

Exam Questions 220-1202

CompTIA A+ Certification Exam: Core 2

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



NEW QUESTION 1

After a recent mobile OS upgrade to a smartphone, a user attempts to access their corporate email, but the application does not open. A technician restarts the smartphone, but the issue persists. Which of the following is the most likely way to resolve the issue?

- A. Updating the failed software
- B. Registering the smartphone with an MDM solution
- C. Installing a third-party client
- D. Clearing the cache partition

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Mobile OS updates can sometimes cause compatibility issues with specific apps, including corporate email clients. The most likely resolution is to check for and apply an update to the affected application, especially if it hasn't been updated to support the latest OS version.

* B. Registering with MDM might be required for access but wouldn't address app crashes due to incompatibility.

* C. A third-party client might help, but it's not the best first step if the default app is expected to work.

* D. Clearing the cache can help resolve some minor issues, but updating the app directly addresses compatibility concerns.

Reference:

CompTIA A+ 220-1102 Objective 3.3: Troubleshoot mobile OS and application issues. Study Guide Section: App compatibility and mobile software updates

=====

NEW QUESTION 2

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 3

Which of the following prevents forced entry into a building?

- A. PIV card
- B. Motion-activated lighting
- C. Video surveillance
- D. Bollard

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

A bollard is a sturdy physical barrier—often a steel or concrete post—designed to prevent vehicles or unauthorized individuals from ramming into or entering secure areas of a building. It provides physical security and is commonly used outside entrances to prevent forced entry.

* A. PIV (Personal Identity Verification) cards are used for identity access control, not physical blocking.

* B. Motion lighting may deter activity but doesn't physically prevent entry.

* C. Surveillance records activity but cannot stop a forced entry. Reference:

CompTIA A+ 220-1102 Objective 2.4: Compare and contrast physical security measures. Study Guide Section: Physical security devices — barriers, bollards, and deterrents

NEW QUESTION 4

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 5

Which of the following is found in an MSDS sheet for a battery backup?

- A. Installation instructions
- B. Emergency procedures
- C. Configuration steps
- D. Voltage specifications

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

An MSDS (Material Safety Data Sheet), now commonly referred to as SDS (Safety Data Sheet), is a document that provides detailed information on the properties of a particular substance. It includes safety guidelines and emergency procedures related to handling, exposure, fire hazards, and first aid—not installation or configuration instructions.

For a battery backup (UPS device), the MSDS would include emergency procedures such as what to do in case of a chemical spill, exposure to battery acid, or fire hazard due to overheating or chemical leakage. This ensures the safety of personnel and complies with hazardous materials handling regulations.

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: MSDS/SDS usage and safety documentation

NEW QUESTION 6

A technician is deploying mobile devices and needs to prevent access to sensitive data if the devices are lost. Which of the following is the best way to prevent unauthorized access if the user is unaware that the phone is lost?

- A. Encryption
- B. Remote wipe
- C. Geofencing
- D. Facial recognition

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Remote wipe is the best option to prevent unauthorized access to data when a mobile device is lost or stolen—especially if the user is unaware of the loss. It allows administrators or mobile device management (MDM) systems to remotely erase all data on the device, rendering it unusable for unauthorized users.

- * A. Encryption protects the data, but if the device remains powered and logged in, it may still be accessible.
- * C. Geofencing can restrict features based on location but does not erase data.
- * D. Facial recognition helps secure access but can be bypassed in some cases or fail in practical situations.

Reference:

CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and tools. Study Guide Section: Mobile device security (remote wipe, lockout, MDM tools)

NEW QUESTION 7

A customer is unable to open some files on their system. Each time the customer attempts to open a file, the customer receives a message that the file is encrypted. Which of the following best describes this issue?

- A. Keylogger
- B. Ransomware
- C. Phishing
- D. Cryptominer

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Ransomware is a type of malware that encrypts the user's files and demands a payment (ransom) for the decryption key. When a user receives a message stating that their files are encrypted and cannot be accessed, ransomware is the most likely cause. The attacker's goal is to hold the data hostage until the victim pays to restore access.

- * A. Keylogger records keystrokes and doesn't encrypt files.
- * C. Phishing is a social engineering tactic to gather credentials, not to encrypt data.
- * D. Cryptominer uses system resources to mine cryptocurrency, not encrypt files. Reference: CompTIA A+ 220-1102 Objective 2.3: Compare and contrast common types of malware and threats. Study Guide Section: Ransomware behavior and user impact

=====

NEW QUESTION 8

A user is experiencing issues with outdated images while browsing websites. Which of the following settings should a technician use to correct this issue?

- A. Administrative Tools

- B. Windows Defender Firewall
- C. Internet Options
- D. Ease of Access

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract: Outdated images and website data often result from cached files in the browser. The Internet Options panel in Windows (specifically under the General tab) allows users to clear browsing history, including cached images and files, which forces the browser to load the most current versions of web content.

- * A. Administrative Tools is used for advanced system management, not browser settings.
- * B. Windows Defender Firewall controls network traffic and security rules, not caching.
- * D. Ease of Access provides accessibility features for users with disabilities — unrelated to web browsing issues.

Reference:

CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software and application issues.

Study Guide Section: Internet Options and browser cache clearing for display issues

NEW QUESTION 9

Which of the following provides information to employees, such as permitted activities when using the organization's resources?

- A. AUP
- B. MNDA
- C. DRM
- D. EULA

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

An Acceptable Use Policy (AUP) outlines the rules and guidelines for employees or users regarding the appropriate use of company systems, resources, and internet access. It defines permitted and prohibited activities, helping to mitigate security risks and establish clear behavioral expectations.

- * B. MNDA (Mutual Non-Disclosure Agreement) deals with confidentiality, not usage guidelines.
- * C. DRM (Digital Rights Management) controls access to copyrighted content.
- * D. EULA (End User License Agreement) pertains to software licensing, not internal policies.

Reference:

CompTIA A+ 220-1102 Objective 4.3: Explain common safety and environmental impacts and procedures.

Study Guide Section: Organizational policies — AUP, security best practices

=====

NEW QUESTION 10

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 to formally 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 10

Which of the following is the best way to distribute custom images to 800 devices that include four device vendor classes with two types of user groups?

- A. Use xcopy to clone the hard drives from one to another
- B. Use robocopy to move the files to each device
- C. Use a local image deployment tool for each device
- D. Use a network-based remote installation tool

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

In enterprise environments, network-based deployment solutions (such as Windows Deployment Services or SCCM) allow administrators to push images across

the network to hundreds of devices efficiently. These tools support hardware-specific drivers (for different vendor classes) and can accommodate user-group configurations using task sequences or answer files.

A and B (xcopy and robocopy) are file-level tools and not designed for full OS image deployment.

* C. Using local tools per device is inefficient for large-scale rollouts (800 devices).

* D. Network-based deployment is the industry standard for this scale. Reference:

CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.

Study Guide Section: Deployment methods (including PXE boot, image deployment)

=====

NEW QUESTION 12

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 16

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 18

A help desk technician needs to remove RAM from retired workstations and upgrade other workstations that have applications that use more memory with this RAM. Which of the following actions would the technician most likely take?

- A. Demagnetize memory for security.
- B. Use antistatic bags for storage and transport.
- C. Plug in the power supply to ground each workstation.
- D. Install memory in identical pairs.

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

RAM is an electrostatic-sensitive component. When removing or transporting RAM modules, they should be stored in antistatic bags to protect against electrostatic discharge (ESD), which can damage the memory. This is a standard best practice in hardware handling.

* A. Demagnetization is not applicable to RAM.

* C. Plugging in power to ground is not safe or recommended for static protection.

* D. Installing identical memory pairs is applicable for dual-channel configuration, but not directly related to transporting or handling RAM.

Reference:

CompTIA A+ 220-1102 Objective 4.3: Explain environmental impacts and procedures. Study Guide Section: ESD safety practices and component handling procedures

—

NEW QUESTION 22

A technician needs to provide remote support for a legacy Linux-based operating system from their Windows laptop. The solution needs to allow the technician to see what the user is doing and provide the ability to interact with the user's session. Which of the following remote access technologies would support the use case?

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

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The correct answer is VNC (Virtual Network Computing). VNC is a graphical desktop-sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer. It is platform-independent and widely supported on Linux, which makes it ideal for providing interactive remote support for a Linux-based operating system. It allows the technician not only to view the remote desktop session but also to control it, fulfilling the need to see and interact with the user's session.

* A. VPN (Virtual Private Network) creates a secure tunnel to a network but does not provide desktop sharing or session control by itself.

* C. SSH (Secure Shell) provides secure command-line access to Unix/Linux systems but does not offer graphical desktop interaction, which is a requirement in this case.

* D. RDP (Remote Desktop Protocol) is primarily a Microsoft protocol, and although it can be made to work on Linux, it is not natively supported on legacy Linux systems, and thus less suitable than VNC in this scenario.

CompTIA A+ 220-1102 Core 2 Objective Reference:

Objective 1.8 – Given a scenario, use features and tools of the operating system. Under this objective, candidates are expected to be familiar with remote access technologies, including RDP, SSH, and VNC, and understand their appropriate uses and limitations on different platforms such as Windows and Linux.

NEW QUESTION 26

A user's new smartphone is not staying charged throughout the day. The smartphone charges fully every night. Which of the following should a technician review first to troubleshoot the issue?

- A. Storage usage
- B. End of software support
- C. Charger wattage
- D. Background applications

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract: Background applications can significantly drain a smartphone's battery, even when the device is idle. A technician should first review which apps are running in the background

and consuming power through the battery usage section of the OS. Disabling or restricting power-hungry apps often resolves poor battery life.

* A. Storage usage doesn't significantly affect battery life.

* B. End of software support is unrelated to battery performance unless it's causing inefficient processes, which would still be secondary.

* C. Charger wattage affects charging speed, not battery life after charging. Reference:

CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common mobile OS and application issues.

Study Guide Section: Diagnosing battery and app performance issues on mobile devices

NEW QUESTION 28

A support specialist needs to decide whether to install a 32-bit or 64-bit OS architecture on a new computer. Which of the following specifications will help the specialist determine which OS architecture to use?

- A. 16GB RAM
- B. Intel i7 CPU
- C. 500GB HDD
- D. 1Gbps Ethernet

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The amount of installed RAM is the key factor in determining whether a 64-bit OS is needed. A 32-bit operating system cannot effectively address more than 4GB of RAM. Since this system has 16GB of RAM, a 64-bit OS is required to utilize the full memory.

* B. An Intel i7 CPU supports both 32-bit and 64-bit OS installations, so it alone doesn't determine the need.

* C. HDD size does not influence OS architecture selection.

* D. Ethernet speed is a network consideration and not related to OS architecture. Reference:

CompTIA A+ 220-1102 Objective 1.4: Given a scenario, choose the appropriate Microsoft OS installation methods and configurations.

Study Guide Section: 32-bit vs. 64-bit system requirements and memory limitations

=====

NEW QUESTION 30

A customer's computer does not have an active connection to the network. A technician goes through a few troubleshooting steps but is unable to resolve the issue. The technician has exhausted their knowledge. The customer expresses frustration at the time taken to resolve this issue. Which of the following should the technician do?

- A. Escalate the issue to a senior team member and provide next steps to the customer.
- B. Dismiss the customer and reschedule another troubleshooting session at a later date.
- C. Interrupt the customer and express that troubleshooting support tickets can take time.
- D. Maintain a positive attitude and continue to ask questions regarding the scope of the issue.

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

When a technician exhausts all troubleshooting steps within their knowledge and the issue remains unresolved, the best practice is to escalate the issue to a higher-level technician or team. Additionally, the technician should clearly communicate the next steps to the customer to maintain transparency and reduce frustration. This ensures continuity of support and upholds customer satisfaction.

* B. Dismissing the customer is unprofessional and violates proper customer service protocols.

* C. Interrupting the customer and providing excuses escalates the tension and is inappropriate.

* D. Continuing to ask questions without new troubleshooting steps wastes time and increases frustration.

Reference:

CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement best practices associated with documentation and support systems information.

Study Guide Section: Customer service best practices — escalation and communication

=====

NEW QUESTION 35

A user reports some single sign-on errors to a help desk technician. Currently, the user is able to sign in to the company's application portal but cannot access a specific SaaS-based tool. Which of the following would the technician most likely suggest as a next step?

- A. Reenroll the user's mobile device to be used as an MFA token
- B. Use a private browsing window to avoid local session conflicts
- C. Bypass single sign-on by directly authenticating to the application
- D. Reset the device being used to factory defaults

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

SSO issues are often related to cached session data, cookies, or browser artifacts. The fact that the user can access the company portal but not one specific SaaS tool suggests a session or token problem. Using a private/incognito browsing window allows a clean session to be initiated, which often resolves SSO conflicts.

* A. Reenrolling MFA is not related unless access issues stem from failed multifactor authentication.

* C. Bypassing SSO may not be possible depending on the SaaS tool and company policies.

* D. Factory resetting a device is a last resort and unnecessary in this case. Reference:

CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software, application, and OS security issues.

Study Guide Section: Troubleshooting login and authentication issues, especially with SSO services.

=====

NEW QUESTION 37

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 220-1202 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 220-1202 Product From:

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

Money Back Guarantee

220-1202 Practice Exam Features:

- * 220-1202 Questions and Answers Updated Frequently
- * 220-1202 Practice Questions Verified by Expert Senior Certified Staff
- * 220-1202 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 220-1202 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year