EDUSUM

#1 Online Certification Guide

Excel at 220-1102 A+ Core 2 Exam: Proven Study Methods for Triumph

CompTIA A+ Core 2 CERTIFICATION QUESTIONS & ANSWERS

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

Table of Contents

Getting Ready for the 220-1102 Exam:

Use proven study tips and techniques to prepare for the 220-1102 exam confidently. Boost your readiness, improve your understanding regarding the Core, and increase your chances of success in the CompTIA A+ with our comprehensive guide. Start your journey towards exam excellence today.

CompTIA A+ Certification Details:

Exam Name	CompTIA A+
Exam Code	220-1102
Exam Price	$253 (USD)
Duration	90 mins
Number of Questions	90
Passing Score	700 / 900
Books / Training	CertMaster Learn for A+ CompTIA A+ Certification Training
Schedule Exam	Pearson VUE
Sample Questions	CompTIA A+ Core 2 Sample Questions
Practice Exam	CompTIA 220-1102 Certification Practice Exam

Explore 220-1102 Syllabus:

Topic	Details
Operating Systems - 31%	
Identify basic features of Microsoft Windows editions.	- Windows 10 editions • Home • Pro • Pro for Workstations • Enterprise - Feature differences • Domain access vs. workgroup • Desktop styles/user interface • Availability of Remote Desktop Protocol (RDP) • Random-access memory (RAM) support limitations • BitLocker • gpedit.msc

Topic	Details
	- Upgrade paths • In-place upgrade
Given a scenario, use the appropriate Microsoft command-line tool.	- Navigation • cd • dir • rmdir • Drive navigation inputs: - C: or D: or x: - Command-line tools • ipconfig • ping • hostname • netstat • nslookup • chkdsk • net user • net use • tracert • format • xcopy • copy • robocopy • gpupdate • gpresult • shutdown • sfc • [command name] /? • diskpart • pathping • winver
Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).	- Task Manager • Services • Startup • Performance

Topic	Details
	• Processes • Users - Microsoft Management Console (MMC) snap-in • Event Viewer (eventvwr.msc) • Disk Management (diskmgmt.msc) • Task Scheduler (taskschd.msc) • Device Manager (devmgmt.msc) • Certificate Manager (certmgr.msc) • Local Users and Groups (lusrmgr.msc) • Performance Monitor (perfmon.msc) • Group Policy Editor (gpedit.msc) - Additional tools • System Information (msinfo32. exe) • Resource Monitor (resmon.exe) • System Configuration (msconfig. exe) • Disk Cleanup (cleanmgr.exe) • Disk Defragment (dfrgui.exe) • Registry Editor (regedit.exe)
Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.	- Internet Options - Devices and Printers - Programs and Features - Network and Sharing Center - System - Windows Defender Firewall - Mail - Sound - User Accounts - Device Manager - Indexing Options - Administrative Tools - File Explorer Options • Show hidden files • Hide extensions • General options • View options - Power Options

Topic	Details
	• Hibernate • Power plans • Sleep/suspend • Standby • Choose what closing the lid does • Turn on fast startup • Universal Serial Bus (USB) selective suspend - Ease of Access
Given a scenario, use the appropriate Windows settings.	- Time and Language - Update and Security - Personalization - Apps - Privacy - System - Devices - Network and Internet - Gaming - Accounts
Given a scenario, configure Microsoft Windows networking features on a client/desktop.	- Workgroup vs. domain setup • Shared resources • Printers • File servers • Mapped drives - Local OS firewall settings • Application restrictions and exceptions • Configuration - Client network configuration • Internet Protocol (IP) addressing scheme • Domain Name System (DNS) settings • Subnet mask • Gateway • Static vs. dynamic - Establish network connections • Virtual private network (VPN) • Wireless

Topic	Details
	• Wired • Wireless wide area network (WWAN) - Proxy settings - Public network vs. private network - File Explorer navigation – network paths - Metered connections and limitations
Given a scenario, apply application installation and configuration concepts.	- System requirements for applications • 32-bit vs. 64-bit dependent application requirements • Dedicated graphics card vs. integrated • Video random-access memory (VRAM) requirements • RAM requirements • Central processing unit (CPU) requirements • External hardware tokens • Storage requirements - OS requirements for applications • Application to OS compatibility • 32-bit vs. 64-bit OS - Distribution methods • Physical media vs. downloadable • ISO mountable - Other considerations for new applications • Impact to device • Impact to network • Impact to operation • Impact to business
Explain common OS types and their purposes.	- Workstation OSs • Windows • Linux • macOS • Chrome OS - Cell phone/tablet OSs

Topic	Details
	• iPadOS • iOS • Android - Various filesystem types • New Technology File System (NTFS) • File Allocation Table 32 (FAT32) • Third extended filesystem (ext3) • Fourth extended filesystem (ext4) • Apple File System (APFS) • Extensible File Allocation Table (exFAT) - Vendor life-cycle limitations • End-of-life (EOL) • Update limitations - Compatibility concerns between OSs
Given a scenario, perform OS installations and upgrades in a diverse OS environment.	- Boot methods • USB • Optical media • Network • Solid-state/flash drives • Internet-based • External/hot-swappable drive • Internal hard drive (partition) - Types of installations • Upgrade • Recovery partition • Clean install • Image deployment • Repair installation • Remote network installation • Other considerations - Third-party drivers - Partitioning • GUID [globally unique identifier] Partition Table

Topic	Details
	(GPT) • Master boot record (MBR) - Drive format - Upgrade considerations • Backup files and user preferences • Application and driver support/backward compatibility • Hardware compatibility - Feature updates • Product life cycle
Identify common features and tools of the macOS/desktop OS.	- Installation and uninstallation of applications • File types - .dmg - .pkg - .app • App Store • Uninstallation process - Apple ID and corporate restrictions - Best practices • Backups • Antivirus • Updates/patches - System Preferences • Displays • Networks • Printers • Scanners • Privacy • Accessibility • Time Machine - Features • Multiple desktops • Mission Control

Topic	Details
	• Keychain • Spotlight • iCloud • Gestures • Finder • Remote Disc • Dock - Disk Utility - FileVault - Terminal - Force Quit
Identify common features and tools of the Linux client/desktop OS.	- Common commands • ls • pwd • mv • cp • rm • chmod • chown • su/sudo • apt-get • yum • ip • df • grep • ps • man • top • find • dig • cat • nano - Best practices • Backups • Antivirus

Topic	Details
	• Updates/patches - Tools • Shell/terminal • Samba
Security - 25%	
Summarize various security measures and their purposes.	- Physical security • Access control vestibule • Badge reader • Video surveillance • Alarm systems • Motion sensors • Door locks • Equipment locks • Guards • Bollards • Fences - Physical security for staf • Key fobs • Smart cards • Keys • Biometrics - Retina scanner - Fingerprint scanner - Palmprint scanner • Lighting • Magnetometers - Logical security • Principle of least privilege • Access control lists (ACLs) • Multifactor authentication (MFA) • Email • Hard token • Soft token • Short message service (SMS)

Topic	Details
	• Voice call • Authenticator application - Mobile device management (MDM) - Active Directory • Login script • Domain • Group Policy/updates • Organizational units • Home folder • Folder redirection • Security groups
Compare and contrast wireless security protocols and authentication methods.	- Protocols and encryption • WiFi Protected Access 2 (WPA2) • WPA3 • Temporal Key Integrity Protocol (TKIP) • Advanced Encryption Standard (AES) - Authentication • Remote Authentication Dial-In User Service (RADIUS) • Terminal Access Controller Access-Control System (TACACS+) • Kerberos • Multifactor
Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.	- Malware • Trojan • Rootkit • Virus • Spyware • Ransomware • Keylogger • Boot sector virus • Cryptominers - Tools and methods • Recovery mode

Topic	Details
	• Antivirus • Anti-malware • Software firewalls • Anti-phishing training • User education regarding common threats • OS reinstallation
Explain common social-engineering attacks, threats, and vulnerabilities.	- Social engineering • Phishing • Vishing • Shoulder surfing • Whaling • Tailgating • Impersonation • Dumpster diving • Evil twin - Threats • Distributed denial of service (DDoS) • Denial of service (DoS) • Zero-day attack • Spoofing • On-path attack • Brute-force attack • Dictionary attack • Insider threat • Structured Query Language (SQL) injection • Cross-site scripting (XSS) - Vulnerabilities • Non-compliant systems • Unpatched systems • Unprotected systems (missing antivirus/missing firewall) • EOL OSs • Bring your own device (BYOD)
Given a scenario, manage and configure	- Defender Antivirus

Topic	Details
basic security settings in the Microsoft Windows OS.	• Activate/deactivate • Updated definitions - Firewall • Activate/deactivate • Port security • Application security - Users and groups • Local vs. Microsoft account • Standard account • Administrator • Guest user • Power user - Login OS options • Username and password • Personal identification number (PIN) • Fingerprint • Facial recognition • Single sign-on (SSO) - NTFS vs. share permissions • File and folder attributes • Inheritance - Run as administrator vs. standard user • User Account Control (UAC) - BitLocker - BitLocker To Go - Encrypting File System (EFS)
Given a scenario, configure a workstation to meet best practices for security.	- Data-at-rest encryption - Password best practices • Complexity requirements - Length - Character types • Expiration requirements

Topic	Details
	• Basic input/output system (BIOS)/Unified Extensible Firmware Interface (UEFI) passwords - End-user best practices • Use screensaver locks • Log off when not in use • Secure/protect critical hardware (e.g., laptops) • Secure personally identifiable information (PII) and passwords - Account management • Restrict user permissions • Restrict login times • Disable guest account • Use failed attempts lockout • Use timeout/screen lock - Change default administrator's user account/password - Disable AutoRun - Disable AutoPlay
Explain common methods for securing mobile and embedded devices.	- Screen locks • Facial recognition • PIN codes • Fingerprint • Pattern • Swipe - Remote wipes - Locator applications - OS updates - Device encryption - Remote backup applications - Failed login attempts restrictions - Antivirus/anti-malware - Firewalls - Policies and procedures • BYOD vs. corporate owned • Profile security requirements

Topic	Details
	- Internet of Things (IoT)
Given a scenario, use common data destruction and disposal methods.	- Physical destruction • Drilling • Shredding • Degaussing • Incinerating - Recycling or repurposing best practices • Erasing/wiping • Low-level formatting • Standard formatting - Outsourcing concepts • Third-party vendor • Certification of destruction/recycling
Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.	- Home router settings • Change default passwords • IP filtering • Firmware updates • Content filtering • Physical placement/secure locations • Dynamic Host Configuration Protocol (DHCP) reservations • Static wide-area network (WAN) IP • Universal Plug and Play (UPnP) • Screened subnet - Wireless specific • Changing the service set identifier (SSID) • Disabling SSID broadcast • Encryption settings • Disabling guest access • Changing channels - Firewall settings • Disabling unused ports

Topic	Details
	• Port forwarding/mapping
Given a scenario, install and configure browsers and relevant security settings.	- Browser download/installation • Trusted sources - Hashing • Untrusted sources - Extensions and plug-ins • Trusted sources • Untrusted sources - Password managers - Secure connections/sites – valid certificates - Settings • Pop-up blocker • Clearing browsing data • Clearing cache • Private-browsing mode • Sign-in/browser data synchronization • Ad blockers
Software Troubleshooting - 22%	
Given a scenario, troubleshoot common Windows OS problems.	- Common symptoms • Blue screen of death (BSOD) • Sluggish performance • Boot problems • Frequent shutdowns • Services not starting • Applications crashing • Low memory warnings • USB controller resource warnings • System instability • No OS found • Slow profile load • Time drift - Common troubleshooting steps • Reboot

Topic	Details
	• Restart services • Uninstall/reinstall/update applications • Add resources • Verify requirements • System file check • Repair Windows • Restore • Reimage • Roll back updates • Rebuild Windows profiles
Given a scenario, troubleshoot common personal computer (PC) security issues.	- Common symptoms • Unable to access the network • Desktop alerts • False alerts regarding antivirus protection • Altered system or personal files - Missing/renamed files • Unwanted notifications within the OS • OS update failures - Browser-related symptoms • Random/frequent pop-ups • Certificate warnings • Redirection
Given a scenario, use best practice procedures for malware removal.	- Investigate and verify malware symptoms - Quarantine infected systems - Disable System Restore in Windows - Remediate infected systems • Update anti-malware software • Scanning and removal techniques (e.g., safe mode, preinstallation environment) - Schedule scans and run updates - Enable System Restore and create a restore point in Windows - Educate the end user
Given a scenario, troubleshoot common mobile OS and	- Common symptoms • Application fails to launch

Topic	Details
application issues.	• Application fails to close/crashes • Application fails to update • Slow to respond • OS fails to update • Battery life issues • Randomly reboots • Connectivity issues - Bluetooth - WiFi - Near-field communication (NFC) - AirDrop • Screen does not autorotate
Given a scenario, troubleshoot common mobile OS and application security issues.	- Security concerns • Android package (APK) source • Developer mode • Root access/jailbreak • Bootleg/malicious application - Application spoofing - Common symptoms • High network traffic • Sluggish response time • Data-usage limit notification • Limited Internet connectivity • No Internet connectivity • High number of ads • Fake security warnings • Unexpected application behavior • Leaked personal files/data
Operational Procedures - 22%	
Given a scenario, implement best practices associated with documentation and support systems information management.	- Ticketing systems • User information • Device information • Description of problems • Categories • Severity

Topic	Details
	• Escalation levels • Clear, concise written communication - Problem description - Progress notes - Problem resolution - Asset management • Inventory lists • Database system • Asset tags and IDs • Procurement life cycle • Warranty and licensing • Assigned users - Types of documents • Acceptable use policy (AUP) • Network topology diagram • Regulatory compliance requirements - Splash screens • Incident reports • Standard operating procedures - Procedures for custom installation of software package • New-user setup checklist • End-user termination checklist - Knowledge base/articles
Explain basic change-management best practices.	- Documented business processes • Rollback plan • Sandbox testing • Responsible staff member - Change management • Request forms • Purpose of the change • Scope of the change • Date and time of the change • Affected systems/impact

Topic	Details
	• Risk analysis - Risk level • Change board approvals • End-user acceptance
Given a scenario, implement workstation backup and recovery methods.	- Backup and recovery • Full • Incremental • Differential • Synthetic - Backup testing • Frequency - Backup rotation schemes • On site vs. off site • Grandfather-father-son (GFS) • 3-2-1 backup rule
Given a scenario, use common safety procedures.	- Electrostatic discharge (ESD) straps - ESD mats - Equipment grounding - Proper power handling - Proper component handling and storage - Antistatic bags - Compliance with government regulations - Personal safety • Disconnect power before repairing PC • Lifting techniques • Electrical fire safety • Safety goggles • Air filtration mask
Summarize environmental impacts and local environmental controls.	- Material safety data sheet (MSDS)/documentation for handling and disposal • Proper battery disposal • Proper toner disposal • Proper disposal of other devices and assets - Temperature, humidity-level awareness, and proper ventilation

Topic	Details
	• Location/equipment placement • Dust cleanup • Compressed air/vacuums - Power surges, under-voltage events, and power failures • Battery backup • Surge suppressor
Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.	- Incident response • Chain of custody • Inform management/law enforcement as necessary • Copy of drive (data integrity and preservation) • Documentation of incident - Licensing/digital rights management (DRM)/end-user license agreement (EULA) • Valid licenses • Non-expired licenses • Personal use license vs. corporate use license • Open-source license - Regulated data • Credit card transactions • Personal government-issued information • PII • Healthcare data • Data retention requirements
Given a scenario, use proper communication techniques and professionalism.	- Professional appearance and attire • Match the required attire of the given environment - Formal - Business casual - Use proper language and avoid jargon, acronyms, and slang, when applicable - Maintain a positive attitude/project confidence - Actively listen, take notes, and avoid interrupting the customer

Topic	Details
	- Be culturally sensitive • Use appropriate professional titles, when applicable - Be on time (if late, contact the customer) - Avoid distractions • Personal calls • Texting/social media sites • Personal interruptions - Dealing with difficult customers or situations • Do not argue with customers or be defensive • Avoid dismissing customer problems • Avoid being judgmental • Clarify customer statements (ask open-ended questions to narrow the scope of the problem, restate the issue, or question to verify understanding) • Do not disclose experience via social media outlets - Set and meet expectations/time line and communicate status with the customer • Offer repair/replacement options, as needed • Provide proper documentation on the services provided • Follow up with customer/user at a later date to verify satisfaction - Deal appropriately with customers' confidential and private materials • Located on a computer, desktop, printer, etc.
Identify the basics of scripting.	- Script file types • .bat • .ps1 • .vbs • .sh • .js

Topic	Details
	• .py - Use cases for scripting • Basic automation • Restarting machines • Remapping network drives • Installation of applications • Automated backups • Gathering of information/data • Initiating updates - Other considerations when using scripts • Unintentionally introducing malware • Inadvertently changing system settings • Browser or system crashes due to mishandling of resources
Given a scenario, use remote access technologies.	- Methods/tools • RDP • VPN • Virtual network computer (VNC) • Secure Shell (SSH) • Remote monitoring and management (RMM) • Microsoft Remote Assistance (MSRA) • Third-party tools - Screen-sharing software - Video-conferencing software - File transfer software - Desktop management software - Security considerations of each access method

Prepare with 220-1102 Sample Questions:

Question: 1

A sales staff member recently left a laptop at a hotel and needs a new one immediately. After remotely wiping the old laptop, a support technician prepares to take a new laptop out of inventory to begin the deployment process.
Which of the following should the technician do FIRST?

a) Recycle all the cardboard and other shipping materials appropriately.
b) Call the hotel and demand the old laptop be sent back to the repair depot.
c) Confirm the shipping address for the new laptop with the sales staff member.
d) Document the serial numbers and usernames for asset management.

Answer: d

Question: 2

A user's Windows desktop continuously crashes during boot. A technician runs the following command in safe mode and then reboots the desktop: c:\Windows\system32> sfc /scannow
Which of the following BEST describes why the technician ran this command?

a) The user's profile is damaged.
b) The system files are corrupted.
c) The hard drive needs to be defragmented.
d) The system needs to have a restore performed.

Answer: b

Question: 3

A network engineer needs to update a network firewall, which will cause a temporary outage. The network engineer submits a change request form to perform the required maintenance. If the firewall update fails, which of the following is the NEXT step?

a) Perform a risk analysis.
b) Execute a backout plan.
c) Request a change approval.
d) Acquire end user acceptance.

Answer: b

Question: 4

Which of the following Linux commands will display a directory of files?

a) chown
b) ls
c) chmod
d) cls

Answer: b

Question: 5

A user calls the IT help desk and explains that all the data on the user's computer is encrypted. The user also indicates that a pop-up message on the screen is asking for payment in Bitcoins to unlock the encrypted data.
The user's computer is MOST likely infected with which of the following?

a) Botnet
b) Spyware
c) Ransomware
d) Rootkit

Answer: c

Question: 6

A technician has been directed to dispose of hard drives from company laptops properly. Company standards require the use of a high-powered magnet to destroy data on decommissioned hard drives.
Which of the following data destruction methods should the technician choose?

a) Degaussing
b) Drilling
c) Incinerating
d) Shredding

Answer: a

Question: 7

A user reports being unable to access the Internet or use wireless headphones on a mobile device. The technician confirms the headphones properly connect to another device.
Which of the following should the technician do to solve the issue?

a) Turn off airplane mode.
b) Connect to a different service set identifier.
c) Test the battery on the device.
d) Disable near-field communication.

Answer: a

Question: 8

Which of the following workstation operating systems uses NTFS for the standard filesystem type?

a) macOS
b) Windows
c) Chrome OS
d) Linux

Answer: b

Question: 9

Which of the following symptoms is MOST likely a sign of ransomware?

a) Internet connectivity is lost.
b) Battery life is reduced.
c) Files on devices are inaccessible.
d) A large number of ads appear.

Answer: c

Question: 10

A technician is installing M.2 devices in several workstations. Which of the following would be required when installing the devices?

a) Air filtration
b) Heat-resistant gloves
c) Ergonomic floor mats
d) Electrostatic discharge straps

Answer: d

Study Tips to Pass the CompTIA A+ (Core 2) Exam:

Understand the 220-1102 Exam Format:

Before diving into your study routine, it's essential to familiarize yourself with the 220-1102 exam format. Take the time to review the **exam syllabus**, understand the test structure, and identify the key areas of focus. Prior knowledge of what to expect on exam day will help you tailor your study plan.

Make A Study Schedule for the 220-1102 Exam:

To effectively prepare for the 220-1102 exam, make a study schedule that fits your lifestyle and learning style. Set specific time slots for studying each day and focus on the topics based on their importance and your proficiency level. Consistency is a must, so stick to your schedule and avoid procrastination.

Study from Different Resources:

Make sure to expand beyond one source of study material. Utilize multiple resources such as textbooks, online courses, practice exams, and study guides to understand the 220-1102 exam topics comprehensively. Each

resource offers unique insights and explanations that can enhance your learning experience.

Practice Regularly for the 220-1102 Exam:

Practice makes you perfect for the 220-1102 exam preparation as well. Regular practice allows you to reinforce your knowledge of key concepts, enhance your problem-solving skills, and familiarize yourself with the exam format. Dedicate time to solving practice questions and sample tests to gauge your progress.

Take Breaks and Rest:

While it's essential to study, taking breaks and allowing yourself to rest is equally important. Overloading your brain with information without adequate rest can lead to burnout and decreased productivity. Set short breaks during your study sessions to recharge and maintain focus.

Stay Organized During the 220-1102 Exam Preparation:

Stay organized throughout your 220-1102 study journey by keeping track of your progress and materials. Maintain a tidy study space, use folders or digital tools to organize your notes and resources, and create a checklist of topics to cover. An organized approach helps you stay on track and minimize stress.

Seek Clarification from Mentors:

Feel free to seek clarification if you encounter any confusing or challenging concepts during your study sessions. Reach out to peers, instructors, or online forums for assistance. Clarifying doubts early on will prevent misunderstandings and ensure you have a solid grasp of the material.

Regular Revision Plays A vital Role for the 220-1102 Exam:

Consistent revision is essential for the long-term retention of information. Review previously covered topics to reinforce your understanding and identify any areas requiring additional attention. Reviewing regularly will help solidify your knowledge and boost your confidence.

Practice Time Management for the 220-1102 Exam:

Effective time management is crucial on exam day to ensure you complete all sections within the allocated time frame. During your practice sessions, simulate 220-1102 exam conditions and practice pacing yourself accordingly. Develop strategies for tackling each section efficiently to maximize your score.

Stay Positive and Confident:

Lastly, always have a positive mindset and believe in your abilities. Stay confident in your preparation efforts and trust that you have adequately equipped yourself to tackle the 220-1102 exam. Visualize success, stay focused, and approach the exam calmly and confidently.

Benefits of Earning the 220-1102 Exam:

- Achieving the 220-1102 certification opens doors to new career opportunities and advancement within your field.
- The rigorous preparation required for the 220-1102 exam equips you with in-depth knowledge and practical skills relevant to your profession.
- Holding the 220-1102 certification demonstrates your expertise and commitment to excellence, earning recognition from peers and employers.
- Certified professionals often grab higher salaries and enjoy greater earning potential than their non-certified counterparts.
- Obtaining the 220-1102 certification validates your proficiency and credibility, instilling confidence in clients, employers, and colleagues.

Discover the Reliable Practice Test for the 220-1102 Certification:

EduSum.com brings you comprehensive information about the 220-1102 exam. We offer genuine practice tests tailored for the 220-1102 certification. What benefits do these practice tests offer? You'll encounter authentic exam-like questions crafted by industry experts, providing an opportunity to enhance your performance in the actual exam. Count on EduSum.com for rigorous, unlimited access to 220-1102 practice tests over two months, enabling you to bolster your confidence steadily. Through dedicated practice, many candidates have succeeded in streamlining their journey towards obtaining the CompTIA A+.

Concluding Thoughts:

Preparing for the 220-1102 exam requires dedication, strategy, and effective study techniques. These study tips can enhance your preparation, boost your confidence, and improve your chances of passing the exam with flying colors. Remember to stay focused, stay organized, and believe in yourself. Good luck!

Here is the Trusted Practice Test for the 220-1102 Certification

EduSum.com offers comprehensive details about the 220-1102 exam. Our platform provides authentic practice tests designed for the 220-1102 exam. What benefits do these practice tests offer? By accessing our practice tests, you will encounter questions closely resembling those crafted by industry experts in the exam. This allows you to enhance your performance and readiness for the real exam. Count on EduSum.com to provide rigorous practice opportunities, offering unlimited attempts over two months for the 220-1102 practice tests. Through consistent practice, many candidates have found success and simplified their journey towards attaining the CompTIA A+.

Start Online Practice of 220-1102 Exam by Visiting URL

https://www.edusum.com/comptia/220-1102-comptia-core-2