

220-1102 Dumps

CompTIA A+ Certification Exam: Core 2

<https://www.certleader.com/220-1102-dumps.html>



NEW QUESTION 1

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 2

A systems administrator is monitoring an unusual amount of network traffic from a kiosk machine and needs to investigate to determine the source of the traffic.

Which of the following tools can the administrator use to view which processes on the kiosk machine are connecting to the internet?

- A. Resource Monitor
- B. Performance Monitor
- C. Command Prompt
- D. System Information

Answer: A

Explanation:

Resource Monitor is a tool that shows the network activity of each process on a Windows machine, including the TCP connections and the sent and received bytes. Performance Monitor is a tool that shows the performance metrics of the system, such as CPU, memory, disk and network usage. Command Prompt is a tool that allows running commands and scripts on a Windows machine. System Information is a tool that shows the hardware and software configuration of a Windows machine. Verified References:

<https://www.comptia.org/blog/how-to-use-resource-monitor> <https://www.comptia.org/certifications/a>

NEW QUESTION 3

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

- A. High availability
- B. Regionally diverse backups
- C. On-site backups
- D. Incremental backups

Answer: B

Explanation:

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

NEW QUESTION 4

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

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

Answer: C

Explanation:

Incremental backup is a backup method that only backs up the files that have changed since the last backup, whether it was a full or an incremental backup. Incremental backup can save storage space and bandwidth, as it does not copy the same files over and over again. Incremental backup can also retain more versions of backups, as it only stores the changes made to the files. However, incremental backup can have longer restore times, as it requires restoring the last full backup and all the subsequent incremental backups in order to recover the data. The law firm is not concerned about restore times but asks the technician to retain more versions when possible, so incremental backup would be a suitable choice for them.

NEW QUESTION 5

Which of the following data is MOST likely to be regulated?

- A. Name in a Phone book
- B. Name on a medical diagnosis
- C. Name on a job application
- D. Name on a employer's website

Answer: B

Explanation:

A name on a medical diagnosis (B) is most likely to be regulated. This is because it falls under the category of protected health information (PHI), which is subject to regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. These regulations aim to protect the privacy and security of individuals' health information.

NEW QUESTION 6

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 7

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 8

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

- A. Stop code
- B. Event Mewer
- C. Services
- D. System Configuration

Answer: A

Explanation:

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

In this scenario, the user has encountered a BSOD and has restarted the PC, only to see the BSOD reappear. This suggests that the problem is persistent and

requires further investigation. By analyzing the stop code displayed on the BSOD, a technician can begin to identify the underlying issue and take appropriate actions to resolve it.

NEW QUESTION 9

A technician is troubleshooting a Windows 10 PC that is unable to start the GUI. A new SSD and a new copy of Windows were recently installed on the PC. Which of the following is the most appropriate command to use to fix the issue?

- A. msconfig
- B. chkdsk
- C. sfc
- D. diskpart
- E. mstsc

Answer: C

Explanation:

The sfc command is a tool for scanning and repairing system files that are corrupted or missing on Windows operating systems¹². System files are essential files that are required for the proper functioning of the operating system, such as the GUI, drivers, services, and applications. If system files are damaged or deleted, the operating system may fail to start or run properly, causing errors, crashes, or blue screens.

The sfc command can be used to fix the issue of the PC that is unable to start the GUI, assuming that the problem is caused by corrupted or missing system files. The sfc command can be run from the command prompt, which can be accessed by booting the PC from the installation media, choosing the repair option, and selecting the command prompt option³. The sfc command can be used with different switches, such as /scannow, /verifyonly, /scanfile, or /offbootdir, depending on the situation and the desired action⁴. The

most common switch is /scannow, which scans all the system files and repairs any problems that are found⁵. The syntax of the sfc command with the /scannow switch is: sfc /scannow

The sfc command will then scan and repair the system files, and display the results on the screen. If the sfc command is able to fix the system files, the PC should be able to start the GUI normally after rebooting. If the sfc command is unable to fix the system files, the PC may need further troubleshooting or a clean installation of Windows.

References¹: CompTIA A+ Certification Exam Core 2 Objectives, page 10 ²: CompTIA A+ Core 2 (220-1102) Complete Video Course, Lesson 26 Documentation ³: How to use SFC Scannow to repair Windows system files ⁴: SFC Command (System File Checker) ⁵: How to Repair Windows 10 using Command Prompt

NEW QUESTION 10

A user notices a small USB drive is attached to the user's computer after a new vendor visited the office. The technician notices two files named grabber.exe and output.txt. Which of the following attacks is MOST likely occurring?

- A. Trojan
- B. Rootkit
- C. Cryptominer
- D. Keylogger

Answer: D

Explanation:

A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote attacker. A keylogger can be used to steal passwords, credit card numbers, personal information, and other sensitive data. A keylogger can be delivered through a USB drive that contains a malicious executable file, such as grabber.exe, and an output file that stores the captured keystrokes, such as output.txt. The other options are not likely to use this method of attack. References: : <https://www.comptia.org/training/resources/exam-objectives/comptia-a-core-2-exam-objectives> : <https://www.kaspersky.com/resource-center/definitions/keylogger>

NEW QUESTION 10

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 14

A user reports a PC is running slowly. The technician suspects it has a badly fragmented hard drive. Which of the following tools should the technician use?

- A. resmon.exe
- B. msconfig.extf
- C. dfrgui.exe
- D. msmf32.exe

Answer: C

Explanation:

The technician should use dfrgui.exe to defragment the hard drive1

NEW QUESTION 16

A Linux technician needs a filesystem type that meets the following requirements:

- All changes are tracked.
- The possibility of file corruption is reduced.
- Data recovery is easy.

Which of the following filesystem types best meets these requirements?

- A. FAT32
- B. ext3
- C. exFAT
- D. NTFS

Answer: A

Explanation:

The ext3 file system is a Linux native file system that meets the requirements of the question. It has the following features:

? All changes are tracked. The ext3 file system uses a journaling mechanism that records all changes to the file system metadata in a special log called the journal before applying them to the actual file system. This ensures that the file system can be restored to a consistent state in case of a power failure or system crash12.

? The possibility of file corruption is reduced. The journaling feature of ext3 also reduces the possibility of file corruption, as it avoids the need for a full file system check after an unclean shutdown. The file system can be quickly replayed from the journal and any inconsistencies can be fixed12.

? Data recovery is easy. The ext3 file system supports undeletion of files using tools such as ext3grep or extundelete, which can scan the file system for deleted inodes and attempt to recover the data blocks associated with them34.

References:

- 1: Introduction to Linux File System [Structure and Types] - MiniTool1
- 2: 7 Ways to Determine the File System Type in Linux (Ext2, Ext3 or Ext4) - Tecmint3
- 3: How to Recover Deleted Files in Linux with ext3grep
- 4: How to Recover Deleted Files from ext3 Partitions

NEW QUESTION 17

A technician installed Windows 10 on a workstation. The workstation only has 3.5GB of usable RAM, even though the technician installed 8GB. Which of the following is the MOST likely reason this system is not utilizing all the available RAM?

- A. The system is missing updates.
- B. The systems utilizing a 32-bit OS.
- C. The system's memory is failing.
- D. The system requires BIOS updates.

Answer: B

Explanation:

The most likely reason that the system is not utilizing all the available RAM is that it is running a 32-bit OS. A 32-bit OS can only address up to 4GB of RAM, and some of that is reserved for hardware and system use1. Therefore, even if the technician installed 8GB of RAM, the system can only use around 3.5GB of usable RAM. To use the full 8GB of RAM, the technician would need to install a 64-bit OS, which can address much more memory2. The system missing updates, the system's memory failing, or the system requiring BIOS updates are not likely to cause this issue.

References: 2: <https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715> 1: <https://www.makeuseof.com/tag/unlock-64gb-ram-32-bit-windows-pae-patch/>

NEW QUESTION 21

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

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

Answer: B

Explanation:

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

NEW QUESTION 23

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 28

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 29

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

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

Answer: C

Explanation:

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

NEW QUESTION 32

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 36

A customer called the help desk to report that a machine that was recently updated is no longer working. The support technician checks the latest logs to see what updates were deployed, but nothing was deployed in more than three weeks. Which of the following should the support technician do to BEST resolve the situation?

- A. Offer to wipe and reset the device for the customer.
- B. Advise that the help desk will investigate and follow up at a later date.
- C. Put the customer on hold and escalate the call to a manager.
- D. Use open-ended questions to further diagnose the issue.

Answer: D

Explanation:

Open-ended questions are questions that require more than a yes or no answer and encourage the customer to provide more details and information. Using open-ended questions can help the support technician to understand the problem better, identify the root cause, and find a suitable solution.

Some examples of open-ended questions are:
? What exactly is not working on your machine?
? When did you notice the problem?
? How often does the problem occur?

? What were you doing when the problem happened?
? What have you tried to fix the problem?

Offering to wipe and reset the device for the customer is not a good option, as it may result in data loss and inconvenience for the customer. It should be used as a last resort only if other troubleshooting steps fail. Advising that the help desk will investigate and follow up at a later date is not a good option, as it may leave the customer unsatisfied and frustrated. It should be used only if the problem requires further research or escalation and cannot be resolved on the first call. Putting the customer on hold and escalating the call to a manager is not a good option, as it may waste time and resources. It should be used only if the problem is beyond the support technician's scope or authority and requires managerial intervention.

NEW QUESTION 40

Which of the following is the most likely reason a filtration system is critical for data centers?

- A. Plastics degrade over time.
- B. High humidity levels can rust metal.
- C. Insects can invade the data center.
- D. Dust particles can clog the machines.

Answer: B

Explanation:

A filtration system is critical for data centers because it can control the humidity and temperature levels in the environment. High humidity levels can cause condensation and corrosion on the metal components of the servers and other equipment, leading to malfunction and damage. A filtration system can also prevent dust, dirt, and other contaminants from entering the data center and clogging the machines or causing overheating.

NEW QUESTION 41

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

- A. gpupdate
- B. net use
- C. hostname
- D. dir

Answer: B

Explanation:

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

NEW QUESTION 42

An office is experiencing constant connection attempts to the corporate Wi-Fi. Which of the following should be disabled to mitigate connection attempts?

- A. SSID
- B. DHCP
- C. Firewall
- D. SSD

Answer: A

Explanation:

The SSID (Service Set Identifier) is the name of a wireless network that is broadcasted by the router or the Wi-Fi base station. The SSID helps nearby devices to identify and connect to the available networks. However, broadcasting the SSID also exposes the network to potential connection attempts from unauthorized or malicious users. Therefore, disabling the SSID can mitigate connection attempts by making the network invisible or hidden to the devices that are not already connected to it. To connect to a hidden network, the user would need to know the exact SSID and enter it manually. The other options are not related to mitigating connection attempts to the corporate Wi-Fi. DHCP (Dynamic Host Configuration Protocol) is a protocol that assigns IP addresses to the devices on a network. Firewall is a software or hardware device that filters the incoming and outgoing network traffic based on predefined rules. SSD (Solid State Drive) is a type of storage device that uses flash memory to store data. Disabling any of these options would not prevent connection attempts to the Wi-Fi network, and may cause other problems or issues for the network functionality and performance.

References:

- ? What is SSID + how to find (and change) it¹
- ? Choosing an SSID²
- ? SSID Meaning: Finding Your Network's Name³

NEW QUESTION 47

Which of the following features allows a technician to configure policies in a Windows 10 Professional desktop?

- A. gpedit
- B. gpmmc
- C. gpresult
- D. gpupdate

Answer: A

Explanation:

The feature that allows a technician to configure policies in a Windows 10 Professional desktop is gpedit. Gpedit is a command that opens the Local Group Policy Editor, which is a utility that allows users to view and modify local group policies on their Windows PC. Local group policies are a set of rules and settings that control the behavior and configuration of the system and its users. Local group policies can be used to configure policies such as security, network, software

installation and user rights. Gpmc is a command that opens the Group Policy Management Console, which is a utility that allows users to view and modify domain-based group policies on a Windows Server. Domain-based group policies are a set of rules and settings that control the behavior and configuration of the computers and users in a domain. Domain-based group policies are not available on a Windows 10 Professional desktop. Gpresult is a command that displays the result of applying group policies on a Windows PC. Gpresult can be used to troubleshoot or verify group policy settings but not to configure them. Gpupdate is a command that updates or refreshes the group policy settings on a Windows PC. Gpupdate can be used to apply new or changed group policy settings but not to configure them.

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

NEW QUESTION 48

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

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

Answer: B

Explanation:

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

NEW QUESTION 51

A user reports a virus is on a PC. The user installs additional real-time protection antivirus software, and the PC begins performing extremely slow. Which of the following steps should the technician take to resolve the issue?

- A. Uninstall one antivirus software program and install a different one.
- B. Launch Windows Update, and then download and install OS updates
- C. Activate real-time protection on both antivirus software programs
- D. Enable the quarantine feature on both antivirus software programs.
- E. Remove the user-installed antivirus software program.

Answer: E

Explanation:

Removing the user-installed antivirus software program is the best way to resolve the issue of extremely slow performance caused by installing additional real-time protection antivirus software on a PC. Having more than one antivirus software program running at the same time can cause conflicts, resource consumption and performance degradation. Uninstalling one antivirus software program and installing a different one, activating real-time protection on both antivirus software programs, enabling the quarantine feature on both antivirus software programs and launching Windows Update are not effective ways to resolve the issue. Verified References: <https://www.comptia.org/blog/why-you-shouldnt-run-multiple-antivirus-programs-at-the-same-time> <https://www.comptia.org/certifications/a>

NEW QUESTION 53

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

- A. Scanning the system with a Linux live disc, flashing the BIOS, and then returning the computer to service
- B. Flashing the BIOS, reformatting the drive, and then reinstalling the OS
- C. Degaussing the hard drive, flashing the BIOS, and then reinstalling the OS
- D. Reinstalling the OS
- E. flashing the BIOS, and then scanning with on-premises antivirus

Answer: B

Explanation:

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

NEW QUESTION 55**SIMULATION**

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

INSTRUCTIONS

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

- ? Index number of the Event Viewer issue
- ? First command to resolve the issue
- ? Second command to resolve the issue

BSOD

```
A problem has been detected and system has been shutdown to prevent damage to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this stop error screen, restart your computer. If this screen appears again,
follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware
or software manufacturer for any system updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as
caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to
select Advanced Startup Options, and then select Safe Mode.

Technical information:

*** STOP: 0x00000001 (0x00000008, 0x00000007, 0x00000000, 0xG74H2574)

*** strtl.sys - Address G74H2574 base at G74H0000, DateStamp 4eh2534df

Beginning dump of physical memory

Physical memory dump complete.

Contact your system administrator or technical support group for further assistance.
```

Commands:

BSOD | **Commands** | Event Viewer | System Error | Show Question | Reset All Answers

```
Select a command
Select a command
PS C:\> Get-WmiObject win32_computersystem
PS C:\> Get-WmiObject win32_logicaldisk
PS C:\> ls msvc*
PS C:\> ls
PS C:\> tasklist | sort
```

Event Viewer:

BSOD | Commands | **Event Viewer** | System Error | Show Question | Reset All Answers

Index	Time	EntryType	Source	InstanceID	Message
2191	Mar 03 10:35	Information	Service Control M...	1073748860	The Multimedia Class Scheduler service entered ...
2190	Mar 03 10:35	Error	Application Error	100	Application has encountered an internal error a...
2189	Mar 03 10:29	Information	Service Control M...	1073748860	The TCP/IP NetBIOS Helper service entered the r...
2188	Mar 03 10:29	Information	Service Control M...	1073748860	The Multimedia Class Scheduler service entered ...
2187	Mar 03 10:29	Information	Wainstaller	1033	Error Code 0: Windows Installer has successfull...
2186	Mar 03 10:29	Warning	DistributedCOM	10016	The application-specific permission settings do...
2185	Mar 03 10:29	Information	MEIx64	1074200578	Intel(R) Management Engine Interface driver has...
2184	Mar 03 10:29	Information	MEIx64	1074200578	Intel(R) Management Engine Interface driver has...

System Error:

BSOD | Commands | Event Viewer | **System Error** | Show Question | Reset All Answers



The program can't start because MSVCP100.dll is missing from your computer. Try reinstalling the program to fix this problem.

OK



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



The user is experiencing a system error that prevents them from using the Testing program. The error message indicates that the file MSVCP100.dll is missing from the computer. This file is part of the Microsoft Visual C++ 2010 Redistributable Package, which is required by some applications to run properly. The error may have occurred due to a corrupted or incomplete software deployment.

To resolve this issue, the user needs to restore the missing file and register it in the system. One possible way to do this is to copy the file from another computer that has the

Testing program installed and working, and then use the regsvr32 command to register it. The steps are as follows:

- ? On another computer (User-PC02) that has the Testing program installed and working, locate the file MSVCP100.dll in the folder C:\Program Files\Testing.
- ? Share the folder C:\Windows\System32 on User-PC02 by right-clicking on it, selecting Properties, then Sharing, then Advanced Sharing, then checking Share this folder, then clicking OK.
- ? On the user's computer (User-PC01), open a command prompt as an administrator by clicking Start, typing cmd, right-clicking on Command Prompt, and selecting Run as administrator.
- ? In the command prompt, type the following command to copy the file MSVCP100.dll from User-PC02 to User-PC01: copy "C:\Program Files\Testing\msvcp100.dll" "\\User-PC02\C\$\Windows\System32"
- ? After the file is copied, type the following command to register it in the system: regsvr32 msvc100.dll
- ? Restart the user's computer and try to run the Testing program again. Therefore, based on the instructions given by the user, the correct answers are: Select Event Viewer Issue: 2187
Select First Command: copy "C:\Program Files\Testing\msvcp100.dll" "\\User- PC02\C\$\Windows\System32"
Select Second Command: regsvr32 msvc100.dll

NEW QUESTION 57

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 60

A technician is troubleshooting application crashes on a Windows workstation. Each time the workstation user tries to open a website in a browser, the following message is displayed:

crypt32.d11 is missing not found

Which of the following should the technician attempt FIRST?

- A. Rebuild Windows profiles.
- B. Reimage the workstation
- C. Roll back updates
- D. Perform a system file check

Answer: D

Explanation:

If this file is missing or corrupted, it can cause application crashes or errors when trying to open websites in a browser. To fix this, the technician can perform a system file check, which is a utility that scans and repairs corrupted or missing system files. To perform a system file check, the technician can follow these steps:

- ? Open the Command Prompt as an administrator. To do this, type cmd in the search box on the taskbar, right-click on Command Prompt, and select Run as administrator.
- ? In the Command Prompt window, type sfc /scannow and hit Enter. This will start the scanning and repairing process, which may take some time.
- ? Wait for the process to complete. If any problems are found and fixed, you will see a message saying Windows Resource Protection found corrupt files and successfully repaired them. If no problems are found, you will see a message saying Windows Resource Protection did not find any integrity violations.
- ? Restart your computer and check if the issue is resolved.

NEW QUESTION 63

Which of the following is also known as something you know, something you have, and something you are?

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

Answer: B

Explanation:

MFA stands for Multi-Factor Authentication, which is a method of verifying a user's identity using two or more different factors of authentication. The three factors of authentication are something you know, something you have, and something you are. These factors correspond to different types of information or evidence that only the legitimate user should possess or provide. For example:

- ? Something you know: a password, a PIN, a security question, etc.
- ? Something you have: a smart card, a token, a mobile device, etc.
- ? Something you are: a fingerprint, a face, an iris, etc.

MFA provides a higher level of security than single-factor authentication, which only uses one factor, such as a password. MFA reduces the risk of unauthorized access, identity theft, and data breaches, as an attacker would need to compromise more than one factor to impersonate a user. MFA is commonly used for online banking, email accounts, cloud services, and other sensitive applications

NEW QUESTION 64

While trying to repair a Windows 10 OS, a technician receives a prompt asking for a key. The technician tries the administrator password, but it is rejected. Which of the following does the technician need in order to continue the OS repair?

- A. SSL key
- B. Preshared key
- C. WPA2 key
- D. Recovery key

Answer: D

Explanation:

A recovery key is a code that can be used to unlock a BitLocker-encrypted drive when the normal authentication methods (such as password or PIN) are not available or have been forgotten. BitLocker is a feature of Windows that encrypts the entire drive to protect data from unauthorized access. If a technician is trying to repair a Windows 10 OS that has BitLocker enabled, they will need the recovery key to access the drive and continue the OS repair. SSL key, preshared key, and WPA2 key are not keys that are related to BitLocker or OS repair.

NEW QUESTION 69

A technician downloads a validated security tool and notes the vendor hash of a58e87a2. When the download is complete, the technician again validates the hash, but the value returns as 2a876a7d3. Which of the following is the MOST likely cause of the issue?

- A. Private-browsing mode
- B. Invalid certificate
- C. Modified file
- D. Browser cache

Answer: C

Explanation:

The most likely cause of the issue of having different hash values for a downloaded security tool is a modified file. A hash value is a unique and fixed-length string that is

generated from an algorithm that processes data or files. A hash value can be used to verify the integrity and authenticity of data or files by comparing it with a known or expected value. If the hash values do not match, it means that the data or file has been altered or corrupted in some way. A modified file may result from intentional or unintentional changes, such as editing, encryption, compression or malware infection. Private-browsing mode is a feature that allows users to browse the web without storing any browsing history, cookies or cache on their browser. Private-browsing mode does not affect the hash value of a downloaded file but only how the browser handles user data. Invalid certificate is an error that occurs when a website or a server does not have a valid or trusted digital certificate that proves its identity and secures its communication. Invalid certificate does not affect the hash value of a downloaded file but only how the browser verifies the website or server's credibility. Browser cache is a temporary storage that stores copies of web pages, images and other content that users have visited on their browser.

NEW QUESTION 72

A technician is working with a company to determine the best way to transfer sensitive personal information between offices when conducting business. The company currently uses USB drives and is resistant to change. The company's compliance officer states that all media at rest must be encrypted. Which of the following would be the BEST way to secure the current workflow?

- A. Deploy a secondary hard drive with encryption on the appropriate workstation
- B. Configure a hardened SFTP portal for file transfers between file servers
- C. Require files to be individually password protected with unique passwords
- D. Enable BitLocker To Go with a password that meets corporate requirements

Answer: D

Explanation:

The BEST way to secure the current workflow of transferring sensitive personal information between offices when conducting business is to enable BitLocker To Go with a password that meets corporate requirements. This is because BitLocker To Go is a full-disk encryption feature that encrypts all data on a USB drive, which is what the company currently uses, and requires a password to access the data.

NEW QUESTION 77

A company is deploying mobile phones on a one-to-one basis, but the IT manager is concerned that users will root/jailbreak their phones. Which of the following technologies can be implemented to prevent this issue?

- A. Signed system images
- B. Antivirus
- C. SSO
- D. MDM

Answer: D

Explanation:

MDM stands for Mobile Device Management, and it is a way of remotely managing and securing mobile devices that are used for work purposes¹. MDM can enforce policies and restrictions on the devices, such as preventing users from installing unauthorized apps, modifying system settings, or accessing root privileges². MDM can also monitor device status, wipe data, lock devices, or locate lost or stolen devices¹.

NEW QUESTION 79

A homeowner recently moved and requires a new router for the new ISP to function correctly. The internet service has been installed and has been confirmed as functional. Which of the following is the FIRST step the homeowner should take after installation of all relevant cabling and hardware?

- A. Convert the PC from a DHCP assignment to a static IP address.
- B. Run a speed test to ensure the advertised speeds are met.
- C. Test all network sharing and printing functionality the customer uses.
- D. Change the default passwords on new network devices.

Answer: D

Explanation:

When a homeowner moves and sets up a new router for the new ISP it is important to take appropriate security measures to protect their network from potential security threats. The FIRST step that the homeowner should take after installation of all relevant cabling and hardware is to change the default passwords on new network devices. Most modern routers come with default usernames and passwords that are widely known to potential attackers. If these defaults are not changed, it could make it easier for external attackers to gain unauthorized access to the network. Changing the passwords on new network devices is a simple but effective way to improve the security posture of the network.

NEW QUESTION 81

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. Device Manager
- D. Administrative Tools

Answer: D

NEW QUESTION 85

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

- A. Quarantine the computer.
- B. Use a previous restore point.
- C. Educate the end user about viruses.
- D. Download the latest virus definitions.

Answer: D

Explanation:

The first step in removing a virus from a computer is to update the antivirus software with the latest virus definitions. Virus definitions are files that contain information about the characteristics and behavior of known viruses and malware. They help the antivirus software to identify and remove the malicious threats from the computer. Without the latest virus definitions, the antivirus software may not be able to detect or remove the virus that infected the user's computer. Therefore, the technician should download the latest virus definitions from the antivirus vendor's website or use the update feature in the antivirus program before scanning the computer for viruses.

References:

- ? How to remove malware or viruses from my Windows 10 PC, section 21
- ? How to Remove a Virus From a Computer in 2023, section 32
- ? The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2193

NEW QUESTION 89

Which of the following options should MOST likely be considered when preserving data from a hard drive for forensic analysis? (Select TWO).

- A. Licensing agreements
- B. Chain of custody
- C. Incident management documentation
- D. Data integrity
- E. Material safety data sheet
- F. Retention requirements

Answer: B

Explanation:

Chain of custody and data integrity are two options that should most likely be considered when preserving data from a hard drive for forensic analysis. Chain of custody refers to the documentation and tracking of who has access to the data and how it is handled, stored, and transferred. Data integrity refers to the assurance that the data has not been altered, corrupted, or tampered with during the preservation process

NEW QUESTION 93

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

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

Answer: D

Explanation:

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

NEW QUESTION 97

A user's corporate phone was stolen, and the device contains company trade secrets. Which of the following technologies should be implemented to mitigate this risk? (Select TWO).

- A. Remote wipe
- B. Firewall
- C. Device encryption
- D. Remote backup
- E. Antivirus
- F. Global Positioning System

Answer: AC

Explanation:

Remote wipe is a feature that allows data to be deleted from a device or system remotely by an administrator or owner¹. It is used to protect data from being compromised if the device is lost, stolen, or changed hands¹. Device encryption is a feature that helps protect the data on a device by making it unreadable to unauthorized users². It requires a key or a password to access the data². Both features can help mitigate the risk of losing company trade secrets if a corporate phone is stolen.

References: 1: How to remote wipe Windows laptop (<https://www.thewindowsclub.com/remote-wipe-windows-10>) 2: Device encryption in Windows (<https://support.microsoft.com/en-us/windows/device-encryption-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d>)

NEW QUESTION 100

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 105

A user reports a workstation has been performing strangely after a suspicious email was opened on it earlier in the week. Which of the following should the technician perform FIRST?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

When a user reports that their workstation is behaving strangely after opening a suspicious email, the first step a technician should take is to run a virus scan on the computer. This is because opening a suspicious email is a common way for viruses and malware to infect a computer. Running a virus scan can help identify and remove any infections that may be causing the computer to behave strangely.

NEW QUESTION 106

A user's application is unresponsive. Which of the following Task Manager tabs will allow the user to address the situation?

- A. Performance
- B. Startup
- C. Application history
- D. Processes

Answer: D

Explanation:

The Processes tab in the Task Manager shows all the running processes on the computer, including applications and background services. The user can use this tab to identify the unresponsive application and end its process by right-clicking on it and selecting End task. This will free up the system resources and close the application. The other tabs in the Task Manager do not allow the user to address the situation. The Startup tab shows the programs that run when the computer starts, the Performance tab shows the system resource usage and statistics, and the Application history tab shows the resource usage of the applications over time

NEW QUESTION 107

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

```

Hostname:      corp-laptop-222
IP Address:    192.168.0.45
Gateway:      192.168.1.1
Subnet Mask:   255.255.252.0
Open Ports:   21, 22, 80, 443
    
```

Which of the following should the technician do to connect via RDP?

- A. Confirm the user can ping the default gateway.
- B. Change the IP address on the user's laptop.
- C. Change the subnet mask on the user's laptop.
- D. Open port 3389 on the Windows firewall.

Answer: D

Explanation:

In order to connect to a user's laptop via RDP, the technician should open port 3389 on the Windows firewall. This is because RDP uses port 3389 for communication^{1,2}. The other options are not necessary or relevant for establishing an RDP connection.

? Confirming the user can ping the default gateway is not required for RDP, as it

only tests the network connectivity between the user's laptop and the router. RDP works over the internet, so the technician should be able to ping the user's laptop directly using its IP address³.

? Changing the IP address on the user's laptop is not needed for RDP, as long as

the IP address is valid and not conflicting with another device on the network. The user's laptop has a valid IP address of 192.168.0.45, which belongs to the same subnet as the gateway (192.168.0.1) and the subnet mask (255.255.255.0)⁴.

? Changing the subnet mask on the user's laptop is not required for RDP, as long as

the subnet mask matches the network configuration. The user's laptop has a correct subnet mask of 255.255.255.0, which defines a network with 254 possible hosts⁴.

References:

- 1: [What is RDP and How Does It Work? - CompTIA]
- 2: CompTIA A+ Certification Exam Core 2 Objectives - CompTIA
- 3: [Ping (networking utility) - Wikipedia]
- 4: [IP address - Wikipedia] : What is RDP and How Does It Work? - CompTIA : CompTIA A+ Certification Exam Core 2 Objectives - CompTIA : Ping (networking utility) - Wikipedia) : IP address - Wikipedia

NEW QUESTION 111

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 113

An organization is updating the monitors on kiosk machines. While performing the upgrade, the organization would like to remove physical input devices. Which of the following utilities in the Control Panel can be used to turn on the on-screen keyboard to replace the physical input devices?

- A. Devices and Printers
- B. Ease of Access
- C. Programs and Features
- D. Device Manager

Answer: B

Explanation:

Ease of Access is a utility in the Control Panel that allows users to adjust various accessibility settings on Windows, such as the on-screen keyboard, magnifier, narrator, high contrast, etc. The on-screen keyboard can be turned on by going to Ease of Access > Keyboard and toggling the switch to On12. Alternatively, the on-screen keyboard can be opened by pressing Windows + Ctrl + O keys or by typing osk.exe in the Run dialog box3.

References: 1 Use the On-Screen Keyboard (OSK) to type(<https://support.microsoft.com/en-us/windows/use-the-on-screen-keyboard-osk-to-type-ecbb5e08-5b4e-d8c8-f794-81dbf896267a>)2 How to Enable or Disable the On-Screen Keyboard in Windows 10 - Lifewire(<https://www.lifewire.com/enable-or-disable-on-screen-keyboard-in-windows-10-5180667>)3 On-Screen Keyboard Settings, Tips and Tricks in Windows 11/10(<https://www.thewindowsclub.com/windows-onscreen-keyboard>).

NEW QUESTION 114

A developer's Type 2 hypervisor is performing inadequately when compiling new source code. Which of the following components should the developer upgrade to improve the hypervisor's performance?

- A. Amount of system RAM
- B. NIC performance
- C. Storage IOPS
- D. Dedicated GPU

Answer: A

Explanation:

The correct answer is A. Amount of system RAM. A Type 2 hypervisor is a virtualization software that runs on top of a host operating system, which means it shares the system resources with the host OS and other applications. Therefore, increasing the amount of system RAM can improve the performance of the hypervisor and the virtual machines running on it. RAM is used to store data and instructions that are frequently accessed by the CPU, and having more RAM can reduce the need for swapping data to and from the storage device, which is slower than RAM.

NIC performance, storage IOPS, and dedicated GPU are not as relevant for improving the hypervisor's performance in this scenario. NIC performance refers to the speed and quality of the network interface card, which is used to connect the computer to a network. Storage IOPS refers to the number of input/output operations per second that can be performed by the storage device, which is a measure of its speed and efficiency. Dedicated GPU refers to a separate graphics processing unit that can handle complex graphics tasks, such as gaming or video editing. These components may affect other aspects of the computer's performance, but they are not directly related to the hypervisor's ability to compile new source code.

NEW QUESTION 117

The network was breached over the weekend System logs indicate that a single user's account was successfully breached after 500 attempts with a dictionary attack. Which of the following would BEST mitigate this threat?

- A. Encryption at rest
- B. Account lockout
- C. Automatic screen lock
- D. Antivirus

Answer: B

Explanation:

Account lockout would best mitigate the threat of a dictionary attack1

NEW QUESTION 120

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 123

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 124

A technician is setting up a newly built computer. Which of the following is the fastest way for the technician to install Windows 10?

- A. Factory reset
- B. System Restore
- C. In-place upgrade
- D. Unattended installation

Answer: D

Explanation:

Windows 10



The correct answer is D. Unattended installation. An unattended installation is a way of installing Windows 10 without requiring any user input or interaction. It uses a configuration file called answer file that contains the settings and preferences for the installation, such as the product key, language, partition, and network settings. An unattended installation can be performed by using a bootable USB flash drive or DVD that contains the Windows 10 installation files and the answer file¹. This is the fastest way for the technician to install Windows 10 on a newly built computer, as it automates the whole process and saves time. A factory reset is a way of restoring a computer to its original state by deleting all the data and applications and reinstalling the operating system. A factory reset can be performed by using the recovery partition or media that came with the computer, or by using the Reset this PC option in Windows 10 settings². A factory reset is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system to be present.

A system restore is a way of undoing changes to a computer's system files and settings by using a restore point that was created earlier. A system restore can be performed by using the System Restore option in Windows 10 settings or by using the Advanced Startup Options menu³. A system restore is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system and restore points to be present.

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

NEW QUESTION 127

An Android user reports that when attempting to open the company's proprietary mobile application it immediately closes. The user states that the issue persists, even after rebooting the phone. The application contains critical information that cannot be lost. Which of the following steps should a systems administrator attempt FIRST?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The systems administrator should clear the application cache¹

If clearing the application cache does not work, the systems administrator should uninstall and reinstall the application²

Resetting the phone to factory settings is not necessary at this point²

Installing an alternative application with similar functionality is not necessary at this point²

NEW QUESTION 131

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 all 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 135

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 138

A user installed a new application that automatically starts each time the user logs in to a Windows 10 system. The user does not want this to happen and has asked for this setting to be changed. Which of the following tools would the technician MOST likely use to safely make this change?

- A. Mastered
- B. Not Mastered

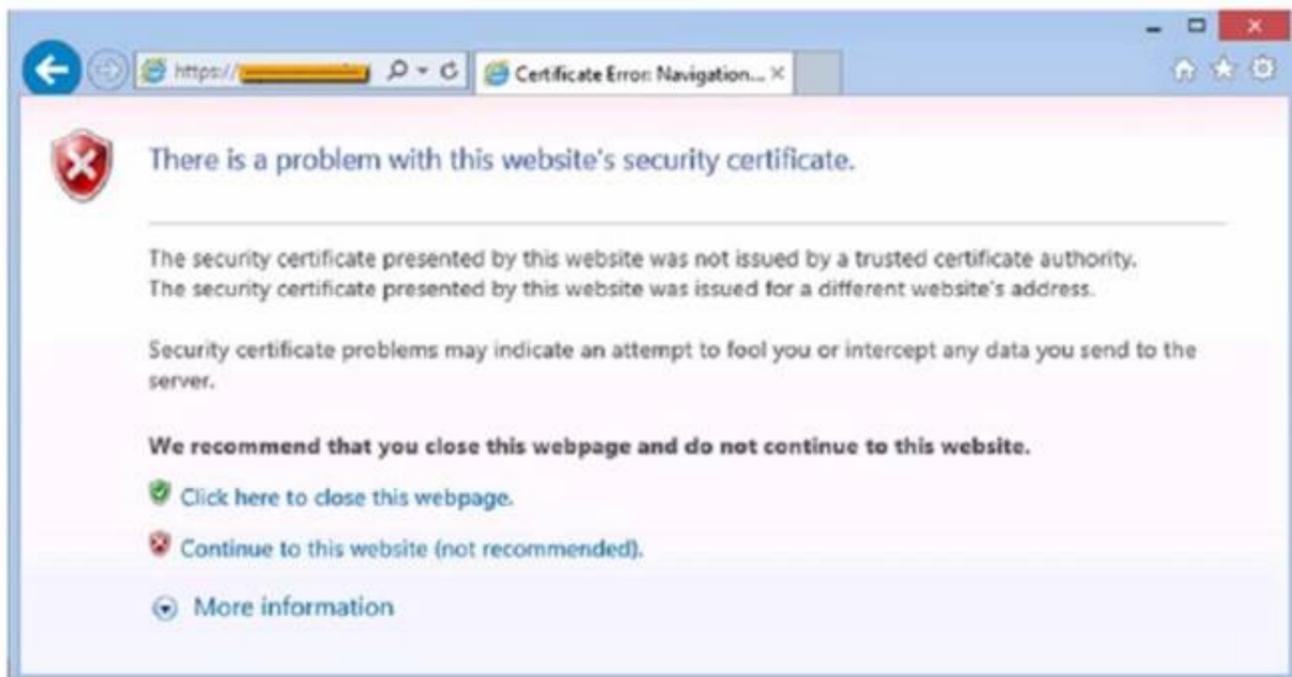
Answer: A

Explanation:

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

NEW QUESTION 142

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



The CFO then reported the incident to a technician. The link is purportedly to the organization's bank. Which of the following should the technician perform FIRST?

- A. Update the browser's CRLs
- B. File a trouble ticket with the bank.
- C. Contact the ISP to report the CFO's concern
- D. Instruct the CFO to exit the browser

Answer: A

Explanation:

The technician should update the browser's CRLs first. The error message indicates that the certificate revocation list (CRL) is not up to date. Updating the CRLs will ensure that the browser can verify the authenticity of the bank's website.

NEW QUESTION 146

Which of the following protocols supports fast roaming between networks?

- A. WEP
- B. WPA
- C. WPA2
- D. LEAP
- E. PEAP

Answer: B

Explanation:

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

References:

- ? The Official CompTIA A+ Core 2 Study Guide², page 263.
- ? WiFi Fast Roaming, Simplified³

NEW QUESTION 147

A user wants to acquire antivirus software for a SOHO PC. A technician recommends a licensed software product, but the user does not want to pay for a license. Which of the following license types should the technician recommend?

- A. Corporate
- B. Open-source
- C. Personal
- D. Enterprise

Answer: B

Explanation:

Open-source software is software that has its source code available for anyone to inspect, modify, and distribute. Open-source software is usually free of charge and does not require a license to use. Some examples of open-source antivirus software are ClamAV, Comodo, and Immunit12. The other license types are either suitable for a SOHO PC. Corporate and enterprise licenses are designed for large-scale organizations and networks, and they usually require a subscription fee. Personal licenses are for individual users and may have limited features or support.

References: 1 What is Open Source Software? - Definition from Techopedia(<https://www.tomsguide.com/us/best-antivirus,review-2588.html>). 2 7 Best Lifetime License Antivirus Tools [2023 Guide] - Windows Report(<https://windowsreport.com/antivirus-with-unlimited-validity/>).

NEW QUESTION 149

A user's antivirus software reports an infection that it is unable to remove. Which of the following is the most appropriate way to remediate the issue?

- A. Disable System Restore.
- B. Utilize a Linux live disc.
- C. Quarantine the infected system.
- D. Update the anti-malware.

Answer: C

Explanation:

Quarantining the infected system is the most appropriate way to remediate the issue of an infection that the antivirus software cannot remove. Quarantining means isolating the system from the network and other devices to prevent the infection from spreading or causing further damage. Quarantining also allows the technician to perform further analysis and removal of the infection without risking the security of other systems or data.

Some of the steps involved in quarantining an infected system are:

- ? Disconnect the system from the internet and any local network connections, such as Wi-Fi, Ethernet, Bluetooth, or USB.
- ? Disable any file-sharing or remote access services on the system, such as Windows File Sharing, Remote Desktop, or TeamViewer.
- ? Use a separate device to download and update the antivirus software and any other tools that may be needed to remove the infection, such as malware scanners, rootkit removers, or bootable rescue disks.
- ? Transfer the updated antivirus software and tools to the infected system using a removable media, such as a CD, DVD, or USB flash drive. Scan the removable media for any infections before and after using it on the infected system.
- ? Run the antivirus software and tools on the infected system and follow the instructions to delete or quarantine the infection. If the infection is persistent or complex, it may require booting the system from a rescue disk or using a Linux live disc to access and clean the system files.
- ? After the infection is removed, restore the system to a previous clean state using System Restore, backup, or recovery partition. Scan the system again to ensure that it is clean and secure. Reconnect the system to the network and update the system and the antivirus software.

References:

- ? How to Identify and Repair Malware or Virus Infected Computers, section 31
- ? Uninstalling Antivirus Software, the Clean Way: 40 Removal Tools & Instructions, section 22
- ? How to manually remove an infected file from a Windows computer³
- ? The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2194

NEW QUESTION 151

A technician is editing the hosts file on a few PCs in order to block certain domains. Which of the following would the technician need to execute after editing the hosts file?

- A. Enable promiscuous mode.
- B. Clear the browser cache.
- C. Add a new network adapter.
- D. Reset the network adapter.

Answer: D

Explanation:

Resetting the network adapter is the best way to apply the changes made to the hosts file on a few PCs. The hosts file is a text file that maps hostnames to IP addresses and can be used to block certain domains by redirecting them to invalid or local addresses. Resetting the network adapter will clear the DNS cache and force the PC to use the new entries in the hosts file.

NEW QUESTION 155

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

"The user thought the company-provided antivirus software would prevent this issue." The most likely steps to resolve the issue are to deploy an ad-blocking extension to the browser and perform a reset on the user's web browser. Ad-blocking extensions can help to prevent pop-ups and other unwanted content from appearing in the browser, and resetting the browser can help to remove any malicious extensions or settings that may be causing the issue.

NEW QUESTION 156

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

- A. .exe
- B. .dmg
- C. .app
- D. .rpm
- E. .pkg

Answer: C

Explanation:

app files are application bundles that contain all the necessary files and resources for a Mac app. They can be easily deleted by dragging them to the Trash or using Launchpad¹². Other file types, such as .exe, .dmg, .rpm, and .pkg, are either not compatible with macOS or require additional steps to uninstall³⁴.
References: 1 Uninstall apps on your Mac - Apple Support(<https://support.apple.com/en-us/102610>)² How to Uninstall Apps on a Mac (and Make Sure Leftover Files Are ...(<https://www.pcmag.com/how-to/uninstall-delete-apps-from-mac>)³ How to install and uninstall software on a Mac - Laptop Mag(<https://www.laptopmag.com/articles/install-uninstall-mac-software>)⁴ How to completely uninstall an app on a Mac and delete all junk files(<https://www.xda-developers.com/how-to-uninstall-app-mac/>).

NEW QUESTION 158

Which of the following macOS utilities uses AES-128 to encrypt the startup disk?

- A. fdisk
- B. Diskpart
- C. Disk Utility
- D. FileVault

Answer: D

Explanation:

FileVault is a macOS utility that uses AES-128 (Advanced Encryption Standard) to encrypt the startup disk of a Mac computer. It protects the data from unauthorized access if the computer is lost or stolen. fdisk and Diskpart are disk partitioning utilities for Linux and Windows, respectively. Disk Utility is another macOS utility that can perform disk management tasks, such as formatting, resizing, repairing, etc. Verified References: <https://www.comptia.org/blog/what-is-filevault> <https://www.comptia.org/certifications/a>

NEW QUESTION 163

A user notices a small USB drive is attached to the user's computer after a new vendor visited the office. The technician notices two files named grabber.exe and output.txt. Which of the following attacks is MOST likely occurring?

- A. Trojan
- B. Rootkit
- C. Cryptominer
- D. Keylogger

Answer: D

Explanation:

A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote attacker¹. The attacker can use the captured information to steal passwords, credit card numbers, or other sensitive data. A keylogger can be installed on a computer by attaching a small USB drive that contains a malicious executable file, such as grabber.exe². The output.txt file may contain the recorded keystrokes. The user should remove the USB drive and scan the computer for malware.

References: ²: What is grabber.exe? (<https://www.freefixer.com/library/file/grabber.exe-55857/>) ¹: What is a keylogger? (<https://www.kaspersky.com/resource-center/definitions/keylogger>)

NEW QUESTION 167

A technician needs to transfer a file to a user's workstation. Which of the following would BEST accomplish this task utilizing the workstation's built-in protocols?

A.

VPN

- B. SMB
- C. RMM
- D. MSRA

Answer: B

Explanation:

SMB stands for Server Message Block, which is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network. SMB is a built-in protocol in Windows operating systems and can be used to transfer files between computers over a network. The technician can use SMB to access a file share on the user's workstation and copy the file to or from it. VPN stands for virtual private network, which is a technology that creates a secure and encrypted connection over a public network. VPN is not a built-in protocol in Windows operating systems and does not directly transfer files between computers. RMM stands for remote monitoring and management, which is a type of software solution that allows remote management and monitoring of devices and networks. RMM is not a built-in protocol in Windows operating systems and does not directly transfer files between computers. MSRA stands for Microsoft Remote Assistance, which is a feature that allows a user to invite another user to view or control their computer remotely. MSRA is not a protocol, but an application that uses Remote Desktop Protocol (RDP) to establish a connection. MSRA does not directly transfer files between computers. <https://www.pcmag.com/picks/the-best-desktop-workstations>

NEW QUESTION 172

Which of the following would MOST likely be used to change the security settings on a user's device in a domain environment?

- A. Security groups
- B. Access control list

- C. Group Policy
- D. Login script

Answer: C

Explanation:

Group Policy is the most likely tool to be used to change the security settings on a user's device in a domain environment. Group Policy is a feature of Windows that allows administrators to manage and configure settings for multiple devices and users in a centralized way. Group Policy can be used to enforce security policies such as password

complexity, account lockout, firewall rules, encryption settings, etc.

NEW QUESTION 173

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

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

Answer: B

Explanation:

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

NEW QUESTION 175

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 180

A technician is setting up a SOHO wireless router. The router is about ten years old. The customer would like the most secure wireless network possible. Which of the following should the technician configure?

- A. WPA2 with TKIP
- B. WPA2 with AES
- C. WPA3 with AES-256
- D. WPA3 with AES-128

Answer: B

Explanation:

This is because WPA2 with AES is the most secure wireless network configuration that is available on a ten-year-old SOHO wireless router.

NEW QUESTION 181

A technician has identified malicious traffic originating from a user's computer. Which of the following is the best way to identify the source of the attack?

- A. Investigate the firewall logs.
- B. Isolate the machine from the network.
- C. Inspect the Windows Event Viewer.
- D. Take a physical inventory of the device.

Answer: B

Explanation:

Isolating the machine from the network is the best way to identify the source of the attack, because it prevents the malicious traffic from spreading to other devices or reaching the attacker. Isolating the machine can also help preserve the evidence of the attack, such as the malware files, the network connections, the registry entries, or the system logs. By isolating the machine, a technician can safely analyze the machine and determine the source of the attack, such as a phishing email, a compromised website, a removable media, or a network vulnerability.

NEW QUESTION 184

A technician is troubleshooting boot times for a user. The technician attempts to use MSConfig to see which programs are starting with the OS but receives a message that it can no longer be used to view startup items. Which of the following programs can the technician use to view startup items?

- A. msinfo32
- B. perfmon
- C. regedit
- D. taskmgr

Answer: D

Explanation:

When troubleshooting boot times for a user, a technician may want to check which programs are starting with the operating system to identify any that may be slowing down the boot process. MSConfig is a tool that can be used to view startup items on a Windows system, but it may not always be available or functional. In this scenario, the technician receives a message that MSConfig cannot be used to view startup items. As an alternative, the technician can use Task Manager (taskmgr), which can

also display the programs that run at startup. To access the list of startup items in Task Manager, the technician can follow these steps:

- ? Open Task Manager by pressing Ctrl+Shift+Esc.
- ? Click the "Startup" tab.
- ? The list of programs that run at startup will be displayed.

NEW QUESTION 188

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 192

A neighbor successfully connected to a user's Wi-Fi network. Which of the following should the user do after changing the network configuration to prevent the neighbor from being able to connect again?

- A. Disable the SSID broadcast.
- B. Disable encryption settings.
- C. Disable DHCP reservations.
- D. Disable logging.

Answer: A

Explanation:

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

NEW QUESTION 195

A user is setting up a new Windows 10 laptop. Which of the following Windows settings should be used to input the SSID and password?

- A.

Network & Internet

- B. System
- C. Personalization
- D. Accounts

Answer: A

Explanation:

The Network & Internet settings in Windows 10 allow the user to input the SSID and password of a Wi-Fi network, as well as manage other network-related options, such as airplane mode, mobile hotspot, VPN, proxy, etc¹. To access the Network & Internet settings, the user can select the Start button, then select Settings > Network & Internet². Alternatively, the user can right-click the Wi-Fi icon on the taskbar and click "Open Network & Internet Settings"³.

The System settings in Windows 10 allow the user to configure the display, sound, notifications, power, storage, and other system-related options¹. The Personalization settings in Windows 10 allow the user to customize the background, colors, lock screen, themes, fonts, and other appearance-related options¹. The Accounts settings in Windows 10 allow the user to manage the user accounts, sign-in options, sync settings, and other account-related options¹. None of these settings can be used to input the SSID and password of a Wi-Fi network.

References:

? The Official CompTIA A+ Core 2 Study Guide¹, page 221, 222, 223, 224.

NEW QUESTION 197

A technician is setting up a newly built computer. Which of the following is the fastest way for the technician to install Windows 10?

- A. Factory reset
- B. System Restore
- C. In-place upgrade
- D. Unattended installation

Answer: D

Explanation:

An unattended installation is a method of installing Windows 10 that does not require any user input or interaction during the installation process. An unattended installation can be performed by using an answer file, which is a file that contains all the configuration settings and preferences for the installation, such as the product key, the language, the partition size, and the user accounts. An unattended installation can be the fastest way to install Windows 10, as it automates and streamlines the installation process. Factory reset, System Restore, and in-place upgrade are not methods of installing Windows 10.

NEW QUESTION 201

A technician is setting up a backup method on a workstation that only requires two sets of

tapes to restore. Which of the following would BEST accomplish this task?

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

Answer: D

Explanation:

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

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

NEW QUESTION 205

A macOS user reports seeing a spinning round cursor on a program that appears to be frozen. Which of the following methods does the technician use to force the program to close in macOS?

- A. The technician presses the Ctrl+Alt+Del keys to open the Force Quit menu, selects the frozen application in the list, and clicks Force Quit.
- B. The technician clicks on the frozen application and presses and holds the Esc key on the keyboard for 10 seconds Which causes the application to force quit.
- C.

The technician opens Finder, navigates to the Applications folder, locates the application that is frozen in the list, right-clicks on the application, and selects the Force Quit option.

D. The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit.

Answer: D

Explanation:

The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit. This is the most common method of force quitting a program in macOS. This can be done by clicking on the Apple icon in the top left of the screen, selecting Force Quit, selecting the frozen application in the list, and then clicking Force Quit. This will force the application to quit and the spinning round cursor will disappear.

NEW QUESTION 209

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 214

An engineer is configuring a new server that requires a bare-metal installation. Which of the following installation methods should the engineer use if installation media is not available on site?

- A. Image deployment
- B. Recovery partition installation
- C. Remote network installation
- D. Repair installation

Answer: C

Explanation:

Remote network installation is the best option for configuring a new server that requires a bare-metal installation without installation media on site. A remote network installation is a method of installing an operating system or an application over a network connection, such as LAN, WAN, or Internet. A remote network installation can use various protocols, such as PXE, HTTP, FTP, or SMB, to access the installation files from a server or a cloud service. A remote network installation can also use various tools, such as Windows Deployment Services, Microsoft Deployment Toolkit, or Red Hat Kickstart, to automate and customize the installation process. A remote network installation can save time and resources by eliminating the need for physical media and allowing centralized management of multiple installations. Image deployment, recovery partition installation, and repair installation are not correct answers for this question. Image deployment is a method of installing an operating system or an application by copying a preconfigured image file to a target device. Image deployment requires an existing image file and a compatible device. Recovery partition installation is a method of restoring an operating system or an application from a hidden partition on the hard disk that contains the original factory settings. Recovery partition installation requires an existing recovery partition and a functional hard disk. Repair installation is a method of fixing an operating system or an application that is corrupted or damaged by replacing or repairing the system files without affecting the user data or settings. Repair installation requires an existing operating system or application and a working device. References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 16

? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 106

NEW QUESTION 218

A SOHO client is having trouble navigating to a corporate website. Which of the following should a technician do to allow access?

- A. Adjust the content filtering.
- B. Unmap port forwarding.
- C. Disable unused ports.
- D. Reduce the encryption strength

Answer: A

Explanation:

Content filtering is a process that manages or screens access to specific emails or webpages based on their content categories¹. Content filtering can be used by organizations to control content access through their firewalls and enforce corporate policies around information system management². A SOHO client may have content filtering enabled on their network and may need to adjust it to allow access to a corporate website that is blocked by default. The client can use a software program, a hardware device, or a subscription service to configure the content filtering settings and whitelist the desired website².

References: 1: Web content filtering (<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-worldwide>) 2: What is Content Filtering? Definition and Types of Content Filters (<https://www.fortinet.com/resources/cyberglossary/content-filtering>)

NEW QUESTION 223

A user has been unable to receive emails or browse the internet from a smartphone while traveling. However, text messages and phone calls are working without issue. Which of the following should a support technician check FIRST?

- A. Mobile OS version
- B. User account status
- C. Data plan coverage
- D. Network traffic outages

Answer: C

Explanation:

The first thing that a support technician should check to resolve the issue of not being able to receive emails or browse the internet from a smartphone while traveling is the data plan coverage. The data plan coverage determines how much data and where the user can use on the smartphone's cellular network. The data plan coverage may vary depending on the user's location, carrier and subscription. The data plan coverage may not include or support certain areas or countries that the user is traveling to, or may charge extra fees or limit the speed or amount of data that the user can use. The data plan coverage does not affect text messages and phone calls, which use different network services and protocols. User account status is not likely to cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, unless the user account has been suspended or terminated by the carrier or the email provider. Mobile OS version is not likely to cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, unless the mobile OS has a major bug or compatibility problem with the network or the email app. Network traffic outages may cause the issue of not being able to receive emails or browse the internet from a smartphone while traveling, but they are less likely and less common than data plan coverage issues, and they should also affect text messages and phone calls. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.5

NEW QUESTION 226

A user updates a mobile device's OS. A frequently used application becomes consistently unresponsive immediately after the device is launched. Which of the following troubleshooting steps should the user perform FIRST?

- A. Delete the application's cache.
- B. Check for application updates.
- C. Roll back the OS update.
- D. Uninstall and reinstall the application.

Answer: B

Explanation:

Checking for application updates is the first troubleshooting step that the user should perform, because the application may not be compatible with the new OS version and may need an update to fix the issue. Deleting the application's cache, rolling back the OS update, or uninstalling and reinstalling the application are possible solutions, but they are more time-consuming and disruptive than checking for updates. References: : <https://www.comptia.org/training/resources/exam-objectives/comptia-a-core-2-exam-objectives>
: <https://www.lifewire.com/how-to-update-apps-on-android-4173855>

NEW QUESTION 229

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 232

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 236

Which of the following is the most likely to use NTFS as the native filesystem?

- A. macOS
- B. Linux
- C. Windows
- D. Android

Answer: C

Explanation:

NTFS stands for New Technology File System, which is a proprietary file system developed by Microsoft⁴. NTFS is the default file system for the Windows NT family of operating systems, which includes Windows 10, Windows Server 2019, and other versions⁵. NTFS provides features such as security, encryption, compression, journaling, and large volume support⁴⁵. NTFS is not the native file system for other operating systems, such as macOS, Linux, or Android, although some of them can read or write to NTFS volumes with third-party drivers or tools

NEW QUESTION 237

A remote user is having issues accessing an online share. Which of the following tools would MOST likely be used to troubleshoot the issue?

- A. Screen-sharing software
- B. Secure shell
- C. Virtual private network
- D. File transfer software

Answer: A

Explanation:

Screen-sharing software is a tool that allows a technician to remotely view and control a user's screen over the internet. It can be used to troubleshoot issues with accessing an online share, as well as other problems that require visual inspection or guidance. Secure shell (SSH) is a protocol that allows remote access and command execution on another device, but it does not allow screen-sharing. Virtual private network (VPN) is a protocol that creates a secure tunnel between two devices over the internet, but it does not allow remote troubleshooting. File transfer software is a tool that allows transferring files between two devices over the internet, but it does not allow screen-sharing. Verified References: <https://www.comptia.org/blog/what-is-screen-sharing-software>
<https://www.comptia.org/certifications/a>

NEW QUESTION 242

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

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

Answer: C

Explanation:

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

NEW QUESTION 244

A macOS user is installing a new application. Which of the following system directories is the software MOST likely to install by default?

- A. /etc/services
- B. /Applications
- C. /usr/bin
- D. C:\Program Files

Answer: B

Explanation:

The software is most likely to install by default in the /Applications directory, which is the standard location for macOS applications. This directory can be accessed from the Finder sidebar or by choosing Go > Applications from the menu bar. The /Applications directory contains all the applications that are available to all users on the system¹. Some applications might also offer the option to install in the ~/Applications directory, which is a personal applications folder for a single user². The /etc/services directory is a system configuration file that maps service names to port numbers and protocols³. The /usr/bin directory is a system directory that contains executable binaries for various commands and utilities⁴. The C:\Program Files directory is a Windows directory that does not exist on macOS.

NEW QUESTION 247

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 applications.

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.

NEW QUESTION 251

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

- A. Mount the ISO and run the installation file.
- B. Copy the ISO and execute on the server.
- C. Copy the ISO file to a backup location and run the ISO file.
- D. Unzip the ISO and execute the setup.exe file.

Answer: A

Explanation:

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

NEW QUESTION 252

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

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

Answer: B

Explanation:

Bollards are the best solution to enhance building security in order to prevent vehicles from driving into the building while also maintaining easy access for customers. References: 2. Bollards. Retrieved from <https://en.wikipedia.org/wiki/Bollard>

NEW QUESTION 253

A user tries to access commonly used web pages but is redirected to unexpected websites. Clearing the web browser cache does not resolve the issue. Which of the following should a technician investigate NEXT to resolve the issue?

- A. Enable firewall ACLs.
- B. Examine the localhost file entries.
- C. Verify the routing tables.
- D. Update the antivirus definitions.

Answer: B

Explanation:

A possible cause of the user being redirected to unexpected websites is that the localhost file entries have been modified by malware or hackers to point to malicious or unwanted websites. The localhost file is a text file that maps hostnames to IP addresses and can override DNS settings. By examining the localhost file entries, a technician can identify and remove any suspicious or unauthorized entries that may cause the redirection issue. Enabling firewall ACLs may not resolve the issue if the firewall rules do not block the malicious or unwanted websites. Verifying the routing tables may not resolve the issue if the routing configuration is correct and does not affect the web traffic. Updating the antivirus definitions may help prevent future infections but may not remove the existing malware or changes to the localhost file. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.3

NEW QUESTION 257

A user requires local administrative access to a workstation. Which of the following Control Panel utilities allows the technician to grant access to the user?

- A. System
- B. Network and Sharing Center
- C. User Accounts
- D. Security and Maintenance

Answer: C

Explanation:

User Accounts is a Control Panel utility that allows the technician to manage user accounts and groups on a workstation¹. The technician can use User Accounts to grant local administrative access to a user by adding the user to the Administrators group¹. The Administrators group has full control over the workstation and can perform tasks such as installing software, changing system settings, and accessing all files.

References: 1: User Accounts (Control Panel) (<https://docs.microsoft.com/en-us/windows/win32/shell/user-accounts>) : Local Users and Groups practices/local-users-and-groups)
(<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best->

NEW QUESTION 262

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

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

Answer: B

Explanation:

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

NEW QUESTION 264

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

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

Answer: B

Explanation:

The security benefits realized after deploying a client certificate to be used for Wi-Fi access for all devices in an organization are that all Wi-Fi traffic will be encrypted in transit. This means that any data transmitted over the Wi-Fi network will be protected from eavesdropping attempts. Rogue access points will not connect to the network because they will not have the client certificate. However, multifactor authentication will not be forced for Wi-Fi because the client certificate is being used in conjunction with the user's existing username and password¹²

NEW QUESTION 267

A Windows user reported that a pop-up indicated a security issue. During inspection, an antivirus system identified malware from a recent download, but it was unable to remove the malware. Which of the following actions would be BEST to remove the malware while also preserving the user's files?

- A. Run the virus scanner in an administrative mode.
- B. Reinstall the operating system.
- C. Reboot the system in safe mode and rescan.
- D. Manually delete the infected files.

Answer: C

Explanation:

Rebooting the system in safe mode will limit the number of programs and processes running, allowing the antivirus system to more effectively identify and remove the malware. Rescanning the system will allow the antivirus system to identify and remove the malware while preserving the user's files.

NEW QUESTION 272

After a company installed a new SOHO router customers were unable to access the company-hosted public website. Which of the following will MOST likely allow customers to access the website?

- A. Port forwarding
- B. Firmware updates
- C. IP filtering
- D. Content filtering

Answer: B

Explanation:

If customers are unable to access the company-hosted public website after installing a new SOHO router, the company should check for firmware updates¹. Firmware updates can fix bugs and compatibility issues that may be preventing customers from accessing the website¹. The company should also ensure that the router is properly configured to allow traffic to the website¹. If the router is blocking traffic to the website, the company should configure the router to allow traffic to the website¹.

NEW QUESTION 275

A technician is partitioning a hard disk. The five primary partitions should contain 4TB of free space. Which of the following partition styles should the technician use to partition the device?

- A. EFS

- B. GPT
- C. MBR
- D. FAT32

Answer: B

Explanation:

GPT is the correct answer for this question. GPT stands for GUID Partition Table, and it is a partition style that supports up to 128 primary partitions and up to 18 exabytes of disk size per partition. GPT also uses a unique identifier for each partition and provides better data protection and recovery. GPT is suitable for partitioning a hard disk that has five primary partitions with 4TB of free space each. EFS, MBR, and FAT32 are not correct answers for this question. EFS stands for Encrypting File System, and it is a feature that allows encrypting files and folders on NTFS volumes. EFS is not a partition style, but rather a file system attribute. MBR stands for Master Boot Record, and it is an older partition style that supports up to four primary partitions and up to 2TB of disk size per partition. MBR cannot handle five primary partitions with 4TB of free space each. FAT32 stands for File Allocation Table 32, and it is a file system that supports up to 32GB of disk size per partition and up to 4GB of file size. FAT32 is not a partition style, but rather a file system type. References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 14

? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 105

NEW QUESTION 279

Which of the following provide the BEST way to secure physical access to a data center server room? (Select TWO).

- A. Biometric lock
- B. Badge reader
- C. USB token
- D. Video surveillance
- E. Locking rack
- F. Access control vestibule

Answer: AB

Explanation:

A biometric lock requires an authorized user to provide a unique biometric identifier, such as a fingerprint, in order to gain access to the server room. A badge reader requires an authorized user to swipe an access card in order to gain access. Both of these methods ensure that only authorized personnel are able to access the server room. Additionally, video surveillance and access control vestibules can be used to further secure the server room. Finally, a locking rack can be used to physically secure the servers, so that they cannot be accessed without the appropriate key.

NEW QUESTION 283

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.
- 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 284

A developer reports that a workstation's database file extensions have been changed from .db to .enc. The developer is also unable to open the database files manually. Which of the following is the best option for recovering the data?

- A. Accessing a restore point
- B. Rebooting into safe mode
- C. Utilizing the backups
- D. Using an AV to scan the affected files

Answer: C

Explanation:

The scenario described in the question suggests that the workstation has been infected by a ransomware, which is a type of malware that encrypts the files on the target system and demands a ransom for the decryption key. The file extension .enc is commonly used by some ransomware variants to mark the encrypted files. The developer is unable to open the database files manually because they are encrypted and require the decryption key, which is usually held by the attacker.

The best option for recovering the data is to utilize the backups, assuming that the backups are recent, valid, and not affected by the ransomware. Backups are copies of the data that are stored in a separate location or device, and can be used to restore the data in case of a disaster, such as a ransomware attack. By restoring the data from the backups, the developer can avoid paying the ransom and losing the data permanently.

Accessing a restore point is not a good option, because restore points are snapshots of the system settings and configuration, not the data files. Restore points can help to undo some system changes, such as installing a faulty driver or software, but they cannot recover the encrypted data files.

Rebooting into safe mode is also not a good option, because safe mode is a diagnostic mode that allows the system to run with minimal drivers and services, but it does not affect the data files. Safe mode can help to troubleshoot some system issues, such as malware infections, but it cannot decrypt the data files.

Using an AV to scan the affected files is also not a good option, because an AV is a software that can detect and remove some malware, but it cannot decrypt the data files. An AV can help to prevent or remove some ransomware infections, but it cannot recover the encrypted data files.

References: 1: CompTIA A+ Certification Exam Core 2 Objectives, page 10 2: CompTIA A+ Core 2 (220-1102) Complete Video Course, Lesson 26 Documentation

3: How to remove

.enc file virus (Ransomware virus removal guide) 4: Enc File Extension - What is an .enc file and how do I open it? : CompTIA A+ Certification Exam Core 2

Objectives, page 13 : CompTIA A+ Core 2 (220-1102) Complete Video Course, Lesson 26 Documentation

: What is a restore point? : How to use System Restore on Windows 10 : [What is Safe Mode?] : [How to boot into Safe Mode on Windows 10] : CompTIA A+ Certification Exam Core 2 Objectives, page 10 : [Can antivirus software remove ransomware?]

NEW QUESTION 287

A technician receives a help desk ticket from a user who is unable to update a phone. The technician investigates the issue and notices the following error message: Insufficient storage space

While analyzing the phone, the technician does not discover any third-party' applications or photos. Which of the following is the best way to resolve the issue?

- A. Exchange the device for a newer one.
- B. Upgrade the onboard storage
- C. Allocate more space by removing factory applications
- D. Move factory applications to external memory.

Answer: D

Explanation:

The best way to resolve the issue is to move factory applications to external memory. This will free up some space on the phone's internal storage, which is required for updating the phone. To do this, you can follow these steps1:

? Insert a microSD card into your phone if you don't have one already.

? Go to Settings > Apps and tap on the app you want to move.

? Tap on Storage and then on Change.

? Select the SD card option and tap on Move.

You may need to repeat this process for multiple apps until you have enough space to update your phone. Alternatively, you can also clear the cache and data of some apps, or uninstall the apps that you don't use frequently. You can find more information on how to fix insufficient storage error on your phone in these articles234. I hope this helps.

NEW QUESTION 292

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 220-1102 Exam with Our Prep Materials Via below:

<https://www.certleader.com/220-1102-dumps.html>