

CompTIA

Exam Questions 220-1202

CompTIA A+ Certification Exam: Core 2



NEW QUESTION 1

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 a DNS resolution problem, not a network connectivity issue. The workstation is currently using public 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 to change the DNS settings to point to the internal DNS server, which in most domain setups is the domain 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, including proper DNS settings in domain environments.

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

A user frequently misplaces their Windows laptop and is concerned about it being stolen. The user would like additional security controls on their laptop. Which of the following is a built-in technology that a technician can use to enable full drive encryption?

- A. Active Directory
- B. New Technology File System
- C. Encrypting File System
- D. BitLocker

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract: BitLocker is Microsoft’s full disk encryption technology built into Windows Pro and Enterprise editions. It encrypts the entire drive, protecting data if the device is lost or stolen. BitLocker can use TPM (Trusted Platform Module) and can be configured with PINs or USB keys for added security.

* A. Active Directory is for centralized user and policy management in domains.

* B. NTFS is the file system format and doesn’t provide encryption by itself.

* C. EFS (Encrypting File System) encrypts individual files or folders, not the entire drive. Reference:

CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and encryption tools.

Study Guide Section: Encryption options — BitLocker vs. EFS

=====

NEW QUESTION 4

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 5

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 6

Which of the following methods involves requesting a user's approval via a push notification to verify the user's identity?

- A. Call
- B. Authenticator
- C. Hardware token
- D. SMS

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Authenticator apps (e.g., Microsoft Authenticator, Google Authenticator, Duo) often support push notifications. When the user logs in, the app sends a push to their mobile device, prompting the user to approve or deny the authentication request — a common and user- friendly form of multi-factor authentication (MFA).

- * A. Phone call verification is a separate method involving voice-based confirmation.
- * C. Hardware tokens generate one-time codes but do not send push notifications.
- * D. SMS sends a text message with a code — again, no push mechanism. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast multi-factor authentication methods.
Study Guide Section: Authentication apps and push notification verification

=====

NEW QUESTION 7

A help desk team was alerted that a company-owned cell phone has an unrecognized password-cracking application. Which of the following should the help desk team do to prevent further unauthorized installations from occurring?

- A. Configure Group Policy.
- B. Implement PAM.
- C. Install anti-malware software.
- D. Deploy MDM.

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Mobile Device Management (MDM) is used to control, monitor, and enforce policies on mobile devices. It allows IT teams to restrict app installations, push

approved apps, and monitor device compliance. Deploying MDM would prevent unauthorized applications, such as password crackers, from being installed on company-managed devices.

* A. Group Policy is for managing Windows environments and not applicable to smartphones.

* B. PAM (Privileged Access Management) controls administrative access, not app installation.

* C. Anti-malware can help detect malicious apps but doesn't prevent their installation proactively.

Reference:

CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and tools.

Study Guide Section: Mobile Device Management (MDM) capabilities — app control, security enforcement

NEW QUESTION 8

A user is attempting to open on a mobile phone a HD video that is hosted on a popular media streaming website. The user is receiving connection timeout errors. The mobile reception icon area is showing two bars next to 3G. Which of the following is the most likely cause of the issue?

A. The user does not have Wi-Fi enabled.

B. The website's subscription has run out.

C. The bandwidth is not fast enough.

D. The mobile device storage is full.

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

3G networks generally do not provide the bandwidth required for seamless HD video streaming. With only two signal bars and a 3G connection, the mobile device likely cannot maintain the necessary data throughput, resulting in timeouts or buffering failures. This is a classic symptom of insufficient network speed or signal strength.

* A. Lack of Wi-Fi may contribute, but the root cause is the low mobile bandwidth, not the Wi-Fi state.

* B. A website subscription lapse would return an account error, not a timeout.

* D. Full device storage can affect downloads but not streaming from the internet. Reference:

CompTIA A+ 220-1102 Objective 3.3: Troubleshoot mobile OS and application issues. Study Guide Section: Connectivity and network performance issues on mobile devices

=====

NEW QUESTION 9

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 10

A technician is troubleshooting an issue in which a service runs momentarily and stops at certain points in the process. The technician needs to determine the root cause of this issue. Which of the following tools should the technician use?

A. Event Viewer

B. Task Manager

C. Internet Options

D. Process Explorer

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Event Viewer is the best tool to analyze the root cause of service failures in Windows. It provides detailed logs from system processes, including errors, warnings, and crash reports related to services and applications. When a service starts and stops unexpectedly, Event Viewer will often record the cause, such as dependency failures or access violations.

* B. Task Manager shows active processes but doesn't retain logs or causes of failure.

* C. Internet Options is used for configuring browser settings, not troubleshooting services.

* D. Process Explorer is powerful but more suited for live monitoring and detailed process trees, not post-failure log analysis.

Reference:

CompTIA A+ 220-1102 Objective 3.1: Given a scenario, troubleshoot common Windows OS problems.

Study Guide Section: Log file analysis using Event Viewer

=====

NEW QUESTION 10

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 14

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 17

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 22

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 23

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 26

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 network issues, 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: curl http://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 29

A technician is setting up a surveillance system for a customer. The customer wants access to the system's web interface on the LAN via the system's IP address. Which of the following should the technician use to prevent external log-in attempts from the internet?

A. Port mapping

B. Subnetting

C. Static IP

D. Content filtering

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

To prevent external access, the technician should avoid exposing the surveillance system's port to the public internet. Port mapping (also known as port forwarding) is the method used to control which internal devices and ports are accessible from the outside. By not configuring port forwarding for the device, external login attempts are effectively blocked.

* B. Subnetting organizes IP addresses but doesn't directly restrict access.

* C. A static IP ensures consistent addressing but does not secure access.

* D. Content filtering is used to restrict web content, not to block access to a web interface. Reference:

CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and tools. Study Guide Section: SOHO router security — port forwarding and blocking external access

=====

NEW QUESTION 33

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 38

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 43

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The 220-1202 Practice Test Here](#)