ISO stored on the file server.
B. Locate an external USB DVD-ROM optical disc drive, insert the DVD-ROM from the vendor into the drive, and install the software from the USB DVD-ROM optical disc drive.
C. Use a computer that has an optical disc drive to create an ISO file from the DVD-ROM, copy the ISO file to a USB flash drive, and install the software from the USB flash drive.
D. Locate an ISO file of the software from a website unrelated to the vendor, store the ISO file on the file server, connect remotely to each laptop, and install the software on each laptop using the ISO stored on the file server.
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth
The best method is to create an ISO file from the DVD and store it on a file server, allowing remote installations across multiple devices.
B . Use an external USB DVD-ROM - Not practical for remote installations.
C . Copy ISO to a USB flash drive - Requires physically transferring the USB to each laptop.
D . Download an ISO from an unrelated website - Unsafe and violates security best practices.

NEW QUESTION: 297
A user is unable to log in to a workstation. The user reports an error message about the date being incorrect. A technician reviews the date and verifies it is correct, but the system clock is an hour behind. The technician also determines this workstation is the only one affected. Which of the following is the most likely issue?

A. Time drift
B. NTP failure
C. Windows Update
D. CMOS battery
Answer: A (LEAVE A REPLY)
Time drift occurs when the internal clock of a computer is not properly synchronized, often leading to discrepancies like being an hour behind. In this case, the workstation is the only device affected, indicating that it's likely a local issue. Time drift can happen if the system clock isn't syncing properly with an NTP (Network Time Protocol) server or if automatic daylight savings adjustments aren't enabled. It's less likely to be a CMOS battery issue since the technician has already verified the correct date and the system clock isn't completely reset (which is what happens when the CMOS battery fails).
Reference:
Troubleshooting Time Synchronization Issues in Windows (Help Desk Geek) (Zendesk)

NEW QUESTION: 298
An administrator has received approval for a change request for an upcoming server deployment. Which of the following steps should be completed NEXT?
A. Perform a risk analysis.
B. Implement the deployment.
C. Verify end user acceptance
D. Document the lessons learned.
Answer: A (LEAVE A REPLY)
Before making any changes to the system, it is important to assess the risks associated with the change and determine whether it is worth implementing. Risk analysis involves identifying potential risks, assessing their likelihood and impact, and determining what steps can be taken to mitigate them. It is important to perform this step before making any changes, as this allows the administrator to make an informed decision about whether or not the change should be implemented. Once the risks have been assessed and the administrator has decided to go ahead with the change, the next step is to implement the deployment.

NEW QUESTION: 299
While trying to repair a Windows 10 OS, a technician receives a prompt asking for a key. The technician tries the administrator password, but it is rejected. Which of the following does the technician need in order to continue the OS repair?
A. SSL key
B. Preshared key
C. WPA2 key
D. Recovery key
Answer: D (LEAVE A REPLY)
A recovery key is a code that can be used to unlock a BitLocker-encrypted drive when the normal authentication methods (such as password or PIN) are not available or have been forgotten. BitLocker is a feature of Windows that encrypts the entire drive to protect data from unauthorized access. If a technician is trying to repair a Windows 10 OS that has BitLocker

enabled, they will need the recovery key to access the drive and continue the OS repair. SSL key, preshared key, and WPA2 key are not keys that are related to BitLocker or OS repair.

NEW QUESTION: 300
A user reports seeing random, seemingly non-malicious advertisement notifications in the Windows 10 Action Center. The notifications indicate the advertisements are coming from a web browser. Which of the following is the best solution for a technician to implement?
A. Disable the browser from sending notifications to the Action Center.
B. Run a full antivirus scan on the computer.
C. Disable all Action Center notifications.
D. Move specific site notifications from Allowed to Block.
Answer: D (LEAVE A REPLY)
The best solution for a technician to implement is to disable the browser from sending notifications to the Action Center. This will prevent the random advertisement notifications from appearing in the Windows 10 Action Center, which can be annoying and distracting for the user. The technician can follow these steps to disable the browser notifications1:
Open the browser that is sending the notifications, such as Microsoft Edge, Google Chrome, or Mozilla Firefox.
Go to the browser settings or options menu, and look for the privacy and security section.
Find the option to manage site permissions or notifications, and click on it.
You will see a list of sites that are allowed or blocked from sending notifications to the browser and the Action Center. You can either block all sites from sending notifications, or select specific sites that you want to block or allow.
Save the changes and close the browser settings.
This solution is better than the other options because:
Running a full antivirus scan on the computer (B) is not necessary, as the advertisement notifications are not malicious or harmful, and they are not caused by a virus or malware infection. Running a scan will not stop the notifications from appearing, and it will consume system resources and time.
Disabling all Action Center notifications is not advisable, as the Action Center is a useful feature that shows notifications and alerts from various apps and system events, such as email, calendar, security, updates, etc. Disabling all notifications will make the user miss important information and reminders, and reduce the functionality of the Action Center.
Moving specific site notifications from Allowed to Block (D) is not the best solution, as it will only stop the notifications from some sites, but not from others. The user may still receive advertisement notifications from other sites that are not blocked, or from new sites that are added to the Allowed list. This solution will also require the user to manually manage the list of sites, which can be tedious and time-consuming.
Reference:
1: How to Disable Annoying Browser Notifications - PCMag

NEW QUESTION: 301
A technician is troubleshooting a user's PC that is displaying pop-up windows advertising free software downloads. When the technician tries to open a document, the system displays an error message: "Not enough memory to perform this operation." Which of the following should be the technician's next step to resolve this issue?
A. Upgrade the browser
B. Install antivirus software

C. Install antispyware
D. Disable the pop-up blocker
E. Relmage the system
Answer: C (LEAVE A REPLY)

NEW QUESTION: 302
A technician is partitioning a hard disk. The five primary partitions should contain 4TB of free space. Which of the following partition styles should the technician use to partition the device?
A. EFS
B. GPT
C. MBR
D. FAT32
Answer: B (LEAVE A REPLY)
GPT is the correct answer for this question. GPT stands for GUID Partition Table, and it is a partition style that supports up to 128 primary partitions and up to 18 exabytes of disk size per partition. GPT also uses a unique identifier for each partition and provides better data protection and recovery. GPT is suitable for partitioning a hard disk that has five primary partitions with 4TB of free space each. EFS, MBR, and FAT32 are not correct answers for this question. EFS stands for Encrypting File System, and it is a feature that allows encrypting files and folders on NTFS volumes. EFS is not a partition style, but rather a file system attribute. MBR stands for Master Boot Record, and it is an older partition style that supports up to four primary partitions and up to 2TB of disk size per partition. MBR cannot handle five primary partitions with 4TB of free space each. FAT32 stands for File Allocation Table 32, and it is a file system that supports up to 32GB of disk size per partition and up to 4GB of file size. FAT32 is not a partition style, but rather a file system type. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 14 CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 105

NEW QUESTION: 303
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: 304
A user needs assistance changing the desktop wallpaper on a Windows 10 computer. Which of the following methods will enable the user to change the wallpaper using a Windows 10 Settings tool?
A. Open Settings, select Accounts, select Your info, click Browse, and then locate and open the image the user wants to use as the wallpaper.
B. Open Settings, select Personalization, click Browse, and then locate and open the image the user wants to use as the wallpaper.
C. Open Settings, select System, select Display, click Browse, and then locate and open the image the user wants to use as the wallpaper.
D. Open Settings, select Apps, select Apps & features, click Browse, and then locate and open the image the user wants to use as the wallpaper.
Answer: B (LEAVE A REPLY)
The user can change the wallpaper using a Windows 10 Settings tool by following these steps12:
Open Settings by pressing the Windows key and typing Settings, or by clicking the gear icon in the Start menu.
Select Personalization from the left navigation menu.
On the right side of the window, click Background.
In the Background settings, click the drop-down menu and select Picture as the background type.
Click Browse and then locate and open the image the user wants to use as the wallpaper.
The other options are incorrect because they do not lead to the Background settings or they do not allow the user to browse for an image. Accounts, System, and Apps are not related to personalization settings. Your info, Display, and Apps & features are not related to wallpaper settings.

NEW QUESTION: 305
A neighbor successfully connected to a user's Wi-Fi network. Which of the following should the user do after changing the network configuration to prevent the neighbor from being able to connect again?
A. Disable the SSID broadcast.
B. Disable encryption settings.

C. Disable DHCP reservations.
D. Disable logging.
Answer: A (LEAVE A REPLY)
a) Disable the SSID broadcast1: The SSID broadcast is a feature that allows a Wi-Fi network to be visible to nearby devices. Disabling the SSID broadcast can make the network harder to find by unauthorized users, but it does not prevent them from accessing it if they know the network name and password.

NEW QUESTION: 306
An administrator's change was approved by the change management review board. Which of the following should the administrator do next?
A. Perform risk analysis.
B. Assign a change coordinator.
C. Implement the change.
D. Verify testing results.
Answer: C (LEAVE A REPLY)
Once a change has been approved by the change management review board, the next step is to:
* Implement the change:This involves carrying out the approved change in the system or environment according to the change plan.
* Perform risk analysis:This should be done before the change is approved to assess potential impacts.
* Assign a change coordinator:This role should be designated earlier in the process to oversee the change implementation.
* Verify testing results:This should have been done before seeking approval from the review board.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 4.2: Explain basic change-management best practices.
Change management process documentation.

NEW QUESTION: 307
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 (LEAVE A REPLY)
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: 308
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: (SHOW ANSWER)
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: 309
Which of the following filesystem formats would be the BEST choice to ensure read and write compatibility of USB flash drives across several generations of Microsoft operating systems?
A. APFS
B. ext4
C. CDFS
D. FAT32
Answer: (SHOW ANSWER)
The best filesystem format to ensure read and write compatibility of USB flash drives across several generations of Microsoft operating systems is FAT32. FAT32 stands for File Allocation Table 32-bit and is a filesystem format that organizes and manages files and folders on storage devices using 32-bit clusters. FAT32 is compatible with most Microsoft operating systems since Windows 95 OSR2, as well as other operating systems such as Linux and Mac OS X. FAT32 can support storage devices up to 2TB in size and files up to 4GB in size. APFS stands for Apple File System and is a filesystem format that organizes and manages files and folders on storage devices using encryption, snapshots and cloning features. APFS is compatible with Mac OS X 10.13 High Sierra and later versions but not with Microsoft operating systems natively. Ext4 stands for Fourth Extended File System and is a filesystem format that organizes and manages files and folders on storage devices using journaling, extents and delayed allocation features. Ext4 is compatible with Linux operating systems but not with Microsoft operating systems natively.

NEW QUESTION: 310
A user's computer is running slower than usual and takes a long time to start up. Which of the following tools should the technician use first to investigate the issue?
A. Action Center
B. Task Manager
C. Resource Monitor
D. Security Configuration Wizard
E. Event Viewer
Answer: (SHOW ANSWER)
When a computer is running slower than usual and experiences long startup times, the first tool to use is:
* Task Manager: This utility provides real-time data on the processes and applications consuming system resources like CPU, memory, and disk usage. By identifying resource-heavy processes, a technician can take steps to optimize performance or identify malicious software.

NEW QUESTION: 311
A systems administrator at a small company wants to discretely access user machines and verify patch levels without users noticing. Which of the following remote access technologies should the administrator use?
A. RDP
B. MSRA
C. SSH
D. VNC
Answer: C (LEAVE A REPLY)
Detailed Explanation with Core 2 Reference:SSH allows for remote access to systems securely and discretely, suitable for verifying patch levels and other administrative tasks. This meets Core 2 objectives on using secure remote access tools (Core 2 Objective 4.9).

NEW QUESTION: 312
Which of the following file extensions should a technician use for a PowerShell script?
A. .ps1
B. .py
C. .sh
D. .bat
E. .cmd
Answer: A (LEAVE A REPLY)
A PowerShell script is a plain text file that contains one or more PowerShell commands. Scripts have a .ps1 file extension and can be run on your computer or in a remote session. PowerShell scripts can be used to automate tasks and change settings on Windows devices. To create and run a PowerShell script, you need a text editor (such as Visual Studio Code or Notepad) and the PowerShell Integrated Scripting Environment (ISE) console. You also need to enable the correct execution policy to allow scripts to run on your system

NEW QUESTION: 313
A systems administrator is configuring centralized desktop management for computers on a domain. The management team has decided that all users' workstations should have the same network drives, printers, and configurations. Which of the following should the administrator use to accomplish this task?
A. Network and Sharing Center
B. net use
C. User Accounts
D. regedit
E. Group Policy
Answer: E (LEAVE A REPLY)
Group Policy is a feature of Windows that allows administrators to centrally manage and apply policies and settings to computers and users on a domain3. Group Policy can be used to configure network drives, printers, security settings, desktop preferences, and other configurations for all users' workstations3. Network and Sharing Center, net use, User Accounts, and regedit are not tools that can accomplish this task.

NEW QUESTION: 314
A technician received a call from a user who clicked on a web advertisement Now. every time the user moves the mouse, a pop-up display across the monitor. Which of the following procedures should the technician perform?
A. Boot into safe mode.
B. Perform a malware scan.
C. Restart the machine.
D. Reinstall the browser
Answer: A,B (LEAVE A REPLY)
Booting into safe mode and performing a malware scan are the steps that a technician should perform when troubleshooting an issue with pop-up advertising messages on a PC. Safe mode is a diagnostic mode that starts the PC with minimal drivers and services, which can prevent the pop-up malware from running. Malware scan is a tool that can detect and remove the pop-up malware, as well as prevent further infection or damage. Investigating how the malware was installed, reinstalling the browser and restarting the machine are possible steps that can be done after booting into safe mode and performing a malware scan, depending on the situation and the results of the scan. Verified Reference: https://www.comptia.org/blog/how-to-boot-into-safe-mode https://www.comptia.org/certifications/a

NEW QUESTION: 315
A user reported that a laptop's screen turns off very quickly after silting for a few moments and is also very dim when not plugged in to an outlet Everything else seems to be functioning normally. Which of the following Windows settings should be configured?
A. Power Plans
B. Hibernate
C. Sleep/Suspend
D. Screensaver
Answer: A (LEAVE A REPLY)
Power Plans are Windows settings that allow a user to configure how a laptop's screen behaves when plugged in or running on battery power. They can adjust the screen brightness and the time before the screen turns off due to inactivity. Hibernate, Sleep/Suspend and Screensaver are other Windows settings that affect how a laptop's screen behaves, but they do not allow changing the screen brightness or turning off time. Verified Reference: https://www.comptia.org/blog/windows-power-plans https://www.comptia.org/certifications/a

NEW QUESTION: 316
A user visits a game vendor's website to view the latest patch notes, but this information is not available on the page. Which of the following should the user perform before reloading the page?
A. Synchronize the browser data.
B. Enable private browsing mode.
C. Mark the site as trusted.
D. Clear the cached file.
Answer: D (LEAVE A REPLY)
Clearing the cached file is an action that can help resolve the issue of not seeing the latest patch notes on a game vendor's website. A cached file is a copy of a web page or file that is stored locally on the user's browser or device for

faster loading and offline access. However, sometimes a cached file may become outdated or corrupted and prevent the user from seeing the most recent or accurate version of a web page or file. Clearing the cached file can force the browser to download and display the latest version from the server instead of using the old copy from the cache. Synchronizing the browser data, enabling private browsing mode, and marking the site as trusted are not actions that can help resolve this issue.

NEW QUESTION: 317
A systems administrator notices that a server on the company network has extremely high CPU utilization. Upon further inspection, the administrator sees that the server Is consistently communicating with an IP address that is traced back to a company that awards digital currency for solving hash algorithms. Which of the following was MOST likely used to compromise the server?
A. Keylogger
B. Ransomware
C. Boot sector virus
D. Cryptomining malware
Answer: D (LEAVE A REPLY)
Cryptomining malware is a type of malicious program that uses the CPU resources of a compromised server to generate cryptocurrency, such as Bitcoin or Ethereum. It can cause extremely high CPU utilization and network traffic to the IP address of the cryptocurrency service. Keylogger, ransomware and boot sector virus are other types of malware, but they do not cause the same symptoms as cryptomining malware. Verified Reference: https://www.comptia.org/blog/what-is-cryptomining https://www.comptia.org/certifications/a

NEW QUESTION: 318
A user has been unable to receive emails or browse the internet from a smartphone while traveling. However, text messages and phone calls are working without issue. Which of the following should a support technician check FIRST?
A. User account status
B. Mobile OS version
C. Data plan coverage
D. Network traffic outages
Answer: C (LEAVE A REPLY)
The first thing that a support technician should check to resolve the issue of not being able to receive emails or browse the internet from a smartphone while traveling is the data plan coverage. The data plan coverage determines how much data and where the user can use on the smartphone's cellular network. The data plan coverage may vary depending on the

user's location, carrier and subscription. The data plan coverage may not include or support certain areas or countries that the user is traveling to, or may charge extra fees or limit the speed or amount of data that the user can use. The data plan coverage does not affect text messages and phone calls, which use different network services and protocols. User account status is not likely to cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, unless the user account has been suspended or terminated by the carrier or the email provider. Mobile OS version is not likely to cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, unless the mobile OS has a major bug or compatibility problem with the network or the email app. Network traffic outages may cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, but they are less likely and less common than data plan coverage issues, and they should also affect text messages and phone calls. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.5

NEW QUESTION: 319
Due to special job responsibilities, an end user needs the ability to edit the properties of Windows system files. The user has already been granted local administrator privileges. Which of the following Control Panel utilities should be used to provide easy access to the files?
A. File Explorer Options
B. Ease of Access
C. Indexing Options
D. Administrative Tools
Answer: (SHOW ANSWER)
The correct answer is Administrative Tools (Option D), which provides access to several system utilities, including those needed for managing system files and settings. Since the user already has local administrator privileges, this would allow them to edit system properties efficiently.
File Explorer Options (Option A) manage general file display settings but do not provide administrative access.
Ease of Access (Option B) is related to accessibility settings, not file management.
Indexing Options (Option C) control how files are indexed for search, but are unrelated to system file editing.
CompTIA A+ Core 2 Reference:
1.3 - Use features and tools of the Windows operating system, including Administrative Tools.

NEW QUESTION: 320
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: 321
While accessing a website, a user clicks on a menu option and nothing happens. Which of the following actions should the user take to most likely resolve this issue?
A. Clear the cache.
B. Disable pop-up blocker.
C. Enable private-browsing mode.
D. Enable TLS 1.0 in the browser.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 322
A user is unable to open personal files on a PC on a home network. An on-screen message indicates the files are encrypted and demands payment to access the files. Which of the following should a technician recommend the user do first?
A. Reinstall the OS.
B. Run the System Restore feature.
C. Disconnect the PC from the network.
D. Pay the amount demanded.
E. Scan the PC with an anti-malware program.
Answer: (SHOW ANSWER)
Detailed Explanation with Core 2 Reference:The PC is likely infected with ransomware. The immediate step should be to disconnect from the network to prevent the malware from spreading to other devices. Core 2 highlights steps to respond to malware incidents, such as disconnecting from the network as part of containment measures (Core 2 Objective 2.3).

NEW QUESTION: 323
A network technician is deploying a new machine in a small branch office that does not have a DHCP server. The new machine automatically receives the IP address of 169.254.0.2 and is unable to communicate with the rest of the network. Which of the following would restore communication?
Static entry
A. ARP table
B. APIPA address
C. NTP specification
Answer: A (LEAVE A REPLY)
A static entry is the best option to restore communication for the new machine in a small branch office that does not have a DHCP server. A static entry means manually configuring the IP address, subnet mask, default gateway, and DNS server for the network adapter of the machine. A static entry ensures that the machine has a valid and unique IP address that matches the network configuration and can communicate with the rest of the network.
The new machine automatically receives the IP address of 169.254.0.2 because it uses APIPA (Automatic Private IP Addressing), which is a feature that enables computers to self-assign an IP address when a DHCP server is not available. However, APIPA only works for local communication within the same subnet, and does not provide a default gateway or a

DNS server. Therefore, the new machine is unable to communicate with the rest of the network, which may be on a different subnet or require a gateway or a DNS server to access.
The other options are not related to restoring communication for the new machine. ARP table is a cache that stores the mapping between IP addresses and MAC addresses for the devices on the network. NTP specification is a protocol that synchronizes the clocks of the devices on the network.
Reference:
CompTIA A+ Certification Exam Core 2 Objectives1
CompTIA A+ Core 2 (220-1102) Certification Study Guide2
What is APIPA (Automatic Private IP Addressing)? - Study-CCNA3
How to Configure a Static IP Address in Windows and OS X4

NEW QUESTION: 324
A technician has spent hours trying to resolve a computer issue for the company's Chief Executive Officer (CEO). The CEO needs the device returned as soon as possible. Which of the following steps should the technician take NEXT?
A. Continue researching the issue
B. Repeat the iterative processes
C. Inform the CEO the repair will take a couple of weeks
D. Escalate the ticket
Answer: D (LEAVE A REPLY)
The technician should escalate the ticket to ensure that the CEO's device is returned as soon as possible1

NEW QUESTION: 325
A technician is investigating options to secure a small office's wireless network. One requirement is to allow automatic log-ins to the network using certificates instead of passwords. Which of the following should the wireless solution have in order to support this feature?
A. RADIUS
B. AES
C. EAP-EKE
D. MFA
Answer: (SHOW ANSWER)
RADIUS is the correct answer for this question. RADIUS stands for Remote Authentication Dial-In User Service, and it is a protocol that provides centralized authentication, authorization, and accounting for wireless networks. RADIUS can support certificate-based authentication, which allows users to log in to the network automatically without entering passwords. RADIUS also provides other benefits, such as enforcing security policies, logging user activities, and managing network access. AES, EAP-EKE, and MFA are not wireless solutions, but rather encryption algorithms, authentication methods, and security factors, respectively. Reference:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 23 CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 459

NEW QUESTION: 326

A malicious file was executed automatically when a flash drive was plugged in. Which of the following features would prevent this type of incident?

A. Disabling UAC

B. Restricting local administrators

C. Enabling UPnP

D. Turning off AutoPlay

Answer: D (LEAVE A REPLY)

AutoPlay is a feature that automatically runs programs or files when a removable media device, such as a flash drive, is plugged in. This can be exploited by malware authors who place malicious files on flash drives that execute automatically when inserted into a computer. Turning off AutoPlay can prevent this type of incident by requiring the user to manually open or run files from removable media devices. Disabling UAC (user account control), restricting local administrators and enabling UPnP (universal plug and play) are not effective ways to prevent this type of incident. Verified Reference: https://www.comptia.org/blog/autoplay-security-risk https://www.comptia.org/certifications/a

NEW QUESTION: 327

A technician is troubleshooting a smartphone that is unable to download and install the latest OS update. The technician notices the device operates more slowly than expected, even after rebooting and closing all applications. Which of the following should the technician check next?

A. Application permissions

B. Available storage space

C. Battery charge level

D. Wi-Fi connection speed

Answer: (SHOW ANSWER)

When a smartphone is unable to download and install the latest OS update and is operating slower than expected, one of the first things to check is the available storage space. Operating system updates often require a significant amount of free space for downloading and installing, and insufficient space can prevent the update process from initiating or completing.

* Available Storage Space: Smartphones use their internal storage to hold the OS, apps, user data, and temporary files needed for updates. If the storage is nearly full, the device can slow down due to the lack of space for writing temporary files and may not have enough space to download and install updates. Clearing up space can resolve these issues.

Checking application permissions (A) might be relevant for specific app-related issues but is less likely to affect OS updates. The battery charge level (C) can affect the initiation of an update, as some devices require a minimum charge level to start the update process, but it doesn't typically cause slow operation. While a stable Wi-Fi connection (D) is necessary for downloading updates, it's less likely to be the cause of slowed operation and update issues compared to insufficient storage space.

NEW QUESTION: 328

An implementation specialist is replacing a legacy system at a vendor site that has only one wireless network available. When the specialist connects to Wi-Fi. the specialist realizes the insecure network has open authentication. The technician needs to secure the vendor's sensitive dat a. Which of the following should the specialist do FIRST to protect the company's data?

A. Manually configure an IP address, a subnet mask, and a default gateway.

B. Connect to the vendor's network using a VPN.
C. Change the network location to private.
D. Configure MFA on the network.
Answer: B (LEAVE A REPLY)
The first thing that the specialist should do to protect the company's data on an insecure network with open authentication is to connect to the vendor's network using a VPN. A VPN stands for Virtual Private Network and is a technology that creates a secure and encrypted connection over a public or untrusted network. A VPN can protect the company's data by preventing eavesdropping, interception or modification of the network traffic by unauthorized parties. A VPN can also provide access to the company's internal network and resources remotely. Manually configuring an IP address, a subnet mask and a default gateway may not be necessary or possible if the vendor's network uses DHCP to assign network configuration parameters automatically. Manually configuring an IP address, a subnet mask and a default gateway does not protect the company's data from network attacks or threats. Changing the network location to private may not be advisable or effective if the vendor's network is a public or untrusted network. Changing the network location to private does not protect the company's data from network attacks or threats. Configuring MFA on the network may not be feasible or sufficient if the vendor's network has open authentication and does not support or require MFA. Configuring MFA on the network does not protect the company's data from network attacks or threats. Reference: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

NEW QUESTION: 329
After a failed attempt to open an email attachment for an unexpected overdue invoice, a smartphone user experiences abnormal performance when using their mobile browser and other applications. The user restarts the device, but the issue persists. Which of the following actions should the user take next?
A. Shut down and cold start the smartphone
B. Delete the email containing the attachment
C. Wipe the device and reset it to factory defaults
D. Uninstall and reinstall the mobile browser
Answer: (SHOW ANSWER)
In this case, abnormal behavior after opening a suspicious email suggests malware might have infected the device. A full factory reset is recommended to remove any persistent malware, especially when a restart does not resolve the issue. Deleting the email or reinstalling the browser will not remove the malware already on the device.

NEW QUESTION: 330
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 (LEAVE A REPLY)
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: 331
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: 332
A network administrator is showing an email application on a personal cell phone to a coworker. The cell phone is enrolled in the company's MDM program. When launching the application store to download the email application, the coworker receives a security warning stating the device violates company policies due to root-level access. Which of the following should the coworker perform next to resolve the issue?
A. Download and install a similar application.
B. Reimage the device with the OS from the OEM.
C. Return the cell phone to the manufacturer.
D. Install the latest mobile OS updates.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 333
A business lost all data and equipment after a disaster. Due to the disaster, the business no longer maintains system backups. Which of the following should the business implement to prevent future losses?
A. Test environment
B. Local backups
C. Cold site
D. Cloud storage

Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth
Cloud storage ensures that data is backed up off-site, protecting against physical disasters like fires or floods.
A . Test environment - Incorrect. This is for software testing, not data recovery.
B . Local backups - Incorrect. These could also be destroyed in a disaster.
C . Cold site - Useful for disaster recovery but does not automatically back up data.
Reference:
CompTIA A+ 220-1102, Objective 4.1 - Backup and Recovery Best Practices

NEW QUESTION: 334
A technician wants to install Developer Mode on a Windows laptop but is receiving a "failed to install package" message. Which of the following should the technician do first?
A. Ensure internet connectivity.
B. Check for Windows updates.
C. Enable SSH.
D. Reboot computer.
Answer: (SHOW ANSWER)
Developer Mode on Windows 10 is a feature that allows developers to test and debug their applications on their devices, as well as sideload apps and access other developer tools12. To enable Developer Mode, the user needs to go to the Settings app, select Update & Security, choose For Developers, and switch to Developer Mode123. However, enabling Developer Mode requires internet connectivity, as Windows will download and install a package of features, such as Windows Device Portal and SSH services, that are necessary for Developer Mode124. If the user does not have internet connectivity, they will receive a "failed to install package" message when trying to enable Developer Mode4. Therefore, the first thing that the technician should do is to ensure that the laptop has internet access, either through Wi-Fi or Ethernet, and then try to enable Developer Mode again4

NEW QUESTION: 335
A technician is implementing the latest application security updates for endpoints on an enterprise network. Which of the following solutions should the technician use to ensure device security on the network while adhering to industry best practices?
A. Automate the patching process.
B. Monitor the firewall configuration.
C. Implement access control lists.
D. Document all changes.
Answer: A (LEAVE A REPLY)
To ensure device security on the network while adhering to industry best practices, the technician should:
Automate the patching process: This ensures that all devices receive the latest security updates in a timely manner without manual intervention, reducing the risk of vulnerabilities.
Monitor the firewall configuration: Important for network security but does not directly ensure all devices are patched.
Implement access control lists: Controls access to resources but does not ensure devices are patched.
Document all changes: Important for change management but does not directly impact the patching process.

Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 2.6: Given a scenario configure a workstation to meet best practices for security.
Best practices for application security updates and patch management.

NEW QUESTION: 336
A user connected a smartphone to a coffee shop's public Wi-Fi and noticed the smartphone started sending unusual SMS messages and registering strange network activity A technician thinks a virus or other malware has infected the device. Which of the following should the technician suggest the user do to best address these security and privacy concerns? (Select two).
A. Disable Wi-Fi autoconnect.
B. Stay offline when in public places.
C. Uninstall all recently installed applications.
D. Schedule an antivirus scan.
E. Reboot the device
F. Update the OS
Answer: C,D (LEAVE A REPLY)
The best way to address the security and privacy concerns caused by a malware infection on a smartphone is to uninstall all recently installed applications and schedule an antivirus scan. Uninstalling the applications that may have introduced the malware can help remove the source of infection and prevent further damage. Scheduling an antivirus scan can help detect and remove any remaining traces of malware and restore the device's functionality.

NEW QUESTION: 337
A company is recycling old hard drives and wants to quickly reprovision the drives for reuse. Which of the following data destruction methods should the company use?
A. Degaussing
B. Standard formatting
C. Low-level wiping
D. Deleting
Answer: C (LEAVE A REPLY)
Low-level wiping is the best data destruction method for recycling old hard drives for reuse. Low-level wiping is a process that overwrites every bit of data on a hard drive with zeros or random patterns, making it impossible to recover any data from the drive. Low-level wiping also restores the drive to its factory state, removing any bad sectors or errors that may have accumulated over time. Low-level wiping can be done using specialized software tools or hardware devices that connect to the drive. Degaussing, standard formatting, and deleting are not suitable data destruction methods for recycling old hard drives for reuse. Degaussing is a process that exposes a hard drive to a strong magnetic field, destroying both the data and the drive itself. Degaussing renders the drive unusable for reuse. Standard formatting is a process that erases the data on a hard drive by removing the file system structure, but it does not overwrite the data itself. Standard formatting leaves some data recoverable using forensic tools or software utilities. Deleting is a process that removes the data from a hard drive by marking it as free space, but it does not erase or overwrite the data itself. Deleting leaves most data recoverable using undelete tools or software utilities. Reference:

Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15 CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 105

NEW QUESTION: 338
Users report having difficulty using the Windows Hello facial recognition feature. Which of the following is a secondary feature of Windows Hello that can be used to log in?
A. Personal identification number
B. Username/password
C. One-time-use token
D. Cryptographic device
Answer: A (LEAVE A REPLY)
Windows Hello is a biometric-based technology that enables Windows 10 users to authenticate secure access to their devices, apps, online services, and networks with just a look or a touch. If users have difficulty using the facial recognition feature, Windows Hello also supports a Personal Identification Number (PIN) as a secondary feature for logging in. The PIN is tied to the specific device on which it is set up, adding a layer of security even if the PIN is obtained by someone else.
Personal identification number:The PIN serves as an alternative to the facial recognition feature, allowing users to quickly and securely access their devices without relying solely on biometric authentication.
Username/password (B) is the traditional method of authentication but is not specifically a secondary feature of Windows Hello. One-time-use token (C) and cryptographic device (D) could be part of an MFA setup but are not directly related to Windows Hello's alternate authentication options.

NEW QUESTION: 339
A user notices a small USB drive is attached to the user's computer after a new vendor visited the office. The technician notices two files named grabber.exe and output.txt. Which of the following attacks is MOST likely occurring?
A. Trojan
B. Rootkit
C. Cryptominer
D. Keylogger
Answer: D (LEAVE A REPLY)
A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote attacker1. The attacker can use the captured information to steal passwords, credit card numbers, or other sensitive data. A keylogger can be installed on a computer by attaching a small USB drive that contains a malicious executable file, such as grabber.exe2. The output.txt file may contain the recorded keystrokes. The user should remove the USB drive and scan the computer for malware.

NEW QUESTION: 340
A technician needs to perform maintenance on a switch. Which of the following is the best method for this task?
A. Secure Shell
B. Videoconferencing software
C. Phone call

D. Virtual private network
Answer: A (LEAVE A REPLY)

NEW QUESTION: 341
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: 342
A customer reported that a home PC with Windows 10 installed in the default configuration is having issues loading applications after a reboot occurred in the middle of the night. Which of the following is the FIRST step in troubleshooting?
A. Install alternate open-source software in place of the applications with issues
B. Run both CPU and memory tests to ensure that all hardware functionality is normal
C. Check for any installed patches and roll them back one at a time until the issue is resolved
D. Reformat the hard drive, and then reinstall the newest Windows 10 release and all applications.
Answer: C (LEAVE A REPLY)
The first step in troubleshooting is to check for any installed patches and roll them back one at a time until the issue is resolved. This can help to identify any patches that may be causing the issue and allow them to be removed.

NEW QUESTION: 343
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: 344

A technician wants to mitigate unauthorized data access if a computer is lost or stolen. Which of the following features should the technician enable?

A. Network share

B. Group Policy

C. BitLocker

D. Static IP

Answer: C (LEAVE A REPLY)

BitLocker is a Windows security feature that provides encryption for entire volumes, addressing the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned devices1. BitLocker helps mitigate unauthorized data access by enhancing file and system protections, rendering data inaccessible when BitLocker-protected devices are decommissioned or recycled1. Network share, Group Policy, and Static IP are not features that can prevent unauthorized data access if a computer is lost or stolen.

Reference:

BitLocker overview - Windows Security | Microsoft Learn1

The Official CompTIA A+ Core 2 Study Guide2, page 315.

NEW QUESTION: 345

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: 346

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: 347
A technician recently installed a new router for a small business. Afterwards, the technician completed an external port scan and generated the following information:
Which of the following should the technician perform next in order to follow best practices?
A. Implement IP filtering.
B. Disable any unwanted services.
C. Migrate to UPnP.
D. Utilize NAT.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 348
Which of the following is the most practical method to reduce the number of clicks on phishing emails for a public-facing organization?
A. Providing user awareness education
B. Introducing a BYOD policy
C. Setting up SMTP filtering rules
D. Restricting emails from personal email addresses
Answer: A (LEAVE A REPLY)
User awareness education is the most effective method for reducing phishing attacks. Training users to recognize suspicious emails, links, and attachments can prevent them from falling for phishing attempts. Technical solutions like SMTP filtering (C) and restricting emails (D) can help but are not as effective without user vigilance. A BYOD policy (B) does not directly address phishing email threats.

NEW QUESTION: 349
A customer calls desktop support and begins yelling at a technician. The customer claims to have submitted a support ticket two hours ago and complains that the issue still has not been resolved. Which of the following describes how the technician should respond?
Place the customer on hold until the customer calms down.
A. Disconnect the call to avoid a confrontation.
B. Wait until the customer is done speaking and offer assistance.
C. Escalate the issue to a supervisor.
Answer: C (LEAVE A REPLY)
The best way to deal with an angry customer who is yelling at a technician is to wait until the customer is done speaking and offer assistance. This shows respect, empathy, and professionalism, and allows the technician to understand the

customer's problem and find a solution. According to the CompTIA A+ Core 2 (220-1102) Certification Study Guide1, some of the steps to handle angry customers are:
Stay calm and do not take it personally.
Listen actively and acknowledge the customer's feelings.
Apologize sincerely and offer to help.
Restate the customer's issue and ask for clarification if needed.
Explain the possible causes and solutions for the problem.
Provide clear and realistic expectations for the resolution.
Follow up with the customer until the issue is resolved.
The other options are not appropriate ways to deal with angry customers, as they may worsen the situation or damage the customer relationship. Placing the customer on hold may make them feel ignored or dismissed. Disconnecting the call may make them feel disrespected or abandoned. Escalating the issue to a supervisor may make them feel frustrated or powerless, unless the technician cannot resolve the issue or the customer requests to speak to a supervisor.
Reference:
CompTIA A+ Certification Exam Core 2 Objectives2
CompTIA A+ Core 2 (220-1102) Certification Study Guide1
How To Deal with Angry Customers (With Examples and Tips)3
17 ways to deal with angry customers: Templates and examples4
Six Ways to Handle Angry Customers5

NEW QUESTION: 350
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: 351
A Windows computer is experiencing slow performance when the user tries to open programs and files. The user recently installed a new software program from an external website.

Various websites are being redirected to an unauthorized site, and Task Manager shows the CPU usage is consistently at 100%. Which of the following should the technician do first?

A. Uninstall the new program.

B. Check the HOSTS file.

C. Restore from a previous backup.

D. Clear the web browser cache.

Answer: A (LEAVE A REPLY)

The symptoms that the user's Windows computer is experiencing suggest that the new software program that the user installed from an external website may be malicious or incompatible with the system. The program may be consuming a lot of CPU resources, slowing down the performance of other programs and files. The program may also be altering the browser settings or the HOSTS file, causing the web redirection to an unauthorized site. The first step that the technician should do is to uninstall the new program from the Control Panel or the Settings app, and then restart the computer. This may resolve the issue and restore the normal functionality of the computer. If the problem persists, the technician may need to perform additional steps, such as scanning for malware, checking the HOSTS file, clearing the web browser cache, or restoring from a previous backup

NEW QUESTION: 352

An administrator received a new shipment of mobile devices. Per company policy, all enterprise-issued devices must have two authentication methods, and the organization has already enforced the use of PIN codes as one method. Which of the following device features should the administrator enable?

A. Smart card

B. Biometrics

C. Hard token

D. One-time password

Answer: B (LEAVE A REPLY)

For securing mobile devices with two authentication methods, combining something the user knows (a PIN) with something the user is (biometrics) enhances security by implementing multi-factor authentication.

Smart card: Generally requires additional hardware and is not commonly used in mobile devices.

Biometrics: Uses unique biological traits such as fingerprints or facial recognition, providing a convenient and secure second method of authentication.

Hard token: Involves additional physical devices which might not be practical for mobile devices.

One-time password: Usually used for specific applications rather than as a general device authentication method.

NEW QUESTION: 353

A user has been adding data to the same spreadsheet for several years. After adding a significant amount of data, they are now unable to open the file. Which of the following should a technician do to resolve the issue?

A. Defragment the storage drive.

B. Increase the amount of RAM.

C. Upgrade the network connection speed.

D. Revert the spreadsheet to the last restore point.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 354
A company is deploying mobile phones on a one-to-one basis, but the IT manager is concerned that users will root/jailbreak their phones. Which of the following technologies can be implemented to prevent this issue?
A. Signed system images
B. Antivirus
C. SSO
D. MDM
Answer: D (LEAVE A REPLY)
MDM stands for Mobile Device Management, and it is a way of remotely managing and securing mobile devices that are used for work purposes1. MDM can enforce policies and restrictions on the devices, such as preventing users from installing unauthorized apps, modifying system settings, or accessing root privileges2. MDM can also monitor device status, wipe data, lock devices, or locate lost or stolen devices1.

NEW QUESTION: 355
A technician is setting up backup and recovery solutions that must restore quickly. Storage space is not a factor. Which of the following backup methods should the technician implement?
A. Differential
B. Synthetic
C. Full
D. Incremental
Answer: C (LEAVE A REPLY)
The correct answer is C. Full Backup.
A Full Backup creates a complete copy of all selected data every time it runs. This method ensures the fastest possible recovery time because all the necessary data is contained in a single backup file.
Since storage space is not a concern, full backups are ideal because they avoid the need to restore multiple incremental or differential backups.
Recovery Time Objective (RTO) is minimized, making full backups the best choice for quick restoration.
Why Other Options Are Incorrect:
A . Differential Backup - Backs up only the data that has changed since the last full backup. While faster to restore than an incremental backup, it still requires both the last full backup and the most recent differential backup for restoration.
B . Synthetic Backup - A synthetic full backup is created by combining previous full and incremental backups without needing to back up data again from the source. While efficient in terms of backup creation, restoration can be slower compared to a traditional full backup.
D . Incremental Backup - Backs up only data that has changed since the last backup (whether full or incremental). While efficient in storage, restoring from incremental backups can be slow because multiple backups must be restored in sequence.
CompTIA A+ 220-1102 Exam Reference:
Objective 4.3 - Given a scenario, apply best practices to secure a workstation.
Objective 4.4 - Given a scenario, implement methods for securing mobile devices.

NEW QUESTION: 356
A support specialist needs to decide whether to install a 32-bit or 64-bit OS architecture on a new computer. Which of the following specifications will help the specialist determine which OS architecture to use?
A. 16GB RAM
B. Intel i7 CPU
C. 500GB HDD
D. 1Gbps Ethernet
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth
The amount of RAM is the key factor in choosing a 32-bit vs. 64-bit OS:
A 32-bit OS can only address up to 4GB of RAM.
A 64-bit OS is required for 16GB RAM or more to fully utilize the memory.
B . Intel i7 CPU - Incorrect. Most modern CPUs support both 32-bit and 64-bit OS.
C . 500GB HDD - Incorrect. Hard drive size does not determine OS architecture.
D . 1Gbps Ethernet - Incorrect. Network speed has no relation to OS architecture.

NEW QUESTION: 357
Which of the following provides disk encryption on computers running a Windows OS?
A. FileVault
B. BitLocker
C. Private Key
D. PowerShell
Answer: B (LEAVE A REPLY)
BitLocker is a full-disk encryption feature included with certain editions of Windows, designed to protect data by providing encryption for entire volumes.
Option A: FileVaultFileVault is a disk encryption program in macOS, not Windows.
Option B: BitLockerBitLocker is the correct tool for disk encryption on Windows operating systems, providing full disk encryption.
Option C: Private KeyA private key is part of public key infrastructure (PKI) used in encryption, but it is not a tool for disk encryption by itself.
Option D: PowerShellPowerShell is a task automation and configuration management framework from Microsoft, not a tool for disk encryption.
Reference:
CompTIA A+ 220-1102 Objective 2.5 (Manage and configure basic security settings in the Windows OS), particularly BitLocker for disk encryption.

NEW QUESTION: 358
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: (SHOW ANSWER)
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: 359
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: 360
A user's Android phone has been randomly restarting. A technician investigates and finds several applications have been installed that are not available within the standard marketplace. Which of the following is most likely the cause of the issue?
A. The OS update failed.
B. The user downloaded malware.
C. The device is In developer mode.
D. The over-the-air carrier update failed.
Answer: B (LEAVE A REPLY)
Random restarting of an Android phone and the presence of applications not from the standard marketplace strongly suggest the possibility of malware.
Option A: The OS update failedWhile an OS update failure can cause issues, it is less likely to result in random restarts compared to malware.

Option B: The user downloaded malwareMalware is a common cause of erratic behavior, including random restarts, especially when applications are installed from unofficial sources.
Option C: The device is in developer modeDeveloper mode alone does not typically cause random restarts. It may make the device more susceptible to issues if improper apps are installed.
Option D: The over-the-air carrier update failedSimilar to the OS update, this would more likely cause consistent issues rather than random restarts.
Reference:
CompTIA A+ 220-1102 Objective 2.3 (Detect, remove, and prevent malware) and Objective 3.5 (Mobile OS and application security issues).

NEW QUESTION: 361
Which of the following is the MOST cost-effective version of Windows 10 that allows remote access through Remote Desktop?
A. Home
B. Pro for Workstations
C. Enterprise
D. Pro
Answer: B (LEAVE A REPLY)
The most cost-effective version of Windows 10 that allows remote access through Remote Desktop is Windows 10 Pro. Windows 10 Pro includes Remote Desktop, which allows users to connect to a remote computer and access its desktop, files, and applications. Windows 10Home does not include Remote Desktop, whileWindows 10 Pro for Workstations and Windows 10 Enterprise are more expensive versions of Windows10 that include additional features for businesses

NEW QUESTION: 362
Which of the following should be considered when maintaining the environment of a server room?
A. Circuit breaker capacity
B. Power distribution unit placement
C. RAID configurations
D. Virtualization
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth
A server room's environment must account for power capacity and circuit breakers to prevent electrical failures.
B . Power distribution unit placement - Important, but circuit breaker capacity is more critical.

C . RAID configurations - Related to data redundancy, not the physical environment.
D . Virtualization - Does not affect server room conditions.

NEW QUESTION: 363
A user reports that a new, personally owned tablet will not connect to the corporate Wi-Fi network. The user is able to connect to the Wi-Fi network with other devices, and the tablet is running the latest software. Which of the following is the most likely cause of the issue?
A. Incorrect encryption settings
B. Blocked MAC address
C. Outdated drivers
D. Disabled location services
Answer: B (LEAVE A REPLY)
When a user reports that a new, personally owned tablet will not connect to the corporate Wi-Fi network, but other devices can connect, and the tablet is running the latest software, the most likely cause of the issue is a blocked MAC address. Here's why:
* MAC Filtering: Many corporate networks implement MAC address filtering as a security measure. This involves only allowing devices with specific MAC addresses to connect to the network. If the MAC address of the new tablet is not on the allowed list, it will be blocked from connecting.
* Check Network Settings: To troubleshoot this, the network administrator can check the network's MAC filtering settings to see if the tablet's MAC address is blocked.
* Add MAC Address: If the MAC address is blocked, adding the tablet's MAC address to the allowed list will resolve the issue.
Other options like incorrect encryption settings or outdated drivers are less likely because the user can connect with other devices and the tablet is running the latest software. Disabled location services do not affect Wi-Fi connectivity.
Reference:
CompTIA A+ 220-1102 Exam Objectives, Section 2.6: Given a scenario configure basic mobile device network connectivity and application support.
Corporate network security practices documentation.

NEW QUESTION: 364
The following error is displayed on a user's computer screen:
No operating system found
Which of the following is the first troubleshooting step a technician should complete?
A. Disconnect external storage
B. Flash the BIOS
C. Replace the SATA cable
D. Turn on the device in safe mode
Answer: A (LEAVE A REPLY)
The first step is to disconnect external storage (Option A). Sometimes, the system may be attempting to boot from an external drive or USB device instead of the internal hard drive. By removing the external storage, the system will attempt to boot from the correct drive.

Flashing the BIOS (Option B) is more complex and typically unnecessary for this issue.
Replacing the SATA cable (Option C) may help if there's a hardware issue, but it's not the first troubleshooting step.
Turning on the device in safe mode (Option D) would not work if no operating system is detected.
CompTIA A+ Core 2 Reference:
5.1 - Apply troubleshooting methodologies, including steps for resolving boot issues.

NEW QUESTION: 365
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: 366
A technician needs to reimage a desktop in an area without network access. Which of the following should the technician use? (Select two).
A. USB
B. PXE
C. Optical media
D. Partition
E. Boot record
F. SMB
Answer: A,C (LEAVE A REPLY)
A technician needs to reimage a desktop in an area without network access, which means that the technician cannot use network-based methods such as PXE or SMB to deploy the image. Therefore, the technician should use offline methods that involve removable media such as USB or optical media. USB and optical media are common ways to store and transfer system images, and they can be used to boot the desktop and initiate the reimaging process. The technician will need to create a bootable USB or optical media that contains the system image and the imaging software, and then insert it into the desktop and change the boot order in the BIOS or UEFI settings. The technician can then follow the instructions on the screen to reimage the desktop

NEW QUESTION: 367
An administrator needs to back up the following components of a single workstation:
* The installation of the operating system
* Applications
* User profiles

* System settings

Which of the following backup methods can the administrator use to ensure the workstation is properly backed up?

A. Differential

B. Image

C. Synthetic

D. Archive

Answer: B (LEAVE A REPLY)

An image backup captures a complete snapshot of the entire system at a specific point in time, including the operating system, installed applications, user profiles, and system settings. This method is most suitable for backing up the components listed in the question because it ensures that every aspect of the workstation, from the core OS to individual user settings, is preserved and can be restored in its entirety. This is crucial for quickly recovering a system to a fully operational state after a failure or when migrating to new hardware. Other methods like differential, synthetic, and archive backups do not provide the comprehensive one-step restoration capability that an image backup offers for the complete system recovery.

NEW QUESTION: 368

During an enterprise rollout of a new application, a technician needs to validate compliance with an application's EULA while also reducing the number of licenses to manage. Which of the following licenses would best accomplish this goal?

A. Personal use license

B. Corporate use license

C. Open-source license

D. Non-expiring license

Answer: (SHOW ANSWER)

A corporate use license, also known as a volume license, is a type of software license that allows an organization to purchase and use multiple copies of a software product with a single license key. A corporate use license can help validate compliance with an application's EULA (end-user license agreement), which is a legal contract that defines the terms and conditions of using the software. A corporate use license can also reduce the number of licenses to manage, as it eliminates the need to activate and track individual licenses for each copy of the software. Personal use license, open-source license, and non-expiring license are not types of licenses that can best accomplish this goal.

NEW QUESTION: 369

A network administrator is deploying a client certificate lo be used for Wi-Fi access for all devices m 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 (LEAVE A REPLY)

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 organization3 Reference:

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

NEW QUESTION: 370
A remote user is experiencing issues connecting to a corporate email account on a laptop. The user clicks the internet connection icon and does not recognize the connected Wi-Fi. The help desk technician, who is troubleshooting the issue, assumes this is a rogue access point. Which of the following is the first action the technician should take?
A. Restart the wireless adapter.
B. Launch the browser to see if it redirects to an unknown site.
C. Instruct the user to disconnect the Wi-Fi.
D. Instruct the user to run the installed antivirus software.
Answer: C (LEAVE A REPLY)
Instructing the user to disconnect the Wi-Fi is the first action the technician should take if they suspect a rogue access point. A rogue access point is an unauthorized wireless network that could be used to intercept or manipulate network traffic, compromise security, or launch attacks. Disconnecting the Wi-Fi would prevent further exposure or damage to the user's device or data. Restarting the wireless adapter, launching the browser, or running the antivirus software are possible actions to take after disconnecting the Wi-Fi, but they are not as urgent or effective as the first step. Reference: Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 22 CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 456

NEW QUESTION: 371
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 46B 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 (LEAVE A REPLY)
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 RAM1.

NEW QUESTION: 372
A user's company phone has several pending software updates. A technician completes the following steps:
*Rebooted the phone
*Connected to Wi-Fi
*Disabled metered data
Which of the following should the technician do next?
A. Restore the factory settings.
B. Clean the browser history.
C. Uninstall and reinstall the applications.

D. Clear the cache.

Answer: (SHOW ANSWER)

After rebooting the phone, connecting to Wi-Fi, and disabling metered data, the next step the technician should take is to Clear the cache (D). Clearing the cache can resolve issues with the phone's performance and is often necessary before updating software to ensure that the updates can be downloaded and installed without issues. It removes temporary files that may be interfering with the update process.

NEW QUESTION: 373

While browsing the internet, a customer sees a window stating antivirus protection is no longer functioning Which of the following steps should a technician take next? (Select two).

A. Isolate the computer from the network

B. Enable the firewall service.

C. Update the endpoint protection software

D. Use System Restore to undo changes.

E. Delete the browser cookies

F. Run sfc /scannow.

Answer: A (LEAVE A REPLY)

When encountering a warning about antivirus protection malfunctioning, the first step should be to isolate the computer from the network to prevent potential spread of malware. Updating the endpoint protection software is also crucial to ensure the latest virus definitions and security features are in place to effectively identify and remove the threat.

NEW QUESTION: 374

An administrator needs to copy files to a Linux server at another office location so multiple users can access the files. Which of the following is the best for the administrator to use?

A. SFTP

B. RDP

C. DHCP

D. RMM

Answer: A (LEAVE A REPLY)

SFTP (Secure File Transfer Protocol) is the best method to copy files securely to a Linux server remotely. It provides encrypted file transfer over SSH, ensuring data confidentiality and integrity during transit. RDP (Remote Desktop Protocol) is used for remote graphical sessions, not file transfer. DHCP (Dynamic Host Configuration Protocol) is a network service for IP assignment, not related to file copying. RMM (Remote Monitoring and Management) refers to tools for monitoring and managing devices but not a file transfer protocol. The Core 2 objectives on networking and remote access explicitly list SFTP as the secure protocol for remote file transfer to Linux servers.

NEW QUESTION: 375

A user requires a drive to be mapped through a Windows command line. Which of the following command-line tools can be utilized to map the drive?

A. gpupdate

B. net use

C. hostname
D. dir
Answer: (SHOW ANSWER)
Net use is a command-line tool that can be used to map a drive in Windows. Mapping a drive means assigning a drive letter to a network location or a local folder, which allows the user to access it more easily and quickly. Net use can also be used to disconnect a mapped drive, display information about mapped drives, or connect to shared resources on another computer. Gpupdate, hostname, and dir are not command-line tools that can be used to map a drive.

NEW QUESTION: 376
A user reports a virus is on a PC. The user installs additional real-lime protection antivirus software, and the PC begins performing extremely slow. Which of the following steps should the technician take to resolve the issue?
A. Uninstall one antivirus software program and install a different one.
B. Launch Windows Update, and then download and install OS updates
C. Activate real-time protection on both antivirus software programs
D. Enable the quarantine feature on both antivirus software programs.
E. Remove the user-installed antivirus software program.
Answer: (SHOW ANSWER)
Removing the user-installed antivirus software program is the best way to resolve the issue of extremely slow performance caused by installing additional real-time protection antivirus software on a PC. Having more than one antivirus software program running at the same time can cause conflicts, resource consumption and performance degradation. Uninstalling one antivirus software program and installing a different one, activating real-time protection on both antivirus software programs, enabling the quarantine feature on both antivirus software programs and launching Windows Update are not effective ways to resolve the issue. Verified Reference: https://www.comptia.org/blog/why-you-shouldnt-run-multiple-antivirus-programs-at-the-same-time https://www.comptia.org/certifications/a

NEW QUESTION: 377
A technician needs to implement a system to handle both authentication and authorization Which of the following meets this requirement?
A. WPA3
B. MFA
C. TACACS+
D. RADIUS
Answer: (SHOW ANSWER)

To implement a system that handles both authentication and authorization, TACACS+ (Terminal Access Controller Access-Control System Plus) is the best option. TACACS+ is a security protocol that provides centralized Authentication, Authorization, and Accounting (AAA) services for networked access control, meeting the requirement for both authentication and authorization management.

NEW QUESTION: 378
A small-office customer needs three PCs to be configured in a network with no server. Which of the following network types is the customer's BEST choice for this environment?
A. Workgroup network
B. Public network
C. Wide area network
D. Domain network
Answer: A (LEAVE A REPLY)
A workgroup network is a peer-to-peer network where each PC can share files and resources with other PCs without a central server. A public network is a network that is accessible to anyone on the internet. A wide area network is a network that spans a large geographic area, such as a country or a continent. A domain network is a network where a server controls the access and security of the PCs. Verified Reference: https://www.comptia.org/blog/network-types https://www.comptia.org/certifications/a

NEW QUESTION: 379
Which of the following commands lists running processes in Linux?
A. top
B. apt-get
C. ls
D. cat
Answer: A (LEAVE A REPLY)
The 'top' command in Linux is used to display the running processes along with information about system resources like CPU and memory usage. It provides a real-time view of the system's resource consumption, making it an essential tool for monitoring and managing system performance.

NEW QUESTION: 380
Which of the following types of malicious software is most likely to demand payments in cryptocurrency?
A. Ransomware
B. Keylogger
C. Cryptomining
D. Rootkit
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth
Ransomware is a type of malware that encrypts files and demands payment (usually in cryptocurrency) to decrypt them.
B . Keylogger - Tracks keystrokes but does not demand payment.
C . Cryptomining - Uses system resources to mine cryptocurrency without the user's consent.

D . Rootkit - Hides malicious software but does not demand payment.
Reference:
CompTIA A+ 220-1102, Objective 2.5 - Common Security Threats

NEW QUESTION: 381
Which of the following should be used to secure a device from known exploits?
A. Encryption
B. Remote wipe
C. Operating system updates
D. Cross-site scripting
Answer: (SHOW ANSWER)
Operating system updates are used to secure a device from known exploits. Operating system updates are patches or fixes that are released by the vendor to address security vulnerabilities, bugs, or performance issues. Operating system updates can also provide new features or enhancements to the device. It is important to keep the operating system updated to prevent attackers from exploiting known flaws or weaknesses.

NEW QUESTION: 382
A user reports that the pages flash on the screen two or three times before finally staying open when attempting to access banking web pages. Which of the following troubleshooting steps should the technician perform NEXT to resolve the issue?
A. Examine the antivirus logs.
B. Verify the address bar URL.
C. Test the internet connection speed.
D. Check the web service status.
Answer: B (LEAVE A REPLY)
The next troubleshooting step that the technician should perform to resolve the issue of pages flashing on the screen before staying open when accessing banking web pages is to verify the address bar URL. The address bar URL is the web address that appears in the browser's address bar and indicates the location of the web page being accessed. Verifying the address bar URL can help determine if the user is accessing a legitimate or malicious website, as some phishing websites may try to impersonate banking websites by using similar-looking URLs or domains.