PassQueen
a.k.a dumpsqueen.com

CompTIA A+ Certification Exam: Core 2

CompTIA 220-1202

Version Demo

Total Demo Questions: 54

Total Premium Questions: 548

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Security	208
Topic 2, Operating Systems	157
Topic 3, Software Troubleshooting	84
Topic 4, Operational Procedures	96
Topic 5, Mix Questions	3
Total	548

QUESTION NO: 1

A senior administrator asks a help desk technician to run a set of commands on a remote network switch. After running the commands, the technician needs to collect the output and provide it to the administrator. Which of the following should the technician use to fulfill the administrator ' s request?

A. RDP

B. WinRM

C. SSH

D. VNC

ANSWER: C

Explanation:

SSH is the appropriate tool because it provides a secure, encrypted remote command-line session to a network switch. A technician can connect to the switch's management interface, authenticate with authorized credentials, enter the required administrative or diagnostic commands, and capture the resulting command output for the senior administrator. This workflow is a standard use of SSH in network administration: it supports interactive access to a device CLI while protecting authentication data and session traffic from interception. SSH is particularly suitable for managed switches because network-device operating systems commonly expose their administrative CLI through SSH on the network. The SSH architecture is designed for secure remote login and command execution, including the transport, authentication, and connection protocols needed to establish a protected management session. The technician can also save terminal output locally or use session logging, preserving the command results as requested. For technical background on SSH, see RFC 4251: The Secure Shell (SSH) Protocol Architecture. Cisco's guidance on configuring SSH for secure device management is available in the Cisco IOS Secure Shell Configuration Guide.

QUESTION NO: 2

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

• The device is hot even when it is not in use.

•Applications crash, especially when others are launched

• Certain applications, such as GPS, are in portrait mode when they should be in landscape mode

Which of the following can the technician do to MOST likely resolve these issues with minimal impact? (Select TWO).

A. Turn on autorotation

B. Activate airplane mode.

C. Close unnecessary applications

D. Perform a factory reset

E. Update the device's operating system

F. Reinstall the applications that have crashed.

ANSWER: A C

Explanation:

Close unnecessary applications is an appropriate minimal-impact troubleshooting action because background and stalled applications can consume processor time, memory, battery power, and network resources even when the user is not actively using the phone. Resource contention can contribute to applications crashing when additional applications are opened, while sustained processor activity can increase device temperature. Closing unneeded running applications reduces the active

workload without removing user data, changing device-wide configuration, or requiring a disruptive recovery process. Android documents how users can view and close recently used applications at Google Android Help.

Turn on autorotation directly addresses applications displaying in portrait orientation when landscape orientation is expected. Mobile operating systems use motion sensors and the rotation setting to determine whether supported applications may switch between portrait and landscape views. If rotation is locked, an application that normally supports landscape display, including mapping or navigation software, can remain in portrait orientation despite the device being turned. Enabling autorotation restores normal sensor-based orientation changes while preserving applications, settings, and employee data. Apple describes how orientation lock affects screen rotation and how to enable rotation at Apple Support. Together, these actions target the identified resource-use and display-orientation symptoms with the least impact on the employee.

QUESTION NO: 3

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

A. Device drivers

B. Keyboard backlight settings

C. Installed application license keys

D. Display orientation

E. Target device power supply

F. Disabling express charging

ANSWER: A C

Explanation:

Device drivers are a key consideration because the master image must start reliably and provide appropriate hardware support on the devices receiving it. The engineer should use a driver approach compatible with the target hardware fleet, such as including broadly applicable drivers in the image or applying model-specific driver packages during deployment. Microsoft's Sysprep process is designed to generalize a Windows installation before it is captured and deployed, helping the image be used across systems while allowing device-specific setup to occur on first boot. See Microsoft's Sysprep overview.

Installed application license keys must also be considered because a master image can replicate installed software and its activation state to every deployed endpoint. The organization needs to ensure that each deployment uses an appropriate volume-license, subscription-based, or otherwise properly assigned license model, rather than inadvertently duplicating a device-specific or user-specific key. License planning should occur before capture so activation and compliance remain manageable after rollout. Microsoft documents activation methods, including volume activation, at Windows volume activation documentation.

QUESTION NO: 4

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

A. Scan the computer with the company-provided antivirus software

B. Install a new hard drive and clone the user's drive to it

C. Deploy an ad-blocking extension to the browser.

D. Uninstall the company-provided antivirus software

E. Click the link in the messages to pay for virus removal

F. Perform a reset on the user's web browser

ANSWER: C F

Explanation:

Deploying an ad-blocking extension to the browser and performing a reset on the user's web browser are appropriate because the symptoms are confined to browser startup and resemble scareware or malicious advertising rather than a confirmed operating-system infection. An ad-blocking extension reduces exposure to intrusive advertisements, deceptive pop-ups, and malicious ad content that can display fake infection counts and fraudulent payment demands. In an organization, the extension should be approved and deployed in accordance with company policy. Resetting the browser restores key browser settings to their defaults and can remove unwanted extensions, altered startup behavior, and configuration changes that cause recurring pop-ups. It is particularly useful when the issue appears immediately upon opening the browser, which can indicate a malicious extension, changed homepage, restored session content, or notification-related browser configuration. These actions address the browser-specific persistence mechanism while avoiding interaction with the fraudulent message or payment site. After remediation, the technician should verify the browser opens normally and ensure browser updates and approved security protections remain enabled. Microsoft provides guidance on managing unwanted browser extensions and resetting Microsoft Edge settings at Microsoft Support: Manage Edge extensions and Microsoft Support: Reset Edge settings.

QUESTION NO: 5

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

A. Adjust the content filtering.

B. Unmap port forwarding.

C. Disable unused ports.

D. Reduce the encryption strength

ANSWER: A

Explanation:

Adjust the content filtering. Content filtering, which may be configured on a SOHO router, firewall, DNS filtering service, or endpoint-security product, can block web requests according to website categories, reputation, URLs, domains, or organizational policy. If the corporate site is being categorized incorrectly or is included in a blocked category, the technician should review the filtering logs or policy, confirm that the site is legitimate and required for business use, and add the required domain or URL to an allow list. The change should be as narrow as practical—for example, allowing the specific corporate domain rather than broadly disabling web protection. After updating the policy, the technician should retry access and, if applicable, clear cached DNS or browser data so the updated rule is used. This approach restores access while retaining the SOHO network's overall protections against malicious, inappropriate, or otherwise restricted content. Microsoft describes web content filtering as a way to regulate access to sites based on categories and to create custom indicators for specific domains: Microsoft Learn: Web content filtering. Additional background on how content filters screen access to webpages is available from Fortinet: Content filtering.

QUESTION NO: 6

A company is issuing Windows laptops to employees who will frequently work from public locations. Which of the following configurations would BEST protect the laptops if they are lost or stolen? (Select TWO).

A. Enable BitLocker Drive Encryption

B. Disable User Account Control

C. Require a screen lock with a strong password

D. Enable AutoRun for removable media

E. Configure a shared local administrator account

ANSWER: A C

Explanation:

Enable BitLocker Drive Encryption protects data at rest by encrypting the laptop storage. If an unauthorized person obtains the device or removes its drive, the contents remain protected without the required authentication or recovery material.

Require a screen lock with a strong password protects an active or unattended laptop from casual unauthorized use. A short inactivity timeout helps ensure that a user who steps away from the device does not leave an accessible session open. These controls provide complementary protection for stored data and active sessions. Microsoft describes BitLocker in its BitLocker documentation and provides guidance on Windows sign-in and lock-screen settings in Windows account support.

QUESTION NO: 7

A technician installs a Bluetooth headset for a user. During testing, the sound still comes from the speaker on the computer. The technician verifies the headset shows up in Device Manager. Which of the following would the technician most likely do to fix this issue?

A. Update the drivers for the wireless headset

B. Replace the battery on the headset and try again later

C. Verify that the sound is not muted in the control panel

D. Change the headset as the default device in sound settings

ANSWER: D

Explanation:

Change the headset as the default device in sound settings is correct because Device Manager recognition confirms that Windows detects the Bluetooth headset, but it does not necessarily mean Windows is directing audio to it. Windows can retain the computer speakers as the active output device after a headset is paired or installed. The technician should open Sound settings and select the Bluetooth headset as the output device; in the classic Sound control panel, this may be done by selecting the headset on the Playback tab and setting it as the default playback device. This directs system audio and applications that use the default output path to the headset. The technician should also confirm that the appropriate headset playback profile is selected when more than one Bluetooth audio endpoint is shown. Microsoft documents changing an audio output device through the Sound settings output selector, and its Bluetooth guidance explains connecting and managing Bluetooth audio devices in Windows. See Microsoft: Fix sound or audio problems in Windows and Microsoft: Pair a Bluetooth device in Windows.

QUESTION NO: 8

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

A. Encrypting File System

B. FileVault

C. BitLocker

D. Encrypted LVM

ANSWER: C

Explanation:

BitLocker is the appropriate full-disk encryption solution for a Windows laptop. BitLocker Drive Encryption is built into supported Windows editions and encrypts the entire operating-system volume, including the operating system, installed applications, system files, and user data. This protects information if the laptop is lost or stolen because the contents of the drive cannot be accessed without satisfying the configured startup and recovery requirements. BitLocker commonly uses the device's Trusted Platform Module (TPM) to protect encryption keys and verify system integrity during startup. An organization can also require a startup PIN and escrow recovery keys centrally through supported management and identity services, helping meet corporate security and recovery requirements for mobile endpoints. Microsoft distinguishes BitLocker drive encryption from file-level protection: its purpose is to protect data at rest across the full volume. For a newly deployed Windows corporate laptop, the technician should enable BitLocker and ensure that a recovery-key process is in place before the device is issued. See Microsoft Learn: BitLocker overview and Microsoft Learn: BitLocker Drive Encryption overview.

QUESTION NO: 9 - (HOTSPOT)

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

use the Testing program.

INSTRUCTIONS

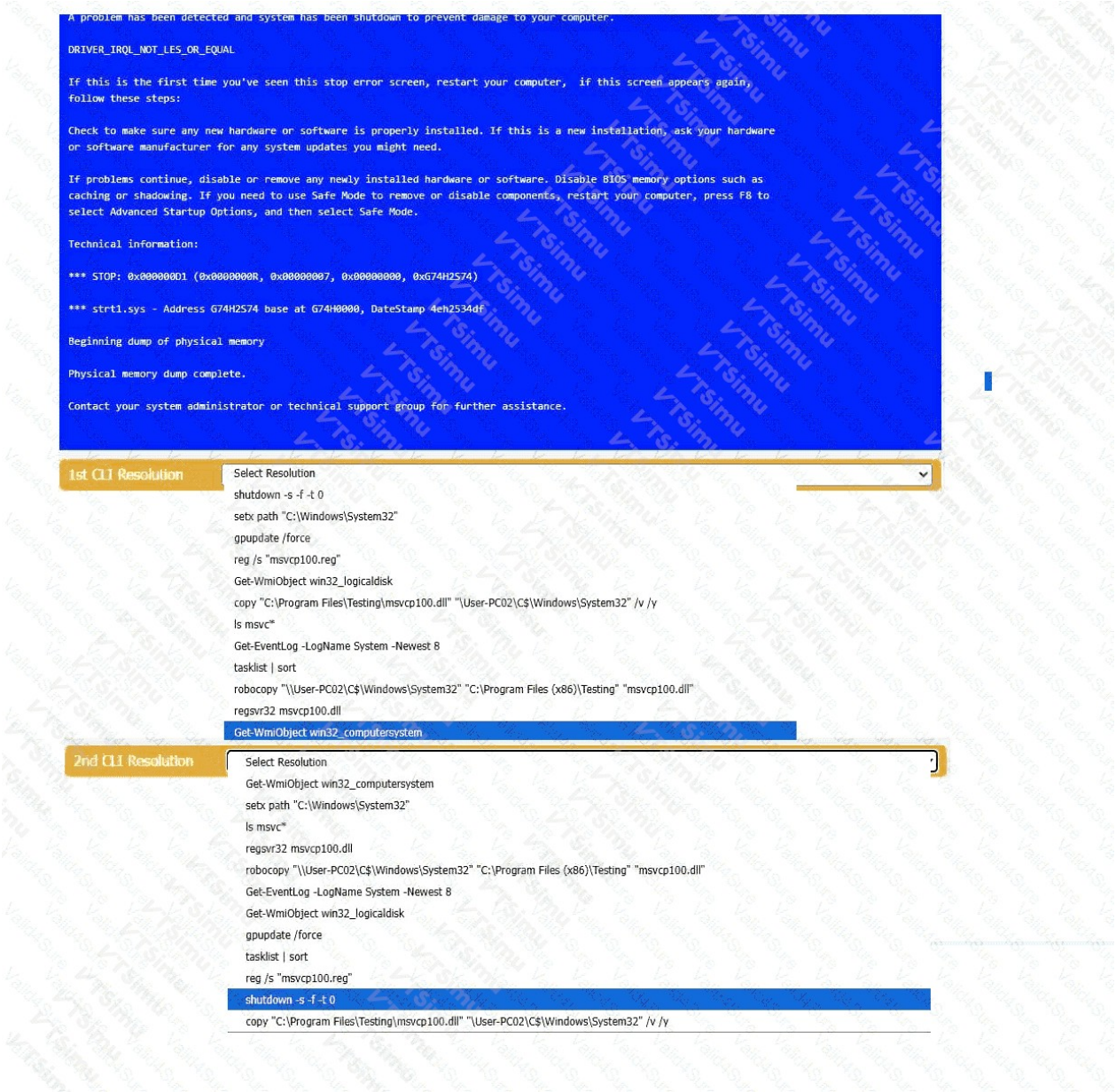
Review the information in each tab to verify the results of the deployment and resolve

any issues discovered by selecting the:

Â· First command to resolve the issue

Â· Second command to resolve the issue


BSOD
Commands
System Error
Show Question
Reset All Answers
The program can't start because MSVCP100.dll is missing from your computer. Try reinstalling the program to fix this problem.
OK


A problem has been detected and system has been shutdown to prevent damage to your computer.
DRIVER_IRQL_NOT_LES_OR_EQUAL
If this is the first time you've seen this stop error screen, restart your computer, if this screen appears again, follow these steps:
Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any system updates you might need.
If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.
Technical information:
*** STOP: 0x000000D1 (0x0000000R, 0x00000007, 0x00000000, 0xG74H2S74)
*** strt1.sys - Address G74H2S74 base at G74H0000, DateStamp 4eh2534df
Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further assistance.
1st CLI Resolution
Select Resolution
shutdown -s -f -t 0
setx path "C:\Windows\System32"
gpupdate /force
reg /s "msvcp100.reg"
Get-WmiObject win32_logicaldisk
copy "C:\Program Files\Testing\msvcp100.dll" "\User-PC02\C$\Windows\System32" /v /y
ls msvc*
Get-EventLog -LogName System -Newest 8
tasklist | sort
robocopy "\\User-PC02\C$\Windows\System32" "C:\Program Files (x86)\Testing" "msvcp100.dll"
regsvr32 msvcp100.dll
Get-WmiObject win32_computersystem
2nd CLI Resolution
Select Resolution
Get-WmiObject win32_computersystem
setx path "C:\Windows\System32"
ls msvc*
regsvr32 msvcp100.dll
robocopy "\\User-PC02\C$\Windows\System32" "C:\Program Files (x86)\Testing" "msvcp100.dll"
Get-EventLog -LogName System -Newest 8
Get-WmiObject win32_logicaldisk
gpupdate /force
tasklist | sort
reg /s "msvcp100.reg"
shutdown -s -f -t 0
copy "C:\Program Files\Testing\msvcp100.dll" "\User-PC02\C$\Windows\System32" /v /y

ANSWER:

Explanation:

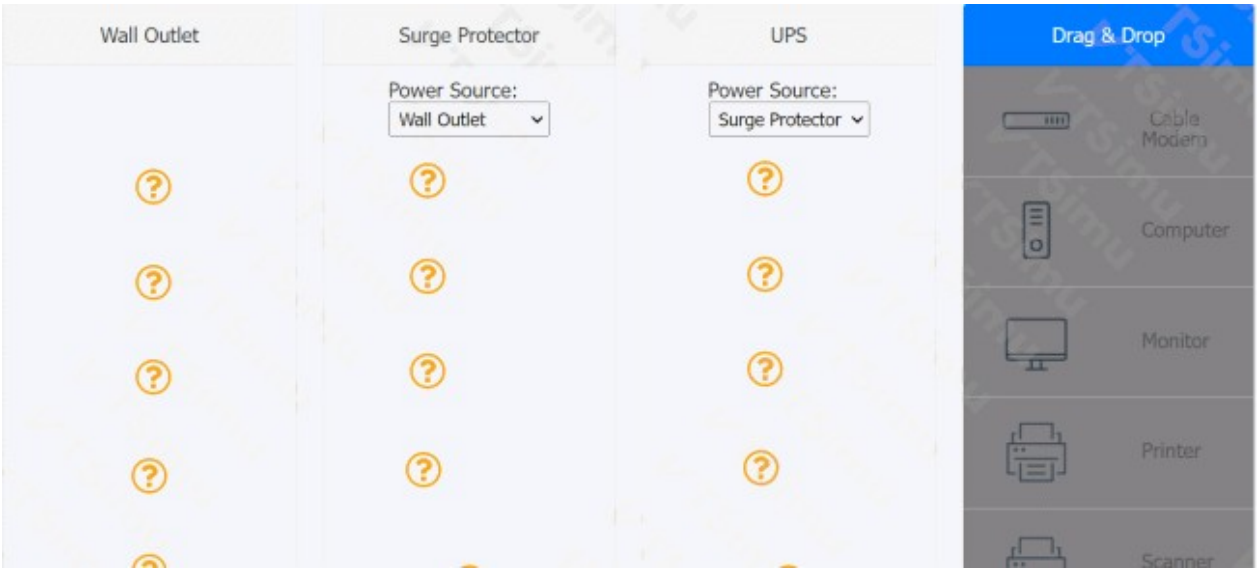
The error shown after the Testing application upgrade is specific: Windows reports that `MSVCP100.dll` is missing. Because other employees can still open and use Testing, the deployment problem is isolated to the affected workstation rather than being a general outage of the application or its shared services. The appropriate repair is therefore to restore the missing dependency on that workstation.

The first selected command copies `msvcp100.dll` from `C:\Program Files\Testing\msvcp100.dll` to `\\User-PC02\C$\Windows\System32`. This directly supplies the file named in the error to the affected computer. The administrative `C$` share targets the remote computer's Windows drive, allowing the repair to be performed remotely. The `/v` parameter requests verification that the copy was written correctly, while `/y` suppresses an overwrite confirmation so the command can complete without interaction. Microsoft documents the behavior of these COPY parameters in its COPY command reference.

After restoring the file, the selected `regsvr32 msvcp100.dll` command is the intended second remediation step in this scenario. Running Regsvr32 registers the DLL so Windows can make the library available to the application following the deployment repair. Microsoft describes Regsvr32 as the Windows command-line utility used to register DLL modules in its Regsvr32 command reference. Performing the copy first is essential because the registration command requires the DLL to be present locally before it can process it. Together, the selected commands restore the missing Testing dependency on User-PC02 and then complete the required registration step.

QUESTION NO: 10 - (DRAG DROP)

A customer recently experienced a power outage at a SOHO. The customer does not think the components are connected properly. A print job continued running for several minutes after the power failed, but the customer was not able to interact with the computer. Once the UPS stopped beeping, all functioning devices also turned off. In case of a future power failure, the customer wants to have the most time available to save cloud documents and shut down the computer without losing any data.



ANSWER:

Explanation:

For the longest practical amount of time to save cloud-based work safely, the UPS must be powered directly by the wall outlet and must supply the equipment required for both computer use and Internet access. That includes the computer, monitor, cable modem, and Wi-Fi router. The monitor is necessary because the user must be able to see and interact with the computer while saving documents and performing an orderly shutdown. The cable modem and Wi-Fi router must remain online so that cloud documents can synchronize before the UPS battery is depleted.

A UPS provides battery-backed power during an outage, allowing a workstation to continue operating briefly rather than shutting off immediately. This is precisely the purpose described in APC's guidance on UPS use: it provides temporary battery power so equipment can remain operational and be shut down safely. See APC UPS frequently asked questions. Connecting the UPS directly to a wall receptacle is the appropriate power arrangement; UPS manufacturers commonly advise against plugging a UPS into a surge strip because it can interfere with safe operation and power delivery. CyberPower also documents this guidance at CyberPower's UPS connection FAQ.

The surge protector should be powered from the wall outlet and used for the printer and scanner. These peripherals do not need to remain available to save cloud documents, and keeping them off the battery-backed UPS outlets preserves battery capacity for the computer, display, modem, and router. This layout separates essential outage-time equipment from nonessential peripherals while still providing surge protection where it is needed.

QUESTION NO: 11

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

A. macOS

B. Linux

C. Chrome OS

D. Windows

ANSWER: C

Explanation:

Chrome OS is the most likely operating system because it is Google's proprietary, cloud-centric operating system designed around web applications, browser-based workflows, and online services. ChromeOS devices, commonly called Chromebooks, were initially strongly associated with lightweight, low-cost notebook and netbook-style hardware. The platform starts quickly and centers the Chrome browser as the primary interface for accessing web apps, files, collaboration tools, and cloud storage. Although ChromeOS supports local applications and can provide offline capabilities, its design and user experience are fundamentally web based, matching the description in the question. Google identifies ChromeOS as the

operating system that powers Chromebooks and describes its integration with Google services and web-oriented productivity. Its streamlined architecture and automatic security updates also make it well suited to portable systems intended for straightforward internet use. For additional product information, see Google ChromeOS. Google's technical documentation also explains the platform's device-management and operating-system features at ChromeOS Help.

QUESTION NO: 12

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

A. Multifactor authentication will be forced for Wi-Fi

B. All Wi-Fi traffic will be encrypted in transit

C. Eavesdropping attempts will be prevented

D. Rogue access points will not connect

ANSWER: A

Explanation:

Multifactor authentication will be forced for Wi-Fi because access requires two distinct types of authentication evidence: the client certificate and the user's existing username and password. The certificate is a cryptographic credential installed on, or otherwise available to, the client device and represents something the user or device possesses. The username and password represent something the user knows. Requiring both during enterprise wireless authentication provides stronger assurance than relying on credentials alone: a party attempting to join the wireless network must have access to the enrolled certificate as well as valid user credentials.

In a typical enterprise Wi-Fi deployment, this arrangement is implemented with certificate-based Extensible Authentication Protocol methods, such as EAP-TLS or a related 802.1X configuration, backed by a RADIUS authentication service. Certificates enable the network to validate an approved client identity cryptographically, while the existing credentials provide an additional authentication factor when the selected method requires them. This meets the core security principle of multifactor authentication by combining different factor categories rather than merely requesting multiple passwords or repeated versions of the same credential. For background on multifactor authentication factors, see NIST SP 800-63B; for enterprise Wi-Fi authentication concepts, see Microsoft's EAP network access documentation.

QUESTION NO: 13

Which of the following methods would make data unrecoverable but allow the drive to be repurposed?

A. Deleting the partitions

B. Implementing EFS

C. Performing a low-level format

D. Degaussing the device

ANSWER: C

Explanation:

Performing a low-level format is the best answer in the context of this question because it is intended to overwrite the drive's storage areas, removing the previously stored data while leaving the physical device available for subsequent use. This meets both requirements: the original information is rendered unrecoverable through overwriting, and the drive itself remains operational so it can be repurposed. In modern storage environments, this concept is commonly implemented using a manufacturer-supported secure erase, sanitize command, or other approved overwrite-based sanitization procedure rather than a literal hardware-level format. These approaches are designed to clear data without physically destroying the media.

NIST SP 800-88 Rev. 1 describes sanitization methods that can render data recovery infeasible while allowing media to be reused when the selected technique and verification process are appropriate. It also emphasizes choosing a method supported by the storage technology and documenting verification. For solid-state drives especially, a drive-supported sanitize or cryptographic erase operation is generally preferable to a conventional overwrite because of wear leveling and inaccessible flash areas. See NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization and the NIST SP 800-88 Rev. 1 PDF.

QUESTION NO: 14

A technician is assigned to repair a customer laptop that contains personal photographs and financial documents. Which of the following actions demonstrate appropriate handling of the customer's private information? (Select TWO).

A. Obtain authorization before accessing user files

B. Limit access to files needed to resolve the issue

C. Copy personal files to a technician-owned USB drive

D. Review documents that are unrelated to the repair

E. Share interesting customer files with other technicians

F. Disable the customer account password permanently

ANSWER: A B

Explanation:

Obtain authorization before accessing user files is appropriate because the technician should have a business need and the customer’s permission before opening personal data. Authorization establishes the scope of the work and helps protect the customer’s privacy.

Limit access to files needed to resolve the issue is also appropriate. A technician should access only the information necessary for diagnosis, backup, repair, or validation and should avoid browsing unrelated personal files. These practices reduce unnecessary exposure of confidential information and support professional conduct.

QUESTION NO: 15

Which of the following is MOST likely contained in an EULA?

A. Chain of custody

B. Backup of software code

C. Personally identifiable information

D. Restrictions of use

ANSWER: D

Explanation:

Restrictions of use are most likely contained in an End-User License Agreement (EULA). A EULA is the legal agreement that governs a customer’s right to install, access, and use licensed software. It commonly defines the permitted scope of use, such as whether the software may be installed on a limited number of devices, used only by a particular individual or organization, or used for commercial rather than personal purposes. It also establishes restrictions, which can include prohibitions on copying, redistributing, reverse engineering, modifying, renting, sublicensing, or transferring the software except where applicable law permits those activities.

These use restrictions protect the software publisher’s intellectual-property rights and clarify the licensee’s obligations. The agreement can also state what happens if its terms are violated, including termination of the license. For a CompTIA A+

technician, recognizing restrictions of use as EULA content is important because software installation, deployment, and troubleshooting must remain within the rights granted by the vendor's license. The U.S. Copyright Office describes software as protected intellectual property, while Microsoft's license terms illustrate how software licenses specify authorized use and limitations. See the U.S. Copyright Office's computer-program copyright circular and Microsoft Software License Terms.

QUESTION NO: 16

A client reports that their browser ' s home page changed. Every time they run an internet search, the results are returned from unfamiliar websites. Which of the following actions should a technician take first to resolve the issue? (Select two)

A. Clear the browsing history

B. Run operating system updates

C. Check the system date and time

D. Uninstall malicious extensions

E. Reset browser startup page

F. Restart the user ' s machine

ANSWER: D E

Explanation:

The combination of an unexpectedly changed home page and searches being redirected to unfamiliar sites is a common sign of a browser hijacker or potentially unwanted browser modification. **Uninstall malicious extensions** is an appropriate first action because extensions can control browser settings, alter the default search provider, inject redirects, and persistently reapply unwanted configuration changes. The technician should inspect the browser's installed extensions and remove anything unauthorized or suspicious.

Reset browser startup page directly restores the user's intended startup behavior after the unauthorized setting change. This should include reviewing the configured home page, startup pages, and default search engine as applicable to the browser. Addressing both the likely persistence mechanism and the altered startup configuration returns the browser to a known-good state and resolves the reported symptoms at their source. These actions align with CompTIA A+ malware-removal concepts, which include identifying and remediating browser-based threats and restoring affected settings. See the CompTIA exam objectives and Google Chrome guidance for managing extensions.

QUESTION NO: 17

While assisting a customer with an issue, a support representative realizes the appointment is taking longer than expected and will cause the next customer meeting to be delayed by five minutes. Which of the following should the support representative do NEXT?

A. Send a quick message regarding the delay to the next customer.

B. Cut the current customer's time short and rush to the next customer.

C. Apologize to the next customer when arriving late.

D. Arrive late to the next meeting without acknowledging the time.

ANSWER: A

Explanation:

Send a quick message regarding the delay to the next customer. Proactively communicating the expected five-minute delay is the appropriate next step because it manages the customer's expectations before the scheduled meeting time and demonstrates professionalism, respect, and accountability. The representative should provide a brief, clear update as soon as the conflict is recognized, ideally including the revised expected start time. This lets the next customer use the time

productively, adjust their schedule if necessary, and avoid uncertainty about whether the representative will attend. Effective support interactions depend not only on resolving technical issues, but also on keeping customers informed when service commitments may be affected. A timely notification preserves trust while allowing the representative to continue giving the current customer appropriate assistance rather than abruptly ending an active support session. This approach aligns with customer-service best practices for setting expectations, communicating status, and following through on commitments. Microsoft's customer-service guidance emphasizes keeping customers informed through timely communications, and CompTIA's A+ Core 2 objectives include applying professional communication and customer-service practices. See Microsoft Learn: Customer Service and CompTIA Exam Objectives.

QUESTION NO: 18

A technician is closing a ticket after resolving an issue that prevented an employee from accessing a line-of-business application. Which of the following should the technician include in the ticket documentation? (Select TWO).

A. The symptoms and actions taken

B. The final resolution and user confirmation

C. The technician's personal password

D. Unrelated issues reported by other employees

E. The user's complete financial records

F. Unverified speculation about the cause

ANSWER: A B

Explanation:

The symptoms and actions taken should be documented so future technicians can understand the reported problem, troubleshooting process, and resolution. Accurate notes also help establish whether a similar incident is recurring.

The final resolution and user confirmation should also be included. Recording the implemented fix and confirmation that the service is functioning establishes that the issue was resolved and that the user accepted the outcome before closure. Effective ticket documentation supports knowledge sharing, accountability, and service-management reporting.

QUESTION NO: 19

A technician is troubleshooting a Windows workstation that displays repeated access-denied messages when a user attempts to open a shared folder. Which of the following should the technician verify? (Select TWO).

A. Share permissions

B. NTFS permissions

C. Display resolution

D. Default printer settings

E. Browser cache settings

ANSWER: A B

Explanation:

Share permissions should be verified because they control the access level granted when users connect to a folder over the network. A user may be denied access if the assigned share permission does not allow the requested action.

NTFS permissions should also be verified because they control access to folders and files on an NTFS-formatted volume. When a user accesses a shared NTFS folder across the network, the effective permissions are limited by both share and

NTFS permissions. The technician should confirm group membership and the permissions assigned to the user or the user's groups. Microsoft describes NTFS permissions and access control in NTFS overview.

QUESTION NO: 20

After a failed update, an application no longer launches and generates the following error message: Application needs to be repaired. Which of the following Windows 10 utilities should a technician use to address this concern?

A. Device Manager

B. Administrator Tools

C. Programs and Features

D. Recovery

ANSWER: C

Explanation:

Programs and Features is the appropriate utility because it provides access to maintenance actions for installed desktop applications, including a repair action when the application installer supports it. A failed application update can leave program files, registry entries, or installed components in an incomplete or inconsistent state. Selecting the affected program in Programs and Features and choosing its available Change or Repair maintenance option reruns the application's installer logic to restore required files and configuration without requiring a full Windows recovery operation. This directly addresses an error stating that the application itself needs repair.

In Windows, this interface is reached from Control Panel under Programs and Features. The exact maintenance choices displayed depend on how the software vendor packaged the application; some applications expose Repair directly, while others provide it after selecting Change. Microsoft documents that Programs and Features is used to change or repair installed programs, and that the available options are determined by the program's publisher. See Microsoft Support: Repair apps and programs in Windows and Microsoft Support: Uninstall or remove apps and programs.

QUESTION NO: 21

A company wants to use a single operating system for its workstations and servers and avoid licensing fees. Which of the following operating systems would the company most likely select?

A. Linux

B. Windows

C. macOS

D. Chrome OS

ANSWER: A

Explanation:

Linux is the most likely selection because it can be deployed on both workstation and server hardware while generally avoiding per-device operating-system licensing fees. Organizations can use Linux distributions with desktop environments for end-user workstations and purpose-built server distributions or configurations for services such as web hosting, file sharing, databases, virtualization, and directory-related infrastructure. Its open-source licensing model permits organizations to use, modify, and redistribute the underlying software under the applicable license terms, which makes it well suited to an organization seeking a common platform without traditional proprietary OS license costs. Although a company may choose to purchase optional enterprise support, security management, or subscription services from a vendor, those support costs are separate from mandatory workstation and server OS licensing fees. Linux also has broad hardware support and an extensive ecosystem of administrative tools and applications, allowing IT teams to standardize operational practices across endpoints and servers. The Linux kernel is released under the GNU General Public License version 2, and many

distributions are available without a license purchase. See the Linux kernel project overview and the GNU GPL version 2 license.

QUESTION NO: 22

A user is being directed by the help desk to look up a Windows PC's network name so the help desk can use a remote administration tool to assist the user. Which of the following commands would allow the user to give the technician the correct information? (Select TWO).

A. ipconfig /all

B. hostname

C. netstat /?

D. nslookup localhost

E. arp —a

F. ping :: 1

ANSWER: A B

Explanation:

The correct commands are **ipconfig /all** and **hostname**. In Windows, a PC's network name is its host name, which remote-management staff can use to identify or connect to the endpoint when name resolution and the organization's remote administration configuration support it. Running **hostname** at Command Prompt directly returns the local computer's host name, making it a quick and focused way for the user to provide the requested identifier. Microsoft documents that the hostname command displays the host name portion of the computer's full name: Microsoft hostname command reference.

Running **ipconfig /all** provides detailed TCP/IP configuration for every network adapter and includes a system-wide *Host Name* field near the top of its output. This lets the user locate and report the same computer name while also giving the technician useful contextual network details if further remote-connectivity troubleshooting is needed. The command's comprehensive output includes host and adapter configuration information, as described in the Microsoft ipconfig command reference. Therefore, either command enables the user to supply the Windows PC name requested by the help desk.

QUESTION NO: 23

A user reports that a workstation is displaying a ransomware message and is unable to open business documents. Which of the following should the technician do FIRST? (Select TWO).

A. Disconnect the workstation from the network

B. Notify the incident-response team

C. Pay the ransom using a corporate credit card

D. Reconnect all mapped network drives

E. Delete the ransom message

F. Immediately restore files to the workstation

ANSWER: A B

Explanation:

Disconnect the workstation from the network is appropriate because ransomware can spread to shared folders, mapped drives, and other reachable systems. Isolating the affected workstation limits the opportunity for the malware to encrypt additional organizational data or communicate with attacker-controlled infrastructure.

Notify the incident-response team is also appropriate because ransomware is a security incident that may require coordinated containment, evidence preservation, recovery, communication, and reporting actions. The technician should follow organizational incident-response procedures rather than attempting unapproved remediation that could destroy evidence or worsen the impact. CISA provides ransomware-response guidance at StopRansomware Guide.

QUESTION NO: 24

A company employee receives a text message stating that the employee's payroll account will be disabled unless a link is opened immediately. Which of the following describes this attack?

A. Smishing

B. Vishing

C. Whaling

D. Shoulder surfing

ANSWER: A

Explanation:

Smishing is correct because it is a phishing attack delivered through SMS or text messages. The attacker uses urgency and a payroll-related pretext to persuade the recipient to open a malicious link and potentially disclose credentials or other sensitive information.

The employee should avoid opening the link and report the message using the organization’s established security process. CISA describes phishing attempts delivered through text messages as smishing at CISA: Recognize and Report Phishing.

QUESTION NO: 25 - (SIMULATION)

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, and view applicable attachments to

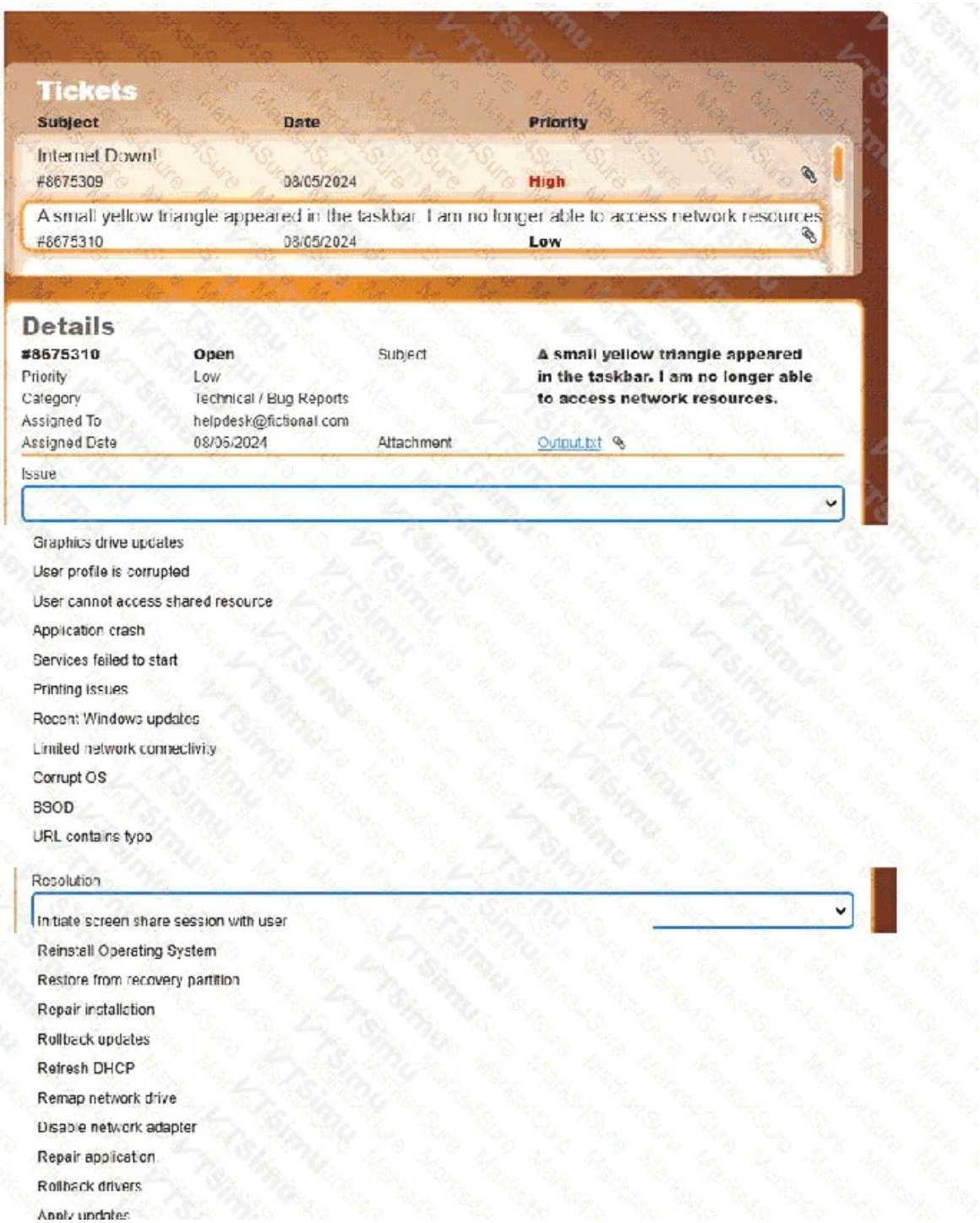
determine the problem.

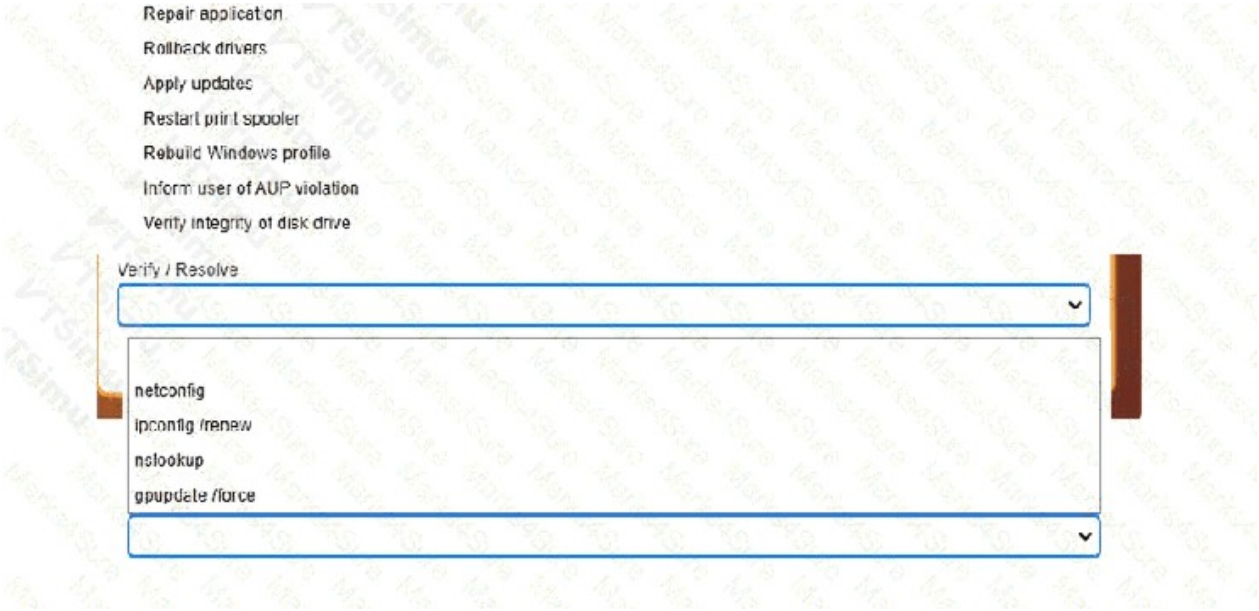
Select the appropriate issue from the ' Issue ' drop-down menu. Then, select the most

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.


Tickets
Subject
Date
Priority
Internet Down!
#8675309
08/05/2024
High
A small yellow triangle appeared in the taskbar. I am no longer able to access network resources
#8675310
08/05/2024
Low
Details
#8675310
Open
Subject
A small yellow triangle appeared in the taskbar. I am no longer able to access network resources.
Priority
Low
Category
Technical / Bug Reports
Assigned To
helpdesk@fictional.com
Assigned Date
08/05/2024
Attachment
Output.txt
Issue
Graphics drive updates
User profile is corrupted
User cannot access shared resource
Application crash
Services failed to start
Printing issues
Recent Windows updates
Limited network connectivity
Corrupt OS
BSOD
URL contains typo
Resolution
Initiate screen share session with user
Reinstall Operating System
Restore from recovery partition
Repair installation
Rollback updates
Refresh DHCP
Remap network drive
Disable network adapter
Repair application
Rollback drivers
Apply updates



ANSWER: See the explanation for the answer

Explanation:

Ticket #8675310 selections:

The yellow warning triangle on the Windows network icon indicates the device has limited connectivity. Renewing the DHCP lease is the most efficient remediation to obtain a valid IP address, default gateway, and DNS configuration.

QUESTION NO: 26

The Chief Executive Officer at a bark recently saw a news report about a high-profile cybercrime where a remote-access tool that the bank uses for support was also used in this crime. The report stated that attackers were able to brute force passwords to access systems. Which of the following would BEST limit the bark's risk? (Select TWO)

A. Enable multifactor authentication for each support account

B. Limit remote access to destinations inside the corporate network

C. Block all support accounts from logging in from foreign countries

D. Configure a replacement remote-access tool for support cases.

E. Purchase a password manager for remote-access tool users

F. Enforce account lockouts after five bad password attempts

ANSWER: A F

Explanation:

Enable multifactor authentication for each support account directly reduces the likelihood that a remotely brute-forced or otherwise compromised password alone can be used to access the support tool. Multifactor authentication requires an additional factor, such as an authenticator prompt, hardware security key, or time-based one-time code. This provides an important access-control layer for privileged or remotely accessible support accounts, which are valuable targets in real-world attacks.

Enforce account lockouts after five bad password attempts limits repeated online password guesses against an account. A lockout threshold interrupts a rapid sequence of failed authentication attempts and makes automated brute-force activity substantially less effective. In an operational environment, this should be paired with alerting, logging, and an account-recovery process so administrators can investigate whether the failed attempts indicate an attack. Together,

multifactor authentication and a failed-attempt lockout policy address both successful password compromise and the repeated guessing behavior specifically described in the scenario. NIST identifies throttling failed authentication attempts as a control for resisting online guessing attacks and describes the use of multiple authentication factors. See NIST SP 800-63B and CISA guidance on multifactor authentication.

QUESTION NO: 27

A technician needs to deploy scripts that run natively on Windows and Linux computers. Which of the following file extensions would MOST likely be used? (Select TWO).

A. .ps1

B. .sh

C. .msi

D. .dmg

E. .jpg

F. .iso

ANSWER: A B

Explanation:

.ps1 is the standard filename extension for PowerShell scripts. PowerShell is available on Windows and is also supported on Linux, allowing administrators to use PowerShell scripts across both operating systems when PowerShell is installed.

.sh is commonly used for shell scripts on Linux and other Unix-like operating systems. These scripts are normally executed by a shell such as Bash. A technician should ensure scripts are reviewed, approved, and granted only the necessary permissions before deployment. Microsoft documents PowerShell scripting at Microsoft Learn: PowerShell scripting overview.

QUESTION NO: 28

A technician is setting up a conference room computer with a script that boots the application on login. Which of the following would the technician use to accomplish this task? (Select TWO).

A. File Explorer

B. Startup Folder

C. System Information

D. Programs and Features

E. Task Scheduler

F. Device Manager

ANSWER: B E

Explanation:

The Startup Folder and Task Scheduler are appropriate ways to make a conference-room application launch automatically when a user signs in. The Startup Folder is a Windows folder that supports placing a shortcut to an application, script, or batch file so it runs at user logon. A technician can place the required script or a shortcut to that script in either the current user's Startup folder or the all-users Startup folder, depending on whether the application should start for one account or for every user of the computer.

Task Scheduler provides a more configurable and manageable method. The technician can create a task whose trigger is *At log on*, then configure the action to start the script or application. This is especially useful for a shared conference-room device because it can target any user, run with specified privileges, define a working directory, and apply conditions or retry behavior. These mechanisms support the stated requirement to launch the application as part of the login process. Microsoft documents startup applications and Task Scheduler's logon trigger at Microsoft Support: Configure startup applications and Microsoft Learn: Task triggering on logon.

QUESTION NO: 29 - (SIMULATION)

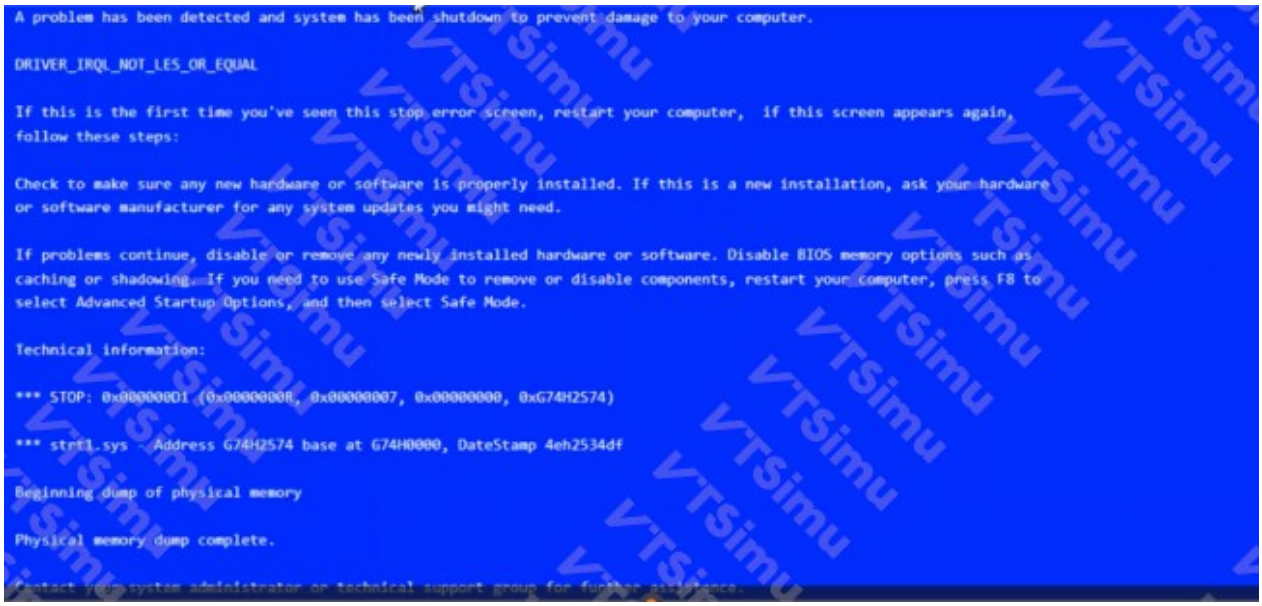
A user reports that after a recent software deployment to upgrade applications, the user can no longer use the Testing program.

However, other employees can successfully use the Testing program.

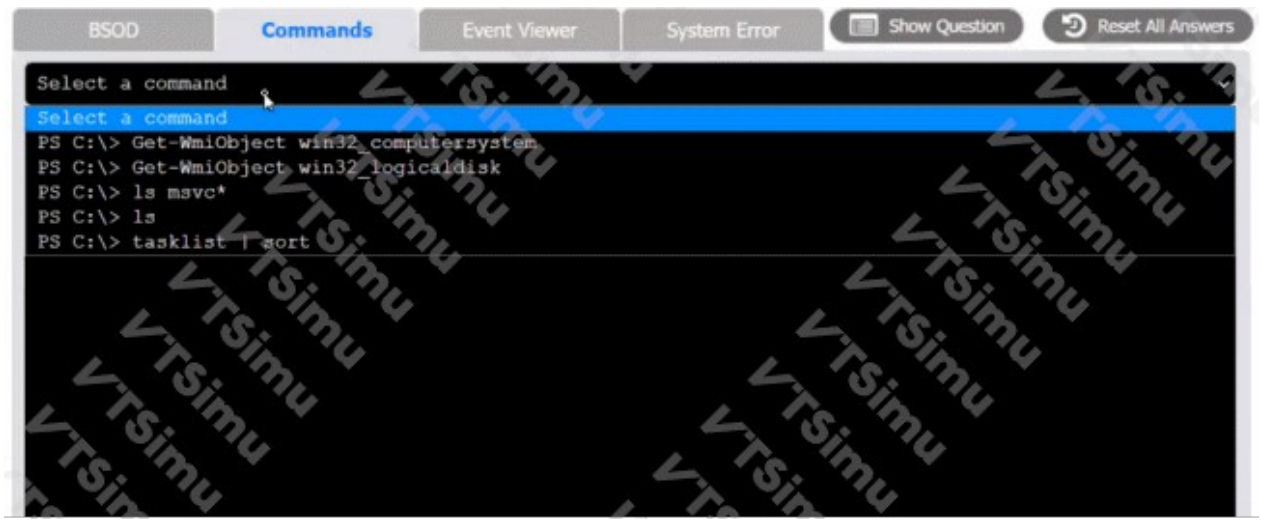
INSTRUCTIONS

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

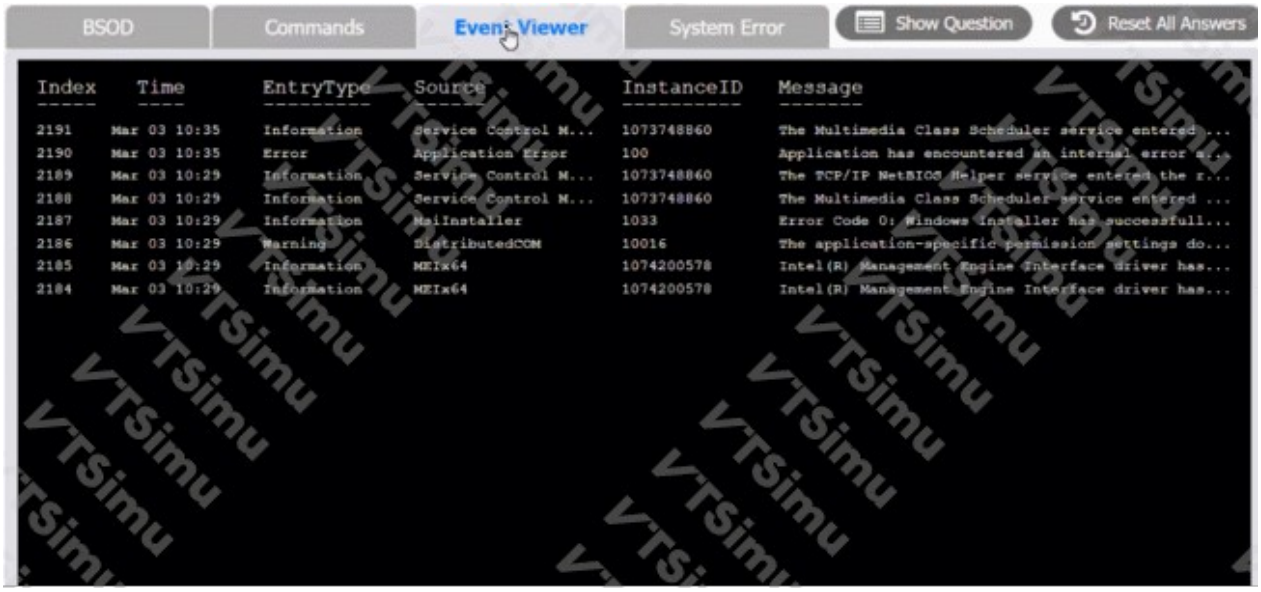
BSOD



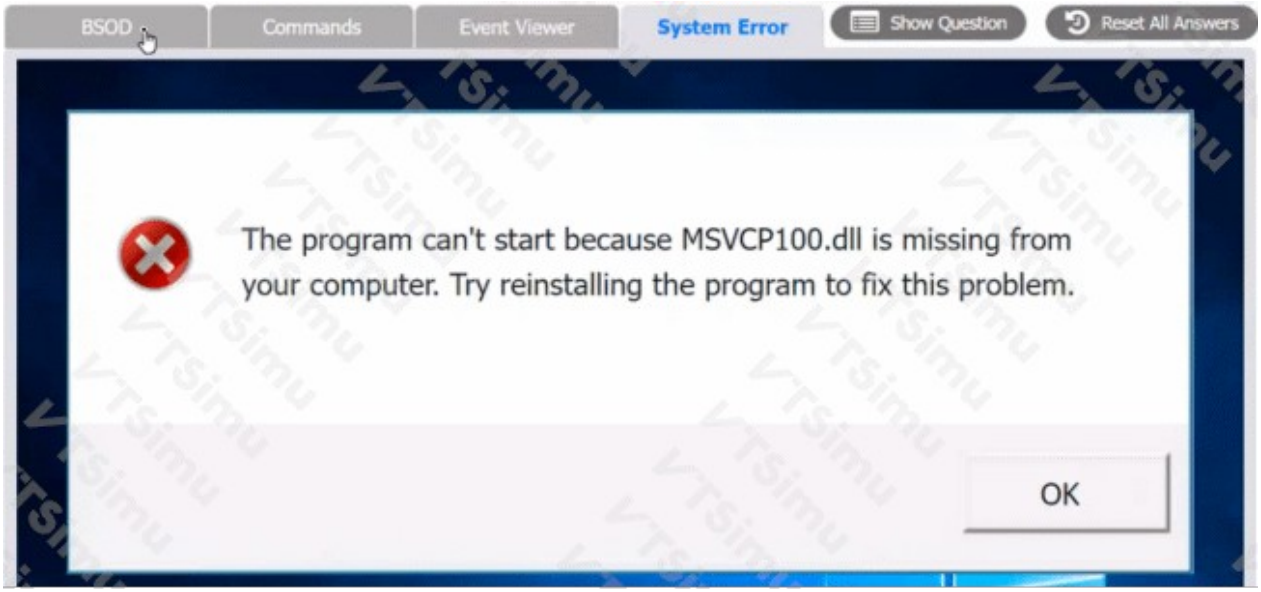
Commands:



Event Viewer:



System Error:



ANSWER: See the explanation for the answer

Explanation:

Select and run: `PS C:\> ls msvcp*`

The Testing application error identifies the actual deployment problem: `MSVCP100.dll` is missing. This DLL is part of the **Microsoft Visual C++ 2010 runtime**. Reinstall/repair the Testing application deployment and install or repair the appropriate Microsoft Visual C++ 2010 Redistributable package (normally the x86 package for a 32-bit application; install the matching x64 package as well if the application is 64-bit).

Do not download an individual DLL from an untrusted DLL site. The local runtime/application installation should supply the correct version.

The BSOD is a separate driver issue: `DRIVER_IRQL_NOT_LESS_OR_EQUAL` identifies `strtl.sys`. If the blue screen persists, update, roll back, or remove/reinstall the software driver associated with `strtl.sys`.

QUESTION NO: 30

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

A. Remote wipe

B. Firewall

C. Device encryption

D. Remote backup

E. Antivirus

F. Global Positioning System

ANSWER: A C

Explanation:

Remote wipe and device encryption are the appropriate controls for protecting company trade secrets when a corporate phone is stolen. Remote wipe, normally managed through a mobile-device-management platform, enables an authorized administrator to erase corporate data from a lost or stolen device once it reconnects to a network. This provides a direct response capability after the theft and limits the duration for which sensitive information remains exposed on the phone.

Device encryption protects the information stored locally on the phone by converting it into unreadable ciphertext. Access to encrypted data requires the appropriate authentication and encryption keys, so someone who obtains the physical device cannot simply remove or browse its storage to read company files. Encryption is especially important because a remote wipe may not occur immediately if the stolen phone is powered off or remains disconnected. Together, encryption provides protection at rest while remote wipe provides a post-loss remediation mechanism. Organizations should deploy these controls through centralized endpoint or mobile-device management and ensure recovery keys, compliance status, and wipe policies are administered securely. See NIST SP 800-124 Rev. 2 for enterprise mobile-device security guidance and Microsoft's device encryption documentation for an example of data-at-rest encryption.

QUESTION NO: 31

A technician downloaded software from the Internet that required the technician to scroll through a text box and at the end of the text box, click a

button labeled Accept Which of the following agreements IS MOST likely in use?

A. DRM

B. NDA

C. EULA

D. MOU

ANSWER: C

Explanation:

EULA is the most likely agreement because an End User License Agreement presents the legal terms governing a person's use of software. During an Internet download or installation, the software publisher commonly displays the license terms in a scrollable text area and requires the user to select an "Accept" button before installation or use can continue. This acceptance step records the user's agreement to conditions such as permitted use, license scope, ownership of the software, restrictions on copying or reverse engineering, warranty limitations, and liability terms. In practical support work, a technician should review the EULA sufficiently to ensure that installing the application is authorized and that its licensing terms are appropriate for the individual or organization. The U.S. Copyright Office explains that software is generally protected as a literary work, while licensing supplies the permission and conditions under which the user may use that protected software. The Federal Trade Commission also provides consumer guidance on software-related terms and digital transactions. See the U.S. Copyright Office's Computer Programs circular and the Federal Trade Commission's data security guidance.

QUESTION NO: 32

A technician is installing a cloud-based productivity suite and gets an error saying the installation is unavailable. What should be tried first?

A. Reinstall the productivity suite

B. Download an open-source alternative

C. Check the license device limit

D. Update the device OS

ANSWER: C

Explanation:

Check the license device limit is the appropriate first action because cloud-based productivity suites commonly tie installation and activation rights to a named user subscription and enforce a maximum number of devices on which that user can be signed in or have the software activated. If the subscription has reached its permitted device count, a new installation may be unavailable until the user signs out of, deactivates, or removes an existing device installation. This is a fast, non-destructive check that directly addresses a likely account- or entitlement-related cause before making changes to the endpoint.

For example, Microsoft states that Microsoft 365 subscribers can install the desktop apps on multiple devices but may need to sign out on another device when activation or sign-in limits are reached. Reviewing the user's subscription status and device assignments in the relevant cloud account portal confirms whether an available license entitlement exists and whether a prior device needs to be removed. This approach aligns with sound troubleshooting practice: verify account permissions, licensing, and service entitlement before attempting software repair or operating-system changes. See Microsoft Support: Install Microsoft 365 and Microsoft Support: Manage a Microsoft 365 subscription.

QUESTION NO: 33

A user's mobile phone has become sluggish A systems administrator discovered several malicious applications on the device and reset the phone. The administrator installed MDM software. Which of the following should the administrator do to help secure the device against this threat in the future? (Select TWO).

A. Prevent a device root

B. Disable biometric authentication

C. Require a PIN on the unlock screen

D. Enable developer mode

E. Block a third-party application installation

F. Prevent GPS spoofing

ANSWER: A E

Explanation:

"Prevent a device root" and "Block a third-party application installation" are the appropriate MDM controls for reducing the risk of future malicious-application infections. Rooting removes or bypasses important operating-system security boundaries and can permit untrusted software to obtain privileged access. An MDM platform can evaluate device integrity or compliance and deny enrollment, access to organizational resources, or continued use when a device is rooted. This helps keep managed devices within the platform's supported security model. Android's enterprise guidance describes using device-integrity signals to evaluate whether a device has been compromised: Android Play Integrity for enterprise.

Blocking third-party application installation directly limits the paths through which malicious apps can be introduced. MDM policies can require applications to come only from approved sources, restrict unknown-source or sideloaded installations, and allow the organization to distribute and manage approved applications. This creates an application-control boundary

after the device reset, rather than relying on a user to recognize every unsafe application. Apple documents that device-management restrictions can control app installation and related App Store behavior on supervised devices: Apple Platform Deployment: Restrictions. Together, root prevention and managed application-installation restrictions address both device compromise and the delivery of untrusted software.

QUESTION NO: 34

A user is trying to use a third-party USB adapter but is experiencing connection issues. Which of the following tools should the technician use to resolve this issue?

A. taskschd.msc

B. eventvwr.msc

C. devmgmt.msc

D. diskmgmt.msc

ANSWER: C

Explanation:

devmgmt.msc is the appropriate tool because it opens Windows Device Manager, the primary administrative console for examining and managing installed hardware and its drivers. A third-party USB adapter depends on Windows correctly detecting the device, loading a compatible driver, and reporting a healthy device status. In Device Manager, a technician can locate the adapter under the applicable hardware category, check for a warning indicator or error code, review device status and driver details, and identify whether Windows recognizes the USB hardware.

Device Manager also provides the direct remediation actions needed for this type of connection problem. The technician can scan for hardware changes after reconnecting the adapter, update the driver from the manufacturer's supported package, roll back a recently changed driver when appropriate, disable and re-enable the adapter, or uninstall the device so Windows can redetect it. These actions make **devmgmt.msc** the most direct tool for diagnosing and restoring a USB adapter's hardware-driver connection. Microsoft documents Device Manager's use for managing devices and driver packages at Microsoft Learn: Using Device Manager and its general device-management capabilities at Microsoft Support: Open Device Manager.

QUESTION NO: 35

Which of the following is a proprietary Cisco AAA protocol?

A. TKIP

B. AES

C. RADIUS

D. TACACS+

ANSWER: D

Explanation:

TACACS+ is the proprietary Cisco protocol used to provide Authentication, Authorization, and Accounting (AAA) services for administrative access to network devices. It was designed to let a network access device, such as a router, switch, or firewall, send a user's login request to a centralized AAA server rather than relying solely on local credentials. TACACS+ supports the separation of authentication, authorization, and accounting functions, which enables granular control over what an authenticated administrator is permitted to do. For example, an organization can authenticate an administrator, assign an appropriate privilege level or command authorization policy, and log the administrative activity for auditing. TACACS+ commonly uses TCP port 49 and encrypts the full packet payload, helping protect administrative-session information exchanged between the client device and AAA server. Cisco identifies TACACS+ as its proprietary AAA protocol, and it

remains widely used for centralized management access control in Cisco-oriented enterprise environments. See Cisco's TACACS+ and RADIUS comparison and the Cisco IOS TACACS+ configuration guide.

QUESTION NO: 36

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

A. Application updates

B. Anti-malware software

C. OS reinstallation

D. File restore

ANSWER: C

Explanation:

OS reinstallation is the best resolution when a rootkit is suspected because rootkits are specifically designed to obtain privileged access and conceal their presence from the operating system, security tools, and the user. A rootkit may modify kernel components, boot components, drivers, or other trusted system resources, which means the integrity of the installed operating system can no longer be reliably established. Even if a security product reports that it removed detected files, there may still be hidden persistence mechanisms or altered components remaining.

A clean OS reinstallation removes the compromised system partition and replaces potentially modified operating-system files with known-good copies. In a real remediation process, the technician should first preserve any required evidence according to organizational policy, back up only necessary user data after carefully scanning it, reinstall the OS from trusted installation media, fully patch the system, and restore data cautiously. Credentials used on the affected device should also be reset because a rootkit may have captured them. This approach restores a trustworthy computing base rather than attempting to trust a system that may still be covertly controlled. NIST discusses reimaging systems as a recovery action for malware incidents in NIST SP 800-83 Rev. 1. Microsoft also provides guidance on recovering from malware in its malware prevention and recovery information.

QUESTION NO: 37

While browsing a website, a staff member received a message that the website could not be trusted. Shortly afterward, several other colleagues reported the same issue across numerous other websites. Remote users who were not connected to corporate resources did not have any issues. Which of the following is MOST likely the cause of this issue?

A. A bad antivirus signature update was installed.

B. A router was misconfigured and was blocking traffic.

C. An upstream internet service provider was flapping.

D. The system time or date was incorrect.

ANSWER: D

Explanation:

The system time or date was incorrect is the most likely cause because browser trust decisions for HTTPS sites include validating the certificate's effective date range. A certificate is considered valid only if the client's current clock falls between its "not before" and "not after" dates. If corporate devices receive an incorrect time or date from an internal time source, many employees can suddenly receive warnings that otherwise legitimate websites cannot be trusted. The fact that the reports involve numerous unrelated websites strongly supports a local client or corporate environment issue rather than an issue with any individual website's certificate.

The difference between corporate-connected and remote users is especially important. Devices connected to corporate resources may be obtaining time through a domain controller, internal Network Time Protocol service, or centralized endpoint configuration. A fault in that shared time configuration can affect many on-network users at once, while remote users using unaffected time sources continue to browse normally. Correct time synchronization is therefore essential for certificate validation and secure web browsing. Microsoft describes how Windows Time maintains clock synchronization in domain environments, and Google's certificate guidance explains that browsers evaluate certificate validity dates: Microsoft Windows Time Service documentation; Chromium certificate verification documentation.

QUESTION NO: 38

A technician needs to change hibernation settings on a Windows computer via a batch file. Domain policies are unavailable. Which is the best method?

A. Use Power Options in Control Panel

B. Update the computer's firmware

C. Run gpupdate from command prompt

D. Use the powercfg command in a batch file

ANSWER: D

Explanation:

Use the powercfg command in a batch file because Powercfg.exe is Windows' built-in command-line utility for viewing and configuring power-management settings, including hibernation. A technician can place commands such as `powercfg /hibernate on` or `powercfg /hibernate off` in a `.bat` or `.cmd` file, allowing the hibernation configuration to be applied consistently and repeatably without relying on domain-based policy delivery. The command can also be used to configure supported hibernation modes where applicable. Because these settings affect system-level power behavior, the batch file should normally be run from an elevated Command Prompt or otherwise executed with administrator privileges. This approach directly meets the requirement to automate the setting locally through a script, and it is suitable for systems that are not managed through Active Directory Group Policy. Microsoft documents the `powercfg /hibernate` syntax and its on/off settings in the Powercfg command reference: Microsoft Powercfg command-line options. Microsoft also provides guidance on hibernation behavior and configuration in Windows hibernation documentation.

QUESTION NO: 39

Multiple users clicked a phishing link from a compromised email account. The security team isolates and removes the threat. Then, the management team provides security awareness training to the company. What step is this?

A. Provide user education.

B. Compile lessons learned.

C. Update the antivirus software.

D. Perform additional scans.

ANSWER: A

Explanation:

Provide user education. is correct because the stated action is security awareness training delivered to employees after a phishing incident. User education helps reduce the likelihood and impact of recurring social-engineering attacks by teaching personnel how to recognize suspicious messages, validate links and senders, report potential phishing, and follow organizational security procedures. In this scenario, isolation and threat removal have already addressed the immediate incident. Management's subsequent training is a preventive improvement activity focused directly on the human factor that enabled the event: multiple users clicking a malicious link. This type of awareness activity can reinforce reporting expectations and help employees identify future phishing attempts before credentials, malware, or other sensitive information

are compromised. It also supports an organization's broader incident-response improvement process by turning an observed incident pattern into practical guidance for users. NIST identifies awareness and training as an important security control area and explains that organizations should provide role-appropriate security awareness education to personnel. CompTIA's Core 2 objectives likewise include recognizing social-engineering attacks and applying appropriate security practices. See NIST SP 800-50: Building an Information Technology Security Awareness and Training Program and CompTIA exam objectives.

QUESTION NO: 40

Which of the following are system folders on macOS? (Select two)

A. Applications

B. Spotlight

C. Time Machine

D. Library

E. FileVault

F. iCloud

ANSWER: A D

Explanation:

Applications and Library are standard top-level folders in the macOS file-system hierarchy. The Applications folder is the conventional location for installed macOS applications, including built-in apps and software installed for all users. It is accessible in Finder and is represented by the `/Applications` path. This centralized location helps users, administrators, and the operating system locate application bundles and manage installed software.

Library is also a core macOS folder. macOS uses several Library locations, including the system-wide `/Library`, the protected `/System/Library`, and each user's `~/Library`. These directories hold resources required by applications and macOS, such as application-support data, preferences, fonts, caches, frameworks, launch agents, and other configuration files. The presence of Library folders at different scopes allows macOS to separate resources shared by the computer from resources belonging to an individual user or to the operating system itself.

Apple's Finder documentation describes Applications as a primary folder for apps, while Apple's macOS deployment documentation identifies Library directories as locations used for system, local, and user resources. See Apple: Find and open apps and Apple: File system organization.

QUESTION NO: 41

A customer wants to be able to work from home but does not want to be responsible for bringing company equipment back and forth. Which of the following would allow the user to remotely access and use a Windows PC at the main office? (Choose two.)

A. SPICE

B. SSH

C. RDP

D. VPN

E. RMM

F. WinRM

ANSWER: C D

Explanation:

RDP is appropriate because Remote Desktop Protocol provides an interactive graphical session on a Windows computer that remains at the main office. The employee can sign in to that office PC from a home computer and use its installed applications, files, peripherals, and network-connected resources as permitted by company policy. The processing and desktop session occur on the office computer, so the employee does not need to transport company equipment between locations.

VPN is also appropriate because it creates an encrypted connection from the employee's home network to the organization's private network. This securely extends access to internal network resources and can make the office PC reachable for an RDP connection without exposing Remote Desktop directly to the public internet. In a typical deployment, the user first establishes the VPN connection, then starts an RDP session to the internal IP address or hostname of the Windows PC. This combination supports secure remote work while keeping the primary workstation in the office. Microsoft describes Remote Desktop configuration and use in its Remote Desktop documentation, and its VPN overview explains how VPNs provide secure remote access to organizational networks.

QUESTION NO: 42

An international traveler is concerned about others accessing the contents of their smartphone if it is lost or stolen. The traveler has enabled biometrics. Which of the following additional security measures further reduces the risk of unauthorized data access?

A. Remote backups

B. Location tracking

C. PIN code screen lock

D. Device encryption

ANSWER: D

Explanation:

Device encryption is the appropriate additional measure because it protects the smartphone's data at rest. Encryption converts locally stored information—such as photos, messages, application data, and saved documents—into ciphertext that cannot be meaningfully read without the appropriate cryptographic key. On modern smartphones, that key is typically protected by the device's secure hardware and the user's passcode or other approved unlock method. Consequently, if the device is lost or stolen, physical possession of the phone or removal of its storage does not provide usable access to the encrypted contents.

Biometrics provide a convenient authentication mechanism for normal device use, but encryption provides the underlying protection for the data itself. This distinction is particularly important for a traveler, who may face a greater risk of loss, theft, or physical access by an unauthorized party. Apple explains that Data Protection uses hardware and passcode-derived keys to protect files on supported devices: Apple Platform Security: Data Protection overview. Android also documents file-based encryption as a means of encrypting user data and protecting it through user credentials: Android Open Source Project: File-based encryption.

QUESTION NO: 43

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

A. resmon.exe

B. msconfig.exe

C. dfrgui.exe

D. msinfo32.exe

ANSWER: C

Explanation:

dfrgui.exe is the appropriate tool because it opens the Windows Defragment and Optimize Drives interface, which can analyze and defragment a traditional hard disk drive. Fragmentation occurs when portions of files are stored in noncontiguous locations on a mechanical disk. Reading a fragmented file can require additional movement of the drive's read/write heads, increasing access time and potentially contributing to slow performance. Running the defragmentation process reorganizes file fragments into more contiguous disk locations and consolidates available space where possible, reducing unnecessary disk-head movement. A technician should first confirm that the affected storage device is a conventional HDD, as defragmentation is intended for spinning disks. In modern Windows versions, the same Optimize Drives interface also recognizes solid-state drives and applies an appropriate optimization process rather than conventional defragmentation. Microsoft documents the `defrag` utility and its role in locating and consolidating fragmented files on local volumes: Microsoft Learn: defrag. Microsoft also provides guidance on using the Windows drive optimization feature: Defragment/optimize data drives in Windows.

QUESTION NO: 44

A technician is documenting a completed service call for a workstation that was unable to print. Which of the following information should be included in the ticket? (Select TWO).

A. The actions taken to resolve the issue

B. The technician's personal phone number

C. The user's confirmation that printing is working

D. Passwords used during remote support

E. Unrelated tickets from other users

ANSWER: A C

Explanation:

The actions taken to resolve the issue should be documented so that future technicians can understand what changes were made and use the information if the issue recurs. Accurate resolution notes also provide accountability and support the organization's knowledge base.

The user's confirmation that printing is working should be included because it records that the service was validated with the affected user before the ticket was closed. This confirms that the resolution addressed the reported issue rather than only a suspected cause. Good ticket documentation includes symptoms, troubleshooting steps, changes made, final status, and user verification where applicable.

QUESTION NO: 45

A technician is preparing to dispose of several failed solid-state drives that contained confidential company information. Which of the following methods would BEST ensure the data cannot be recovered? (Select TWO).

A. Physical destruction

B. Quick format

C. Cryptographic erase

D. Delete all partitions

E. Reinstall the operating system

ANSWER: A C

Explanation:

Physical destruction is an appropriate method because it renders the storage media unusable by destroying the flash chips that contain the data. This is a suitable option for failed SSDs that will not be reused.

Cryptographic erase is also appropriate when the SSD was protected by strong encryption and the encryption keys can be securely destroyed. Once the keys are destroyed, the encrypted data remaining on the drive is computationally unreadable. NIST media-sanitization guidance identifies both destroy methods and cryptographic erase as sanitization techniques when used under appropriate conditions. See NIST SP 800-88 Rev. 1.

QUESTION NO: 46

A technician is preparing a Windows workstation for use by a temporary employee. The employee should be able to use approved applications but should not be able to install software or make system-wide configuration changes. Which of the following should the technician configure? (Select TWO).

A. A standard user account

B. User Account Control

C. A local administrator account

D. The built-in Administrator account

E. A shared account with no password

F. Developer Mode

ANSWER: A B

Explanation:

A standard user account supports least privilege by allowing the temporary employee to run applications and perform normal user tasks without granting administrative control of the workstation. Standard users generally cannot install software that requires elevated privileges or modify protected operating-system settings.

User Account Control should also remain enabled because it prompts for administrator approval or administrator credentials when an action requires elevated permissions. This prevents the employee from silently elevating a standard account to perform administrative tasks. Microsoft describes User Account Control and privilege elevation at Microsoft Learn: User Account Control.

QUESTION NO: 47

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: B

Explanation:

Resale is the most environmentally friendly choice because it extends the usable life of functional Ethernet cards. The cards may be unsuitable for the specific government contract because they do not meet that contract's technical or regulatory

requirements, but that does not necessarily mean they are defective or unusable in another environment. Reusing equipment avoids the immediate need to manufacture a replacement device for another buyer, reducing demand for raw-material extraction, component manufacturing, packaging, and transportation. This follows the waste-management hierarchy: preventing waste and preparing items for reuse are preferable to recycling or disposal. Before resale, the organization should confirm that the cards contain no organizational data or asset-management information and that transfer is permitted by its contract, security policy, and applicable regulations. Ethernet adapters ordinarily do not store user data, but an appropriate asset-disposition process should still document the transfer and remove any identifying labels if required. The U.S. Environmental Protection Agency identifies reuse as a preferred sustainable-materials-management practice because it keeps products in service and conserves resources. See the EPA guidance on sustainable management of electronics and the EPA waste-reduction hierarchy.

QUESTION NO: 48

A technician is securing a newly deployed workstation. Only authorized users should access it. Which actions should the technician take? (Select two)

A. Defragment the hard drive

B. Enable SSH

C. Enable screensaver locks

D. Disable iCloud integration

E. Enable the firewall

F. Apply the BIOS password

ANSWER: C F

Explanation:

Enable screensaver locks is correct because an automatic screen lock protects an authenticated, unattended session. After the configured idle timeout, the workstation requires the user's credentials before the desktop and its open applications can be accessed again. This is an essential endpoint control because users may leave a device temporarily without signing out. Microsoft documents the screen-saver timeout and password-protection policies used to enforce this behavior centrally: Windows screen saver security.

Apply the BIOS password is also correct because it adds a pre-operating-system authentication or configuration-protection layer. Depending on the firmware and password type configured, it can require authorization before startup and/or prevent unauthorized users from changing firmware settings, boot order, and other controls that could be used to bypass operating-system protections. This complements, rather than replaces, normal operating-system account passwords and screen locking. CompTIA includes workstation security configuration and authentication controls within its current Core 2 objectives; see the CompTIA exam objectives resource. Together, an idle-session lock and firmware password protection address both an already logged-in workstation and access during the startup process.

QUESTION NO: 49

A desktop technician is mapping a remote Windows share \\WinNAS\shared as local drive Z:. Which command should the technician run?

A. nslookup -opt 3: \WinNAS\shared

B. net use Z: \\WinNAS\shared

C. chkdsk /R 2: \WinNAS\shared

D. sfc /offwindir 3: \WinNAS\shared

E. net use Z: \\WinNAS\shared /persistent:yes

ANSWER: B E

Explanation:

`net use Z: \\WinNAS\shared` is the standard Windows command to connect a network share by its Universal Naming Convention (UNC) path and assign it the local drive letter `Z:`. The `net use` command manages network connections; placing the drive letter first specifies the local mapping, followed by the remote server and share path. This lets the technician access the shared folder through `Z:` in File Explorer, Command Prompt, and applications that require a drive-letter path.

`net use Z: \\WinNAS\shared /persistent:yes` performs the same mapping and additionally requests that Windows restore the connection after the user signs in again. This is appropriate when the mapped drive should remain available across logon sessions. The connection still depends on the user having the necessary share and NTFS permissions, as well as network access to the server. Microsoft documents the required `net use` syntax, including a local device name, UNC resource name, and the optional persistence setting, at Net use command reference. For UNC naming conventions used for shared resources, see Microsoft UNC path documentation.

QUESTION NO: 50

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

A. Encryption

B. Antivirus

C. AutoRun

D. Guest accounts

E. Default passwords

F. Backups

ANSWER: A B

Explanation:

Encryption and **Antivirus** are appropriate controls for workstations that store credit card data. PCI DSS requires stored account data to be rendered unreadable when it is kept electronically, using strong cryptography and appropriate key-management practices. Full-disk encryption or properly implemented encryption for the files and databases containing account data helps prevent unauthorized disclosure if a workstation, drive, or exported data is accessed outside approved processes. The organization must also ensure that encryption keys are protected separately from the encrypted data.

Antivirus, more broadly described in PCI DSS as anti-malware protection, is also required where systems are susceptible to malware. Workstations used by support personnel are common malware targets because they process email, web content, removable media, and user downloads. Anti-malware tooling must be deployed, kept current, actively operating, and capable of detecting, preventing, or alerting on malicious software. Together, encryption protects the confidentiality of stored cardholder data, while antivirus helps preserve the security of the endpoint that handles it. These measures align with PCI DSS requirements for protecting stored account data and defending systems against malicious software. See the PCI DSS v4.0.1 standard and the PCI Security Standards Council PCI DSS overview.

QUESTION NO: 51

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

A. Language

B. System

C. Personalization

D. Ease of Access

ANSWER: D

Explanation:

Ease of Access is the appropriate Windows Settings category for configuring speech-recognition accessibility features. In the Windows 10 Settings layout relevant to this type of A+ question, the Speech page under Ease of Access provides controls for speech-related accessibility capabilities, including enabling and configuring Windows Speech Recognition. This area is designed to help users interact with the computer without relying exclusively on a keyboard, mouse, or other conventional input devices.

After speech recognition is enabled, Windows can guide the user through initial setup, including microphone configuration and voice training where applicable. Correct microphone setup is important because the feature needs a working input device and an appropriate audio level to recognize spoken commands accurately. The user can then use voice commands to open applications, dictate text, and control supported Windows functions. This is an accessibility configuration task rather than a general hardware or display-customization task.

Microsoft documents Windows Speech Recognition commands and their use at Windows Speech Recognition commands. For current Windows accessibility voice-control information, see Use voice access to control your PC.

QUESTION NO: 52

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

A. File Explorer

B. User Account Control

C. Windows Backup and Restore

D. Windows Firewall

E. Windows Defender

F. Network Packet Analyzer

ANSWER: A E

Explanation:

Windows Defender is an appropriate malware-removal tool because it is Microsoft's built-in endpoint antimalware protection. A technician can update its security intelligence, run a full scan or an offline scan when needed, quarantine identified threats, and remove detected malicious files. Microsoft documents how Microsoft Defender Antivirus detects, quarantines, and remediates threats, including actions that can be taken after detection: Microsoft Defender threat remediation.

File Explorer can also be used as part of the cleanup process to locate and remove known malicious files, unwanted downloads, malicious shortcuts, or persistence-related files after the infection has been identified and the system has been scanned. Manual removal should be performed carefully and in accordance with organizational procedures, since deleting the wrong system file can affect workstation stability. File Explorer provides access to the workstation's files and folders, including the ability to search for items and permanently delete them: Microsoft Support: Find and open File Explorer.

QUESTION NO: 53

Why would a network engineering team provide a help desk technician with IP addresses for a wired network segment?

A. Only specific DNS servers are allowed outbound.

B. The network allow list is set to a specific address.

C. DHCP is not enabled for this subnet.

D. NAC servers only allow security updates to be installed.

ANSWER: C

Explanation:

DHCP is not enabled for this subnet. is correct because devices on a subnet without Dynamic Host Configuration Protocol must receive their network settings through manual, static configuration. A help desk technician preparing or troubleshooting a wired workstation would therefore need an approved IP address, subnet mask or prefix length, default gateway, and usually DNS server information from the network engineering team. This ensures that the device is configured within the correct network range and can communicate with local and remote resources as intended.

DHCP normally automates the assignment of IP addresses and related TCP/IP settings when a client connects to a network. If that service is intentionally unavailable on a particular wired segment, providing a documented static address is the appropriate operational process. The technician should use only the address details supplied by engineering, rather than selecting an unused-looking address, because address management must avoid duplication and preserve the organization's network design. Microsoft's guidance explains that IPv4 settings can be assigned automatically through DHCP or entered manually when static addressing is required: Change TCP/IP settings in Windows. CompTIA lists network configuration and troubleshooting as Core 2 skills in its exam objectives: CompTIA exam objectives.

QUESTION NO: 54

A user logs in daily and cannot print a report. Help desk fixes it each day, but the issue recurs. What should be done so the issue doesn't recur? (Select two)

A. Set the print spooler to have no dependencies

B. Set the print spooler recovery to take no action

C. Start the printer extensions and notifications service

D. Start the print spooler service

E. Set the print spooler to Automatic

F. Set the print spooler log-on to the user's account

ANSWER: D E

Explanation:

"Start the print spooler service" is required because the Windows Print Spooler service manages print jobs and coordinates communication between applications, printers, and print drivers. If the service is stopped, users cannot submit reports or other documents to a printer. Starting it restores the immediate ability to print. "Set the print spooler to Automatic" provides the permanent corrective action: Windows will start the service during system startup rather than requiring the help desk to start it manually after a reboot or service interruption. Together, these steps address both the current symptom and the recurring nature of the incident. This follows the standard troubleshooting principle of identifying and implementing a long-term fix, then confirming the affected service is running and configured to persist through normal restarts. Microsoft documents the Print Spooler as the service that spools print jobs and handles printer interaction, while its Windows service-management guidance describes configuring a service startup type so it starts automatically with Windows. See Microsoft Print Spooler documentation and Microsoft sc.exe config documentation.