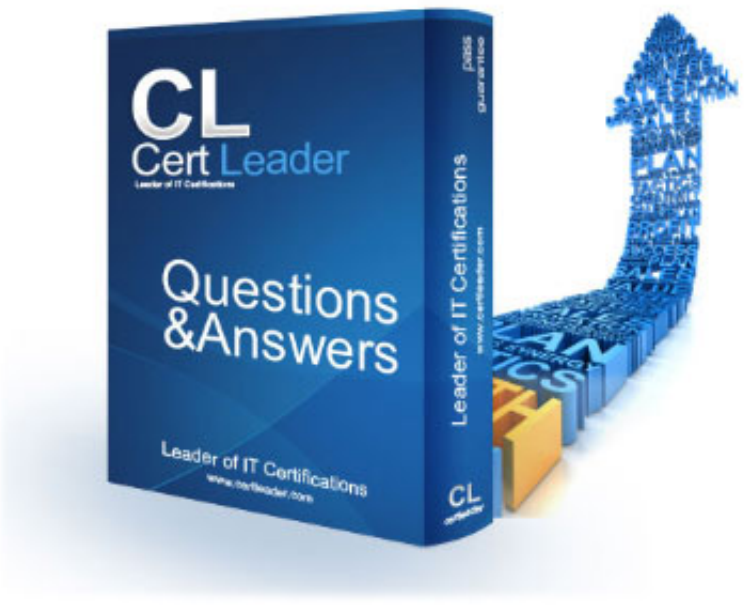
220-1202 Dumps

CompTIA A+ Certification Exam: Core 2

https://www.certleader.com/220-1202-dumps.html



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
Recently, the number of users sharing smartphone passcodes has increased. The management team wants a technician to deploy a more secure screen lock method. Which of the following technologies should the technician use?

A. Pattern lock
B. Facial recognition
C. Device encryption
D. Multifactor authentication

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Facial recognition is a biometric authentication method that ties access to a unique physical feature of the user. Unlike passcodes or pattern locks—which can be easily shared—facial recognition provides a more secure and non-transferable form of access. It also enhances user convenience and is widely supported by modern smartphones.
* A. Pattern locks can still be shared and are less secure.
* C. Device encryption protects data but does not prevent screen access if a passcode is shared.
* D. Multifactor authentication typically applies to app or account access, not basic phone unlocking.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and authentication technologies.
Study Guide Section: Biometric screen lock technologies (e.g., facial recognition, fingerprint)
==========

NEW QUESTION 3
A technician uses AI to draft a proposal about the benefits of new software. When reading the draft, the technician notices that the draft contains factually incorrect information. Which of the following best describes this scenario?

A. Data privacy
B. Hallucinations
C. Appropriate use
D. Plagiarism

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In the context of artificial intelligence, "hallucinations" refer to instances where an AI system generates information that is plausible-sounding but factually incorrect or entirely fabricated. This is a known limitation of large language models, including generative AI tools.
* A. Data privacy refers to the protection of personal or sensitive data, not content accuracy.
* C. Appropriate use relates to ethical and policy-based concerns, not factual correctness.
* D. Plagiarism involves presenting someone else's work as your own — this situation is about accuracy, not ownership.
Reference:
CompTIA A+ 220-1102 Objective 4.4: Identify basic concepts of scripting and automation. Study Guide Section: AI tools and responsible usage — hallucinations and fact-checking outputs
==========

NEW QUESTION 4
A company would like to deploy baseline images to new computers as they are started up on the network. Which of the following boot processes should the company use for this task?

A. ISO
B. Secure
C. USB
D. PXE

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
PXE (Preboot Execution Environment) allows workstations to boot over the network and download an OS image from a server. It is ideal for automating mass deployments using
baseline images across many machines without the need for physical media.
* A. An ISO is a disk image file but requires mounting or physical media.
* B. Secure Boot is a security feature, not a method of deploying OS images.
* C. USB requires manual installation and is not suitable for automated deployment at scale. Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: Remote installation methods — PXE boot deployment
==========

NEW QUESTION 5
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 6
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 7
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 8
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 9
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 10
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 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 13
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 14
A security administrator teaches all of an organization's staff members to use BitLocker To Go. Which of the following best describes the reason for this training?

A. To ensure that all removable media is password protected in case of loss or theft
B. To enable Secure Boot and a BIOS-level password to prevent configuration changes
C. To enforce VPN connectivity to be encrypted by hardware modules
D. To configure all laptops to use the TPM as an encryption factor for hard drives

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
BitLocker To Go is a Microsoft encryption feature specifically designed for removable drives such as USB flash drives and external hard drives. It allows users to protect the data on these devices by requiring a password to decrypt the contents, thereby preventing unauthorized access in the event the device is lost or stolen.
A is correct because BitLocker To Go is directly tied to password-protecting removable media.
B and C are unrelated to BitLocker To Go; Secure Boot and VPN encryption are entirely
different security layers.
D applies to BitLocker (not BitLocker To Go) and full disk encryption on internal drives using TPM.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and tools.
Study Guide Section: Encryption technologies (BitLocker, BitLocker To Go)
==========

NEW QUESTION 16
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 19
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 24
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 28
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 29
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 30
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 31
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 34
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 36
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 37
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 40
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 42
An administrator received an email stating that the OS they are currently supporting will no longer be issued security updates and patches. Which of the following is most likely the reason the administrator received this message?

A. Support from the computer's manufacturer is expiring
B. The OS will be considered end of life
C. The built-in security software is being removed from the next OS version
D. A new version of the OS will be released soon

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Operating systems periodically reach a status known as "end of life" (EOL), at which point the developer (e.g., Microsoft, Apple) ceases to provide security updates, patches, or technical support. When this happens, the OS becomes vulnerable and non-compliant with security best practices, which is why organizations typically receive advance notifications from vendors or support teams.
* A. Manufacturer support expiration only applies to hardware, not OS patching.
* C. Security software may be upgraded or removed, but that does not affect patching the OS itself.
* D. The release of a new version doesn??t automatically stop updates for the current version. Reference:
CompTIA A+ 220-1102 Objective 1.3: Given a scenario, use appropriate Microsoft operating system features and tools.
Study Guide Section: OS lifecycle management and vendor support phases (e.g., EOL)
==========

NEW QUESTION 45
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 50
A technician is assigned to offboard a user. Which of the following are common tasks on an offboarding checklist? (Choose two.)

A. Quarantine the hard drive in the user's laptop.
B. Deactivate the user's key fobs for door access.
C. Purge all PII associated with the user.
D. Suspend the user's email account.
E. Turn off the network ports underneath the user's desk.
F. Add the MAC address of the user's computer to a blocklist.

Answer: BD

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
User offboarding involves disabling the departing user's access to company systems and facilities. Two key tasks typically include:
? Deactivating physical access credentials (e.g., key fobs or badges) to prevent unauthorized entry (B).
? Suspending or disabling the user??s email account to prevent future use and to retain business communications (D).
* A. Quarantining a hard drive is not standard unless malware or legal issues are involved.
* C. Purging PII must follow legal retention policies; it's not typically an immediate offboarding task.
* E. Disabling network ports may be relevant in some cases but is not a standard offboarding step.
* F. Blocking MAC addresses is not typical unless the device is considered a security threat. Reference:
CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement proper documentation and offboarding procedures.
Study Guide Section: User lifecycle management — onboarding and offboarding tasks
==========

NEW QUESTION 53
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 55
An organization is experiencing an increased number of issues. A technician notices applications that are not installed by default. Users are reporting an increased number of system prompts for software licensing. Which of the following would the security team most likely do to remediate the root cause?

A. Deploy an internal PKI to filter encrypted web traffic.
B. Remove users from the local admin group.
C. Implement stronger controls to block suspicious websites.
D. Enable stricter UAC settings on Windows.

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
If unauthorized or non-standard applications are appearing on systems and users are receiving licensing prompts, it??s likely users are installing software themselves. Removing users from the local administrators group will prevent them from installing software without approval and reduce the likelihood of introducing unapproved or malicious programs.
* A. Deploying a PKI helps with secure communications but doesn??t address user software installation rights.
* C. Blocking suspicious websites is helpful but doesn??t prevent local installations.
* D. Stricter UAC may add prompts but can still be bypassed by admin users. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast access control methods and user privilege settings.
Study Guide Section: Principle of least privilege and managing local admin rights
==========

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 61
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 62
MFA for a custom web application on a user's smartphone is no longer working. The last time the user remembered it working was before taking a vacation to another country. Which of the following should the technician do first?

A. Verify the date and time settings
B. Apply mobile OS patches
C. Uninstall and reinstall the application
D. Escalate to the website developer

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Multi-Factor Authentication (MFA) apps, especially time-based one-time password (TOTP) apps (e.g., Google Authenticator, Authy), rely on accurate time synchronization between the device and the authentication server. If the user recently traveled internationally, the device may have incorrect date/time settings due to time zone changes or failed synchronization, leading to MFA failure.
The most logical and non-intrusive first step is to verify and correct the date and time settings. This aligns with basic troubleshooting principles—start with the simplest and most likely cause before taking more drastic action.
Reference:
CompTIA A+ 220-1102 Objective 2.6: Given a scenario, apply cybersecurity best practices to secure a workstation.
Study Guide Section: Authentication technologies and MFA troubleshooting
==========

NEW QUESTION 67
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 72
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 77
A user reports some single sign-on errors to a help desk technician. Currently, the user is able tosign 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 82
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 220-1202 Exam with Our Prep Materials Via below:

https://www.certleader.com/220-1202-dumps.html