



CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

NEW QUESTION 1

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

Explanation:

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 system. Device Manager, Administrator Tools, and Programs and Features are not Windows 10 utilities that can fix a failed update.

NEW QUESTION 2

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

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

Answer: D

Explanation:

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

NEW QUESTION 3

A developer receives the following error while trying to install virtualization software on a workstation:

VTx not supported by system

Which of the following upgrades will MOST likely fix the issue?

- A. Processor
- B. Hard drive
- C. Memory
- D. Video card

Answer: A

Explanation:

The processor is the component that determines if the system supports virtualization technology (VTx), which is required for running virtualization software. The hard drive, memory and video card are not directly related to VTx support, although they may affect the performance of the virtual machines. Verified References: <https://www.comptia.org/blog/what-is-virtualization> <https://www.comptia.org/certifications/a>

NEW QUESTION 4

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

Explanation:

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.

References:

? 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 5

A Windows user recently replaced a computer. The user can access the public internet on the computer; however, an internal site at <https://companyintranet.com:8888> is no longer loading. Which of the following should a technician adjust to resolve the issue?

- A. Default gateway settings
- B. DHCP settings
- C. IP address settings
- D. Firewall settings
- E. Antivirus settings

Answer: D

Explanation:

The technician should adjust the firewall settings to resolve the issue of not being able to access an internal site at <https://companyintranet.com:8888>. The firewall settings control how the firewall filters and allows network traffic based on rules and policies. The firewall settings may be blocking or preventing the access to the internal site by mistake or by default, especially if the site uses a non-standard port number such as 8888. The technician should check and modify the firewall settings to allow the access to the internal site or its port number. Default gateway settings determine how a computer connects to other networks or the internet. Default gateway settings are not likely to cause the issue of not being able to access an internal site if the user can access the public internet. DHCP settings determine how a computer obtains its IP address and other network configuration parameters automatically from a DHCP server. DHCP settings are not likely to cause the issue of not being able to access an internal site if the user can access other network resources. IP address settings determine how a computer identifies itself and communicates with other devices on a network. IP address settings are not likely to cause the issue of not being able to access an internal site if the user can access other network resources. Antivirus settings control how the antivirus software scans and protects the computer from malware and threats. Antivirus settings are less likely to cause the issue of not being able to access an internal site than firewall settings, unless the antivirus software has its own firewall feature that may interfere with the network traffic. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.6

NEW QUESTION 6

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: B

Explanation:

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. References:

? 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 7

Which of the following is used to identify potential issues with a proposed change prior to implementation?

- A. Request form
- B. Rollback plan
- C. End-user acceptance
- D. Sandbox testing

Answer: D

Explanation:

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 References: <https://www.comptia.org/blog/what-is-sandbox-testing> <https://www.comptia.org/certifications/a>

NEW QUESTION 8

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: A

Explanation:

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. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.3

NEW QUESTION 9

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

Explanation:

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. References:

? 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 10

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

Explanation:

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 10

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

Explanation:

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 11

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: C

Explanation:

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. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.7

NEW QUESTION 12

A system drive is nearly full, and a technician needs to free 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

Explanation:

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 References: <https://www.comptia.org/blog/how-to-use-disk-cleanup> <https://www.comptia.org/certifications/a>

NEW QUESTION 17

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?

- A. Turn off the machine.
- B. Run a full antivirus scan.
- C. Remove the LAN card.
- D. Install a different endpoint solution.

Answer: A

Explanation:

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 network. 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.

References: 1 3 steps to prevent and recover from ransomware(<https://www.microsoft.com/en-us/security/blog/2021/09/07/3-steps-to-prevent-and-recover-from-ransomware/>)2 #StopRansomware Guide | CISA(<https://www.cisa.gov/stopransomware/ransomware-guide>).

NEW QUESTION 20

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

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

Answer: C

Explanation:

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

NEW QUESTION 24

Which of the following would MOST likely be deployed to enhance physical security for a building? (Select TWO).

- A. Multifactor authentication
- B. Badge reader
- C. Personal identification number
- D. Firewall
- E. Motion sensor
- F. Soft token

Answer: BE

Explanation:

Badge reader and motion sensor are devices that can be deployed to enhance physical security for a building. A badge reader is a device that scans and verifies an identification card or tag that grants access to authorized personnel only. A badge reader can help prevent unauthorized entry or intrusion into a building or a restricted area. A motion sensor is a device that detects movement and triggers an alarm or an action when motion is detected. A motion sensor can help deter or alert potential intruders or trespassers in a building or an area. Multifactor authentication is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. Multifactor authentication is not a device that can be deployed to enhance physical security for a building but a technique that can be used to enhance logical security for systems or services. Personal identification number is a numeric code that can be used as part of authentication or access control. Personal identification number is not a device that can be deployed to enhance physical security for a building but an example of something you know factor in multifactor authentication. Firewall is a device or software that filters network traffic based on rules and policies. Firewall is not a device that can be deployed to enhance physical security for a building but a device that can be used to enhance network security for systems or services. Soft token is an application or software that generates one-time passwords or codes for authentication purposes. Soft token is not a device that can be deployed to enhance physical security for a building but an example of something you have factor in multifactor authentication. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 3.3

NEW QUESTION 25

A salesperson's computer is unable to print any orders on a local printer that is connected to the computer. Which of the following tools should the salesperson use to restart the print spooler?

- A. Control Panel
- B. Processes
- C. Startup
- D. Services**

Answer: D

Explanation:

The correct answer is D. Services. The print spooler is a service that manages the print queue and sends print jobs to the printer. To restart the print spooler, the salesperson can use the Services app, which allows them to stop and start the service. Alternatively, they can also use the Task Manager or the Command Prompt to restart the print spooler.

References and Explanation

? The Services app is a tool that displays all the services that are running on the

computer. It can be accessed by typing services.msc in the Run window or by searching for Services in the Start menu. The Services app allows users to start, stop, restart, or configure any service, including the print spooler123.

? The Task Manager is a tool that shows information about the processes,

applications, and services that are running on the computer. It can be accessed by pressing Ctrl + Shift + Esc or by right-clicking on the taskbar and selecting Task Manager. The Task Manager allows users to start, stop, or restart any service by going to the Services tab and right-clicking on the service name12.

? The Command Prompt is a tool that allows users to execute commands and

perform tasks using text input. It can be accessed by typing cmd in the Run window or by searching for Command Prompt in the Start menu. The Command Prompt allows users to start, stop, or restart any service by using the net command with the service name. For example, to restart the print spooler, users can type net stop spooler and then net start spooler1.

? The Control Panel is a tool that provides access to various settings and options for

the computer. It can be accessed by typing control panel in the Run window or by searching for Control Panel in the Start menu. The Control Panel does not allow users to restart the print spooler directly, but it can be used to access other tools such as Devices and Printers, Troubleshooting, or Administrative Tools2.

? The Processes tab is a part of the Task Manager that shows information about the

processes that are running on the computer. It can be accessed by opening the Task Manager and selecting the Processes tab. The Processes tab does not allow users to restart the print spooler directly, but it can be used to end any process that is related to printing or causing problems with the print spooler2.

? The Startup tab is a part of the Task Manager that shows information about the

programs that run automatically when the computer starts. It can be accessed by opening the Task Manager and selecting the Startup tab. The Startup tab does not allow users to restart the print spooler directly, but it can be used to disable or enable any program that affects printing or interferes with the print spooler2.

NEW QUESTION 29

A company is looking for 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

Explanation:

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 References:

<https://www.comptia.org/blog/what-is-a-synthetic-backup> <https://www.comptia.org/certifications/a>

NEW QUESTION 32

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: B

Explanation:

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 36

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

Explanation:

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). 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 38

A team of support agents will be using their workstations to store credit card data. Which of the following should the IT department enable on the workstations in order to remain compliant with common regulatory controls? (Select TWO).

- A. Encryption
- B. Antivirus
- C. AutoRun
- D. Guest accounts
- E. Default passwords
- F. Backups

Answer: AF

Explanation:

Encryption is a way of protecting cardholder data by transforming it into an unreadable format that can only be decrypted with a secret key. Backups are a way of ensuring that cardholder data is not lost or corrupted in case of a disaster or system failure. Both encryption and backups are part of the PCI DSS requirements that apply to any entity that stores, processes, or transmits cardholder data. The other options are not directly related to credit card data security or compliance.

NEW QUESTION 43

A user recently purchased a second monitor and wants to extend the Windows desktop to the new screen. Which of the following Control Panel options should a technician adjust to help the user?

- A. Color Management
- B. Troubleshooting System
- C. Troubleshooting
- D. Device Manager
- E. Administrative Tools

Answer: D

NEW QUESTION 45

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

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

Answer: B

Explanation:

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

NEW QUESTION 50

A hard drive that previously contained PI I 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. Shredding
- B. Degaussing
- C. Low-level formatting
- D. Recycling

Answer: A

Explanation:

Shredding is a data destruction method that physically destroys the hard drive by cutting it into small pieces using a machine. Shredding ensures that data is completely removed from the hard drive and cannot be recovered by any means. Shredding is suitable for hard drives that contain PII (personally identifiable information) which is any information that can be used to identify, contact, or locate an individual. Degaussing, low-level formatting, and recycling are not data destruction methods that can guarantee complete data removal from a hard drive.

NEW QUESTION 55

A user's computer unexpectedly shut down immediately after the user plugged in a USB headset. Once the user turned the computer back on, everything was functioning properly, including the headset. Which of the following Microsoft tools would most likely be used to determine the root cause?

- A. Event Viewer
- B. System Configuration
- C. Device Manager
- D. Performance Monitor

Answer: A

Explanation:

Event Viewer is a Microsoft tool that records and displays system events, errors, warnings, and information. Event Viewer can help troubleshoot and diagnose problems, such as unexpected shutdowns, by showing the details of what happened before, during, and after the incident. Event Viewer can also show the source of the event such as an application, a service, a driver, or a hardware device. By using Event Viewer, a technician can identify the root cause of the unexpected shutdown, such as a power failure, a thermal event, a driver conflict, or a malware infection.

NEW QUESTION 59

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. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 62

A technician, who is working at a local office, has found multiple copies of home edition software installed on computers. Which of the following does this MOST likely violate?

- A. EULA
- B. PII
- C. DRM
- D. Open-source agreement

Answer: A

Explanation:

The installation of home edition software on computers at a local office most likely violates the EULA. EULA stands for End User License Agreement and is a legal contract that specifies the terms and conditions for using a software product or service. EULA typically covers topics such as license scope, duration and limitations, rights and obligations of the parties, warranties and disclaimers, liability and indemnity clauses, and termination procedures. EULA may also restrict the use of home edition software to personal or non-commercial purposes only, and prohibit the use of home edition software in business or professional settings. Violating EULA may result in legal actions or penalties from the software vendor or developer. PII stands for Personally Identifiable Information and is any information that can be used to identify or locate an individual, such as name, address, phone number, email address, social security number or credit card number. PII is not related to software installation or licensing but to data protection and privacy. DRM stands for Digital Rights Management and is a technology that controls or restricts the access and use of digital content, such as music, movies, books or games. DRM is not related to software installation or licensing but to content distribution and piracy prevention. Open-source agreement is a type of license that allows users to access, modify and distribute the source code of a software product or service freely and openly. Open-source agreement does not restrict the use of software to home edition only but encourages collaboration and innovation among developers and users. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 5.1

NEW QUESTION 66

A technician is unable to completely start up a system. The OS freezes when the desktop background appears, and the issue persists when the system is restarted. Which of the following should the technician do next to troubleshoot the issue?

- A. Disable applicable BIOS options.
- B. Load the system in safe mode.
- C. Start up using a flash drive OS and run System Repair.
- D. Enable Secure Boot and reinstall the system.

Answer: B

Explanation:

Loading the system in safe mode is a common troubleshooting step that allows the technician to isolate the problem by disabling unnecessary drivers and services. This can help determine if the issue is caused by a faulty device, a corrupted system file, or a malware infection.

NEW QUESTION 71

Which of the following filesystem types does macOS use?

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

Answer: D

Explanation:

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 72

A technician is setting up a desktop computer in a small office. The user will need to access files on a drive shared from another desktop on the network. Which of the following configurations should the technician employ to achieve this goal?

- A. Configure the network as private
- B. Enable a proxy server
- C. Grant the network administrator role to the user
- D. Create a shortcut to public documents

Answer: A

Explanation:

The technician should configure the network as private to allow the user to access files on a drive shared from another desktop on the network1

NEW QUESTION 75

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

Explanation:

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 77

An architecture firm is considering upgrading its computer-aided design (CAD) software to the newest version that forces storage of backups of all CAD files on the software's cloud server. Which of the following is MOST likely to be of concern to the IT manager?

- A. All updated software must be tested with alt system types and accessories
- B. Extra technician hours must be budgeted during installation of updates
- C. Network utilization will be significantly increased due to the size of CAD files
- D. Large update and installation files will overload the local hard drives.

Answer: C

Explanation:

The IT manager is most likely to be concerned about network utilization being significantly increased due to the size of CAD files. Backing up all CAD files to the software's cloud server can result in a large amount of data being transferred over the network, which can cause network congestion and slow down other network traffic.

NEW QUESTION 79

Which of the following is a proprietary Cisco AAA protocol?

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

Answer: D

Explanation:

TACACS+ is a proprietary Cisco AAA protocol

NEW QUESTION 83

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

do before returning the laptop to the user?

- A. Educate the user on malware removal.
- B. Educate the user on how to reinstall the laptop OS.
- C. Educate the user on how to access recovery mode.
- D. Educate the user on common threats and how to avoid them.

Answer: D

Explanation:

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

NEW QUESTION 88

Which of the following Linux commands would be used to install an application?

- A. yum
- B. grep
- C. ls
- D. sudo

Answer: D

Explanation:

The Linux command used to install an application is sudo. The sudo command allows users to run programs with the security privileges of another user, such as the root user. This is necessary to install applications because it requires administrative privileges¹

NEW QUESTION 93

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

- A. VNC
- B. MFA
- C. MSRA
- D. RDP

Answer: A

Explanation:

The tool that the technician will most likely use to remotely connect to a Linux desktop is VNC. VNC stands for Virtual Network Computing and is a protocol that allows remote access and control of a graphical desktop environment over a network. VNC is natively designed for Linux and can also support other operating systems, such as Windows and Mac OS. VNC can be used to assist users with troubleshooting by viewing and interacting with their desktops remotely. MFA stands for Multi-Factor Authentication and is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. MFA is not a tool that can be used to remotely connect to a Linux desktop but a technique that can be used to enhance security

for systems or services. MSRA stands for Microsoft Remote Assistance and is a feature that allows remote access and control of a Windows desktop environment over a network. MSRA is not natively designed for Linux and may not be compatible or supported by Linux systems. RDP stands for Remote Desktop Protocol and is a protocol that allows remote access and control of a Windows desktop environment over a network. RDP is not natively designed for Linux and may not be compatible or supported by Linux systems. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.6

NEW QUESTION 97

A user's corporate laptop with proprietary work Information was stolen from a coffee shop. The user toggled in to the laptop with a simple password. and no other security mechanisms were in place. Which of the following would MOST likely prevent the stored data from being recovered?

- A. Biometrics
- B. Full disk encryption
- C. Enforced strong system password
- D. Two-factor authentication

Answer: B

Explanation:

Full disk encryption is a security mechanism that encrypts the entire data on a hard drive, making it unreadable without the correct decryption key or password. It can prevent the stored data from being recovered by unauthorized persons who steal or access the laptop. Biometrics, enforced strong system password and two-factor authentication are other security mechanisms, but they only protect the login access to the laptop, not the data on the hard drive. Verified References: <https://www.comptia.org/blog/what-is-full-disk-encryption> <https://www.comptia.org/certifications/a>

NEW QUESTION 100

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

Explanation:

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 103

Which of the following is used to explain issues that may occur during a change implementation?

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

Answer: C

Explanation:

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. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 5.2

NEW QUESTION 108

A technician is replacing the processor in a desktop computer prior to opening the computer, the technician wants to ensure the internal components are protected. Which of the following safety procedures would BEST protect the components in the PC? (Select TWO).

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

Answer: AC

Explanation:

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

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

<https://www.professormesser.com/free-a-plus-training/220-902/computer-safety-procedures-2/>

<https://www.skillsoft.com/course/comptia-a-core-2-safety-procedures-environmental-impacts-cbdf0f2c-61c0-4f4a-a659-dc98f1f00158>

NEW QUESTION 110

All the desktop icons on a user's newly issued PC are very large. The user reports that the PC was working fine until a recent software patch was deployed. Which of the following would BEST resolve the issue?

- A. Rolling back video card drivers
- B. Restoring the PC to factory settings
- C. Repairing the Windows profile
- D. Reinstalling the Windows OS

Answer: A

Explanation:

Rolling back video card drivers is the best way to resolve the issue of large desktop icons on a user's newly issued PC. This means restoring the previous version of the drivers that were working fine before the software patch was deployed. The software patch may have caused compatibility issues or corrupted the drivers, resulting in display problems

NEW QUESTION 112

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

Explanation:

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 117

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

Explanation:

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 121

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

Explanation:

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 125

Which of the following would cause a corporate-owned iOS device to have an Activation Lock issue?

- A. A forgotten keychain password
- B. An employee's Apple ID used on the device
- C. An operating system that has been jailbroken
- D. An expired screen unlock code

Answer: B

Explanation:

Activation Lock is a feature that prevents anyone from erasing or activating an iOS device without the owner's Apple ID and password. If a corporate-owned iOS device is linked to an employee's Apple ID, it will have an Activation Lock issue when the employee leaves the company or forgets their Apple ID credentials. Reference: CompTIA A+ Core 2 Exam Objectives, Section 4.1

NEW QUESTION 127

Which of the following is an advantage of using WPA2 instead of WPA3?

- A. Connection security
- B. Encryption key length
- C. Device compatibility
- D. Offline decryption resistance

Answer: C

Explanation:

Device compatibility is an advantage of using WPA2 instead of WPA3. WPA2 is the previous version of the Wi-Fi Protected Access protocol, which provides security and encryption for wireless networks. WPA3 is the latest version, which offers improved security features, such as stronger encryption, enhanced protection against brute-force attacks, and easier configuration. However, WPA3 is not backward compatible with older devices that only support WPA2 or earlier protocols. Therefore, using WPA3 may limit the range of devices that can connect to the wireless network. Connection security, encryption key length, and offline decryption resistance are advantages of using WPA3 instead of WPA2. References:

- ? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 24
- ? CompTIA A+ Certification All-in-One Exam Guide (Exams 220-1101 & ..., page 1000

NEW QUESTION 129

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

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

Answer: A

Explanation:

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

NEW QUESTION 134

A department manager submits a help desk ticket to request the migration of a printer's port utilization from USB to Ethernet so multiple users can access the printer. This will be a new network printer, thus a new IP address allocation is required. Which of the following should happen immediately before network use is authorized?

- A. Document the date and time of the change.
- B. Submit a change request form.
- C. Determine the risk level of this change.
- D. Request an unused IP address.

Answer: B

Explanation:

A change request form is a document that describes the proposed change, the reason for the change, the impact of the change, and the approval process for the change. A change request form is required for any planned changes to the network, such as adding a new network printer, to ensure that the change is authorized, documented, and communicated to all stakeholders. Submitting a change request form should happen immediately before network use is authorized, as stated in the Official CompTIA A+ Core 2 Study Guide. The other options are either too late (documenting the date and time of the change) or too early (determining the risk level of the change and requesting an unused IP address) in the change management process.

NEW QUESTION 139

A technician needs to ensure that USB devices are not suspended by the operating system Which of the following Control Panel utilities should the technician use to configure the setting?

- A. System
- B. Power Options
- C. Devices and Printers
- D. Ease of Access

Answer: B

Explanation:

The correct answer is B. Power Options. The Power Options utility in the Control Panel allows you to configure various settings related to how your computer uses and saves power, such as the power plan, the sleep mode, the screen brightness, and the battery status. To access the Power Options utility, you can follow these steps:

- ? Go to Control Panel > Hardware and Sound > Power Options.
- ? Click on Change plan settings for the power plan you are using.
 - ? Click on Change advanced power settings.
- ? Expand the USB settings category and then the USB selective suspend setting subcategory.
- ? Set the option to Disabled for both On battery and Plugged in.
- ? Click on OK and then on Save changes.

This will prevent the operating system from suspending the USB devices to save power. System, Devices and Printers, and Ease of Access are not the utilities that should be used to configure the setting. System is a utility that provides information about your computer's hardware and software, such as the processor, memory, operating system, device manager, and system protection. Devices and Printers is a utility that allows you to view and manage the devices and printers connected to your computer, such as adding or removing devices, changing device settings, or troubleshooting problems. Ease of Access is a utility that allows you to customize your computer's accessibility options, such as the narrator, magnifier, high contrast, keyboard, mouse, and speech recognition. None of these utilities have any option to configure the USB selective suspend setting.

NEW QUESTION 143

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. taskmgr.exe
- E. gpmsvc.msc
- F. services.msc

Answer: F

Explanation:

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, taskmgr.exe and gpmsvc.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 References: <https://www.comptia.org/blog/what-is-services-msc> <https://www.comptia.org/certifications/a>

NEW QUESTION 147

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: D

Explanation:

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 151

Which of the following would typically require the most computing resources from the host computer?

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

Answer: B

Explanation:

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 follows:

- ? 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.

References:

- ? 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 156

Users access files in the department share. When a user creates a new subfolder, only that user can access the folder and its files. Which of the following will MOST likely allow all users to access the new folders?

- A. Assigning share permissions
- B. Enabling inheritance
- C. Requiring multifactor authentication
- D. Removing archive attribute

Answer: B

Explanation:

Enabling inheritance is a method that allows new subfolders to inherit the permissions and settings from their parent folder. If users can access files in the department share, but not in the new subfolders created by other users, it may indicate that inheritance is disabled and that each new subfolder has its own permissions and settings that restrict access to only the creator. Enabling inheritance can help resolve this issue by allowing all users to access the new subfolders with the same permissions and settings as the department share. Assigning share permissions, requiring multifactor authentication, and removing archive attribute are not methods that can most likely allow all users to access the new folders.

NEW QUESTION 160

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

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

Answer: B

Explanation:

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

The MOST efficient solution that allows for parallel execution of the Linux application and Windows applications is to install and run Linux and the required application as a virtual machine installed under the Windows OS. This is because it allows you to run both Linux and Windows together without the need to keep the Linux portion confined to a VM window 3.

NEW QUESTION 162

A company implemented a BYOD policy and would like to reduce data disclosure caused by malware that may infect these devices. Which of the following should the company deploy to address these concerns?

- A. UAC
- B. MDM
- C. LDAP
- D. SSO

Answer: B

Explanation:

MDM stands for mobile device management, which is a type of software solution that allows remote management and security of mobile devices. MDM can help a company reduce data disclosure caused by malware that may infect these devices by enforcing security policies, such as encryption, password protection, antivirus software, and remote wipe. MDM can also monitor and control the access of personal devices to corporate data and networks. UAC stands for user account control, which is a feature of Windows that prompts users for permission or an administrator password before making changes that affect the system. UAC may not be effective in preventing malware infection or data disclosure on personal devices. LDAP stands for lightweight directory access protocol, which is a protocol for accessing and managing information stored in a directory service, such as user names and passwords. LDAP does not directly address the issue of malware infection or data disclosure on personal devices. SSO stands for single sign-on, which is a feature that allows users to access multiple applications or services with one set of credentials. SSO may not prevent malware infection or data disclosure on personal devices, and may even increase the risk if the

credentials are compromised.

<https://www.nist.gov/news-events/news/2021/03/mobile-device-security-bring-your-own-device-byod-draft-sp-1800-22>

NEW QUESTION 163

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

Explanation:

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. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

NEW QUESTION 165

Which of the following command-line tools will delete a directory?

- A. md
- B. del
- C. dir
- D. rd
- E. cd

Answer: D

Explanation:

To delete an empty directory, enter rd Directory or rmdir Directory . If the directory is not empty, you can remove files and subdirectories from it using the /s switch. You can also use the /q switch to suppress confirmation messages (quiet mode).

NEW QUESTION 167

Which of the following is command options is used to display hidden files and directories?

- A. -a
- B. -s
- C. -lh
- D. -t

Answer: A

Explanation:

The -a option is used to display hidden files and directories in a command- line interface. Hidden files and directories are those that start with a dot (.) and are normally not shown by default. The -a option stands for “all” and shows all files and directories, including the hidden ones. The -a option can be used with commands such as ls, dir, or find to list or search for hidden files and directories. The -s, -lh, and -t options are not used to display hidden files and directories. The -s option stands for “size” and shows the size of files or directories in bytes. The -lh option stands for “long human-readable” and shows the size of files or directories in a more readable format, such as KB, MB, or GB. The -t option stands for “time” and sorts the files or directories by modification time. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 17
? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 107

NEW QUESTION 169

A call center handles inquiries into billing issues for multiple medical facilities. A security analyst notices that call center agents often walk away from their workstations, leaving patient data visible for anyone to see. Which of the following should a network administrator do to BEST prevent data theft within the call center?

- A. Encrypt the workstation hard drives.
Lock the workstations after five minutes of inactivity.
- B. Install privacy screens.
- C. Lock the workstations after five minutes of inactivity.
- D. Log off the users when their workstations are not in use.

Answer: B

Explanation:

The BEST solution for preventing data theft within the call center in this scenario would be to lock the workstations after a period of inactivity. This would prevent unauthorized individuals from accessing patient data if call center agents were to step away from their workstations without logging out.

NEW QUESTION 174

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

Explanation:

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.

References: 1: <https://support.microsoft.com/en-us/windows/change-your-desktop-background-image-175618be-4cf1-c159-2785-ec2238b433a8> 2:

<https://www.computerhope.com/issues/ch000592.htm>

NEW QUESTION 178

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

Explanation:

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.

References:

? BitLocker overview - Windows Security | Microsoft Learn¹

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

NEW QUESTION 183

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

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

Answer: B

Explanation:

The technician should disable the user's access to the device's command shell. This will prevent the user from accessing sensitive data and will help to prevent further data leaks. The technician should then investigate the unapproved application to determine if it is the cause of the data leak. If the application is found to be the cause of the leak, the technician should uninstall the application and restore the device to factory settings. If the application is not the cause of the leak, the technician should investigate further to determine the cause of the leak. Disabling the ability to install applications from unknown sources can help to prevent future data leaks, but it is not the next step the technician should take in this scenario. Ensuring the device is connected to the corporate WiFi network is not relevant to this scenario¹

NEW QUESTION 188

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?

- A. Group Policy
- B. User accounts
- C. Access control lists
- D. Authenticator applications

Answer: A

Explanation:

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.

References¹: 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 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: A

Explanation:

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 194

An organization is creating guidelines for the incorporation of generative AI solutions. In which of the following would these guidelines be published?

- A. Standard operating procedure
- B. Acceptable use policy
- C. Security protocols
- D. Data flow diagram

Answer: B

Explanation:

An acceptable use policy (AUP) is a document that defines the rules and expectations for the users of a system, network, or service. It typically covers topics such as the purpose, scope, responsibilities, and restrictions of using the system, network, or service¹. An AUP is a suitable place to publish the guidelines for the incorporation of generative AI solutions, as it can inform the users of the benefits, risks, and ethical implications of using such tools. It can also specify the conditions and limitations for using generative AI solutions, such as the types of data, content, and applications that are allowed or prohibited, the security and privacy requirements, the legal and regulatory compliance, and the accountability and reporting mechanisms²³.

References: 1 What is an Acceptable Use Policy (AUP)? - Definition from Techopedia([https://security.stackexchange.com/questions/84168/the-difference-of-security-](https://security.stackexchange.com/questions/84168/the-difference-of-security-policy-and-acceptable-use-policy)

[policy-and-acceptable-use-policy](https://security.stackexchange.com/questions/84168/the-difference-of-security-policy-and-acceptable-use-policy)). 2 Guide on the use of Generative AI -

Canada.ca(<https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-use-generative-ai.html>)³

Key Considerations for Developing Organizational Generative AI Policies - ISACA(<https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-44/key-considerations-for-developing-organizational-generative-ai-policies>).

NEW QUESTION 195

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

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

Answer: C

Explanation:

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

NEW QUESTION 200

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

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

Answer: B

Explanation:

The type of malware that is most likely to blame for a PC running more slowly than usual and having an extremely high GPU temperature is a "cryptominer". Cryptominers are a type of malware that use the resources of a computer to mine cryptocurrency. This can cause the computer to run more slowly than usual and can cause the GPU temperature to rise. Spyware is a type of malware that is used to spy on a user's activities, but it does not typically cause high GPU temperatures. Ransomware is a type of malware that encrypts a user's files and demands payment to unlock them, but it does not typically cause high GPU temperatures. Boot sector viruses are a type of malware that infects the boot sector of a hard drive, but they do not typically cause high GPU temperatures¹²

NEW QUESTION 203

A user is unable to access several documents saved on a work PC. A technician discovers the files were corrupted and must change several system settings within Registry Editor to correct the issue. Which of the following should the technician do before modifying the registry keys?

- A. Update the anti-malware software.
- B. Create a restore point.
- C. Run the PC in sate mode.

D. Roll back the system updates.

Answer: B

Explanation:

A restore point is a snapshot of the system settings and configuration at a specific point in time². Creating a restore point before modifying the registry keys allows the technician to revert the system back to a previous state if something goes wrong or causes instability². Updating the anti-malware software, running the PC in safe mode, and rolling back the system updates are not necessary steps before modifying the registry keys.

NEW QUESTION 205

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

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

Answer: B

Explanation:

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

NEW QUESTION 208

Which of the following allows access to the command line in macOS?

- A. PsExec
- B. command.com
- C. Terminal
- D. CMD

Answer: C

Explanation:

Terminal is an application that allows access to the command line in macOS. The command line is an interface that allows users to interact with the operating system and perform various tasks by typing commands and arguments. Terminal can be used to launch programs, manage files and folders, configure settings, troubleshoot issues, and run scripts in macOS. PsExec, command.com, and CMD are not applications that allow access to the command line in macOS.

NEW QUESTION 211

A PC is taking a long time to boot Which of the following operations would be best to do to resolve the issue at a minimal expense?

(Select two).

- A. Installing additional RAM
- B. Removing the applications from startup
- C. Installing a faster SSD
- D. Running the Disk Cleanup utility
- E. Defragmenting the hard drive
- F. Ending the processes in the Task Manager

Answer: BD

Explanation:

The best operations to do to resolve the issue of a long boot time at a minimal expense are B. Removing the applications from startup and D. Running the Disk Cleanup utility. These are two simple and effective ways to speed up your PC's boot time without spending any money on hardware upgrades.

Removing the applications from startup means preventing unnecessary programs from launching automatically when you turn on your computer. This can reduce the load on your system resources and make the boot process faster. You can do this in Windows 10 by pressing Ctrl + Alt + Esc to open the Task Manager, and going to the Startup tab. There, you can see a list of programs that start with your computer, and their impact on the startup performance. You can disable any program that you don't need by right-clicking on it and choosing Disable¹².

Running the Disk Cleanup utility means deleting temporary files, system files, and other unnecessary data that may be taking up space and slowing down your computer. This can free up some disk space and improve the performance of your system. You can do this in Windows 10 by typing disk cleanup in the search box and selecting the Disk Cleanup app. There, you can choose which files you want to delete, such as Recycle Bin, Temporary Internet Files, Thumbnails, etc. You can also click on Clean up system files to delete more files, such as Windows Update Cleanup, Previous Windows installation(s), etc³⁴.

NEW QUESTION 215

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

Explanation:

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 References: <https://www.comptia.org/blog/what-is->

cryptomining <https://www.comptia.org/certifications/a>

NEW QUESTION 220

A company discovered that numerous computers from multiple geographic locations are sending a very high number of connection requests which is causing the company's web server to become unavailable to the general public. Which of the following attacks is occurring?

- A. Zero day
- B. SQL injection
- C. Cross-site scripting
- D. Distributed denial of service

Answer: D

Explanation:

The company is experiencing a distributed denial of service (DDoS) attack. A DDoS attack is a type of cyber attack in which multiple compromised systems are used to target a single system, causing a denial of service for users of the targeted system.

NEW QUESTION 224

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

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

Answer: C

Explanation:

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

NEW QUESTION 228

Which of the following commands can a technician use to get the MAC address of a Linux distribution?

- A. net use
- B. ifconfig
- C. netstat
- D. ping

Answer: B

Explanation:

The ifconfig command is a tool for configuring network interfaces that any Linux system administrator should know. It is used to bring interfaces up or down, assign and remove addresses and routes, manage ARP cache, and much more¹. One of the information that ifconfig can display is the MAC address of each network interface, which is a unique identifier of the physical layer of the network device. The MAC address is usually shown as a hexadecimal string separated by colons, such as 00:0c:29:3f:5c:1f. To get the MAC address of a Linux distribution, a technician can use the ifconfig command without any arguments, which will show the details of all the active network interfaces, or specify the name of a particular interface, such as eth0 or wlan0, to show only the details of that interface.

References¹: Linux Commands - CompTIA A+ 220-1102 - 1.11 - Professor Messer IT Certification Training Courses¹

NEW QUESTION 231

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

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

Answer: B

Explanation:

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

NEW QUESTION 235

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: B

Explanation:

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 237

A user is unable to log in to the domain with a desktop PC, but a laptop PC is working properly on the same network. A technician logs in to the desktop PC with a local account but is unable to browse to the secure intranet site to get troubleshooting tools. Which of the following is the MOST likely cause of the issue?

- A. Time drift
- B. Dual in-line memory module failure
- C. Application crash
- D. Filesystem errors

Answer: A

Explanation:

The most likely cause of the issue is a "time drift". Time drift occurs when the clock on a computer is not synchronized with the clock on the domain controller. This can cause authentication problems when a user tries to log in to the domain. The fact that the technician is unable to browse to the secure intranet site to get troubleshooting tools suggests that there may be a problem with the network connection or the firewall settings on the desktop PC.

NEW QUESTION 238

A systems administrator is creating a new document with a list of the websites that users are allowed to access. Which of the following types of documents is the administrator MOST likely creating?

- A. Access control list
- B. Acceptable use policy
- C. Incident report
- D. Standard operating procedure

Answer: A

Explanation:

An access control list (ACL) is a list of permissions associated with a system resource (object), such as a website. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. A systems administrator can create an ACL to define the list of websites that users are allowed to access.

References: 1: Access-control list - Wikipedia (https://en.wikipedia.org/wiki/Access-control_list)

NEW QUESTION 242

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

Explanation:

the user should change the default passwords first when configuring a new SOHO Wi-Fi router.

NEW QUESTION 244

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 245

A technician downloaded a software program to a network share. When the technician attempts to copy the program to the Windows tablet for installation, the technician receives an error. Which of the following is the best procedure for the technician to use to complete the assignment?

- A. Copy the program file to a USB drive and install.
- B. Burn the program file to a CD and install.
- C. Format the HDD and then do the installation.
- D. Replace the HDD and then do the installation.

Answer: A

Explanation:

Copying the program file to a USB drive and installing it from there is the simplest and most reliable way to transfer the software from the network share to the Windows tablet. The other options are either unnecessary, risky, or impractical. Burning the program file to a CD requires a CD burner and a CD reader, which may not be available on the tablet. Formatting or replacing the HDD will erase all the data and settings on the tablet, which is not advisable unless there is a backup or a serious problem. Moreover, formatting or replacing the HDD will not solve the issue of copying the program file from the network share.

References: 1 How To Copy A Program From One Computer To Another: 5 Ways(<https://www.minitool.com/news/transfer-copy-programs-from-one-computer-to-another.html>)2 Transfer files between your Android tablet and PC using Wi-Fi(<https://www.techrepublic.com/article/transfer-files-between-your-android-tablet-and-pc-using-wi-fi/>)3 Share Files Between Your Tablet and Computer with Huawei

Share(<https://consumer.huawei.com/en/support/content/en-us15819174/>)4 How to Transfer Installed Programs to Another PC on

Windows

10(<https://www.diskpart.com/articles/transfer-installed-program-to-another-pc-windows-10-0825.html>).

NEW QUESTION 246

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

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

Answer: B

Explanation:

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

NEW QUESTION 250

An administrator has submitted a change request for an upcoming server deployment. Which of the following must be completed before the change can be approved?

- A. Risk analysis
- B. Sandbox testing
- C. End user acceptance
- D. Lessons learned

Answer: A

Explanation:

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

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

NEW QUESTION 254

A desktop engineer is deploying a master image. Which of the following should the desktop engineer consider when building the master image? (Select TWO).

- A. Device drivers
- B. Keyboard backlight settings
- C. Installed application license keys
- D. Display orientation
- E. Target device power supply
- F. Disabling express charging

Answer: AC

Explanation:

? A. Device drivers23: Device drivers are software components that enable the operating system to communicate with hardware devices. Different devices may require different drivers, so the desktop engineer should include the appropriate drivers in the master image or configure the deployment process to install them automatically.

? C. Installed application license keys2: Installed application license keys are codes that activate or authenticate software applications. Some applications may require license keys to be entered during installation or after deployment. The desktop engineer should include the license keys in the master image or configure the deployment process to apply them automatically.

NEW QUESTION 257

A technician receives a call from 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

Explanation:

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 258

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 vmgm
- D. msc
- E. diskmgmt.msc

Answer: C

Explanation:

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. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.6

NEW QUESTION 261

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

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

Answer: D

Explanation:

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

NEW QUESTION 263

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

Explanation:

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.

References:

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 266

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

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

Answer: B

Explanation:

In Windows 10, there are privacy settings that control access to certain devices, such as microphones, cameras, and other input devices. If the microphone is not enabled under these privacy settings, the VoIP application may not have access to it, causing a lack of outgoing audio.

The technician can go to the Windows 10 Settings menu, select the Privacy submenu, and under App permissions, select Microphone.

The technician should then turn on the toggle switch for the VoIP application to allow it to access the microphone.

Removing the microphone from the USB hub and plugging it directly into a USB port on the PC may or may not solve the issue, as the issue could be related to the privacy settings. Deleting the microphone from Device Manager and scanning for new hardware may also not solve the issue, as the issue could be related to the privacy settings. Replacing the USB microphone with one that uses a traditional 3.5mm plug is not recommended, as it would require purchasing a new microphone and may not solve the issue.

NEW QUESTION 271

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+Alt+> to correct the display orientation
- D. Updating the display drivers for the video card

Answer: B

Explanation:

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 272

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

Explanation:

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 276

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

Explanation:

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 277

Which of the following statements describes the purpose of scripting languages?

- A. To access the hardware of the computer it is running on
- B. To automate tasks and reduce the amount of manual labor
- C. To abstract the complexity of the computer system

D. To compile the program into an executable file

Answer: B

Explanation:

Scripting languages are used to write small to medium-sized programs that perform specific tasks. Some common uses of scripting languages are: automating repetitive processes, web development, system administration, data processing, multimedia and games, report generation, document and text processing, writing plugins and extensions for existing programs and applications¹.

References: 1 What is Scripting Language?: Introduction, Types, Uses & Career
...(https://leverageedu.com/blog/scripting-language/)

NEW QUESTION 281

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

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

Answer: B

Explanation:

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

NEW QUESTION 284

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

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

Answer: C

Explanation:

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

NEW QUESTION 287

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

Explanation:

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 289

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. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 293

A new service desk is having a difficult time managing the volume of requests. Which of the following is the BEST solution for the department?

- A. Implementing a support portal
- B. Creating a ticketing system
- C. Commissioning an automated callback system
- D. Submitting tickets through email

Answer: A

Explanation:

A support portal is an online system that allows customers to access customer service tools, submit requests and view status updates, as well as access information such as how-to guides, FAQs, and other self-service resources. This would be the best solution for the service desk, as it would allow them to easily manage the volume of requests by allowing customers to submit their own requests and view the status of their requests. Additionally, the portal would provide customers with self-service resources that can help them resolve their own issues, reducing the amount of tickets that need to be handled by the service desk.

NEW QUESTION 297

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

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

Answer: D

Explanation:

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

NEW QUESTION 298

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

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

Answer: C

Explanation:

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

NEW QUESTION 299

A technician needs to replace a PC's motherboard. The technician shuts down the PC. Which of the following steps should the technician take next?

- A. Turn off the monitor.
- B. Remove the power cord.
- C. Remove the PSU.
- D. Remove the RAM modules.

Answer: B

Explanation:

Removing the power cord is the first step to ensure the safety of the technician and the PC components. This will prevent any electrical shock or damage that may occur if the PC is still connected to a power source. The technician should also press the power button to drain any residual power from the capacitors.

NEW QUESTION 300

Which of the following environmental factors are most important to consider when planning the configuration of a data center? (Select two).

- ☐ A. Temperature levels
- ☐ B: Location of the servers
- ☐ C. Humidity levels
- ☐ D. Noise levels
- ☐ E. Lighting levels
- ☐ F. Cable management

Answer: AC

Explanation:

Temperature and humidity levels are the most important environmental factors to consider when planning the configuration of a data center, as they directly affect the performance, reliability, and energy efficiency of the IT equipment. Excessive heat or moisture can cause overheating, corrosion, condensation, or static electricity, which can damage the hardware and lead to data loss or service disruption. Therefore, data centers need to monitor and control the temperature and humidity levels within the recommended ranges by using various cooling systems, airflow management, and sensors12.

References: 1 5 Factors to Consider for Data Center Environmental Monitoring(<https://community.fs.com/blog/5-factors-to-consider-for-data-center-environmental-monitoring.html>)2 Data Center Environmental standards and Controls DataSpan(<https://dataspan.com/blog/data-center-environmental-standards/>).

NEW QUESTION 302

A company recently experienced a security incident in which a USB drive containing malicious software was able to covertly install malware on a workstation_ following actions should be taken to prevent this Incident from happening again? (Select two).

Which of the

- A. Install a host-based IDS
- B. Restrict log-in times.
- C. Enable a BIOS password
- D. Update the password complexity
- E. Disable AutoRun.
- F. Update the antivirus definitions.
- G. Restrict user permissions.

Answer: EF

Explanation:

The correct answers are E and F. Disabling AutoRun and updating the antivirus definitions are two actions that should be taken to prevent the incident from happening again.

AutoRun is a feature of Windows that automatically executes a predetermined action when a removable media such as a USB drive is inserted in a computer. For example, AutoRun can launch or install a new program on the media, or open the file in File Explorer. However, this feature can also be exploited by malicious software that can run without the user's consent or knowledge. Therefore, disabling AutoRun can help prevent accidental installation of viruses and other malware from USB drives¹²³.

Updating the antivirus definitions is another important action that can help prevent malware infections from USB drives. Antivirus definitions are files that contain information about the latest known threats and how to detect and remove them. By updating the antivirus definitions regularly, you can ensure that your antivirus software can recognize and block any malicious software that may be on the USB drive before it can harm your computer⁴⁵. A host-based IDS is a system that monitors and analyzes the activity on a single computer or device for any signs of intrusion or malicious behavior. A host-based IDS can help detect and prevent malware infections from USB drives, but it is not a sufficient action by itself. A host-based IDS needs to be complemented by other security measures, such as disabling AutoRun and updating the antivirus definitions⁶.

Restricting login times, enabling a BIOS password, and updating the password complexity are all actions that can help improve the security of a computer or device, but they are not directly related to preventing malware infections from USB drives. These actions can help prevent unauthorized access to the computer or device, but they do not affect how the computer or device interacts with the USB drive or its contents.

Restricting user permissions is an action that can help limit the damage that malware can cause on a computer or device, but it does not prevent the malware from being installed in the first place. Restricting user permissions means limiting what actions a user can perform on the computer or device, such as installing or deleting programs, modifying system settings, or accessing certain files or folders. By restricting user permissions, you can reduce the impact of malware infections by preventing them from affecting other users or system components⁷.

NEW QUESTION 304

A technician is moving a Windows workstation from the accounting department to the sales department and needs to update the IP and gateway settings. Which of the following Control Panel utilities should the technician use?

- A. Programs and Features
- B. Network and Sharing Center
- C. User Accounts
- D. Device Manager

Answer: B

Explanation:

The Network and Sharing Center is a Control Panel utility that allows users to view and modify network settings, such as IP address, subnet mask, default gateway, DNS servers, and network profiles. To change the IP and gateway settings of a Windows workstation, the technician can follow these steps:

? Open the Network and Sharing Center by clicking on the network icon in the system tray or by searching for it in the Start menu.

? Click on Change adapter settings on the left sidebar.

? Right-click on the network adapter that is connected to the network and select Properties.

? Double-click on Internet Protocol Version 4 (TCP/IPv4) or Internet Protocol Version 6 (TCP/IPv6) depending on the network protocol used.

? Select Use the following IP address and enter the desired IP address, subnet mask, and default gateway for the workstation. Alternatively, select Obtain an IP address automatically if the network uses DHCP to assign IP addresses dynamically.

? Click OK to save the changes and close the dialog boxes. References:

? The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2171

? How to change the IP address in Windows 10 and Windows 11 (4 ways), section 12

NEW QUESTION 305

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

220-1102 Practice Exam Features:

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

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