

CPMT 2050

Course Syllabus

1. Name of Course:

Linux + Certification Training

2. Number of Clock Hours: 48

3. Course Description:

This course prepares students for the Linux + certification examination. Through lectures, demonstrations, and hands-on experience, students learn to install, administer, and operate computers running the Linux operating system.

4. Course Objectives

Domain 1: Planning a Linux Implementation

This domain includes basic knowledge and skills to associate different hardware, software and services options with the specific purposes and requirements of Linux users.

- 1.1 Identify purpose of Linux machine based on predetermined customer requirements (e.g., appliance, desktop system, database, mail server)
- 1.2 Identify all system hardware required and validate that it is supported by Linux (e.g., CPUs, RAM, graphics cards, storage devices, network interface cards, modem)
- 1.3 Determine what software and services should be installed (e.g., client applications for workstation, server services for desired task), check requirements and validate that it is supported by Linux
- 1.4 Determine how storage space will be allocated to file systems. (e.g., partition schemes)
- 1.5 Compare and contrast how major Linux licensing schemes work (e.g., GNU/GPL, freeware, shareware, open source, closed source, artistic license)
- 1.6 Identify the function of different Linux services (e.g., Apache, Squid, SAMBA, Sendmail, ipchains, BIND)
- 1.7 Identify strengths and weaknesses of different distributions and their packaging solutions (e.g, tar ball vs. RPM/DEB)
- 1.8 Describe the functions, features, and benefits of a Linux solutions as compared with other operating systems (e.g., Linux players, distributions, available software)
- 1.9 Identify how the Linux kernel version numbering works
- 1.10 Identify where to obtain software and resources
- 1.11 Determine customer resources for a solution (e.g., staffing, budget, training)

Domain 2: Installation

This domain includes basic knowledge and skills to determine installation methods, select appropriate settings, protocols and software packages, and validate correct performance.

- 2.1 Determine appropriate method of installation based on the environment (e.g., boot disk, CD-ROM, Network (HTTP, FTP, NFS, SMB))
- 2.2 Describe the different types of Linux installation interaction and determine which to use for a given situation (e.g., GUI, text, network)
- 2.3 Select appropriate parameters for Linux installation (e.g., language, time zones, keyboard, mouse)
- 2.4 Select packages based on the machine's "role" (e.g., Workstation, Server, Custom)

- 2.5 Select appropriate options for partitions based on pre-installation choices (e.g., FDISK, third party partitioning software)
- 2.6 Partition according to your pre-installation plan using fdisk (e.g., /boot, / , /usr, /var/home, SWAP)
- 2.7 Configure file systems (e.g., (ext2) or (ext3) or REISER)
- 2.8 Select appropriate networking configuration and protocols (e.g., modems, Ethernet, Token-Ring)
- 2.9 Select appropriate security settings (e.g., Shadow password, root password, umask value, password limitations and password rules)
- 2.10 Create users and passwords during installation
- 2.11 Install and configure Xfree86 server
- 2.12 Select Video card support (e.g., chipset, memory, support resolution(s))
- 2.13 Select appropriate monitor manufacturer and settings (e.g., custom, vertical, horizontal, refresh)
- 2.14 Select the appropriate window managers or desktop environment (e.g., KDE, GNOME)
- 2.15 Explain when and why the kernel will need to be recompiled
- 2.16 Install boot loader (e.g., LILO, MBR vs. first sector of boot partition)
- 2.17 Install and uninstall applications after installing the operating system (e.g., RPM, tar, gzip)
- 2.18 Read the Logfiles created during installation to verify the success of the installation
- 2.19 Validate that an installed application is performing correctly in both a test and a production environment

Domain 3: Configuration

This domain includes basic knowledge and skills to configure system settings, network services, and access rights.

- 3.1 Reconfigure the Xwindow System with automated utilities (e.g., Xconfigurator, XF86Setup)
- 3.2 Configure the client's workstation for remote access (e.g., ppp, ISDN)
- 3.3 Set environment variables (e.g., PATH, DISPLAY, TERM)
- 3.4 Configure basic network services and settings (e.g., netconfig, linuxconf; settings for TCP/IP, DNS, DHCP)
- 3.5 Configure basic server services (e.g., X, SMB, NIS, NFS)
- 3.6 Configure basic Internet services (e.g., HTTP, POP, SMTP, SNMP, FTP)
- 3.7 Identify when swap space needs to be increased
- 3.8 Add and configure printers
- 3.9 Install and configure add-in hardware (e.g., monitors, modems, network interfaces, scanners)
- 3.10 Reconfigure boot loader (e.g., LILO)
- 3.11 Identify the purpose and characteristics of configuration files (e.g., BASH, inittab, fstab, /etc/*)
- 3.12 Edit basic configuration files (e.g., BASH files, inittab, fstab)
- 3.13 Load, remove, and edit list modules (e.g., insmod, rmmod, lsmod, modprobe)
- 3.14 Document the installation of the operating system, including configuration
- 3.15 Configure access rights (e.g., rlogin NIS, FTP, TFTP, SSH, Telnet)

Domain 4: Administration

This domain includes basic knowledge and skills to manage users, file systems, services, devices and run levels using common shell commands, administrative utilities, and superuser privileges.

- 4.1 Create and delete users
- 4.2 Modify existing users (e.g., password, groups, personal information)
- 4.3 Create, modify and delete groups
- 4.4 Identify and change file permissions, modes and types by using chmod, chown and chgrp
- 4.5 Manage and navigate the Linux hierarchy (e.g., /etc, /usr, /bin, /var)
- 4.6 Manage and navigate the standard Linux file system (e.g., mv, mkdir, ls, rm)
- 4.7 Perform administrative tasks while logged in as root, or by using the su command (e.g., understand commands that are dangerous to the system)
- 4.8 Mount and manage filesystems and devices (e.g., /mnt, /dev, du, df, mount, umount)
- 4.9 Describe and use the features of the multi-user environment (e.g., virtual terminals, multiple logins)
- 4.10 Use common shell commands and expressions
- 4.11 Use network commands to connect to and manage remote systems (e.g., telnet, ftp, ssh, netstat, transfer files, redirect Xwindow)
- 4.12 Create, extract and edit file and tape archives using tar
- 4.13 Manage runlevels using init and shutdown
- 4.14 Stop, start, and restart services (daemons) as needed (e.g., init files)
- 4.15 Manage print spools and queues
- 4.16 Create, edit and save files using vi
- 4.17 Manage and navigate the Graphical User Interface (e.g., menus, xterm)
- 4.18 Program basic shell scripts using common shell commands (e.g., grep, find, cut, if)

Domain 5: System Maintenance

This domain includes basic knowledge and skills to monitor and maintain processes, network interfaces, system logs, security, and backup.

- 5.1 Create and manage local storage devices and file systems (e.g., fsck, fdisk, mkfs)
- 5.2 Verify user and root cron jobs and understand the function of cron
- 5.3 Identify core dumps and remove or forward as appropriate
- 5.4 Run and interpret ifconfig
- 5.5 Download and install patches and updates (e.g., packages, tgz)
- 5.6 Differentiate core services from non-critical services (e.g., ps, PID, PPID, init, timer)
- 5.7 Identify, execute and kill processes (ps, kill, killall)
- 5.8 Monitor system log files regularly for errors, logins, and unusual activity
- 5.9 Document work performed on a system
- 5.10 Perform and verify backups and restores
- 5.11 Perform and verify security best practices (e.g., passwords, physical environments)
- 5.12 Assess security risks (e.g., location, sensitive data, file system permissions, remove/disable unused accounts, audit system services/programs)
- 5.13 Set daemon and process permissions (e.g., SUID – SGID – Owner/groups)

Domain 6. Troubleshooting

This domain includes basic knowledge and skills to identify, inspect and diagnose problems in the Linux operating system, and apply remedies using common commands and utilities.

- 6.1 Identify and locate the problem by determining whether the problem is hardware, operating system, application software, configuration or the user
- 6.2 Describe troubleshooting best practices (i.e., methodology)

- 6.3 Examine and edit configuration files based on symptoms of a problem using system utilities
- 6.4 Examine, start, and stop processes based on the signs and symptoms of a problem
- 6.5 Use system status tools to examine system resources and statuses (e.g., fsck, setserial)
- 6.6 Use systems boot disk(s) and root disk on workstation and server to diagnose and rescue file system
- 6.7 Inspect and determine cause of errors from system log files
- 6.8 Use disk utilities to solve file system problems (e.g., mount, umount)
- 6.9 Resolve problems based on user feedback (e.g., rights, unable to login to the system, unable to print, unable to receive or transmit mail)
- 6.10 Recognize common errors (e.g., package dependencies, library errors, version conflicts)
- 6.11 Take appropriate action on boot errors (e.g., LILO, bootstrap)
- 6.12 Identify backup and restore errors
- 6.13 Identify application failure on server (e.g., Web page, telnet, ftp, pop3, snmp)
- 6.14 Identify and use trouble shooting commands (e.g., locate, find, grep, ?, <, >, >>, cat, tail)
- 6.15 Locate troubleshooting resources and update as allowable (e.g., Web, man pages, howtos, infopages, LUGs)
- 6.16 Use network utilities to identify network and connectivity problems (e.g., ping, route, traceroute, netstat, lsof)

Domain 7: System Hardware

This domain includes basic knowledge and skills of core and peripheral hardware installation, configuration, and troubleshooting in a Linux environment. It includes generic hardware issues and Linux specific hardware issues.

- 7.1 Identify basic terms, concepts, and functions of system components, including how each component should work during normal operation and during the boot process
- 7.2 Assure that system hardware is configured correctly prior to installation (e.g., IRQs, BIOS, DMA, SCSI settings, cabling) by identifying proper procedures for installing and configuring ATA devices
- 7.3 Assure that system hardware is configured correctly prior to installation (e.g., IRQs, BIOS, DMA, SCSI settings, cabling) by identifying proper procedures for installing and configuring SCSI and IEEE 1394 devices
- 7.4 Assure that system hardware is configured correctly prior to installation (e.g., IRQs, BIOS, DMA, SCSI, cabling) settings by identifying proper procedures for installing and configuring peripheral devices
- 7.5 Assure that system hardware is configured correctly prior to installation (e.g., IRQs, BIOS, DMA, SCSI, cabling) settings by identifying available IRQs, DMAs, and I/O addresses and procedures for device installation and configuration
- 7.6 Remove and replace hardware and accessories (e.g., cables and components) based on symptoms of a problem by identifying basic procedures for adding and removing field replaceable components
- 7.7 Remove and replace hardware and accessories (e.g., cables and components) based on symptoms of a problem by identifying common symptoms and problems associated with each component and how to troubleshoot and isolate the problems
- 7.8 Identify basic networking concepts, including how a network works
- 7.9 Identify proper procedures for diagnosing and troubleshooting ATA devices
- 7.10 Identify proper procedures for diagnosing and troubleshooting SCSI devices
- 7.11 Identify proper procedures for diagnosing and troubleshooting peripheral devices

7.12 Identify proper procedures for diagnosing and troubleshooting core system hardware

7.13 Identify and maintain mobile system hardware (e.g., PCMCIA, APM)

5. Rationale:

- In a survey conducted by the ACC High Technology Institute, 50% of respondents listed Linux skills as important
- Organizations benefit by having employees that can manage and administer computers that utilize the Linux operating system.
- The CompTIA certification supports the transition of IT professionals and organizations from Traditional technical roles into high value business roles.

6. Required Materials:

Required for the class:

Linux+ Certification Student Guide by Bird & Harwood, Osborne; Includes Linux OS CD (Red Hat 7.3)

7. Evaluation

Those who participate in class discussions, and miss no more than three class meetings will be awarded 4.8 continuing education units. Ultimate evaluation of the student will be their successfully passing the CompTIA IT Linux+ examination.

8. Course Outline

Session 1: Planning the Implementation, Installation

Session 2: Configuration

Session 3: Administration

Session 4: System Maintenance

Session 5 Troubleshooting

Session 6: Identify, Install, and Maintain System Hardware