CompTIA A+ Certification Core 2 (Exam: 220-1002)

Duration: *5 Day(s)*

Course Overview

Acquire the essential skills needed to install, configure, optimize, troubleshoot, upgrade, secure, and perform preventive maintenance on PC and digital device operating systems (OS). In this 5-day CompTIA A+ Core 2 (220-1002) certification training course, students will explore various operating systems including Windows, MAC and Linux. Throughout the course, students will work with Microsoft command line tools and control panels with the desktop environment and learn basic scripting. Student will also explore security and troubleshooting objectives for desktop, mobile and wireless systems as well as operational procedures.

The CompTIA A+ (Exam 220-1002) course can benefit you in two ways. Whether you work or plan to work in a mobile or corporate environment where you have a high level of face-to-face customer interaction, where client communication and client training are important, or in an environment with limited customer interaction and an emphasis on application, operating system, and security-related activities, this course provides the background knowledge and skills you will require to be a successful A+ technician. It can also assist you if you are preparing to take the CompTIA A+ Certification Exam: Core 2 Objectives EXAM NUMBER: CORE 2 (220-1002) in order to become a CompTIA A+ Certified Professional.

Note: this is a preliminary course information outline and is subject to change upon final Core 1 (220-1001) curriculum release from CompTIA Accreditation.

Review this course online at https://www.alta3.com/courses/A+1002

Objectives

- Understand networking and security fundamentals
- Diagnose and resolve software issues effectively
- Apply OS troubleshooting and deployment skills
- Provide exceptional customer and technical support

Who Should Attend

- PC Support Professionals
- Entry-Level ICT Career Seekers
- Desktop Engineers
- PC Support Analysts

Prerequisites

To ensure your success in this course, you should have basic computer user skills, be able to complete tasks in a Microsoft® Windows® environment, be able to search for, browse, and access information on the Internet and have basic knowledge of computing concepts.

Course Outline

Lesson 1: Operating Systems

1. Common operating system types and their purposes
2. Microsoft Windows versions
3. OS installation considerations and upgrade methods

4. Microsoft command line tools
5. Microsoft operating system features and tools
6. Microsoft Windows Control Panel utilities
7. Installation and configuration concepts
8. Microsoft Windows networking on a Client/desktop
9. Mac OS and Linux client/desktop operating systems

Lesson 2: Security

10. Physical security measures
11. Logical security concepts
12. Wireless security protocols and authentication methods
13. Detect, remove, and prevent malware using appropriate tools and methods
14. Social engineering, threats, and vulnerabilities
15. Microsoft Windows OS security settings
16. Best practices to secure a workstation
17. Methods for securing mobile devices
18. Appropriate data destruction and disposal methods
19. Configure security on SOHO wireless and wired networks

Lesson 3: Software Troubleshooting

20. Troubleshooting Microsoft Windows OS problems
21. Troubleshoot and resolve PC security issues
22. Best practice procedures for malware removal
23. Mobile OS and application issues
24. Mobile OS and application security issues

Lesson 4: Operation Procedures

25. Best practices associated with types of documentation
26. Change Management best practices
27. Implement basic disaster prevention and recovery methods
28. Common safety procedures
29. Environmental impacts and appropriate controls
30. Addressing prohibited content/activity, and privacy, licensing, and policy concepts
31. Proper communication techniques and professionalism
32. Basics of scripting
33. Remote access technologies

Lesson 5: Best practice methodology to resolve problems

34. Identify the problem
35. Establish a theory of probable cause
36. Test the theory to determine cause

37. Implement the solution
38. Verify full system functionality
39. Document findings