CompTIA

Exam Questions 220-1202

CompTIA A+ Certification Exam: Core 2

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 technician is attempting to join a workstation to a domain but is receiving an error message stating the domain cannot be found. However, the technician is able to ping the server and access the internet. Given the following information:
? IP Address – 192.168.1.210
? Subnet Mask – 255.255.255.0
? Gateway – 192.168.1.1
? DNS1 – 8.8.8.8
? DNS2 – 1.1.1.1
? Server – 192.168.1.10
Which of the following should the technician do to fix the issue?

A. Change the DNS settings.
B. Assign a static IP address.
C. Configure a subnet mask.
D. Update the default gateway.

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The issue described—??domain cannot be found?? despite the ability to ping the server and access the internet—indicates aDNS resolution problem, not a network connectivity issue. The workstation is currently usingpublic DNS servers (8.8.8.8 and 1.1.1.1)which cannot resolve internal domain names, such as the ones used in Active Directory environments. To resolve this, the technician needs tochange the DNS settings to point to the internal DNS server, which in most domain setups is thedomain controller itself (likely 192.168.1.10 in this case).
Here??s the breakdown of the incorrect options:
? B. Assign a static IP address: The IP is already assigned and functioning; the
device can ping and reach the network and internet.
? C. Configure a subnet mask: The subnet mask is appropriate for the network range (Class C /24).
? D. Update the default gateway: The gateway is valid and allows internet access; this is not the issue.
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 must know how to troubleshoot OS-based network configurations, includingproper DNS settings in domain environments.

NEW QUESTION 3
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 4
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 5
A small office reported a phishing attack that resulted in a malware infection. A technician is investigating the incident and has verified the following:
All endpoints are updated and have the newest EDR signatures.
Logs confirm that the malware was quarantined by EDR on one system. The potentially infected machine was reimaged.
Which of the following actions should the technician take next?

A. Install network security tools to prevent downloading infected files from the internet
B. Discuss the cause of the issue and educate the end user about security hygiene
C. Flash the firmware of the router to ensure the integrity of network traffic
D. Suggest alternate preventative controls that would include more advanced security software

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
After containment and remediation, one of the final steps in incident response is user education. Since the root cause was a phishing attack, it is essential to educate users about identifying phishing attempts, safe browsing practices, and how to handle suspicious communications. This improves overall security posture and helps prevent future incidents.
* A. Installing additional tools may be helpful but is a long-term step.
* C. Flashing router firmware is not warranted unless the network hardware is known to be compromised.
* D. Suggesting more advanced tools might be excessive given that the EDR successfully contained the incident.
Reference:
CompTIA A+ 220-1102 Objective 2.5: Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.
Study Guide Section: Incident response and user education after a security event

NEW QUESTION 6
A technician needs to map a shared drive from a command-line interface. Which of the following commands should the technician use?

A. pathping
B. nslookup
C. net use
D. tracert

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The net use command in Windows is used to map (assign) a shared drive from the command line. The syntax typically looks like: net use X: \server\share where X is the drive letter and \server\share is the network path.
* A. pathping tests network latency and packet loss.
* B. nslookup is used for DNS troubleshooting.
* D. tracert shows the route packets take to reach a destination — not for drive mapping. Reference:
CompTIA A+ 220-1102 Objective 1.7: Given a scenario, troubleshoot common operating system problems.
Study Guide Section: Command-line tools — net use for drive mapping
==========

NEW QUESTION 7
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 8
Which of the following is used in addition to a password to implement MFA?

A. Sending a code to the user's phone
B. Verifying the user's date of birth
C. Prompting the user to solve a simple math problem
D. Requiring the user to enter a PIN

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Multi-Factor Authentication (MFA) requires at least two different types of authentication factors:
? Something you know (e.g., password or PIN)
? Something you have (e.g., smartphone or hardware token)
? Something you are (e.g., fingerprint or facial recognition)
Option A, sending a code to the user??s phone, is an example of "something you have" — a physical device that receives a one-time passcode. Combined with a password, this forms a proper MFA implementation.
* B. Date of birth is another knowledge-based factor (like a password), not a second factor type.
* C. Solving a math problem is not a recognized authentication factor.
* D. A PIN is also "something you know" and does not count as a distinct MFA factor when paired with a password.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and authentication technologies.
Study Guide Section: Authentication factors — password, biometrics, tokens, MFA
==========

NEW QUESTION 9
A technician verifies that a malware incident occurred on some computers in a small office. Which of the following should the technician do next?

A. Quarantine the infected systems
B. Educate the end users
C. Disable System Restore
D. Update the anti-malware and scan the computers

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Once a malware incident has been confirmed, the immediate next step is to contain the threat. Quarantining infected systems prevents the malware from spreading to other devices and isolates the malicious code for further analysis or remediation.
* B. Educating end users is important but occurs later in the incident response process.
* C. Disabling System Restore is part of cleanup, not containment.
* D. Updating and scanning should occur after the system is quarantined to prevent further infection or spread.
Reference:
CompTIA A+ 220-1102 Objective 2.5: Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.
Study Guide Section: Malware removal best practices — Step 2: Quarantine the infected system
==========

NEW QUESTION 10
Which of the following describes a vulnerability that has been exploited before a patch or remediation is available?

A. Spoofing
B. Brute-force
C. DoS
D. Zero-day

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
A Zero-day vulnerability refers to a security flaw in software or hardware that is unknown to the vendor or has not yet been patched. If this vulnerability is exploited before the vendor has issued a fix or patch, it becomes a Zero-day exploit. These attacks are highly dangerous because they take advantage of the absence of defenses due to the lack of awareness or mitigation options.
* A. Spoofing is a form of impersonation, not necessarily tied to unpatched vulnerabilities.
* B. Brute-force attacks rely on repeatedly guessing credentials and are not related to software flaws.
* C. DoS (Denial of Service) attacks are meant to overwhelm systems and don't necessarily exploit unknown vulnerabilities.
Reference:
CompTIA A+ 220-1102 Objective 2.3: Compare and contrast common social engineering, threats, and vulnerabilities.
Study Guide Section: Threat types — Zero-day attacks, definitions, and implications

NEW QUESTION 10
A technician thinks that an application a user downloaded from the internet may not be the legitimate one, even though the name is the same. The technician needs to confirm whether the application is legitimate. Which of the following should the technician do?

A. Compare the hash value from the vendor.
B. Run Task Manager and compare the process ID.
C. Run the application in safe mode.
D. Verify the file name is correct.

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
To ensure the authenticity of a downloaded application, the most reliable method is to verify the file??s hash (e.g., SHA256, MD5) against the value provided by the legitimate
vendor. If the hash values match, the file has not been altered or tampered with. This verification confirms the integrity and authenticity of the executable.
* B. Process IDs are dynamic and not unique to specific software.
* C. Running in safe mode doesn??t validate legitimacy—it only runs the app in a minimal environment.
* D. File names can be spoofed; matching the name does not prove authenticity. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast authentication and software integrity verification methods.
Study Guide Section: Hash verification for software authenticity and digital integrity

NEW QUESTION 15
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 18
A company executive is currently attending a major music festival with a large number of attendees and is having trouble accessing a work email account. The email application is not downloading emails and also appears to become stuck during connection attempts. Which of the following is most likely causing the disruption?

A. The phone has no storage space available.
B. Company firewalls are configured to block remote access to email resources.
C. Too many devices in the same area are trying to connect to the mobile network.
D. The festival organizer prohibits internet usage during the event and has blocked the internet signal

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
At large events such as music festivals, cellular towers may become congested due to the high volume of users attempting to connect simultaneously. This congestion causes slow or failed data connections, which explains the email application being unable to sync or connect. This is a common real-world mobile connectivity issue in crowded areas.
* A. Lack of storage would prevent saving attachments, not prevent connection attempts.
* B. Company firewalls usually don??t affect mobile access unless specific device restrictions are enforced.
* D. Organizers do not have the ability to block the internet signal; only carriers manage mobile bandwidth.
Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot mobile OS and connectivity issues. Study Guide Section: Mobile network limitations — signal congestion and bandwidth issues
==========

NEW QUESTION 22
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 27
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 30
A user receives a new personal computer but is unable to run an application. An error displays saying that .NET Framework 3.5 is required and not found. Which of the following actions is the best way to resolve this issue?

A. Resolve the dependency through the 'Turn Windows features on or off' menu.
B. Download the dependency via a third-party repository.
C. Ignore the dependency and install the latest version 4 instead.
D. Forward the trouble ticket to the SOC team because the issue poses a great security risk.

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
NET Framework versions are often required for applications to run. If an older app requires
.NET Framework 3.5, it must be explicitly installed as it is not included by default in newer versions of Windows. The best method to do this safely is through the built-in "Turn Windows features on or off" utility, which downloads and installs it via official Microsoft services.
* B. Using third-party repositories is unsafe and not recommended.
* C. Installing .NET 4 does not include 3.5; versions are not fully backward compatible.
* D. The issue is technical, not a security incident for the SOC team. Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software, application, and OS security issues.
Study Guide Section: Managing application dependencies (e.g., .NET Framework, Java)
==========

NEW QUESTION 35
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 38
A user is working from home and is unable to access work files on a company laptop. Which of the following should a technician configure to fix the network

access issue?

A. Wide-area network
B. Wireless network
C. Proxy network settings
D. Virtual private network

Answer: D

Explanation:
A VPN creates a secure tunnel from the user??s home network into the corporate network, providing the necessary routing and access controls for the laptop to reach internal file servers. Without a VPN, the device remains outside the corporate LAN and cannot directly reach protected resources.
A VPN creates a secure tunnel from the user??s home network into the corporate network, providing the necessary routing and access controls for the laptop to reach internal file servers. Without a VPN, the device remains outside the corporate LAN and cannot directly reach protected resources.

NEW QUESTION 40
Users are reporting that an unsecured network is broadcasting with the same name as the
normal wireless network. They are able to access the internet but cannot connect to the file share servers. Which of the following best describes this issue?

A. Unreachable DNS server
B. Virtual local area network misconfiguration
C. Incorrect IP address
D. Rogue wireless access point

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
This scenario describes a rogue access point — a malicious or unauthorized wireless access point that uses the same SSID as the legitimate network. Users may connect to it unknowingly, which can result in limited network access, data interception, or redirection of traffic. The inability to reach internal file servers supports this being an unauthorized AP with no connection to internal resources.
* A. A DNS issue would impact name resolution, not connectivity to file servers directly.
* B. VLAN issues generally affect segmentation, not mimic SSID problems.
* C. An incorrect IP address could cause connectivity issues, but not in the presence of a malicious AP broadcasting the same SSID.
Reference:
CompTIA A+ 220-1102 Objective 2.4: Compare and contrast wireless and physical security threats.
Study Guide Section: Rogue access points and their detection
==========

NEW QUESTION 44
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 47
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 51
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 52
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 54
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 57
A user recently installed an application that accesses a database from a local server. When launching the application, it does not populate any information. Which of the following command-line tools is the best to troubleshoot the issue?

A. ipconfig
B. nslookup

C. netstat
D. curl

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The scenario involves an application that should retrieve data from a local database server but is failing to do so. This likely indicates a problem in communication between the application and the database server (such as a network issue, port misconfiguration, or service unavailability). The correct troubleshooting approach involves testing the network/service connectivity between the client and the database.
Let??s examine the options:
? A. ipconfig:This command displays IP configuration details for Windows systems, such as IP address, subnet mask, and default gateway. While useful for diagnosing general networkissues, it does not test service connectivity or the availability of a specific application port/service.
? B. nslookup:Used to query DNS servers to resolve domain names to IP addresses.
However, since the question references a local server (likely accessed via IP or static hostname), DNS is probably not involved. Also, it does not test application/service availability.
? C. netstat:Displays active TCP connections, listening ports, and routing tables. It
helps determine whether the local system is listening for or maintaining any network connections, but it does not initiate a connection to test availability. It??s diagnostic but not interactive for service testing.
? D. curl:This is the most appropriate tool for this scenario. curl is used to test
connectivity to services over protocols like HTTP, HTTPS, FTP, and more. If the application retrieves data via a web interface or API (common in database-driven applications), curl can be used to test if the application can successfully reach and retrieve data from the server. It provides immediate, testable feedback on whether the server and service are available and responsive.
Example usage: curlhttp://localhost:8080/api/data
This command would test whether a local server's application programming interface (API) is available and responding on port 8080.
CompTIA A+ 220-1102 Reference Points:
? Objective 2.4: Given a scenario, use appropriate tools to troubleshoot and support Windows OS issues.
? Objective 3.3: Use appropriate tools to troubleshoot and resolve issues.
? The CompTIA A+ Core 2 study guide references curl as a useful command-line utility for testing connectivity and troubleshooting application access to services.
==========

NEW QUESTION 58
A technician needs to install an operating system on a large number of workstations. Which of the following is the fastest method?

A. Physical media
B. Mountable ISO
C. Manual installation
D. Image deployment

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Image deployment is the fastest and most efficient method for installing operating systems on multiple machines. It involves creating a pre-configured image of an OS and deploying it across systems using tools like Windows Deployment Services (WDS) or third-party imaging solutions. This method saves time and ensures consistency across all devices.
* A. Physical media is slow and not scalable.
* B. Mountable ISOs are useful but still require manual installation.
* C. Manual installation is time-consuming and not suitable for large-scale deployment. Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: Deployment methods — image deployment, automation

NEW QUESTION 59
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 60
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 61
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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