EDUSUM

#1 Online Certification Guide

COMPTIA 220-1002

CompTIA A+ Core 2 Certification Questions & Answers

Exam Summary – Syllabus –Questions

220-1002

CompTIA A+

90 Questions Exam – 700/900 Cut Score – Duration of 90 minutes

Table of Contents:

Know Your 220-1002 Certification Well:

The 220-1002 is best suitable for candidates who want to gain knowledge in the CompTIA Core. Before you start your 220-1002 preparation you may struggle to get all the crucial A+ Core 2 materials like 220-1002 syllabus, sample questions, study guide.

But don't worry the 220-1002 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the 220-1002 syllabus?
- How many questions are there in the 220-1002 exam?
- Which Practice test would help me to pass the 220-1002 exam at the first attempt?

Passing the 220-1002 exam makes you CompTIA A+. Having the A+ Core 2 certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CompTIA 220-1002 A+ Core 2 Certification Details:

Exam Name	CompTIA A+
Exam Code	220-1002
Exam Price	$232 (USD)
Duration	90 mins
Number of Questions	90
Passing Score	700 / 900
Books / Training	**CertMaster Learn for A+**
Schedule Exam	**CompTIA Marketplace** **Pearson VUE**
Sample Questions	**CompTIA A+ Core 2 Sample Questions**
Practice Exam	**CompTIA 220-1002 Certification Practice Exam**

220-1002 Syllabus:

Topic	Details
Operating Systems - 27%	
Compare and contrast common operating system types and their purposes.	1. 32-bit vs. 64-bit • RAM limitations • Software compatibility 2. Workstation operating systems • Microsoft Windows • Apple Macintosh OS • Linux 3. Cell phone/tablet operating systems • Microsoft Windows • Android • iOS • Chrome OS 4. Vendor-specific limitations • End-of-life • Update limitations 5. Compatibility concerns between operating systems
Compare and contrast features of Microsoft Windows versions.	1. Windows 7 2. Windows 8 3. Windows 8.1 4. Windows 10 5. Corporate vs. personal needs • Domain access • BitLocker • Media center • BranchCache • EFS 6. Desktop styles/user interface

Topic	Details
Summarize general OS installation considerations and upgrade methods.	1. Boot methods • Optical disc(CD-ROM, DVD, Blu-ray) • External drive/flash drive (USB/eSATA) • Network boot (PXE) • Internal fixed disk (HDD/SSD) • Internal hard drive (partition) 2. Type of installations • Unattended installation • In-place upgrade • Clean install • Repair installation • Multiboot • Remote network installation • Image deployment • Recovery partition • Refresh/restore 3. Partitioning • Dynamic • Basic • Primary • Extended • Logical • GPT 4. File system types/formatting • ExFAT • FAT32 • NTFS • CDFS • NFS • ext3, ext4 • HFS • Swap partition • Quick format vs. full format

Topic	Details
	5. Load alternate third-party drivers when necessary 6. Workgroup vs. Domain setup 7. Time/date/region/language settings 8. Driver installation, software, and Windows updates 9. Factory recovery partition 10. Properly formatted boot drive with the correct partitions/format 11. Prerequisites/hardware compatibility 12. Application compatibility 13. OS compatibility/upgrade path
Given a scenario, use appropriate Microsoft command line tools.	1. Navigation • dir • cd • .. 2. ipconfig 3. ping 4. tracert 5. netstat 6. nslookup 7. shutdown 8. dism 9. sfc 10. chkdsk 11. diskpart 12. taskkill 13. gpupdate 14. gpresult 15. format 16. copy 17. xcopy 18. robocopy 19. net use 20. net user 21. [command name] /? 22. Commands available with standard privileges vs. administrative privileges
Given a scenario, use Microsoft operating system features and tools.	1. Administrative • Computer Management • Device Manager • Local Users and Groups • Local Security Policy

Topic	Details
	• Performance Monitor • Services • System Configuration • Task Scheduler • Component Services • Data Sources • Print Management • Windows Memory Diagnostics • Windows Firewall • Advanced Security • Event Viewer • User Account Management 2. MSConfig • General • Boot • Services • Startup • Tools 3. Task Manager • Applications • Processes • Performance • Networking • Users 4. Disk Management • Drive status • Mounting • Initializing • Extending partitions • Splitting partitions • Shrink partitions • Assigning/changing drive letters • Adding drives • Adding arrays

Topic	Details
	• Storage spaces 5. System utilities • Regedit • Command • Services.msc • MMC • MSTSC • Notepad • Explorer • Msinfo32 • DxDiag • Disk Defragmenter • System Restore • Windows Update
Given a scenario, use Microsoft Windows Control Panel utilities.	1. Internet Options • Connections • Security • General • Privacy • Programs • Advanced 2. Display/Display Settings • Resolution • Color depth • Refresh rate 3. User Accounts 4. Folder Options • View hidden files • Hide extensions • General options • View options 5. System • Performance (virtual memory)

Topic	Details
	• Remote settings • System protection 6. Windows Firewall 7. Power Options • Hibernate • Power plans • Sleep/suspend • Standby 8. Credential Manager 9. Programs and features 10. HomeGroup 11. Devices and Printers 12. Sound 13. Troubleshooting 14. Network and Sharing Center 15. Device Manager 16. BitLocker 17. Sync Center
Summarize application installation and configuration concepts.	1. System requirements • Drive space • RAM 2. OS requirements • Compatibility 3. Methods of installation and deployment • Local (CD/USB) • Network-based 4. Local user permissions • Folder/file access for installation 5. Security considerations • Impact to device • Impact to network
Given a scenario, configure Microsoft	1. HomeGroup vs. Workgroup 2. Domain setup 3. Network shares/administrative shares/mapping drives

Topic	Details
Windows networking on a client/desktop.	4. Printer sharing vs. network printer mapping 5. Establish networking connections • VPN • Dial-ups • Wireless • Wired • WWAN (Cellular) 6. Proxy settings 7. Remote Desktop Connection 8. Remote Assistance 9. Home vs. Work vs. Public network settings 10. Firewall settings • Exceptions • Configuration • Enabling/disabling Windows Firewall 11. Configuring an alternative IP address in Windows • IP addressing • Subnet mask • DNS • Gateway 12. Network card properties • Half duplex/full duplex/auto • Speed • Wake-on-LAN • QoS • BIOS (on-board NIC)
Given a scenario, use features and tools of the Mac OS and Linux client/desktop operating systems.	1. Best practices • Scheduled backups • Scheduled disk maintenance • System updates/App Store • Patch management • Driver/firmware updates • Antivirus/Anti-malware updates

Topic	Details
	2. Tools • Backup/Time Machine • Restore/Snapshot • Image recovery • Disk maintenance utilities • Shell/Terminal • Screen sharing • Force Quit 3. Features • Multiple desktops/Mission Control • Key Chain • Spot Light • iCloud • Gestures • Finder • Remote Disc • Dock • Boot Camp 4. Basic Linux commands • ls • grep • cd • shutdown • pwd vs. passwd • mv • cp • rm • chmod • chown • iwconfig/ifconfig • ps • su/sudo • apt-get • vi

Topic	Details
	• dd • kill
Security - 24%	
Summarize the importance of physical security measures.	1. Access control vestibule 2. Badge reader 3. Smart card 4. Security guard 5. Door lock 6. Biometric locks 7. Hardware tokens 8. Cable locks 9. Server locks 10. USB locks 11. Privacy screen 12. Key fobs 13. Entry control roster
Explain logical security concepts.	1. Active Directory • Login script • Domain • Group Policy/Updates • Organizational Units • Home Folder • Folder redirection 2. Software tokens 3. MDM policies 4. Port security 5. MAC address filtering 6. Certificates 7. Antivirus/Anti-malware 8. Firewalls 9. User authentication/strong passwords 10. Multifactor authentication 11. Directory permissions 12. VPN 13. DLP 14. Access control lists 15. Smart card 16. Email filtering

Topic	Details
	17. Trusted/untrusted software sources 18. Principle of least privilege
Compare and contrast wireless security protocols and authentication methods.	1. Protocols and encryption • WEP • WPA • WPA2 • TKIP • AES 2. Authentication • Single-factor • Multifactor • RADIUS • TACACS
Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.	1. Malware • Ransomware • Trojan • Keylogger • Rootkit • Virus • Botnet • Worm • Spyware 2. Tools and methods • Antivirus • Anti-malware • Recovery console • Backup/restore • End user education • Software firewalls • DNS configuration
Compare and contrast social engineering, threats, and vulnerabilities.	1. Social engineering • Phishing • Spear phishing

Topic	Details
	• Impersonation • Shoulder surfing • Tailgating • Dumpster diving 2. DDoS 3. DoS 4. Zero-day 5. On-path attack (previously known as man-in-the-middle attack) 6. Brute force 7. Dictionary 8. Rainbow table 9. Spoofing 10. Non-compliant systems 11. Zombie
Compare and contrast the differences of basic Microsoft Windows OS security settings.	1. User and groups • Administrator • Power user • Guest • Standard user 2. NTFS vs. share permissions • Allow vs. deny • Moving vs. copying folders and files • File attributes 3. Shared files and folders • Administrative shares vs. local shares • Permission propagation • Inheritance 4. System files and folders 5. User authentication • Single sign-on 6. Run as administrator vs. standard user 7. BitLocker 8. BitLocker To Go 9. EFS

Topic	Details
Given a scenario, implement security best practices to secure a workstation.	1. Password best practices • Setting strong passwords • Password expiration • Screensaver required password • BIOS/UEFI passwords • Requiring passwords 2. Account management • Restricting user permissions • Logon time restrictions • Disabling guest account • Failed attempts lockout • Timeout/screen lock • Change default admin user account/password • Basic Active Directory functions 1. Account creation 2. Account deletion 3. Password reset/unlock account 4. Disable account 3. Disable autorun 4. Data encryption 5. Patch/update management
Given a scenario, implement methods for securing mobile devices.	1. Screen locks • Fingerprint lock • Face lock • Swipe lock • Passcode lock 2. Remote wipes 3. Locator applications 4. Remote backup applications 5. Failed login attempts restrictions 6. Antivirus/Anti-malware 7. Patching/OS updates 8. Biometric authentication 9. Full device encryption 10. Multifactor authentication 11. Authenticator applications 12. Trusted sources vs. untrusted sources

Topic	Details
	13. Firewalls 14. Policies and procedures • BYOD vs. corporate-owned • Profile security requirements
Given a scenario, implement appropriate data destruction and disposal methods.	1. Physical destruction • Shredder • Drill/hammer • Electromagnetic (Degaussing) • Incineration • Certificate of destruction 2. Recycling or repurposing best practices • Low-level format vs. standard format • Overwrite • Drive wipe
Given a scenario, configure security on SOHO wireless and wired networks.	1. Wireless-specific • Changing default SSID • Setting encryption • Disabling SSID broadcast • Antenna and access point placement • Radio power levels • WPS 2. Change default usernames and passwords 3. Enable MAC filtering 4. Assign static IP addresses 5. Firewall settings 6. Port forwarding/mapping 7. Disabling ports 8. Content filtering/parental controls 9. Update firmware 10. Physical security
Software Troubleshooting - 26%	
Given a scenario, troubleshoot Microsoft Windows OS problems.	1. Common symptoms • Slow performance

Topic	Details
	• Limited connectivity • Failure to boot • No OS found • Application crashes • Blue screens • Blank screens • Printing issues • Services fail to start • Slow bootup • Slow profile load 2. Common solutions • Defragment the hard drive • Reboot • Kill tasks • Restart services • Update network settings • Reimage/reload OS • Roll back updates • Roll back devices drivers • Apply updates • Repair application • Update boot order • Disable Windows services/applications • Disable application startup • Safe boot • Rebuild Windows profiles
Given a scenario, troubleshoot and resolve PC security issues.	1. Common symptoms • Pop-ups • Browser redirection • Security alerts • Slow performance • Internet connectivity issues • PC/OS lockup • Application crash • OS updates failures

Topic	Details
	• Rogue antivirus • Spam • Renamed system files • Disappearing files • File permission changes • Hijacked email - Responses from users regarding email - Automated replies from unknown sent email • Access denied • Invalid certificate (trusted root CA) • System/application log errors
Given a scenario, use best practice procedures for malware removal.	1. Identify and research malware symptoms. 2. Quarantine the infected systems. 3. Disable System Restore (in Windows). 4. Remediate the infected systems. • Update the anti-malware software. • Scan and use removal techniques (safe mode, pre-installation environment). 5. Schedule scans and run updates. 6. Enable System Restore and create a restore point (in Windows). 7. Educate the end user.
Given a scenario, troubleshoot mobile OS and application issues.	1. Common symptoms • Dim display • Intermittent wireless • No wireless connectivity • No Bluetooth connectivity • Cannot broadcast to external monitor • Touchscreen non-responsive • Apps not loading • Slow performance • Unable to decrypt email • Extremely short battery life • Overheating • Frozen system • No sound from speakers

Topic	Details
	• Inaccurate touch screen response • System lockout • App log errors
Given a scenario, troubleshoot mobile OS and application security issues.	1. Common symptoms • Signal drop/weak signal • Power drain • Slow data speeds • Unintended WiFi connection • Unintended Bluetooth pairing • Leaked personal files/data • Data transmission over limit • Unauthorized account access • Unauthorized location tracking • Unauthorized camera/microphone activation • High resource utilization
Operational Procedures - 23%	
Compare and contrast best practices associated with types of documentation.	1. Network topology diagrams 2. Knowledge base/articles 3. Incident documentation 4. Regulatory and compliance policy 5. Acceptable use policy 6. Password policy 7. Inventory management • Asset tags • Barcodes
Given a scenario, implement basic change management best practices.	1. Documented business processes 2. Purpose of the change 3. Scope the change 4. Risk analysis 5. Plan for change 6. End-user acceptance 7. Change board • Approvals

Topic	Details
	8. Backout plan 9. Document changes
Given a scenario, implement basic disaster prevention and recovery methods.	1. Backup and recovery • Image level • File level • Critical applications 2. Backup testing 3. UPS 4. Surge protector 5. Cloud storage vs. local storage backups 6. Account recovery options
Explain common safety procedures.	1. Equipment grounding 2. Proper component handling and storage • Antistatic bags • ESD straps • ESD mats • Self-grounding 3. Toxic waste handling • Batteries • Toner • CRT • Cell phones • Tablets 4. Personal safety • Disconnect power before repairing PC • Remove jewelry • Lifting techniques • Weight limitations • Electrical fire safety • Cable management • Safety goggles • Air filter mask 5. Compliance with government regulations

Topic	Details
Explain environmental impacts and appropriate controls.	1. MSDS documentation for handling and disposal 2. Temperature, humidity level awareness, and proper ventilation 3. Power surges, under-voltage events, and power loss • Battery backup • Surge suppressor 4. Protection from airborne particles • Enclosures • Air filters/mask 5. Dust and debris • Compressed air • Vacuums 6. Compliance to government regulations
Explain the processes for addressing prohibited content/ activity, and privacy, licensing, and policy concepts.	1. Incident response • First response - Identify - Report through proper channels - Data/device preservation • Use of documentation/documentation changes • Chain of custody Tracking of evidence/documenting process 2. Licensing/DRM/EULA 1. Open-source vs. commercial license 2. Personal license vs. enterprise licenses 3. Regulated data • PII • PCI • GDPR • PHI 4. Follow all policies and security best practices
Given a scenario, use proper communication	1. Use proper language and avoid jargon, acronyms, and slang, when applicable 2. Maintain a positive attitude/project confidence

Topic	Details
techniques and professionalism.	3. Actively listen (taking notes) and avoid interrupting the customer 4. Be culturally sensitive • Use appropriate professional titles, when applicable 5. Be on time (if late, contact the customer) 6. Avoid distractions • Personal calls • Texting/social media sites • Talking to coworkers while interacting with customers • Personal interruptions 7. Dealing with difficult customers or situations • Do not argue with customers and/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 experiences via social media outlets 8. Set and meet expectations/timeline and communicate status with the customer • Offer different repair/replacement options, if applicable • Provide proper documentation on the services provided • Follow up with customer/user at a later date to verify satisfaction 9. Deal appropriately with customers' confidential and private materials • Located on a computer, desktop, printer, etc.
Identify the basics of scripting.	1. Script file types • .bat • .ps1 • .vbs • .sh • .py • .js

Topic	Details
	2. Environment variables 3. Comment syntax 4. Basic script constructs • Basic loops • Variables 5. Basic data types • Integers • Strings
Given a scenario, use remote access technologies.	1. RDP 2. Telnet 3. SSH 4. Third-party tools • Screen share feature • File share 5. Security considerations of each access method

CompTIA 220-1002 Sample Questions:

Question: 1

Which of the following is the proper way to dispose of batteries?

a) Shred
b) Recycle
c) Dispose in trash
d) Incinerate

Answer: b

Question: 2

A user reports a phone battery does not last the entire day, and the phone's navigation is slow. Which of the following should a technician do FIRST to troubleshoot the device?

a) Examine the running apps.
b) Update the firmware.
c) Reinstall the most-used application.
d) Turn off all network services.

Answer: a

Question: 3

A user connects a printer to a workstation. As the printer drivers are installed, an error message appears. The default drivers appear to be incompatible with the OS.

Which of the following should a technician use FIRST to troubleshoot the problem?

a) Services
b) Device Manager
c) Programs and Features
d) Task Manager

Answer: b

Question: 4

A new security requirement for logging on to a company network has been put in place for all users. Which of the following should a systems administrator enforce to BEST meet this requirement?

(Select TWO).

a) Strong passwords
b) Folder redirection
c) Email filtering
d) Multifactor authentication
e) Remote desktop
f) Anti-malware

Answer: a, d

Question: 5

Which of the following password choices increases the chance that a brute force attack will succeed?

a) Capital letters
b) Long passwords
c) Special characters
d) Dictionary words

Answer: d

Question: 6

An end user has requested assistance from the help desk to install new video editing software. The user wants to create several .wma files.

Which of the following should the help desk consider before installing the software?

a) Disk space
b) Network connection
c) Aspect ratio
d) Power supply

Answer: a

Question: 7

A technician implements a Group Policy change and needs to apply it without restarting the workstation. Which of the following commands can be used to accomplish this task?

a) gpupdate
b) gpresult
c) netstat
d) Dism

Answer: a

Question: 8

Joe, a user, forgot his password and was unable to log in to a workstation. Joe remembers the password later, but he is still unable to log in. Which of the following is the MOST likely cause of the issue?

a) Reset account
b) Deleted account
c) Locked account
d) Limited-user account
e) Unprovisioned account

Answer: c

Question: 9

To prevent electrical damage to a PC while working on it, which of the following should be disconnected before work begins?

a) Video cable
b) Serial cable
c) Power cable
d) USB cable

Answer: c

Question: 10

Which of the following is the BEST use-case scenario for a Chrome OS device?

a) Database queries
b) Application development
c) Photo and video editing
d) Web browsing and email

Answer: d

Study Guide to Crack CompTIA A+ Core 2 220-1002 Exam:

- Getting details of the 220-1002 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 220-1002 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the CompTIA provided training for 220-1002 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 220-1002 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 220-1002 practice tests is must. Continuous practice will make you an expert in all syllabus areas.