Introduction

The Linux+ Certification is designed to measure the competencies of the Linux Professional with six to twelve months experience with the Linux operating system. This person provides basic installation, operation, security, troubleshooting and basic Linux hardware services for the Linux operating system on workstations and servers.

The table below lists the domains measured by this examination and the extent to which they are represented in the examination.

These 2004 exam objectives were written with several of the major distributions in mind (Red Hat, SuSe, Mandrake and TurboLinux) and the exam addresses software and settings that are common across these distributions. In this way, it is a vendor-neutral exam. In order to pass the exam, students need to have the relevant experience with any one of these distributions.

Domain	% of Examination
1.0 Installation	19%
2.0 Management	26%
3.0 Configuration	20%
4.0 Security	21%
5.0 Documentation	6%
6.0 Hardware	8%
Total	100%

Response Limits
The examinee selects the option that best completes the statement or answers the question from four (4) or more response options. Distracters or wrong answers are response options that examinees with incomplete knowledge or skill would likely choose, but are generally plausible responses fitting into the content area. Test item formats used in this examination are:

Multiple-choice: The examinee selects one option that best answers the question or completes the statement. The option may be to point and click on a selection that is embedded in a graphic.

Sample Directions: The examinee reads the statement or question and selects only the option(s) that represent the best answer(s) from the options presented.

Domain 1.0 Installation – 19%

This domain requires the knowledge and skills to determine installation methods, select appropriate settings, protocols and software packages, and validate correct performance. This domain covers activities as they relate to initial installation of the operating system. For example: installing the Apache Web server is covered here, but starting the service is covered in Domain 2.0 and changing its configuration is covered in Domain 3.0.

The candidate is not expected to know how to install a specific distribution, but should be familiar with setting used by installers on the major distributions. The scope of the exam is limited to software and settings common to Linux software from Red Hat, SuSE, Mandrake, and TurboLinux. Students will need to know one, not all, of these distributions.

Candidates must be familiar with systems and peripherals (as well as their modules and utilities) used on 32-bit and 64-bit x86-based PCs and servers, as of October, 2004. Questions requiring knowledge of proprietary software will not be asked.

1.1 Identify all system hardware required (for example: CPU, memory, drive space, scalability) and check compatibility with Linux Distribution

1.2 Determine appropriate method of installation based on environment (for example: boot disk, CD-ROM, network (HTTP, FTP, NFS, SMB))

1.3 Install multimedia options (for example: video, sound, codecs)

1.4 Identify purpose of Linux machine based on predetermined customer requirements (for example: appliance, desktop system, database, mail server, web server, etc.)

1.5 Determine what software and services should be installed (for example: client applications for workstation, server services for desired task)

1.6 Partition according to pre-installation plan using fdisk (for example: /boot, /usr, /var, /home, swap, RAID/volume, hot-spare, lvm)

1.7 Configure file systems (for example: (ext2) or (ext3) or REISER)

1.8 Configure a boot manager (for example: LILO, ELILO, GRUB, multiple boot options)

1.9 Manage packages after installing the operating systems (for example: install, uninstall, update) (for example: RPM, tar, gzip)
1.10 Select appropriate networking configuration and protocols (for example: inetd, xinetd, modems, Ethernet)
1.11 Select appropriate parameters for Linux installation (for example: language, time zones, keyboard, mouse)
1.12 Configure peripherals as necessary (for example: printer, scanner, modem)

Domain 2.0 Management – 26%

Candidates must be able to demonstrate proficiency in everyday management of Linux-based clients and basic management of server systems. The six to 12 month technician is expected to fully support, maintain, and troubleshoot Linux-based desktop systems. Server management questions will focus on day-to-day server operation and basic administration.

The candidate is expected to be able to fully utilize vi, manage the Linux system completely from the command-line, including permission and user account management, and create basic shell scripts.

2.1 Manage local storage devices and file systems (for example:: fsck, fdisk, mkfs) using CLI commands

2.2 Mount and unmount varied filesystems (for example: Samba, NFS) using CLI commands

2.3 Create files and directories and modify files using CLI commands

2.4 Execute content and directory searches using find and grep

2.5 Create linked files using CLI commands

2.6 Modify file and directory permissions and ownership (for example: chmod, chown, sticky bit, octal permissions, chgrp) using CLI commands

2.7 Identify and modify default permissions for files and directories (for example: umask) using CLI commands

2.8 Perform and verify backups and restores (tar, cpio)

2.9 Access and write data to recordable media (for example: CDRW, hard drive, flash memory devices)

2.10 Manage runlevels and system initialization from the CLI and configuration files (for example: /etc/inittab and init command, /etc/rc.d, rc.local)

2.11 Identify, execute, manage and kill processes (for example: ps, kill, killall, bg, fg, jobs, nice, renice, rc)

2.12 Differentiate core processes from non-critical services (for example: init, [kernel processes], PID, and PPID values)

2.13 Repair packages and scripts (for example: resolving dependencies, repairing, installing, updating applications)

2.14 Monitor and troubleshoot network activity (for example: ping, netstat, traceroute)

2.15 Perform text manipulation (for example: sed, awk, vi)

2.16 Manage print jobs and print queues (for example: lpd, lprm, lpq, CUPS)

2.17 Perform remote management (for example: rsh, ssh, rlogin)

2.18 Perform NIS-related domain management (yp commands)

2.19 Create, modify, and use basic shell scripts

2.20 Create, modify, and delete user and group accounts (for example: useradd, groupadd, /etc/passwd, chgrp, quota, chown, chmod, grpmod) using CLI utilities

2.21 Manage and access mail queues (for example: sendmail, postfix, mail, mutt) using CLI utilities

2.22 Schedule jobs to execute in the future using "at" and "cron" daemons

2.23 Redirect output (for example: piping, redirection)

Domain 3.0 Configuration – 20%

This domain requires the basic knowledge and skills to configure system settings, network services and access rights. Candidates must be able to configure files routinely used on client systems, such as mtab, fstab, hosts, resolv.conf, and inittab. Candidates need to identify which files are used to configure common server applications, but are not required to configure them. As they are often used on clients, some knowledge of Samba and HTTP service configuration is required.

Special utilities, such as linuxconf, or distribution-specific utilities will not be used. Using compilers is not required, but candidates should understand basic makefile structure. Candidates must identify settings for the X.org (XFree86) X Window system and utilities that are used to configure it.

3.1 Configure client network services and settings (for example: settings for TCP/IP)

3.2 Configure basic server network services (for example: DNS, DHCP, SAMBA, Apache)

3.3 Implement basic routing and subnetting (for example: /sbin/route, IP forward statement)

3.4 Configure the system and perform basic makefile changes to support compiling applications and drivers

3.5 Configure files that are used to mount drives or partitions (for example: fstab, mtab, SAMBA, nfs, syntax)

3.6 Implement DNS and describe how it works (for example: edit /etc/hosts, edit /etc/host.conf, edit /etc/resolv.conf, dig, host, named)

3.7 Configure a Network Interface Card (NIC) from a command line

3.8 Configure Linux printing (for example: CUPS, BSD LPD, SAMBA)

3.9 Apply basic printer permissions

3.10 Configure log files (for example: syslog, remote logfile storage)

3.11 Configure the X Window system

3.12 Set up environment variables (for example: $PATH, $DISPLAY, $TERM, $PROMPT, $PS1)

Domain 4.0 Security – 21%

The domain requires that candidates describe common security terms and describe practices, as well as implement security options on client systems. The ability to configure security-related files is required.

Candidates are not expected to create security policies, but must know which practices are commonly used and against what a practice protects.

4.1 Configure security environment files (for example: hosts.allow, sudoers, ftpusers, sshd_config, PAM)

4.2 Delete accounts while maintaining data stored in that user's home directory

4.3 Given security requirements, implement appropriate encryption configuration (for example: blowfish 3DES, MD5)

4.4 Detect symptoms that indicate a machine's security has been compromised (for example: review logfiles for irregularities or intrusion attempts)

4.5 Use appropriate access level for login (for example: root level vs user level activities, su, sudo)

4.6 Set process and special permissions (for example: SUID, GUID)

4.7 Identify different Linux Intrusion Detection Systems (IDS) (for example: Snort, PortSentry)

4.8 Given security requirements, implement basic IP tables/chains (note: requires knowledge of common ports)

4.9 Implement security auditing for files and authentication

4.10 Identify whether a package or file has been corrupted / altered (for example: checksum, Tripwire)

4.11 Given a set of security requirements, set password policies to match (complexity / aging / shadowed passwords) (for example: identify systems not shadow passwords)

4.12 Identify security vulnerabilities within Linux services

4.13 Set up user-level security (for example: limits on logins, memory usage and processes)

Domain 5.0 Documentation – 6%

Candidates must be able to provide written documentation about any work they perform. They must identify information that should be recorded for an installation or change in configuration. In addition they must also be able to use system-generated files to monitor or diagnose systems.

5.1 Establish and monitor system performance baseline (for example: top, sar, vmstat, pstree)

5.2 Create written procedures for installation, configuration, security and management

5.3 Document installed configuration (for example: installed packages, package options, TCP/IP assignment list, changes -configuration and maintenance)

5.4 Troubleshoot errors using systems logs (for example: tail, head, grep)

5.5 Troubleshoot application errors using application logs (for example: tail, head, grep)

5.6 Access system documentation and help files (for example: man, info, readme, Web)

Domain 6.0 Hardware – 8%

This domain includes hardware knowledge as it relates to typical Linux client and server systems. Candidates must be able to identify and describe components used in a 32 or 64-bit x86 client computer or laptop. They must also identify corresponding driver modules and common utilities used to configure or troubleshoot them. Proprietary hardware is not included in this domain.

More detailed knowledge of ATAPI , SCSI, USB, RAID devices, and power management is expected.

6.1 Describe common hardware components and resources (for example: connectors, IRQs, DMA, SCSI, memory addresses)

6.2 Diagnose hardware issues using Linux tools (for example: /proc, disk utilities, ifconfig, /dev, live CD rescue disk, dmesg)

6.3 Identify and configure removable system hardware (for example: PCMCIA, USB, IEEE1394)

6.4 Configure advanced power management and Advanced Configuration and Power Interface (ACPI)

6.5 Identify and configure mass storage devices and RAID (for example: SCSI, ATAPI, tape, optical recordable)