



# CompTIA

## Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

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

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

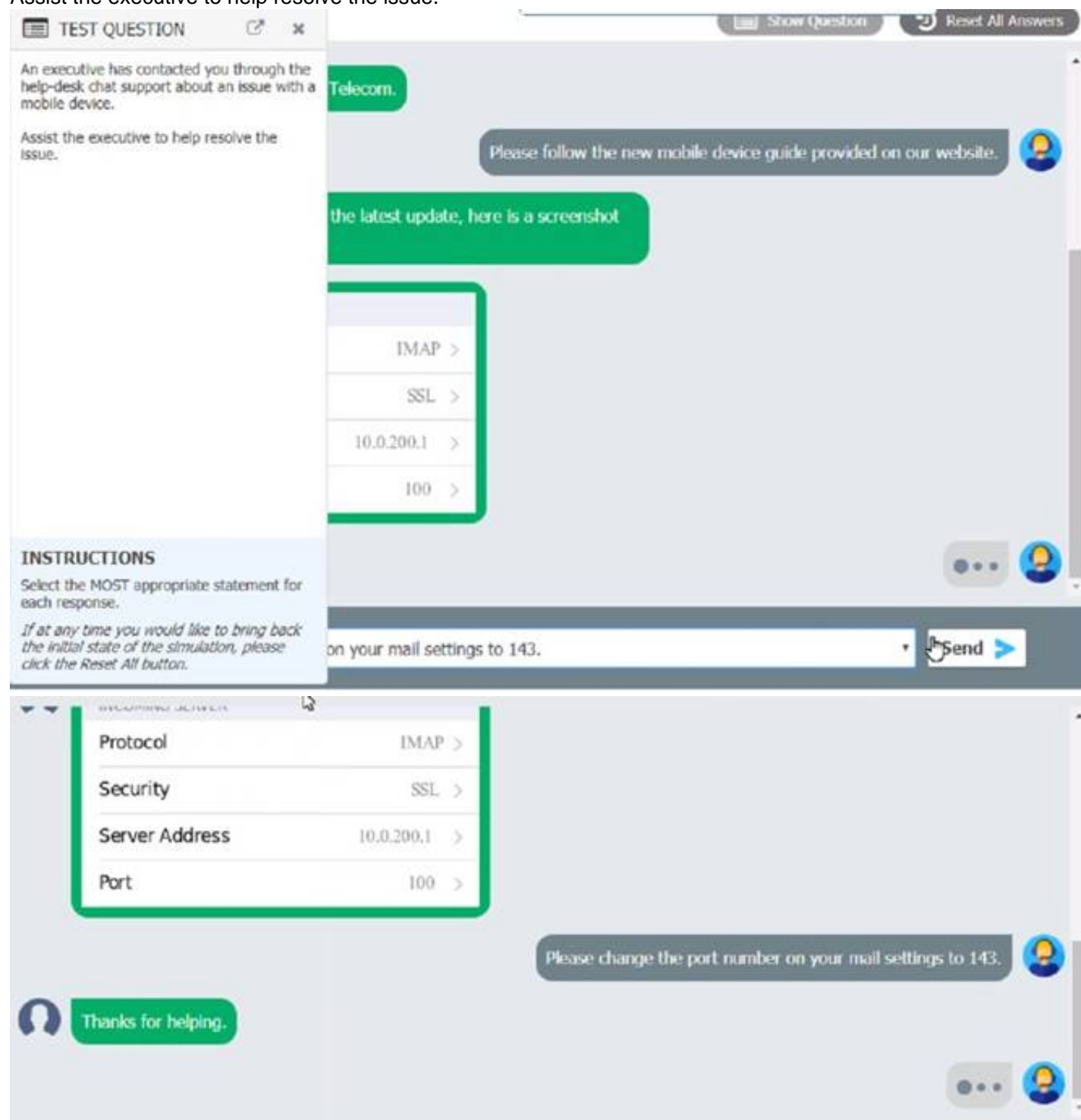
**Answer: D**

#### Explanation:

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

### NEW QUESTION 2

An executive has contacted you through the help-desk chat support about an issue with a mobile device. Assist the executive to help resolve the issue.



The screenshot shows a help-desk chat interface. On the left, a 'TEST QUESTION' sidebar contains the question text and instructions. The main chat area shows a conversation with 'Telecom'. The chat history includes a message from Telecom asking for help, a response from the user providing a link to a mobile device guide, and a screenshot of a settings page. The settings page shows a table with the following information:

Field	Value
Protocol	IMAP
Security	SSL
Server Address	10.0.200.1
Port	100

The chat continues with the user stating 'on your mail settings to 143.' and the user clicking the 'Send' button. The chat history also shows a message from Telecom saying 'Please change the port number on your mail settings to 143.' and a final message from the user saying 'Thanks for helping.'

Which of the following should be done NEXT?

- A. Educate the user on the solution that was performed.  
Tell the user to take time to fix it themselves next time.
- B. Close the ticket out.
- D. Send an email to Telecom to inform them of the Issue and prevent reoccurrence.

**Answer: A**

### NEW QUESTION 3

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

VTx not supported by system

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

- A. Processor
- B. Hard drive
- C. Memory

D. Video card

**Answer:** A

**Explanation:**

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

**NEW QUESTION 4**

A 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 site<sup>1</sup>. 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 accessible<sup>2</sup>. Regionally diverse backups can help ensure business continuity and data recovery in case of a disaster<sup>3</sup>. 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 corruption<sup>4</sup>. 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 5**

A technician installs specialized software on a workstation. The technician then attempts to run the software. The workstation displays a message indicating the software is not authorized to run. Which of the following should the technician do to most likely resolve the issue?

- A. Install the software in safe mode.
- B. Attach the external hardware token.
- C. Install OS updates.
- D. Restart the workstation after installation.

**Answer:** B

**Explanation:**

A hardware token is a physical device that provides an additional layer of security for software authorization. Some specialized software may require a hardware token to be attached to the workstation in order to run. A hardware token may contain a cryptographic key, a password, or a one-time code that verifies the user's identity or permission. Installing the software in safe mode, installing OS updates, and restarting the workstation after installation are not likely to resolve the issue of software authorization.

**NEW QUESTION 6**

A user is unable to access files on a work PC after opening a text document. The text document was labeled "URGENT PLEASE READ.txt - In active folder, .txt file titled urgent please read". Which of the following should a support technician do FIRST?

- A. Quarantine the host in the antivirus system.
- B. Run antivirus scan for malicious software.
- C. Investigate how malicious software was installed.
- D. Reimage the computer.

**Answer:** B

**Explanation:**

Running an antivirus scan for malicious software is the first step that a support technician should do when a user reports a virus on a PC. The antivirus scan can detect and remove the virus, as well as prevent further damage or infection. Quarantining the host, investigating how the malware was installed and reimaging the computer are possible steps that can be done after running the antivirus scan, depending on the situation and the results of the scan. Verified References: <https://www.comptia.org/blog/how-to-remove-a-virus> <https://www.comptia.org/certifications/a>

**NEW QUESTION 7**

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 8

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 use<sup>1</sup>. 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 memory<sup>2</sup>. 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-](https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715)

requirements-6d4e9a79-66bf-7950-467c-795cf0386715 1: <https://www.makeuseof.com/tag/unlock-64gb-ram-32-bit-windows-pae-patch/>

#### NEW QUESTION 9

A systems administrator is configuring centralized desktop management for computers on a domain. The management team has decided that all users' workstations should have the same network drives, printers, and configurations. Which of the following should the administrator use to accomplish this task?

- A. Network and Sharing Center
- B. net use
- C. User Accounts
- D. regedit
- E. Group Policy

**Answer:** E

#### Explanation:

Group Policy is a feature of Windows that allows administrators to centrally manage and apply policies and settings to computers and users on a domain<sup>3</sup>. Group Policy can be used to configure network drives, printers, security settings, desktop preferences, and other configurations for all users' workstations<sup>3</sup>. Network and Sharing Center, net use, User Accounts, and regedit are not tools that can accomplish this task.

#### NEW QUESTION 10

A technician installed a new application on a workstation. For the program to function

properly, it needs to be listed in the Path Environment Variable. Which of the following Control Panel utilities should the technician use?

- A. System
- B. Indexing Options
- C. Device Manager
- D. Programs and Features

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 10

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 15

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 16**

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 20**

An Android user contacts the help desk because a company smartphone failed to complete a tethered OS update A technician determines there are no error messages on the device Which of the following should the technician do NEXT?

- A. Verify all third-party applications are disabled
- B. Determine if the device has adequate storage available.
- C. Check if the battery is sufficiently charged
- D. Confirm a strong internet connection is available using Wi-Fi or cellular data

**Answer:** C

**Explanation:**

Since there are no error messages on the device, the technician should check if the battery is sufficiently charge1d  
If the battery is low, the device may not have enough power to complete the update2

In this scenario, the technician has already determined that there are no error messages on the device. The next best step would be to check if the battery is sufficiently charged. If the battery is low, it could be preventing the device from completing the update process. Verifying that third-party applications are disabled, determining if the device has adequate storage available, and confirming a strong internet connection are all important steps in troubleshooting issues with mobile devices. However, since the problem in this scenario is related to a failed OS update, it is important to first check the battery level before proceeding with further troubleshooting steps.

**NEW QUESTION 21**

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

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

**Answer:** BE

**Explanation:**

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

**NEW QUESTION 24**

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



to restart the print spooler?

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

**Answer: D**

**Explanation:**

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

References and Explanation

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

computer. It can be accessed by typing services.msc in the Run window or by searching for Services in the Start menu. The Services app allows users to start, stop, restart, or configure any service, including the print spooler<sup>123</sup>.

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

applications, and services that are running on the computer. It can be accessed by pressing Ctrl + Shift + Esc or by right-clicking on the taskbar and selecting Task Manager. The Task Manager allows users to start, stop, or restart any service by going to the Services tab and right-clicking on the service name<sup>12</sup>.

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

perform tasks using text input. It can be accessed by typing cmd in the Run window or by searching for Command Prompt in the Start menu. The Command Prompt allows users to start, stop, or restart any service by using the net command with the service name. For example, to restart the print spooler, users can type net stop spooler and then net start spooler<sup>1</sup>.

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

the computer. It can be accessed by typing control panel in the Run window or by searching for Control Panel in the Start menu. The Control Panel does not allow users to restart the print spooler directly, but it can be used to access other tools such as Devices and Printers, Troubleshooting, or Administrative Tools<sup>2</sup>.

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

processes that are running on the computer. It can be accessed by opening the Task Manager and selecting the Processes tab. The Processes tab does not allow users to restart the print spooler directly, but it can be used to end any process that is related to printing or causing problems with the print spooler<sup>2</sup>.

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

programs that run automatically when the computer starts. It can be accessed by opening the Task Manager and selecting the Startup tab. The Startup tab does not allow users to restart the print spooler directly, but it can be used to disable or enable any program that affects printing or interferes with the print spooler<sup>2</sup>.

**NEW QUESTION 26**

A help desk technician needs to remotely access and control a customer's Windows PC by using a secure session that allows the technician the same control as the customer. Which of the following tools provides this type of access?

- A. FTP
- B. RDP
- C. SSH
- D. VNC

**Answer: B**

**Explanation:**

RDP stands for Remote Desktop Protocol, which is a proprietary protocol developed by Microsoft that allows a user to remotely access and control another computer over a network. RDP provides a secure session that encrypts the data between the client and the host, and allows the user to see and interact with the desktop and applications of the remote computer as if they were sitting in front of it. RDP also supports features such as audio, video, clipboard, printer, and file sharing, as well as multiple monitor support and session recording. To use RDP, the host computer must have Remote Desktop enabled and configured, and the client computer must have a Remote Desktop client software installed. The client can connect to the host by entering its IP address, hostname, or domain name, and providing the login credentials of a user account on the host. RDP is commonly used for remote administration, technical support, and remote work scenarios

**NEW QUESTION 29**

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<sup>1</sup>. 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 34

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

- A. MFA
- B. WPA2
- C. AES
- D. RADIUS

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 36

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

- ☒ A. RDP
- ☐ B. VPN
- C. RMM
- D. SSH

**Answer:** B

#### Explanation:

One of the possible ways to access the user's computer remotely is to use RDP, which stands for Remote Desktop Protocol. RDP is a protocol that allows a user to connect to another computer over a network and use its graphical interface. RDP is commonly used for remote desktop software, such as Microsoft Remote Desktop Connection<sup>1</sup>. To use RDP, the user's computer must run RDP server software, and the technician must run RDP client software. The technician can then enter the user's IP address or hostname, and provide the appropriate credentials to log in to the user's computer. Once connected, the technician can view and control the user's desktop, and review the Outlook settings.

#### NEW QUESTION 37

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

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

**Answer:** C

#### Explanation:

The technician should quarantine the system first<sup>1</sup>. Reference:  
CompTIA A+ Certification Exam: Core 2 Objectives Version 4.0. Retrieved from [https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-\(3-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0))

#### NEW QUESTION 42

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 purposes<sup>1</sup>. MDM can enforce policies and restrictions on the devices, such as preventing users from installing unauthorized apps, modifying system settings, or accessing root privileges<sup>2</sup>. MDM can also monitor device status, wipe data, lock devices, or locate lost or stolen devices<sup>1</sup>.

#### NEW QUESTION 43

Which of the following is MOST likely used to run .vbs files on Windows devices?

- A. winmgmt.exe
- B. powershell.exe
- C. cscript.exe
- D. explorer.exe

**Answer:** C



**Explanation:**

A .vbs file is a Virtual Basic script written in the VBScript scripting language. It contains code that can be executed within Windows via the Windows-based script host (Wscript.exe), to perform certain admin and processing functions<sup>1</sup>. Cscript.exe is a command-line version of the Windows Script Host that provides command-line options for setting script properties. Therefore, cscript.exe is most likely used to run .vbs files on Windows devices. References: 1: <https://fileinfo.com/extension/vbs> : <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/cscript>

**NEW QUESTION 44**

A user reported that a laptop's screen turns off very quickly after silting for a few moments and is also very dim when not plugged in to an outlet Everything else seems to be functioning normally. Which of the following Windows settings should be configured?

- A. Power Plans
- B. Hibernate
- C. Sleep/Suspend
- D. Screensaver

**Answer:** A

**Explanation:**

Power Plans are Windows settings that allow a user to configure how a laptop's screen behaves when plugged in or running on battery power. They can adjust the screen brightness and the time before the screen turns off due to inactivity. Hibernate, Sleep/Suspend and Screensaver are other Windows settings that affect how a laptop's screen behaves, but they do not allow changing the screen brightness or turning off time. Verified References: <https://www.comptia.org/blog/windows-power-plans> <https://www.comptia.org/certifications/a>

**NEW QUESTION 46**

A new employee was hired recently. Which of the following documents will the new employee need to sign before being granted login access to the network?

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

A new employee will need to sign an AUP before being granted login access to the network. An AUP is an Acceptable Use Policy that defines the rules and guidelines for using network resources and services in an organization. An AUP typically covers topics such as security, privacy, ethics, compliance and liability issues related to network usage. An AUP helps protect the organization and its users from legal, regulatory and reputational risks associated with network activities. An MSDS is a Material Safety Data Sheet that provides information about hazardous substances and how to handle them safely. An MSDS is not related to network access or usage. A EULA is an End User License Agreement that specifies the terms and conditions for using a software product or service. A EULA is usually provided by software vendors or developers and does not apply to network access or usage in general. A UAC is a User Account Control that is a security feature that prompts users for permission or confirmation before performing certain actions that require elevated privileges or affect system settings. A UAC is not a document that needs to be signed by users but a mechanism that helps prevent unauthorized changes or malware infections on a system. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 5.1

**NEW QUESTION 51**

A help desk technician determines a motherboard has failed. Which of the following is the most logical next step in the remediation process?

- A. Escalating the issue to Tier 2
- B. Verifying warranty status with the vendor
- C. Replacing the motherboard
- D. Purchasing another PC

**Answer:** B

**Explanation:**

Verifying warranty status with the vendor is the most logical next step in the remediation process after determining that a motherboard has failed. A warranty is a guarantee from the vendor that covers the repair or replacement of defective or faulty products within a specified period of time. Verifying warranty status with the vendor can help the technician determine if the motherboard is eligible for warranty service and what steps to take to obtain it. Escalating the issue to Tier 2, replacing the motherboard, and purchasing another PC are not the most logical next steps in the remediation process.

**NEW QUESTION 53**

**HOTSPOT**

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

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

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

Details

#8675310

Open

Priority

Low

Category

Technical / Bug Reports

Assigned To

helpdesk@fictional.com

Assigned Date

7/13/2022

Subject

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

Attachments

[File Explorer.jpg](#)

Issue

Resolution

Verify/Resolve

Close Ticket

TEST QUESTION

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

INSTRUCTIONS

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

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

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

Date

Priority

ing to boot. Screen i...

7/13/2022

High

%

o access Z: on my co...

7/13/2022

Low

%

Corrupt OS

Recent Windows Updates

Graphics Drive Updates

BSOD

Printing Issues

Limited Network Connectivity

Services Failed to Start

User Profile is Corrupted

Application Crash

User cannot access shared resource

URL contains typo

Resolution

Reinstall Operating System

Rollback Updates

Rollback Drivers

Repair Application

Restart Print Spooler

Disable Network Adapter

Update Network Drivers

Refresh DHCP

Rebuild Windows Profile

Apply Updates

Repair Installation

Restore from Recovery Partition

Remap network drive

Verify integrity of disk drive

Initiate screen share session with user

Windows recovery environment

Inform user of AUP violation

Verify/Resolve

chkdsk

dism

diskpart

sfc

dd

ctrl + alt + del

net use

net user

netstat

netsh

bootrec

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

### Details

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

---

Subject	Unable to access Z: on my computer, but I can manually enter the location in the window.
Attachments	<a href="#">File Explorer.jpg</a>

Issue

Corrupt OS

Resolution

Reinstall Operating System

Verify/Resolve

chkdsk

Close Ticket

#### NEW QUESTION 56

A technician suspects a rootkit has been installed and needs to be removed. Which of the following would BEST resolve the issue?

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

If a rootkit has caused a deep infection, then the only way to remove the rootkit is to reinstall the operating system. This is because rootkits are designed to be difficult to detect and remove, and they can hide in the operating system's kernel, making it difficult to remove them without reinstalling the operating system  
<https://www.minitool.com/backup-tips/how-to-get-rid-of-rootkit-windows-10.html>

#### NEW QUESTION 61

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 64

A technician is troubleshooting a customer's PC and receives a phone call. The technician does not take the call and sets the phone to silent. Which of the following BEST describes the technician's actions?

- A. Avoid distractions
- B. Deal appropriately with customer's confidential material
- C. Adhere to user privacy policy
- D. Set and meet timelines

**Answer:** A

**Explanation:**

The technician has taken the appropriate action by not taking the call and setting the phone to silent in order to avoid any distractions and remain focused on the task at hand. This is a good example of how to maintain focus and productivity when working on a customer's PC, and will help to ensure that the job is completed in a timely and efficient manner.

**NEW QUESTION 69**

A user in a corporate office reports the inability to connect to any network drives. No other users have reported this issue. Which of the following is the MOST likely reason the user is having this issue?

- A. Mastered
- B. Not Mastered

**Answer:** A

**NEW QUESTION 73**

**HOTSPOT**

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

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

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

TEST QUESTION

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


**INSTRUCTIONS**  
Click on individual tickets to see the ticket details. View attachments to determine the problem.  
  
Select the appropriate issue from the 'issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the 'Verify/Resolve' drop-down menu.  
  
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Show Question

Reset All Answers

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

Details



**No Ticket Selected**  
Please select a ticket from the list



			Details	
	Date	Priority		
ing to boot. Screen l...	7/13/2022	High	#8675309	Open
9			Priority	High
			Category	Technical / Bug Reports
o access Z: on my co...	7/13/2022	Low	Assigned To	helpdesk@fictional.com
0			Assigned Date	7/13/2022
			Subject	PC is failing to boot. Screen is displaying error message, see attachment.
			Attachments	<a href="#">bootmgr not found.png</a>
			Issue	<input type="text"/>
			Resolution	<input type="text"/>
			Verify/Resolve	<input type="text"/>

A. Mastered  
B. Not Mastered

**Explanation:**

### Details

#8675309

Open

Priority

High

Category

Technical / Bug Reports

Assigned To

helpdesk@fictional.com

Assigned Date

7/13/2022

Subject

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

Attachments

[bootmgr not found.png](#)

Issue

Corrupt OS

Resolution

Reinstall Operating System

Verify/Resolve

chkdsk

Close Ticket

#### NEW QUESTION 77

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

- A. c: \minutes
- B. dir
- C. rmdir
- D. md

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 80

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<sup>12</sup>. 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 address<sup>3</sup>.

? 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)<sup>4</sup>.

? 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 hosts<sup>4</sup>.

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 84**

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) version<sup>1</sup>. APFS is optimized for flash storage and supports features such as encryption, snapshots, cloning, and space sharing<sup>1</sup>.

**NEW QUESTION 86**

Which of the following wireless security features can be enabled to allow a user to use login credentials to attach to available corporate SSIDs?

- A. TACACS+
- B. Kerberos
- C. Preshared key
- D. WPA2/AES

**Answer:** D

**Explanation:**

WPA2/AES (Wi-Fi Protected Access 2/Advanced Encryption Standard) is a wireless security standard that supports enterprise mode, which allows a user to use login credentials (username and password) to authenticate to available corporate SSIDs (service set identifiers). TACACS+ (Terminal Access Controller Access-Control System Plus) and Kerberos are network authentication protocols, but they are not wireless security features. Preshared key is another wireless security feature, but it does not use login credentials. Verified References: <https://www.comptia.org/blog/wireless-security-standards>  
<https://www.comptia.org/certifications/a>

**NEW QUESTION 88**

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 On<sup>12</sup>. Alternatively, the on-screen keyboard can be opened by pressing Windows + Ctrl + O keys or by typing osk.exe in the Run dialog box<sup>3</sup>.

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 92**

A technician is concerned about a large increase in the number of whaling attacks happening in the industry. The technician wants to limit the company's risk to

avoid any issues. Which of the following items should the technician implement?

- A. Screened subnet
- B. Firewall
- C. Anti-phishing training
- D. Antivirus

**Answer:** C

**Explanation:**

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

**NEW QUESTION 96**

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. Automatic screen lock
- C. Account lockout
- D. Antivirus

**Answer:** B

**Explanation:**

Account lockout would best mitigate the threat of a dictionary attack<sup>1</sup>

**NEW QUESTION 101**

A manager called the help desk to ask for assistance with creating a more secure environment for the finance department- which resides in a non-domain environment. Which of the following would be the BEST method to protect against unauthorized use?

- A. Implementing password expiration
- B. Restricting user permissions
- C. Using screen locks
- D. Disabling unnecessary services

**Answer:** B

**Explanation:**

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

**NEW QUESTION 106**

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

- A. incineration
- B. Resale
- C. Physical destruction
- D. Dumpster for recycling plastics

**Answer:** D

**Explanation:**

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

**NEW QUESTION 108**

A company-owned mobile device is displaying a high number of ads, receiving data-usage limit notifications, and experiencing slow response. After checking the device, a technician notices the device has been jailbroken. Which of the following should the technician do next?

- A. Run an antivirus and enable encryption.
- B. Back up the files and do a system restore.
- C. Restore the defaults and reimage the corporate OS.
- D. Undo the jailbreak and enable an antivirus.

**Answer:** B

**Explanation:**

Jailbreaking a device exposes it to various security risks, such as malware, data theft, network attacks, and service disruption<sup>1234</sup>. Running an antivirus and enabling encryption may not be enough to remove the threats and restore the device's functionality. Undoing the jailbreak may not be possible or effective,



depending on the method used. Backing up the files and doing a system restore may preserve the jailbreak and the associated problems. The best option is to erase the device and reinstall the original operating system that is compatible with the corporate policies and standards. This will ensure that the device is clean, secure, and compliant<sup>25</sup>.

References: 1 What is Jailbreaking & Is it safe? - Kaspersky(<https://www.kaspersky.com/resource-center/definitions/what-is-jailbreaking>). 2 Jailbreak Detection: Why is jailbreaking a potential security risk? -

Cybersecurity ASEE(<https://cybersecurity.asee.co/blog/what-is-jailbreaking/>). 3 Jailbreaking Information for iOS Devices | University

IT(<https://uit.stanford.edu/service/mydevices/jailbreak>)<sup>4</sup> What does it mean to jailbreak your phone—and is it legal? - Microsoft(<https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-jailbreaking-a-phone>). 5 Resetting a corporate laptop back to a personal laptop... Enterprise vs Pro -

Windows 10(<https://community.spiceworks.com/topic/2196812-resetting-a-corporate-laptop-back-to-a-personal-laptop-enterprise-vs-pro>).

#### NEW QUESTION 109

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<sup>1</sup>. 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 Guide<sup>2</sup>, page 263.

? WiFi Fast Roaming, Simplified<sup>3</sup>

#### NEW QUESTION 112

A technician is installing new software on a macOS computer. Which of the following file types will the technician MOST likely use?

- A. .vbs
- B. .deb
- C. .exe
- D. .app

**Answer: D**

#### Explanation:

The file type that the technician will MOST likely use when installing new software on a macOS computer is .app. This is because .app is the file extension for applications on macOS<sup>1</sup>.

#### NEW QUESTION 114

A technician needs to perform after-hours service starting at 10:00 p.m. The technician is currently 20 minutes late. The customer will also be late. Which of the following should the technician do considering proper communication techniques and professionalism?

- A. Do not notify the customer if arriving before the customer.
- B. Dismiss the customer and proceed with the after-hours work.
- C. Contact the customer if the technician is arriving late.
- D. Disclose the experience via social media.

**Answer: C**

#### Explanation:

The best option for the technician to demonstrate proper communication techniques and professionalism is to contact the customer if the technician is arriving late. This shows respect for the customer's time and expectations, and allows the customer to adjust their schedule accordingly. It also helps to maintain a positive relationship and trust between the technician and the customer. The technician should apologize for the delay and provide a realistic estimate of their arrival time. The technician should also thank the customer for their patience and understanding.

The other options are not appropriate or professional. Do not notify the customer if arriving before the customer is not a good practice, as it may cause confusion or frustration for the customer. The customer may have made other plans or arrangements based on the technician's original schedule, and may not be available or prepared for the service. Dismiss the customer and proceed with the after-hours work is rude and disrespectful, as it ignores the customer's needs and preferences. The customer may have questions or concerns about the service, or may want to supervise or verify the work. The technician should always communicate with the customer before, during, and after the service.

Disclose the experience via social media is unethical and unprofessional, as it may violate the customer's privacy and the company's policies. The technician should not share any confidential or sensitive information about the customer or the service on social media, or make any negative or inappropriate comments about the customer or the situation. References:

? CompTIA A+ Certification Exam Core 2 Objectives<sup>1</sup>

? CompTIA A+ Core 2 (220-1102) Certification Study Guide<sup>2</sup>

? 8 Ways You Can Improve Your Communication Skills<sup>3</sup>

? Professionalism in Communication | How To Do It And How It Pays<sup>4</sup>

#### NEW QUESTION 117

Which of the following best describes when to use the YUM command in Linux?

- A. To add functionality

- B. To change folder permissions
- C. To show documentation
- D. To list file contents

**Answer:** A

**Explanation:**

YUM stands for Yellowdog Updater Modified and it is a command-line tool that allows users to install, update, remove, and manage software packages in Linux. YUM can be used to add functionality to a Linux system by installing new software packages or updating existing ones. To change folder permissions, show documentation, or list file contents, other commands such as `chmod`, `man`, or `ls` can be used in Linux.

**NEW QUESTION 120**

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 124**

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

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

**Answer:** AC

**Explanation:**

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

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

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

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

#### NEW QUESTION 125

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

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

**Answer:** A

**Explanation:**

The best answer to control security settings on an Android phone in a domain environment is to use “Mobile Device Management (MDM)”. MDM is a type of software that is used to manage and secure mobile devices such as smartphones and tablets. MDM can be used to enforce security policies, configure settings, and remotely wipe data from devices. In a domain environment, MDM can be used to manage Android phones and enforce security policies such as password requirements, encryption, and remote wipe capabilities<sup>12</sup>

#### NEW QUESTION 129

A user is unable to access a web-based application. A technician verifies the computer cannot access any web pages at all. The computer obtains an IP address from the DHCP server. Then, the technician verifies the user can ping localhost, the gateway, and known IP addresses on the internet and receive a response. Which of the following is the MOST likely reason for the issue?

- A. A firewall is blocking the application.
- B. The wrong VLAN was assigned.
- C. The incorrect DNS address was assigned.
- D. The browser cache needs to be cleared

**Answer:** C

**Explanation:**

DNS (domain name system) is a protocol that translates domain names to IP addresses. If the computer has an incorrect DNS address assigned, it will not be able to

resolve the domain names of web-based applications and access them. A firewall, a VLAN (virtual local area network) and a browser cache are not the most likely reasons for the issue, since the computer can ping known IP addresses on the internet and receive a response. Verified References: <https://www.comptia.org/blog/what-is-dns> <https://www.comptia.org/certifications/a>

#### NEW QUESTION 131

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 132

A user is unable to log in to the network. The network uses 802.1X with EAP-TLS to authenticate on the wired network. The user has been on an extended leave and has not logged in to the computer in several months. Which of the following is causing the login issue?

- A. Expired certificate
- B. OS update failure
- C. Service not started
- D.

Application crash

- E. Profile rebuild needed

**Answer:** A

**Explanation:**

EAP-TLS is a method of authentication that uses certificates to establish a secure tunnel between the client and the server<sup>3</sup>. The certificates have a validity period and must be renewed before they expire<sup>1</sup>. If the user has been on an extended leave and has not logged in to the computer in several months, it is possible that the certificate on the client or the server has expired and needs to be renewed<sup>2</sup>. The other options are not directly related to EAP-TLS authentication or 802.1X network access.

**NEW QUESTION 136**

A user is setting up a computer for the first time and would like to create a secondary login with permissions that are different than the primary login. The secondary login will need to be protected from certain content such as games and websites. Which of the following Windows settings should the user utilize to create the secondary login?

- A. Privacy
- B. Accounts
- C. Personalization
- D. Shared resources

**Answer: B**

**Explanation:**

To create a secondary login with different permissions in Windows 10, the user should utilize the Accounts setting. Here are the steps to create a new user account with different permissions:

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

**NEW QUESTION 137**

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 142**

The audio on a user's mobile device is inconsistent when the user uses wireless headphones and moves around. Which of the following should a technician perform to troubleshoot the issue?

- A. Verify the Wi-Fi connection status.
- B. Enable the NFC setting on the device.
- C. Bring the device within Bluetooth range.
- D. Turn on device tethering.

**Answer: C**



**Explanation:**

Bringing the device within Bluetooth range is the best way to troubleshoot the issue of inconsistent audio when using wireless headphones and moving around. Bluetooth is a wireless technology that allows devices to communicate over short distances, typically up to 10 meters or 33 feet. If the device is too far from the headphones, the Bluetooth signal may be weak or interrupted, resulting in poor audio quality or loss of connection.

**NEW QUESTION 143**

A technician has been tasked with troubleshooting audiovisual issues in a conference room. The meeting presenters are unable to play a video with sound. The following error is received:

The Audio Driver is not running.

Which of the following will MOST likely resolve the issue?

- A. compmgmt.msc
- B. regedit.exe
- C. explorer.exe
- D. taskmgmt.exe
- E. gpmmc.msc
- F. services.msc

**Answer:** F

**Explanation:**

services.msc is a tool that can be used to resolve the issue of “The Audio Driver is not running” on a Windows machine. It allows a technician to view, start, stop and configure the services that run on the system, such as the Windows Audio service. compmgmt.msc, regedit.exe, explorer.exe, taskmgmt.exe and gpmmc.msc are other tools that can be used for different purposes on a Windows machine, but they are not related to audio drivers or services. Verified References: <https://www.comptia.org/blog/what-is-services-msc> <https://www.comptia.org/certifications/a>

**NEW QUESTION 147**

Which of the following should be done NEXT?

- A. Send an email to Telecom to inform them of the issue and prevent reoccurrence.
- B. Close the ticket out.
- C. Tell the user to take time to fix it themselves next time.
- D. Educate the user on the solution that was performed.

**Answer:** D

**Explanation:**

educating the user on the solution that was performed is a good next step after resolving an issue. This can help prevent similar issues from happening again and empower users to solve problems on their own.

**NEW QUESTION 148**

A technician requires graphical remote access to various Windows, Linux, and macOS desktops on the company LAN. The security administrator asks the technician to utilize a single software solution that does not require an external internet connection. Which of the following remote access tools is the technician most likely to install?

- A. VNC
- B. RMM
- C. RDP
- D. SSH

**Answer:** A

**Explanation:**

VNC (Virtual Network Computing) is a remote access tool that allows the technician to access and control various Windows, Linux, and macOS desktops on the company LAN using a graphical user interface. VNC does not require an external internet connection, as it works over a local network or a VPN. VNC uses a client-server model, where the server runs on the remote desktop and the client connects to it from another device. VNC can transmit the keyboard and mouse events from the client to the server, and the screen updates from the server to the client, enabling the technician to interact with the remote desktop as if it were local<sup>12</sup>. VNC is a better option than the other choices because:

? RMM (Remote Monitoring and Management) (B) is not a single software solution, but a category of software solutions that enable IT professionals to remotely monitor, manage, and troubleshoot multiple devices and networks. RMM software may include remote access tools, but also other features such as patch management, backup and recovery, security, reporting, and automation. RMM software may require an external internet connection, as it often relies on cloud-based services or web-based consoles<sup>34</sup>.

? RDP (Remote Desktop Protocol) (C) is a remote access tool that allows the technician to access and control Windows desktops on the company LAN using a graphical user interface. However, RDP is not compatible with Linux or macOS desktops, unless they have third-party software installed that can emulate or translate the RDP protocol. RDP also has some security and performance issues, such as encryption vulnerabilities, bandwidth consumption, and latency problems<sup>56</sup>.

? SSH (Secure Shell) (D) is a remote access tool that allows the technician to access and control various Windows, Linux, and macOS desktops on the company LAN using a command-line interface. SSH does not require an external internet connection, as it works over a local network or a VPN. SSH uses encryption and authentication to secure the communication between the client and the server. However, SSH does not provide a graphical user interface, which may limit the functionality and usability of the remote desktop<sup>7</sup>.

References:

1: What is VNC? - Definition from Techopedia<sup>1</sup> 2: How VNC Works - RealVNC<sup>2</sup> 3: What is Remote Monitoring and Management (RMM)? - Definition from Techopedia<sup>3</sup> 4: What is RMM Software? - NinjaRMM<sup>4</sup> 5: What is Remote Desktop Protocol (RDP)? - Definition from Techopedia<sup>5</sup> 6: Remote Desktop Protocol: What it is and how to secure it - CSO Online<sup>6</sup> 7: What is Secure Shell (SSH)? - Definition from Techopedia<sup>7</sup> : How to Use SSH to Access a Remote Server in Linux or Windows - Hostinger Tutorials

**NEW QUESTION 152**

A user enabled a mobile device's screen lock function with pattern unlock. The user is concerned someone could access the mobile device by repeatedly attempting random patterns to unlock the device. Which of the following features BEST addresses the user's concern?

- A. Remote wipe
- B. Anti-malware
- C. Device encryption
- D. Failed login restrictions

**Answer:** A

**Explanation:**

The feature that BEST addresses the user's concern is remote wipe. This is because remote wipe allows the user to erase all data on the mobile device if it is lost or stolen, which will prevent unauthorized access to the device<sup>1</sup>.

**NEW QUESTION 153**

A technician is trying to encrypt a single folder on a PC. Which of the following should the technician use to accomplish this task?

- A. FAT32
- B. exFAT
- C. BitLocker
- D. EFS

**Answer:** D

**Explanation:**

EFS (Encrypting File System) is a feature that allows a user to encrypt a single folder or file on a Windows PC. It uses a public key encryption system to protect the data from unauthorized access. FAT32 and exFAT are file system formats that do not support encryption. BitLocker is a feature that encrypts the entire drive, not a single folder or file. Verified References: <https://www.comptia.org/blog/what-is-efs> <https://www.comptia.org/certifications/a>

**NEW QUESTION 155**

A customer has a USB-only printer attached to a computer. A technician is configuring an arrangement that allows other computers on the network to use the printer. In which of the following locations on the customer's desktop should the technician make this configuration?

- A. Printing Preferences/Advanced tab
- B. Printer Properties/Sharing tab
- C. Printer Properties/Security tab
- D. Printer Properties/Ports tab

**Answer:** B

**Explanation:**

The correct answer is B. Printer Properties/Sharing tab. This is the location where the technician can enable printer sharing and assign a share name for the USB printer. This will allow other computers on the network to access the printer by using the share name or the IP address of the computer that has the printer attached<sup>1</sup>.

1: CompTIA A+ Certification Exam: Core 2 Objectives, page 15, section 1.9.

**NEW QUESTION 159**

A payroll workstation has data on it that needs to be readily available and can be recovered quickly if something is accidentally removed. Which of the following backup methods should be used to provide fast data recovery in this situation?

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

**Answer:** A

**Explanation:**

A full backup does not depend on any previous backups, unlike differential or incremental backups, which only save the changes made since the last backup. A synthetic backup is a type of full backup that combines an existing full backup with incremental backups to create a new full backup, but it still requires multiple backup sets to recover data. Therefore, a full backup is the most suitable for the payroll workstation that needs to have its data readily available and recoverable. You can learn more about the differences between full, differential, incremental, and synthetic backups from this article.

**NEW QUESTION 164**

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<sup>4</sup> References: 2. Bollards. Retrieved from <https://en.wikipedia.org/wiki/Bollard>

#### NEW QUESTION 166

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 workstation<sup>1</sup>. The technician can use User Accounts to grant local administrative access to a user by adding the user to the Administrators group<sup>1</sup>. 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-practices/local-users-and-groups>)

#### NEW QUESTION 169

A technician received a call from a user who clicked on a web advertisement. Now, every time the user moves the mouse, a pop-up display appears across the monitor. Which of the following procedures should the technician perform?

- A. Boot into safe mode.
- B. Perform a malware scan.
- C. Restart the machine.
- D. Reinstall the browser

**Answer:** AB

#### Explanation:

Booting into safe mode and performing a malware scan are the steps that a technician should perform when troubleshooting an issue with pop-up advertising messages on a PC. Safe mode is a diagnostic mode that starts the PC with minimal drivers and services, which can prevent the pop-up malware from running. Malware scan is a tool that can detect and remove the pop-up malware, as well as prevent further infection or damage. Investigating how the malware was installed, reinstalling the browser and restarting the machine are possible steps that can be done after booting into safe mode and performing a malware scan, depending on the situation and the results of the scan. Verified References: <https://www.comptia.org/blog/how-to-boot-into-safe-mode>  
<https://www.comptia.org/certifications/a>

#### NEW QUESTION 174

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

- A. Settings > Personalization
- B. Control Panel > Credential Manager
- C. Settings > Accounts > Family and Other Users
- D. Control Panel > Network and Sharing Center

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 179

A user connected an external hard drive but is unable to see it as a destination to save files. Which of the following tools will allow the drive to be formatted?

- A. Disk Management
- B. Device Manager
- C. Disk Cleanup
- D. Disk Defragmenter

**Answer:** A

#### Explanation:

Disk Management is a tool that allows users to create, format, delete, shrink, extend, and manage partitions on hard drives. If the external hard drive is not formatted or has an incompatible filesystem type, Disk Management can be used to format it with a supported filesystem type such as NTFS, FAT32, or exFAT. Device Manager, Disk Cleanup, and Disk Defragmenter are not tools that can format a hard drive.

#### NEW QUESTION 182

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:**

Power Options is a Control Panel utility that allows users to configure the power settings of their computer, such as when to turn off the display, when to put the computer to sleep, and how to manage the battery life. Power Options also allows users to configure the USB selective suspend setting, which is a feature that automatically suspends the power supply to USB devices that are not in use, in order to save energy. A user can disable this setting if they want to ensure that USB devices are not suspended by the operating system. System, Devices and Printers, and Ease of Access are not Control Panel utilities that can be used to configure the USB selective suspend setting.

**NEW QUESTION 184**

A technician is working to resolve a Wi-Fi network issue at a doctor's office that is located next to an apartment complex. The technician discovers that employees and patients are not the only people on the network. Which of the following should the technician do to BEST minimize this issue?

- A. Disable unused ports.
- B. Remove the guest network
- C. Add a password to the guest network
- D. Change the network channel.

**Answer:** D

**Explanation:**

Changing the network channel is the best solution to minimize the issue of employees and patients not being the only people on the Wi-Fi network<sup>5</sup>

References: 3. Sample CompTIA Security+ exam questions and answers. Retrieved from <https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-Security-exam-questions-and-answers>

**NEW QUESTION 189**

A suite of security applications was installed a few days ago on a user's home computer.

The user reports that the computer has been running slowly since the installation. The user notices the hard drive activity light is constantly solid. Which of the following should be checked FIRST?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 194**

The battery life on an employee's new phone seems to be drastically less than expected,

and the screen stays on for a very long time after the employee sets the phone down. Which of the following should the technician check first to troubleshoot this issue? (Select two).

- A. Screen resolution
- B. Screen zoom
- C. Screen timeout
- D. Screen brightness
- E. Screen damage
- F. Screen motion smoothness

**Answer:** CD

**Explanation:**

Screen timeout is the setting that determines how long the screen stays on after the user stops interacting with the phone. Screen brightness is the setting that determines how much light the screen emits. Both of these settings affect the battery life of the phone, as keeping the screen on longer and brighter consumes more power than turning it off sooner and dimmer. A technician should check these settings first to troubleshoot the issue of low battery life and adjust them accordingly. Screen resolution, screen zoom, screen damage, and screen motion smoothness are not settings that directly affect the battery life or the screen staying on for a long time.

**NEW QUESTION 198**

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

- A. Update the anti-malware software.
- B. Create a restore point.
- C. Run the PC in safe mode.
- D. Roll back the system updates.

**Answer:** B

**Explanation:**

A restore point is a snapshot of the system settings and configuration at a specific point in time<sup>2</sup>. Creating a restore point before modifying the registry keys allows the technician to revert the system back to a previous state if something goes wrong or causes instability<sup>2</sup>. Updating the anti-malware software, running the PC in



safe mode, and rolling back the system updates are not necessary steps before modifying the registry keys.

#### NEW QUESTION 201

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 206

Malware is installed on a device after a user clicks on a link in a suspicious email. Which of the following is the best way to remove the malware?

- A. Run System Restore.
- B. Place in recovery mode.
- C. Schedule a scan.
- D. Restart the PC.

**Answer: B**

#### Explanation:

Recovery mode is a special boot option that allows the user to access advanced tools and features to troubleshoot and remove malware from the device. Recovery mode can also restore the system to a previous state or reset the device to factory settings. Running System Restore, scheduling a scan, or restarting the PC may not be effective in removing the malware, as it may still be active or hidden in the system files.

#### NEW QUESTION 209

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

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

**Answer: B**

#### Explanation:

The most likely reason that the system is not utilizing all the available RAM is that the system is utilizing a 32-bit OS. A 32-bit OS is an operating system that uses 32 bits to address memory locations and perform calculations. A 32-bit OS can only support up to 4GB of RAM, and some of that RAM may be reserved for hardware devices or system functions, leaving less than 4GB of usable RAM for applications and processes. A 32-bit OS cannot recognize or utilize more than 4GB of RAM, even if more RAM is installed on the system. To utilize all the available RAM, the system needs to use a 64-bit OS, which can support much more RAM than a 32-bit OS. The system missing updates may cause some performance or compatibility issues, but it does not affect the amount of usable RAM on the system. The system's memory failing may cause some errors or crashes, but it does not affect the amount of usable RAM on the system. The system requiring BIOS updates may cause some configuration or compatibility issues, but it does not affect the amount of usable RAM on the system. References: CompTIA A+ Core 2 (220-1102) Certification

Exam Objectives Version 4.0, Domain 1.1

#### NEW QUESTION 213

A computer technician is investigating a computer that is not booting. The user reports that the computer was working prior to shutting it down last night. The technician notices a removable USB device is inserted, and the user explains the device is a prize the user received in the mail yesterday. Which of the following types of attacks does this describe?

- A. Phishing
- B. Dumpster diving
- C. Tailgating
- D. Evil twin

**Answer: A**

#### Explanation:

Phishing is the correct answer for this question. Phishing is a type of attack that uses fraudulent emails or other messages to trick users into revealing sensitive information or installing malicious software. Phishing emails often impersonate legitimate entities or individuals and offer incentives or threats to lure users into clicking on malicious links or attachments. In this scenario, the user received a removable USB device in the mail as a prize, which could be a phishing attempt to infect the user's computer with malware or gain access to the user's data. Dumpster diving, tailgating, and evil twin are not correct answers for this question. Dumpster diving is a type of attack that involves searching through trash bins or recycling containers to find discarded documents or devices that contain valuable information. Tailgating is a type of attack that involves following an authorized person into a restricted area without proper identification or authorization. Evil twin is a type of attack that involves setting up a rogue wireless access point that mimics a legitimate one to intercept or manipulate network traffic. References: ? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25 ? [CompTIA Security+ SY0-601 Certification Study Guide], page 1004



#### NEW QUESTION 216

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 218

Which of the following is used to integrate Linux servers and desktops into Windows Active Directory environments?

- A. apt-get
- B. CIFS
- C. Samba
- D. greP

**Answer:** C

#### Explanation:

Samba is a software suite that allows Linux servers and desktops to integrate with Windows Active Directory environments. Samba can act as a domain controller, a file server, a print server, or a client for Windows networks. Samba can also provide authentication and authorization services for Linux users and devices using Active Directory.

#### NEW QUESTION 219

A technician needs to reimage a desktop in an area without network access. Which of the following should the technician use? (Select two).

- ☒ A. PXE
  - ☐ B. CIFS
  - ☐ C. Optical media
  - ☐ D. Partition
  - ☐ E. Boot record
  - ☐ F. SMB
- USB

**Answer:** AC

#### Explanation:

A technician needs to reimage a desktop in an area without network access, which means that the technician cannot use network-based methods such as PXE or SMB to deploy the image. Therefore, the technician should use offline methods that involve removable media such as USB or optical media. USB and optical media are common ways to store and transfer system images, and they can be used to boot the desktop and initiate the reimaging process. The technician will need to create a bootable USB or optical media that contains the system image and the imaging software, and then insert it into the desktop and change the boot order in the BIOS or UEFI settings. The technician can then follow the instructions on the screen to reimage the desktop.

#### NEW QUESTION 223

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

- A. Windows Enterprise Edition
- B. Windows Professional Edition
- ☒ C. Windows Home Edition
- ☐ D. Windows Server Standard Edition

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 225

A user needs assistance installing software on a Windows PC but will not be in the office. Which of the following solutions would a technician MOST likely use to assist the user without having to install additional software?

- A. VPN
- B. MSRA
- C. SSH
- D. RDP

**Answer:** B

#### Explanation:

MSRA stands for Microsoft Remote Assistance, and it is a feature that allows a technician to remotely view and control another user's Windows PC with their permission. MSRA is built-in to Windows and does not require any additional software installation. To use MSRA, the technician and the user need to follow these steps:

? On the user's PC, type msra in the search box on the taskbar and select Invite someone to connect to your PC and help you, or offer to help someone else.

- ? Select Save this invitation as a file and choose a location to save the file. This file contains a password that the technician will need to connect to the user's PC.
- ? Send the file and the password to the technician via email or another secure method.
- ? On the technician's PC, type msra in the search box on the taskbar and select Help someone who has invited you.
- ? Select Use an invitation file and browse to the location where the file from the user is saved. Enter the password when prompted.
- ? The user will see a message asking if they want to allow the technician to connect to their PC. The user should select Yes.
- ? The technician will see the user's desktop and can request control of their PC by clicking Request control on the top bar. The user should allow this request by clicking Yes.
- ? The technician can now view and control the user's PC and assist them with installing software.

#### NEW QUESTION 228

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

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

**Answer:** D

#### Explanation:

The newly installed OS is x86. The x86 version of Windows 10 can only use up to 4GB of RAM. The x64 version of Windows 10 can use up to 2TB of RAM1.

#### NEW QUESTION 232

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

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 234

A user is attempting to browse the internet using Internet Explorer. When trying to load a familiar web page, the user is unexpectedly redirected to an unfamiliar website. Which of the following would MOST likely solve the issue?

- A. Updating the operating system
- B. Changing proxy settings
- C. Reinstalling the browser
- D. Enabling port forwarding

**Answer:** C

#### Explanation:

Reinstalling the browser would most likely solve the issue. This would remove any malicious software or add-ons that may be causing the issue and restore the browser to its default settings.

#### NEW QUESTION 236

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

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

**Answer:** A

#### Explanation:

Copying the program file to a USB drive and installing it from there is the simplest and most reliable way to transfer the software from the network share to the Windows tablet. The other options are either unnecessary, risky, or impractical. Burning the program file to a CD requires a CD burner and a CD reader, which may not be available on the tablet. Formatting or replacing the HDD will erase all the data and settings on the tablet, which is not advisable unless there is a backup or a serious problem. Moreover, formatting or replacing the HDD will not solve the issue of copying the program file from the network share. References: 1 How To Copy A Program From One Computer To Another: 5 Ways(<https://www.minitool.com/news/transfer-copy-programs-from-one-computer-to-another.html>)2 Transfer files between your Android tablet and PC using Wi- Fi(<https://www.techrepublic.com/article/transfer-files-between-your-android-tablet-and-pc-using-wi-fi/>)3 Share Files Between Your Tablet and Computer with Huawei

Share(<https://consumer.huawei.com/en/support/content/en-us15819174/>)4 How to Transfer Installed Programs to Another PC on Windows 10(<https://www.diskpart.com/articles/transfer-installed-program-to-another-pc-windows-10-0825.html>).

#### NEW QUESTION 239

A technician is troubleshooting an issue with a computer that contains sensitive information. The technician determines the computer needs to be taken off site for repair. Which of the following should the technician do NEXT?

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

The next step that the technician should do before taking the computer off site for repair is to get authorization from the manager. Getting authorization from the manager is important because it ensures that the technician has permission and approval to remove the computer from the premises and perform the repair work off site. Getting authorization from the manager can also help document and communicate the reason and duration of the repair and avoid any misunderstanding or conflict with the user or the organization. Removing the HDD and then sending the computer for repair may not be feasible or necessary if the issue is not related to the HDD or if the HDD contains essential data or software for the repair. Checking corporate policies for guidance may be a good step but it does not replace getting authorization from the manager who is responsible for the computer and its data. Deleting the sensitive information before the computer leaves the building may not be possible or advisable if the issue prevents access to the data or if the data is needed for troubleshooting or recovery purposes. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 5.1

**NEW QUESTION 242**

A help desk team lead contacts a systems administrator because the technicians are unable to log in to a Linux server that is used to access tools. When the administrator tries to use remote desktop to log in to the server, the administrator sees the GUI is crashing. Which of the following methods can the administrator use to troubleshoot the server effectively?

- A. SFTP
- B. SSH
- C. VNC
- D. MSRA

**Answer:** C

**Explanation:**

The administrator can use Virtual Network Computing (VNC) to troubleshoot the server effectively. VNC is a graphical desktop sharing system that allows the administrator to remotely control the desktop of a Linux server.

**NEW QUESTION 243**

A user receives a call from someone who claims to be from the user's bank and requests information to ensure the user's account is safe. Which of the following social-engineering attacks is the user experiencing?

- A. Phishing
- B. Smishing
- C. Whaling
- D. Vishing

**Answer:** D

**Explanation:**

The user is experiencing a vishing attack. Vishing stands for voice phishing and is a type of social-engineering attack that uses phone calls or voice messages to trick users into revealing personal or financial information. Vishing attackers often pretend to be from legitimate organizations, such as banks, government agencies or service providers, and use various tactics, such as urgency, fear or reward, to persuade users to comply with their requests. Phishing is a type of social-engineering attack that uses fraudulent emails or websites to trick users into revealing personal or financial information. Phishing does not involve phone calls or voice messages. Smishing is a type of social-engineering attack that uses text messages or SMS to trick users into revealing personal or financial information. Smishing does not involve phone calls or voice messages. Whaling is a type of social-engineering attack that targets high-profile individuals, such as executives, celebrities or politicians, to trick them into revealing personal or financial information. Whaling does not necessarily involve phone calls or voice messages. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 3.1

**NEW QUESTION 248**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 253**

A user called the help desk to report an issue with the internet connection speed on a laptop. The technician thinks that background services may be using extra bandwidth. Which of the following tools should the technician use to investigate connections on the laptop?

- A. nslookup
- B. net use
- C. netstat
- D. net user

**Answer:** C

**Explanation:**

netstat is a tool that can be used to investigate connections on a Windows machine. It displays information about the active TCP connections, listening ports,

routing tables, network statistics, etc. nslookup is a tool that can be used to query DNS servers and resolve domain names to IP addresses. net use is a tool that can be used to connect or disconnect network drives or printers. net user is a tool that can be used to create or modify user accounts on a Windows machine. Verified References: <https://www.comptia.org/blog/what-is-netstat> <https://www.comptia.org/certifications/a>

#### NEW QUESTION 257

A technician receives a call from a user who is having issues with an application. To best understand the issue, the technician simultaneously views the user's screen with the user. Which of the following would BEST accomplish this task?

- A. SSH
- B. VPN
- C. VNC
- D. RDP

**Answer: C**

#### Explanation:

VNC (Virtual Network Computing) is a protocol that allows a technician to simultaneously view and control a user's screen remotely. VNC uses a server-client model, where the user's computer runs a VNC server and the technician's computer runs a VNC client. VNC can work across different platforms and operating systems<sup>3</sup>. SSH (Secure Shell) is a protocol that allows a technician to access a user's command-line interface remotely, but not their graphical user interface. VPN (Virtual Private Network) is a technology that creates a secure and encrypted connection over a public network, but does not allow screen sharing. RDP (Remote Desktop Protocol) is a protocol that allows a technician to access a user's desktop remotely, but not simultaneously with the user.

#### NEW QUESTION 258

A systems administrator received a request to limit the amount of cellular data a user's Windows 10 tablet can utilize when traveling. Which of the following can the administrator do to best solve the user's issue?

- A. Turn on airplane mode.
- B. Set the connection to be metered.
- C. Configure the device to use a static IP address.
- D. Enable the Windows Defender Firewall.

**Answer: B**

#### Explanation:

Setting the connection to be metered is the best solution for limiting the amount of cellular data a user's Windows 10 tablet can utilize when traveling. A metered connection is a network connection that has a data limit or charges fees based on the amount of data used. Windows 10 allows users to set any network connection as metered, which reduces the amount of data that Windows and some apps use in the background. For example, setting a connection as metered will prevent Windows from downloading updates automatically, stop some apps from syncing data online, and disable some live tiles on the Start menu. Setting a connection as metered can help users save cellular data and avoid extra charges when traveling. Turning on airplane mode, configuring the device to use a static IP address, and enabling the Windows Defender Firewall are not effective solutions for limiting the amount of cellular data a user's Windows 10 tablet can utilize when traveling. Turning on airplane mode will disable all wireless connections on the device, including Wi-Fi, Bluetooth, and cellular data. This will prevent the user from accessing any online services or applications on the tablet. Configuring the device to use a static IP address will assign a fixed IP address to the device instead of obtaining one dynamically from a DHCP server. This will not affect the amount of cellular data the device uses, and it may cause IP conflicts or connectivity issues on some networks. Enabling the Windows Defender Firewall will block or allow incoming and outgoing network traffic based on predefined or custom rules. This will not reduce the amount of cellular data the device

uses, and it may interfere with some apps or services that require network access. References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 19

? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 108

#### NEW QUESTION 262

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: D**

#### Explanation:

An IP address is a unique identifier that allows a device to communicate with other devices on a network. A network printer needs an IP address to be accessible by multiple users on the network. Requesting an unused IP address from the network administrator or using an IP address scanner is the step that should happen immediately before network use is authorized, as it ensures that there is no IP address conflict or duplication on the network. Documenting the date and time of the change, submitting a change request form, and determining the risk level of this change are steps that should happen before requesting an unused IP address.

#### NEW QUESTION 267

The calendar application on an employee's smartphone is experiencing frequent crashes, and the smartphone has become unresponsive. Which of the following should a technician do first to resolve the issue?

- A. Reinstall the application on the smartphone.
- B. Update the smartphone's OS.
- C. Reset the smartphone to factory settings.
- D. Reboot the smartphone.

**Answer: D**

#### Explanation:



Rebooting the smartphone is the first and simplest step to resolve the issue of frequent crashes and unresponsiveness. Rebooting clears the memory, closes the background apps, and refreshes the system. It can also fix minor glitches and bugs that may cause the calendar app or the smartphone to malfunction<sup>12</sup>. The other options are either too drastic or unnecessary. Reinstalling the application may not solve the problem if the issue is with the smartphone itself. Updating the smartphone's OS may not be possible or helpful if the device is unresponsive or incompatible. Resetting the smartphone to factory settings will erase all the data and settings on the device, which should be the last resort.

References: 1 How to Reboot an Android Smartphone or Tablet(<https://www.lifewire.com/reboot-android-smartphone-or-tablet-4127180>)2 How to Restart or Shut Down a Smartphone or Tablet(<https://www.computerhope.com/issues/ch001912.htm>).

#### NEW QUESTION 272

A user is unable to use any internet-related functions on a smartphone when it is not connected to Wi-Fi. When the smartphone is connected to Wi-Fi, the user can browse the internet and send and receive email. The user is also able to send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi. Which of the following is the MOST likely reason the user is unable to use the internet on the smartphone when it is not connected to Wi-Fi?

- A. The smartphone's line was not provisioned with a data plan
- B. The smartphone's SIM card has failed
- C. The smartphone's Bluetooth radio is disabled.
- D. The smartphone has too many applications open

**Answer:** A

#### Explanation:

The smartphone's line was not provisioned with a data plan. The user is unable to use any internet-related functions on the smartphone when it is not connected to Wi-Fi because the smartphone's line was not provisioned with a data plan. The user can send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi because these functions do not require an internet connection<sup>1</sup>

#### NEW QUESTION 274

A user is unable to access a remote server from a corporate desktop computer using the appropriate terminal emulation program. The user contacts the help desk to report the issue. Which of the following clarifying questions would be most effective for the help desk technician to ask the user in order to understand the issue?

- A. What is the error message?
- B. Does the program work on another computer?
- C. Did the program ever work?
- D. Is anyone else having this issue?

**Answer:** A

#### Explanation:

The most effective clarifying question for the help desk technician to ask the user in order to understand the issue is A. What is the error message? This question will help the technician to identify the possible cause and solution of the problem, as the error message will provide specific information about the nature and location of the error, such as the server name, the port number, the protocol, the authentication method, or the network status. The error message will also help the technician to troubleshoot the issue by following the suggested steps or searching for the error code online.

This question is more effective than the other choices because:

? B. Does the program work on another computer? is not a very helpful question, as it will not reveal the source of the error or how to fix it. The program may work on another computer for various reasons, such as different network settings, firewall rules, permissions, or software versions. However, this question will not tell the technician what is wrong with the user's computer or the remote server, or what needs to be changed or updated to make the program work.

? C. Did the program ever work? is not a very relevant question, as it will not address the current issue or how to resolve it. The program may have worked in the past, but it may have stopped working due to changes in the network configuration, the server status, the software updates, or the user credentials. However, this question will not tell the technician what has changed or how to restore the program functionality.

? D. Is anyone else having this issue? is not a very useful question, as it will not explain the reason or the solution for the error. The issue may affect only the user, or multiple users, depending on the scope and the impact of the error. However, this question will not tell the technician what is causing the error or how to fix it for the user or the others.

References:

How to Troubleshoot Terminal Emulation Problems - Techwalla : How to Read and Understand Windows Error Messages - Lifewire : How to Troubleshoot Network Connectivity Problems - How-To Geek : How to Troubleshoot Software Problems - dummies : How to Troubleshoot Common PC Issues For Users - MakeUseOf

#### NEW QUESTION 276

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

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

**Answer:** B

#### Explanation:

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

The technician can go to the Windows 10 Settings menu, select the Privacy submenu, and under App permissions, select Microphone. The technician should then turn on the toggle switch for the VoIP application to allow it to access the microphone.

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

#### NEW QUESTION 281

Which of the following does MFA provide?



- ? Security enhancement
- ? Encryption
- ? Digital signature

A. Public key infrastructure

**Answer:** A

**Explanation:**

MFA stands for multi-factor authentication, which is an electronic authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN1. MFA provides security enhancement by making it harder for attackers to compromise the user's identity or credentials, as they would need to obtain more than just the username and password. MFA can also prevent unauthorized access to sensitive data or resources, as well as reduce the risk of identity theft or fraud2.

**NEW QUESTION 283**

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

- A. MSRA
- B. VNC
- C. VPN
- D. SSH

**Answer:** C

**Explanation:**

A technician needs to interconnect two offices to the main branch while complying with good practices and security standards. The technician should implement VPN

**NEW QUESTION 288**

A laptop that was in the evidence room of a police station is missing. Which of the following is the best reason to refer to chain of custody documentation?

- A. To determine which party had the machine and when.
- B. To remotely wipe sensitive data from the machine.
- C. To gather the information needed to replace the machine.
- D. To alert the owner that the password needs to be changed.

**Answer:** A

**Explanation:**

Chain of custody documentation is a record of the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence. It is important to maintain a chain of custody to ensure the integrity and authenticity of the evidence, and to prevent tampering or contamination. If a laptop that was in the evidence room of a police station is missing, the best reason to refer to chain of custody documentation is to determine which party had the machine and when. This can help to identify the possible suspects, locate the missing laptop, and verify if the evidence on the laptop was compromised or not

**NEW QUESTION 291**

A user lost a company tablet that was used for customer intake at a doctor's office. Which of the following actions would BEST protect against unauthorized access of the data?

- A. Changing the office's Wi-Fi SSID and password
- B. Performing a remote wipe on the device
- C. Changing the user's password
- D. Enabling remote drive encryption

**Answer:** B

**Explanation:**

The best action to protect against unauthorized access of the data on the lost company tablet is to perform a remote wipe on the device. A remote wipe is a feature that allows an administrator or a user to erase all the data and settings on a device remotely, usually through a web portal or an email command. A remote wipe can help prevent the data from being accessed or compromised by anyone who finds or steals the device. Changing the office's Wi-Fi SSID and password may prevent the device from connecting to the office network but may not prevent the data from being accessed locally or through other networks. Changing the user's password may prevent the device from logging in to the user's account but may not prevent the data from being accessed by other means or accounts. Enabling remote drive encryption may protect the data from being read by unauthorized parties but may not be possible if the device is already lost or turned off. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 3.1

**NEW QUESTION 293**

Which of the following is the proper way for a technician to dispose of used printer consumables?

- A. Proceed with the custom manufacturer's procedure.
- B. Proceed with the disposal of consumables in standard trash receptacles.
- C. Empty any residual ink or toner from consumables before disposing of them in a standard recycling bin.
- D. Proceed with the disposal of consumables in standard recycling bins.

**Answer:** A

**Explanation:**

When it comes to disposing of used printer consumables , it is important to follow the manufacturer's instructions or guidelines for proper disposal, as different

types of consumables may require different disposal procedures. Some manufacturers provide specific instructions for proper disposal, such as sending the used consumables back to the manufacturer or using special recycling programs. Therefore, the proper way for a technician to dispose of used printer consumables is to proceed with the custom manufacturer's procedure, if provided. This option ensures that the disposal is handled in an environmentally friendly and safe manner.

#### NEW QUESTION 297

A technician is familiar with most personnel at a customer's location and has clearance to work unsupervised. Which of the following describes how the technician should handle personal communication while on site?

- A. Respond to calls and text messages while on site but not when working directly with personnel.
- B. Respond to calls and text messages only from family.
- C. Respond to calls and text messages only when an emergency situation requires a response.
- D. Respond to calls and text messages discreetly while on site.

**Answer:** C

#### Explanation:

A technician should handle personal communication while on site in a professional and respectful manner. According to the CompTIA A+ Core 2 (220-1102) exam objectives, one of the best practices for communication skills is to “avoid distractions and interruptions” when working with customers<sup>1</sup>. This means that the technician should not respond to calls and text messages that are not related to the work or the customer, unless there is an emergency situation that requires a response. Responding to personal communication while on site can be seen as rude, unprofessional, and disrespectful to the customer and their time. It can also affect the quality and efficiency of the technician's work and cause errors or delays. Therefore, the technician should only respond to calls and text messages when an emergency situation requires a response, and inform the customer about the situation and apologize for the interruption.

The other options are not appropriate for handling personal communication while on site.

Responding to calls and text messages while on site but not when working directly with personnel (A) is still distracting and unprofessional, as it can interfere with the technician's focus and productivity. Responding to calls and text messages only from family (B) is not a valid criterion, as the technician may receive calls and text messages from other sources that are not related to the work or the customer. Responding to calls and text messages discreetly while on site (D) is not a good practice, as it can still be noticed by the customer or other personnel and create a negative impression.

References:

1: CompTIA A+ Certification Exam Core 2 Objectives - CompTIA

#### NEW QUESTION 300

A customer reported that a home PC with Windows 10 installed in the default configuration is having issues loading applications after a reboot occurred in the middle of the night. Which of the following is the FIRST step in troubleshooting?

- A. Install alternate open-source software in place of the applications with issues
- B. Run both CPU and memory tests to ensure that all hardware functionality is normal
- C. Check for any installed patches and roll them back one at a time until the issue is resolved
- D. Reformat the hard drive, and then reinstall the newest Windows 10 release and all applications.

**Answer:** C

#### Explanation:

The first step in troubleshooting is to check for any installed patches and roll them back one at a time until the issue is resolved. This can help to identify any patches that may be causing the issue and allow them to be removed.

#### NEW QUESTION 303

A user is receiving repeated pop-up advertising messages while browsing the internet. A malware scan is unable to locate the source of an infection. Which of the following should the technician check NEXT?

- A. Windows updates
- B. DNS settings
- C. Certificate store
- D. Browser plug-ins

**Answer:** D

#### Explanation:

Browser plug-ins are software components that add functionality to a web browser, such as playing videos, displaying animations, etc. However, some browser plug-ins can also be malicious or compromised and cause unwanted pop-up advertising messages while browsing the internet. A malware scan may not be able to locate the source of the infection if it is hidden in a browser plug-in. Windows updates, DNS settings and certificate store are not likely sources of pop-up advertising messages. Verified References: <https://www.comptia.org/blog/browser-security> <https://www.comptia.org/certifications/a>

#### NEW QUESTION 306

A technician receives an invalid certificate error when visiting a website. Other workstations on the same local network are unable to replicate this issue. Which of the following is most likely causing the issue?

- A. Date and time
- B. User access control
- C. UEFI boot mode
- D. Log-on times

**Answer:** A

#### Explanation:

Date and time is the most likely cause of the issue. The date and time settings on a workstation affect the validity of the certificates used by websites to establish secure connections. If the date and time are incorrect, the workstation may not recognize the certificate as valid and display an invalid certificate error. Other

workstations on the same local network may not have this issue if their date and time are correct. User access control, UEFI boot mode, and log-on times are not likely causes of the issue. User access control is a feature that prevents unauthorized changes to the system by prompting for confirmation or credentials. UEFI boot mode is a firmware interface that controls the boot process of the workstation. Log-on times are settings that restrict when a user can log in to the workstation. None of these factors affect the validity of the certificates used by websites. References:  
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 14  
? CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 456

#### NEW QUESTION 308

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

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

**Answer:** C

#### **Explanation:**

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

#### NEW QUESTION 312

.....

## Relate Links

**100% Pass Your 220-1102 Exam with ExamBible Prep Materials**

<https://www.exambible.com/220-1102-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>