Exam Questions 220-1202

CompTIA A+ Certification Exam: Core 2

https://www.2passeasy.com/dumps/220-1202/

NEW QUESTION 1
Every time a user loads a specific spreadsheet, their computer is temporarily unresponsive. The user also notices that the title bar indicates the application is not responding. Which of the following would a technician most likely inspect?

A. Anti-malware logs
B. Workstation repair options
C. Bandwidth status as reported in the Task Manager
D. File size and related memory utilization

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
If a system becomes unresponsive while opening a specific spreadsheet, the issue is likely tied to the file??s size or the complexity of its content (e.g., embedded formulas, macros, or graphics). High memory utilization caused by the file can lead to temporary freezing or application "Not Responding" messages. Checking the spreadsheet's file size and monitoring system memory in Task Manager will help isolate performance bottlenecks.
* A. Anti-malware logs are important for security troubleshooting but less likely relevant to spreadsheet-related performance issues.
* B. Workstation repair is for system-wide problems and not necessary for a single-file issue.
* C. Bandwidth relates to network usage and wouldn??t impact opening a local file. Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common application issues.
Study Guide Section: Troubleshooting application slowness and performance using Task Manager and resource monitoring tools
===========================

NEW QUESTION 2
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:
Comprehensive and Detailed Explanation From Exact Extract:
Linux is an open-source operating system that is freely available and does not require traditional licensing fees. It is highly versatile and scalable, making it suitable for both workstations and servers. Many enterprise environments use Linux to reduce software costs and benefit from robust server features.
* B. Windows requires per-device or per-user licensing for both workstation and server editions.
* C. macOS is proprietary and limited to Apple hardware with licensing restrictions.
* D. Chrome OS is designed for lightweight devices and lacks server functionality. Reference:
CompTIA A+ 220-1102 Objective 1.8 & 1.9: Identify common features and tools of the Linux client/desktop OS.
Study Guide Section: Open-source operating systems and licensing considerations
===========================

NEW QUESTION 3
Which of the following is an example of an application publisher including undisclosed additional software in an installation package?

A. Virus
B. Ransomware
C. Potentially unwanted program
D. Trojan

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
A Potentially Unwanted Program (PUP) is software that a user may not have knowingly installed. It often gets bundled with legitimate software and installs without full disclosure. PUPs can affect performance, change system settings, or display unwanted ads but are not necessarily malicious like viruses or ransomware.
* A. Viruses replicate and spread; they are generally more harmful and not "bundled" in the same way.
* B. Ransomware encrypts files for payment and is deliberately malicious.
* D. A Trojan disguises itself as legitimate software to perform malicious actions but is not typically pre-bundled by legitimate publishers.
Reference:
CompTIA A+ 220-1102 Objective 2.5: Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.
Study Guide Section: Types of malware — PUPs and bundled software
===========================

NEW QUESTION 4
A technician needs to configure laptops so that only administrators can enable virtualization technology if needed. Which of the following should the technician configure?

A. BIOS password
B. Guest account
C. Screen lock
D. AutoRun setting

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Virtualization settings are typically found within the BIOS/UEFI firmware configuration. To prevent unauthorized users from changing these settings, the technician should set a BIOS password. This ensures only administrators with the password can access or modify BIOS settings, including virtualization support.
* B. The guest account is a user-level feature in Windows and doesn??t control BIOS access.
* C. A screen lock prevents casual access to the desktop but doesn??t protect firmware settings.
* D. AutoRun controls how media and devices behave when inserted — unrelated to BIOS security.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and administrative controls.
Study Guide Section: BIOS/UEFI settings protection — password implementation

NEW QUESTION 5
A technician installs VPN client software that has a software bug from the vendor. After the vendor releases an update to the software, the technician attempts to reinstall the software but keeps getting an error message that the network adapter for the VPN already exists. Which of the following should the technician do next to mitigate this issue?

A. Run the latest OS security updates.
B. Map the network adapter to the new software.
C. Update the network adapter's firmware.
D. Delete hidden network adapters.

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
VPN clients often create virtual network adapters. If the software wasn't uninstalled properly or crashed during install, leftover (often hidden) virtual adapters can prevent reinstallation. The proper solution is to delete hidden network adapters using Device Manager (with ??Show hidden devices?? enabled).
* A. OS updates won??t fix a leftover driver or adapter issue.
* B. Mapping an adapter to the software is not a standard or viable solution.
* C. Firmware updates apply to physical adapters, not virtual VPN adapters. Reference:
CompTIA A+ 220-1102 Objective 3.1: Troubleshoot common Windows OS and network issues.
Study Guide Section: Troubleshooting network adapter conflicts and VPN client errors

NEW QUESTION 6
A company recently transitioned to a cloud-based productivity suite and wants to secure the environment from external threat actors. Which of the following is the most effective method?

A. Multifactor authentication
B. Encryption
C. Backups
D. Strong passwords

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Multifactor authentication (MFA) is considered one of the most effective security measures for cloud environments. It requires users to verify their identity using two or more factors (e.g., password + phone app code), making it significantly harder for external attackers to gain access, even if the primary password is compromised.
* B. Encryption is important for data protection but doesn??t prevent unauthorized logins.
* C. Backups protect against data loss but don??t stop breaches.
* D. Strong passwords are helpful but can still be phished or cracked — MFA adds a critical
extra layer. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast authentication technologies. Study Guide Section: Cloud security best practices — MFA and access control

NEW QUESTION 7
An employee is using a photo editing program. Certain features are disabled and require a log-in, which the employee does not have. Which of the following is a way to resolve this issue?

A. License assignment
B. VPN connection
C. Application repair
D. Program reinstallation

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Many modern commercial software applications (including photo editors like Adobe Photoshop) offer tiered features based on user subscriptions or license levels. If certain features are locked and prompt for a login, the issue is likely due to a missing or unassigned software license. Assigning the correct license through a centralized license management system (such as Adobe Admin Console or Microsoft 365 portal) will enable those features.
* B. VPN connection does not affect local software licensing.
* C. Repairing the application does not resolve license entitlement.
* D. Reinstalling the software won??t help unless the license is assigned. Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software and application issues.
Study Guide Section: Troubleshooting licensing and access control for applications
===========================

NEW QUESTION 8
A technician notices that the weekly backup is taking too long to complete. The daily
backups are incremental. Which of the following would most likely resolve the issue?

A. Changing the backup window
B. Performing incremental weekly backups
C. Increasing the backup storage
D. Running synthetic full weekly backups

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
A synthetic full backup combines the last full backup with subsequent incremental backups to create a new full backup without re-reading data from the source system. This method significantly reduces the backup window and network impact. It is especially useful when traditional full backups are too time-consuming.
* A. Changing the backup window only shifts timing, not duration.
* B. Incremental weekly backups would lack a proper full recovery point and aren't ideal alone.
* C. Storage space isn't the bottleneck in backup speed—it??s read/write operations and network load.
Reference:
CompTIA A+ 220-1102 Objective 4.2: Summarize backup and recovery concepts.
Study Guide Section: Backup types — full, incremental, differential, and synthetic backups
===========================

NEW QUESTION 9
Which of the following is the quickest way to move from Windows 10 to Windows 11 without losing data?

A. Using gpupdate
B. Image deployment
C. Clean install
D. In-place upgrade

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
An in-place upgrade is the fastest and most efficient way to upgrade from Windows 10 to Windows 11 while keeping all user data, applications, and settings intact. This method is often used when the hardware meets Windows 11 requirements and no system reconfiguration is necessary.
* A. gpupdate is used to refresh Group Policy settings — unrelated to OS upgrades.
* B. Image deployment typically replaces the current OS and may not retain user data unless specifically customized.
* C. A clean install requires formatting the drive and starting fresh, which removes all data. Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: In-place upgrade vs. clean install methods
===========================

NEW QUESTION 10
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:
Comprehensive and Detailed Explanation From Exact Extract:
A low-level format (also referred to as a zero-fill or full format) writes over every sector on a storage device, effectively destroying the existing data and making recovery nearly impossible. Unlike degaussing, which renders the drive unusable, a low-level format maintains the integrity of the device, allowing it to be repurposed or reused.
* A. Deleting partitions does not fully erase data; it only removes references in the partition table.
* B. EFS (Encrypting File System) encrypts files but does not securely wipe them.
* D. Degaussing destroys the magnetic structure of a drive, making it inoperable and not reusable.
Reference:
CompTIA A+ 220-1102 Objective 4.3: Given a scenario, implement basic change management best practices.
Study Guide Section: Drive sanitation methods — low-level format vs. degaussing vs. deletion
===========================

NEW QUESTION 10
Technicians are failing to document user contact information, device asset tags, and a clear description of each issue in the ticketing system. Which of the following should a help desk management team implement for technicians to use on every call?

A. Service-level agreements
B. Call categories
C. Standard operating procedures
D. Knowledge base articles

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:

Standard Operating Procedures (SOPs) define the mandatory steps and expectations technicians must follow during support calls. This includes documentation standards such as logging user info, asset details, and issue descriptions in the ticketing system. Implementing SOPs ensures consistency and accountability.
* A. SLAs define response/resolution times but not documentation practices.
* B. Call categories organize types of issues but don't guide technician actions.
* D. Knowledge base articles provide solutions to known problems but don't ensure proper ticket documentation.
Reference:
CompTIA A+ 220-1102 Objective 4.2: Summarize best practices associated with types of documentation and support systems information.
Study Guide Section: Documentation practices, SOPs, ticketing protocols
===========================

NEW QUESTION 13
A network technician notices that most of the company's network switches are now end-of- life and need to be upgraded. Which of the following should the technician do first?

A. Implement the change
B. Approve the change
C. Propose the change
D. Schedule the change

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The first step in the IT change management process is to identify and propose the change. In this case, the technician notices a need (end-of-life network switches), so the
appropriate action is toformally propose a change. This proposal would be documented and submitted for approval before any planning or implementation occurs.
According to the CompTIA A+ 220-1102 objectives under Operational Procedures (Domain 4.0), the change management process follows these typical steps:
? Submit a change request (Propose the change)
? Review and approval (Approve the change)
? Planning and scheduling (Schedule the change)
? Implementation
? Documentation and review
Therefore, proposing the change is the correct first step in accordance with standard ITIL- based change management practices.
Reference:
CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement best practices associated with documentation and support systems information management.
Study Guide Section: Change Management Process
===========================

NEW QUESTION 16
Which of the following is the best reason for a network engineering team to provide a help desk technician with IP addressing information to use on workstations being deployed in a secure network segment?

A. Only specific DNS servers are allowed outbound access.
B. The network allow list is set to a specific address.
C. DHCP services are not enabled for this subnet.
D. NAC servers only allow for security updates to be installed.

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In secure or isolated network segments, DHCP may be disabled to reduce the risk of unauthorized device connections or to maintain strict IP assignment control. In such cases, the help desk technician must manually configure IP settings (including IP address, subnet mask, gateway, and DNS servers). This ensures the workstation communicates properly within that segment.
* A. DNS server restriction is unrelated to manual IP configuration.
* B. Allow lists refer to traffic access, but manual IP assignment is due to lack of DHCP, not allow lists.
* D. NAC servers control access but don't replace the need for IP addressing. Reference:
CompTIA A+ 220-1102 Objective 1.7: Given a scenario, troubleshoot common operating system and network issues.
Study Guide Section: IP configuration and DHCP-related deployment scenarios
===========================

NEW QUESTION 21
A user has been adding data to the same spreadsheet for several years. After adding a significant amount of data, they are now unable to open the file. Which of the following should a technician do to resolve the issue?

A. Revert the spreadsheet to the last restore point.
B. Increase the amount of RAM.
C. Defragment the storage drive.
D. Upgrade the network connection speed.

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
When a spreadsheet becomes very large, opening and processing it requires more memory (RAM). If the system doesn't have sufficient memory, it may fail to load the file properly. Upgrading or increasing the available RAM can resolve performance and loading issues with very large files.
* A. Restore points roll back system settings, not individual file content.
* C. Defragmentation optimizes disk performance but won??t help with memory issues.
* D. Network speed has no effect if the file is stored and opened locally. Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common application and performance issues.

Study Guide Section: Troubleshooting large-file performance and system resource limitations
===========================

NEW QUESTION 26
A computer technician is implementing a solution to support a new internet browsing policy for a customer's business. The policy prohibits users from accessing unauthorized websites based on categorization. Which of the following should the technician configure on the SOHO router?

A. Secure management access
B. Group Policy Editor
C. Content filtering
D. Firewall

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Content filtering allows administrators to block or allow access to websites based on categories (e.g., social media, adult content, streaming). On a SOHO (Small Office/Home Office) router, this is often built-in or available via DNS-level filtering, and is the most appropriate method for enforcing browsing policies without needing to touch each individual device.
* A. Secure management access protects router admin interfaces but doesn??t control user browsing.
* B. Group Policy Editor is a Windows tool, not used on routers.
* D. A firewall can block specific IPs or ports, but it doesn't categorize web content. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and tools. Study Guide Section: SOHO router security features — content filtering, parental controls

NEW QUESTION 30
A technician is preparing to replace the batteries in a rack-mounted UPS system. After ensuring the power is turned off and the batteries are fully discharged, the technician needs to remove the battery modules from the bottom of the rack. Which of the following steps should the technician take?

A. Ensure the fire suppression system is ready to be activated.
B. Use appropriate lifting techniques and guidelines.
C. Place the removed batteries in an antistatic bag.
D. Wear a face mask to filter out any harmful fumes.

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
UPS batteries are heavy and often located at the bottom of racks to maintain balance. Safe removal requires the use of correct lifting techniques to avoid injury. OSHA and workplace safety standards emphasize ergonomic handling when dealing with heavy equipment.
* A. Fire suppression readiness is important for fire safety but not specifically relevant to battery removal.
* C. Antistatic bags are for electronic components, not heavy battery modules.
* D. A face mask is not generally necessary unless there is a chemical leak, which is not indicated here.
Reference:
CompTIA A+ 220-1102 Objective 4.3: Explain common safety and environmental impacts
and procedures.
Study Guide Section: Safe handling procedures — lifting techniques, battery handling
===========================

NEW QUESTION 33
An application's performance is degrading over time. The application is slowing, but it never gives an error and does not crash. Which of the following tools should a technician use to start troubleshooting?

A. Reliability history
B. Computer management
C. Resource monitor
D. Disk

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract: Resource Monitor provides real-time monitoring of system performance and resource usage, including CPU, memory, disk, and network usage. It helps technicians identify
performance bottlenecks (e.g., high memory or CPU usage) that can cause slowdowns in applications over time without producing crash errors.
* A. Reliability history logs application crashes or errors — not helpful if the app doesn??t crash.
* B. Computer Management is a broad utility with limited real-time monitoring capability.
* D. Disk is too vague — tools like CHKDSK can help with disk errors but not general performance degradation.
Reference:
CompTIA A+ 220-1102 Objective 3.2: Given a scenario, troubleshoot common personal computer issues.
Study Guide Section: System performance tools — Resource Monitor, Task Manager
===========================

NEW QUESTION 37
Which of the following types of social engineering attacks sends an unsolicited text
message to a user's mobile device?

A. Impersonation
B. Vishing
C. Spear phishing

D. Smishing

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Smishing (SMS phishing) is a type of social engineering attack where attackers send fraudulent text messages to trick users into revealing sensitive information or downloading malware. These messages often impersonate banks, delivery services, or official institutions to lure the victim into clicking malicious links.
* A. Impersonation is an in-person or voice-based tactic.
* B. Vishing refers to voice phishing over phone calls.
* C. Spear phishing is a targeted email-based phishing method. Reference:
CompTIA A+ 220-1102 Objective 2.3: Compare and contrast social engineering techniques.
Study Guide Section: Smishing as a type of phishing via SMS or mobile messaging.
==========================

NEW QUESTION 42
Which of the following is used to detect and record access to restricted areas?

A. Bollards
B. Video surveillance
C. Badge readers
D. Fence

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Badge readers are electronic access control systems that require authorized users to scan a badge (e.g., RFID or magnetic strip cards) to gain access to restricted physical locations. These systemstypically log all access attempts—successful or denied—providing both detection and recording of access events.
* A. Bollards are physical barriers to prevent vehicle access.
* B. Video surveillance can record access visually but does not track identity unless integrated with access control systems.
* D. A fence restricts access but doesn't detect or record who entered. Reference:
CompTIA A+ 220-1102 Objective 2.4: Compare and contrast physical security measures.
Study Guide Section: Physical access controls (e.g., badge readers, mantraps)

NEW QUESTION 47
A customer wants to be able to work from home but does not want to be responsible for bringingcompany 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: CD

Explanation:
Comprehensive and Detailed Explanation From Exact Extract: To work remotely without physically transporting a workstation, the user needs:
? C. RDP (Remote Desktop Protocol): Allows graphical remote access to a Windows
PC at the office.
? D. VPN (Virtual Private Network): Establishes a secure tunnel to access the corporate network remotely, making the internal PC reachable.
* A. SPICE is used in virtual machine environments and is not typically used for end-user remote desktop access.
* B. SSH is a text-based remote access tool used mostly for Linux systems.
* E. RMM (Remote Monitoring and Management) is used by IT administrators for support — not end-user remote access.
* F. WinRM is used for Windows remote management via PowerShell, not for full desktop access.
Reference:
CompTIA A+ 220-1102 Objectives 2.2 & 4.4: Compare and contrast security tools and remote access methods.
Study Guide Section: Remote access tools — RDP and VPN for secure remote work

NEW QUESTION 48
A help desk technician is setting up speech recognition on a Windows system. Which of the following settings should the technician use?

A. Time and Language
B. Personalization
C. System
D. Ease of Access

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In Windows, accessibility tools such as speech recognition are found under the Ease of Access settings. This section includes options for users who require assistive technologies, including screen readers, magnifiers, and voice control interfaces like speech recognition. Setting up speech recognition allows users to control the system and input text using voice commands.
* A. Time and Language is for setting regional preferences and language packs.
* B. Personalization adjusts themes, backgrounds, and colors.
* C. System includes display, storage, notifications, and power settings, but not accessibility tools.
Reference:

CompTIA A+ 220-1102 Objective 1.3: Given a scenario, use appropriate Microsoft operating system features and tools.
Study Guide Section: Accessibility tools and system configuration
===========================

NEW QUESTION 51
A user reports getting a BSOD (Blue Screen of Death) error on their computer at least twice a day. Which of the following should the technician use to determine the cause?

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

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Event Viewer is the primary tool used to investigate system-level errors and logs, including BSODs. When a BSOD occurs, Windows logs the error codes and associated system behavior under ??System?? logs in Event Viewer. This allows the technician to review crash events, identify error codes (e.g., STOP codes), and pinpoint hardware or driver issues.
* B. Performance Monitor is used for real-time performance tracking and trend analysis, not crash logs.
* C. System Information displays system specs but not crash logs or events.
* D. Device Manager shows device status and driver issues but doesn??t retain error logs related to BSODs.
Reference:
CompTIA A+ 220-1102 Objective 3.1: Given a scenario, troubleshoot common Windows OS problems.
Study Guide Section: Troubleshooting BSODs using Event Viewer and system logs
===========================

NEW QUESTION 55
......