CompTIA Linux+ Certification Exam Objectives

EXAM NUMBER: XK0-004

CompTIA

About the Exam

Candidates are encouraged to use this document to help prepare for CompTIA Linux+ XK0-004. CompTIA Linux+ measures the necessary skills of an IT professional with hands-on experience configuring, monitoring, and supporting servers running the Linux operating system. Successful candidates will have the knowledge required to configure, manage, operate, and troubleshoot a Linux environment by using security best practices, scripting, and automation.

These content examples are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

CompTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse or condone utilizing any content provided by unauthorized third-party training sites (aka "brain dumps"). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA's exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement. If a candidate has a question as to whether study materials are considered unauthorized (aka "brain dumps"), he/she should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current and the security of the questions is protected. When necessary, we will publish updated exams based on testing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	XK0-004
Number of questions	Maximum of 90
Type of questions	Multiple choice and performance-based
Length of test	90 minutes
Recommended experience	9 – 12 months of hands-on experience configuring, monitoring, and supporting servers running the Linux OS
Passing score	720 (on a scale of 100–900)

EXAM OBJECTIVES (DOMAINS)

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

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Hardware and System Configuration	21%
2.0 Systems Operation and Maintenance	26%
3.0 Security	19%
4.0 Linux Troubleshooting and Diagnostics	20%
5.0 Automation and Scripting	14%
Total	**100%**

1.0 Hardware and System Configuration

1.1 Explain Linux boot process concepts.

- **Boot loaders**
  - GRUB
  - GRUB2
- **Boot options**
  - UEFI/EFI
  - PXE
  - NFS
  - Boot from ISO
  - Boot from HTTP/FTP
- **File locations**
  - /etc/default/grub
  - /etc/grub2.cfg
  - /boot
  - /boot/grub
  - /boot/grub2
  - /boot/efi
- **Boot modules and files**
  - Commands
    - mkinitrd
    - dracut
    - grub2-install
    - grub2-mkconfig
  - initramfs
  - efi files
  - vmlinuz
  - vmlinux
- **Kernel panic**

1.2 Given a scenario, install, configure, and monitor kernel modules.

- **Commands**
  - lsmod
  - insmod
  - modprobe
  - modinfo
  - dmesg
  - rmmod
  - depmod
- **Locations**
  - /usr/lib/modules/[kernelversion]
  - /usr/lib/modules
  - /etc/modprobe.conf
  - /etc/modprobe.d/

1.3 Given a scenario, configure and verify network connection parameters.

- **Diagnostic tools**
  - ping
  - netstat
  - nslookup
  - dig
  - host
  - route
  - ip
  - ethtool
  - ss
  - iwconfig
  - nmcli
  - brctl
  - nmtui
- **Configuration files**
  - /etc/sysconfig/network-scripts/
  - /etc/sysconfig/network
  - /etc/hosts
  - /etc/network
  - /etc/nsswitch.conf
  - /etc/resolv.conf
  - /etc/netplan
  - /etc/sysctl.conf
  - /etc/dhcp/dhclient.conf
- **Bonding**
  - Aggregation
  - Active/passive
  - Load balancing

1.4 Given a scenario, manage storage in a Linux environment.

- **Basic partitions**
  - Raw devices
  - GPT
  - MBR
- **File system hierarchy**
  - Real file systems
  - Virtual file systems
  - Relative paths
  - Absolute paths
- **Device mapper**
  - LVM
  - mdadm
  - Multipath
- **Tools**
  - XFS tools
  - LVM tools
  - EXT tools
  - Commands
    - mdadm
    - fdisk
    - parted
    - mkfs
    - iostat
    - df
    - du
    - mount
    - umount
    - lsblk
    - blkid
    - dumpe2fs
    - resize2fs
    - fsck
    - tune2fs
    - e2label
- **Location**
  - /etc/fstab
  - /etc/crypttab
  - /dev/
  - /dev/mapper
  - /dev/disk/by-
    - id
    - uuid
    - path
    - multipath
  - /etc/mtab
  - /sys/block
  - /proc/partitions
  - /proc/mounts
- **File system types**
  - ext3
  - ext4
  - xfs
  - nfs
  - smb
  - cifs
  - ntfs

1.5 Compare and contrast cloud and virtualization concepts and technologies.

- **Templates**
  - VM
  - OVA
  - OVF
  - JSON
  - YAML
  - Container images
- **Bootstrapping**
  - Cloud-init
  - Anaconda
  - Kickstart
- **Storage**
  - Thin vs. thick provisioning
  - Persistent volumes
  - Blob
  - Block
- **Network considerations**
  - Bridging
  - Overlay networks
  - NAT
  - Local
  - Dual-homed
- **Types of hypervisors**
- **Tools**
  - libvirt
  - virsh
  - vmm

1.6 Given a scenario, configure localization options.

- **File locations**
  - /etc/timezone
  - /usr/share/zoneinfo
- **Commands**
  - localectl
  - timedatectl
  - date
  - hwclock
- **Environment variables**
  - LC_*
  - LC_ALL
  - LANG
  - TZ
- **Character sets**
  - UTF-8
  - ASCII
  - Unicode

2.0 Systems Operation and Maintenance

2.1 Given a scenario, conduct software installations, configurations, updates, and removals.

- **Package types**
  - .rpm
  - .deb
  - .tar
  - .tgz
  - .gz
- **Installation tools**
  - RPM
  - Dpkg
  - APT
  - YUM
  - DNF
  - Zypper
- **Build tools**
  - Commands
    - make
    - make install
    - ldd
  - Compilers
  - Shared libraries
- **Repositories**
  - Configuration
  - Creation
  - Syncing
  - Locations
- **Acquisition commands**
  - wget
  - curl

2.2 Given a scenario, manage users and groups.

- **Creation**
  - useradd
  - groupadd
- **Modification**
  - usermod
  - groupmod
  - passwd
  - chage
- **Deletion**
  - userdel
  - groupdel
- **Queries**
  - id
  - whoami
  - who
  - w
  - last
- **Quotas**
  - User quota
  - Group quota
- **Profiles**
  - Bash parameters
    - User entries
      - .bashrc
      - .bash_profile
      - .profile
    - Global entries
      - /etc/bashrc
      - /etc/profile.d/
      - /etc/skel
      - /etc/profile
- **Important files and file contents**
  - /etc/passwd
  - /etc/group
  - /etc/shadow

2.3 Given a scenario, create, modify, and redirect files.

- **Text editors**
  - nano
  - vi
- **File readers**
  - grep
  - cat
  - tail
  - head
  - less
  - more
- **Output redirection**
  - <
  - >
  - |
  - <<
  - >>
  - 2>
  - &>
  - stdin
  - stdout
  - stderr
  - /dev/null
  - /dev/tty
  - xargs
  - tee
  - Here documents
- **Text processing**
  - grep
  - tr
  - echo
  - sort
  - awk
  - sed
  - cut
  - printf
  - egrep
  - wc
  - paste
- **File and directory operations**
  - touch
  - mv
  - cp
  - rm
  - scp
  - ls
  - rsync
  - mkdir
  - rmdir
  - ln
    - Symbolic (soft)
    - Hard
  - unlink
  - inodes
  - find
  - locate
  - grep
  - which
  - whereis
  - diff
  - updatedb

2.4 Given a scenario, manage services.

- **Systemd management**
  - Systemctl
    - Enabled
    - Disabled
    - Start
    - Stop
    - Mask
    - Restart
    - Status
    - Daemon-reload
  - Systemd-analyze blame
  - Unit files
    - Directory locations
    - Environment parameters
  - Targets
  - Hostnamectl
  - Automount
- **SysVinit**
  - chkconfig
    - on
    - off
    - level
  - Runlevels
    - Definitions of 0–6
    - /etc/init.d
    - /etc/rc.d
    - /etc/rc.local
    - /etc/inittab
    - Commands
      - runlevel
      - telinit
- Service
  - Restart
  - Status
  - Stop
  - Start
  - Reload

2.5 Summarize and explain server roles.

- **NTP**
- **SSH**
- **Web**
- **Certificate authority**
- **Name server**
- **DHCP**
- **File servers**
- **Authentication server**
- **Proxy**
- **Logging**
- **Containers**
- **VPN**
- **Monitoring**
- **Database**
- **Print server**
- **Mail server**
- **Load balancer**
- **Clustering**

2.6 Given a scenario, automate and schedule jobs.

- **cron**
- **at**
- **crontab**
- **fg**
- **bg**
- **&**
- **kill**
- **Ctrl+c**
- **Ctrl+z**
- **nohup**

2.7 Explain the use and operation of Linux devices.

- **Types of devices**
  - Client devices
  - Bluetooth
  - WiFi
  - USB
  - Monitors
  - GPIO
  - Network adapters
  - PCI
  - HBA
  - SATA
  - SCSI
  - Printers
  - Video
  - Audio
- **Monitoring and configuration tools**
  - lsdev
  - lsusb
  - lspci
  - lsblk
  - dmesg
  - lpr
  - lpq
  - abrt
  - CUPS
  - udevadm
    - add
    - reload-rules
    - control
    - trigger
- **File locations**
  - /proc
  - /sys
  - /dev
  - /dev/mapper
  - /etc/X11
- **Hot pluggable devices**
  - /usr/lib/udev/rules.d (System rules - Lowest priority)
  - /run/udev/rules.d (Volatile Rules)
  - /etc/udev/rules.d (Local Administration - Highest priority)
  - /etc/udev/rules.d

2.8 Compare and contrast Linux graphical user interfaces.

- **Servers**
  - Wayland
  - X11
- **GUI**
  - Gnome
  - Unity
  - Cinnamon
  - MATE
  - KDE
- **Remote desktop**
  - VNC
  - XRDP
  - NX
  - Spice
- **Console redirection**
  - SSH port forwarding
    - Local
    - Remote
    - X11 forwarding
    - VNC
- **Accessibility**

3.0 Security

3.1 Given a scenario, apply or acquire the appropriate user and/or group permissions and ownership.

- **File and directory permissions**
  - Read, write, execute
  - User, group, other
  - SUID
  - Octal notation
  - umask
  - Sticky bit
  - SGID
  - Inheritance
  - Utilities
    - chmod
    - chown
    - chgrp
    - getfacl
    - setfacl
    - ls
    - ulimit
    - chage
- **Context-based permissions**
  - SELinux configurations
    - disabled
    - permissive
    - enforcing
  - SELinux policy
    - targeted
  - SELinux tools
    - setenforce
    - getenforce
    - sestatus
    - setsebool
    - getsebool
    - chcon
    - restorecon
    - ls -Z
    - ps -Z
  - AppArmor
    - aa-disable
    - aa-complain
    - aa-unconfined
    - /etc/apparmor.d/
    - /etc/apparmor.d/tunables
- **Privilege escalation**
  - su
  - sudo
  - wheel
  - visudo
  - sudoedit
- **User types**
  - Root
  - Standard
  - Service

3.2 Given a scenario, configure and implement appropriate access and authentication methods.

- **PAM**
  - Password policies
  - LDAP integration
  - User lockouts
  - Required, optional, or sufficient
  - /etc/pam.d/
  - pam_tally2
  - faillock
- **SSH**
  - ~/.ssh/
    - known_hosts
    - authorized_keys
    - config
    - id_rsa
    - id_rsa.pub
  - User-specific access
  - TCP wrappers
  - /etc/ssh/
    - ssh_config
    - sshd_config
  - ssh-copy-id
  - ssh-keygen
  - ssh-add
- **TTYs**
  - /etc/securetty
  - /dev/tty#
- **PTYs**
- **PKI**
  - Self-signed
  - Private keys
  - Public keys
  - Hashing
  - Digital signatures
  - Message digest
- **VPN as a client**
  - SSL/TLS
  - Transport mode
  - Tunnel mode
  - IPSec
  - DTLS

3.3 Summarize security best practices in a Linux environment.

- **Boot security**
  - Boot loader password
  - UEFI/BIOS password
- **Additional authentication methods**
  - Multifactor authentication
    - Tokens
      - Hardware
      - Software
    - OTP
    - Biometrics
  - RADIUS
  - TACACS+
  - LDAP
  - Kerberos
    - kinit
    - klist
- **Importance of disabling root login via SSH**
- **Password-less login**
  - Enforce use of PKI
- **Chroot jail services**
- **No shared IDs**
- **Importance of denying hosts**
- **Separation of OS data from application data**
  - Disk partition to maximize system availability
- **Change default ports**
- **Importance of disabling or uninstalling unused and unsecure services**
  - FTP
  - Telnet
  - Finger
  - Sendmail
  - Postfix
- **Importance of enabling SSL/TLS**
- **Importance of enabling auditd**
- **CVE monitoring**
- **Discouraging use of USB devices**
- **Disk encryption**
  - LUKS
- **Restrict cron access**
- **Disable Ctrl+Alt+Del**
- **Add banner**
- **MOTD**

3.4 Given a scenario, implement logging services.

- **Key file locations**
  - /var/log/secure
  - /var/log/messages
  - /var/log/[application]
  - /var/log/kern.log
- **Log management**
  - Third-party agents
  - logrotate
  - /etc/rsyslog.conf
  - journald
    - journalctl
- **lastb**

3.5 Given a scenario, implement and configure Linux firewalls.

- **Access control lists**
  - Source
  - Destination
  - Ports
  - Protocol
  - Logging
  - Stateful vs. stateless
  - Accept
  - Reject
  - Drop
  - Log
- **Technologies**
  - firewalld
    - Zones
    - Run time
  - iptables
    - Persistency
    - Chains
  - ufw
    - /etc/default/ufw
    - /etc/ufw/
  - Netfilter
- **IP forwarding**
  - /proc/sys/net/ipv4/ip_forward
  - /proc/sys/net/ipv6/conf/all/forwarding
- **Dynamic rule sets**
  - DenyHosts
  - Fail2ban
  - IPset
- **Common application firewall configurations**
  - /etc/services
  - Privileged ports

3.6 Given a scenario, backup, restore, and compress files.

- **Archive and restore utilities**
  - tar
  - cpio
  - dd
- **Compression**
  - gzip
  - xz
  - bzip2
  - zip
- **Backup types**
  - Incremental
  - Full
  - Snapshot clones
  - Differential
  - Image
- **Off-site/off-system storage**
  - SFTP
  - SCP
  - rsync
- **Integrity checks**
  - MD5
  - SHA

4.0 Linux Troubleshooting and Diagnostics

4.1 Given a scenario, analyze system properties and remediate accordingly.

- **Network monitoring and configuration**
  - Latency
    - Bandwidth
    - Throughput
  - Routing
  - Saturation
  - Packet drop
  - Timeouts
  - Name resolution
  - Localhost vs. Unix socket
  - Adapters
    - RDMA drivers
  - Interface configurations
  - Commands
    - nmap
    - netstat
    - iftop
    - route
    - iperf
    - tcpdump
    - ipset
    - Wireshark
      - tshark
    - netcat
    - traceroute
    - mtr
    - arp
    - nslookup
    - dig
    - host
    - whois
    - ping
    - nmcli
    - ip
    - tracepath
- **Storage monitoring and configuration**
  - iostat
  - ioping
  - IO scheduling
    - cfq
    - noop
    - deadline
    - du
    - df
    - LVM tools
    - fsck
    - partprobe
- **CPU monitoring and configuration**
  - /proc/cpuinfo
  - uptime
  - loadaverage
  - sar
  - sysctl
- **Memory monitoring and configuration**
  - swapon
  - swapoff
  - mkswap
  - vmstat
  - Out of memory killer
  - free
  - /proc/meminfo
  - Buffer cache output
- **Lost root password**
  - Single user mode

4.2 Given a scenario, analyze system processes in order to optimize performance.

- **Process management**
  - Process states
    - Zombie
    - Uninterruptible sleep
    - Interruptible sleep
    - Running
  - Priorities
  - Kill signals
  - Commands
    - nice
    - renice
    - top
    - time
    - ps
    - lsof
    - pgrep
    - pkill
  - PIDs

4.3 Given a scenario, analyze and troubleshoot user issues.

- **Permissions**
  - File
  - Directory
- **Access**
  - Local
  - Remote
- **Authentication**
  - Local
  - External
  - Policy violations
- **File creation**
  - Quotas
  - Storage
  - Inode exhaustion
  - Immutable files
- **Insufficient privileges for authorization**
  - SELinux violations
- **Environment and shell issues**

4.4 Given a scenario, analyze and troubleshoot application and hardware issues.

- **SELinux context violations**
- **Storage**
  - Degraded storage
  - Missing devices
  - Missing volumes
  - Missing mount point
  - Performance issues
  - Resource exhaustion
  - Adapters
    - SCSI
    - RAID
    - SATA
    - HBA
      - /sys/class/scsi_host/host#/scan
  - Storage integrity
    - Bad blocks
- **Firewall**
  - Restrictive ACLs
  - Blocked ports
  - Blocked protocols
- **Permission**
  - Ownership
  - Executables
  - Inheritance
  - Service accounts
  - Group memberships
- **Dependencies**
  - Patching
  - Update issues
  - Versioning
  - Libraries
  - Environment variables
  - GCC compatibility
  - Repositories
- **Troubleshooting additional hardware issues**
  - Memory
  - Printers
  - Video
    - GPU drivers
  - Communications ports
  - USB
  - Keyboard mapping
  - Hardware or software compatibility issues
  - Commands
    - dmidecode
    - lshw

5.0 Automation and Scripting

5.1 Given a scenario, deploy and execute basic BASH scripts.

- **Shell environments and shell variables**
  - PATH
  - Global
  - Local
  - export
  - env
  - set
  - printenv
  - echo
- **#!/bin/bash**
- **Sourcing scripts**
- **Directory and file permissions**
  - chmod
- **Extensions**
- **Commenting**
  - #
- **File globbing**
- **Shell expansions**
  - ${}
  - $()
  - ``
- **Redirection and piping**
- **Exit codes**
  - stderr
  - stdin
  - stdout
- **Metacharacters**
- **Positional parameters**
- **Looping constructs**
  - while
  - for
  - until
- **Conditional statements**
  - if
  - case
- **Escaping characters**

5.2 Given a scenario, carry out version control using Git.

- **Arguments**
  - clone
  - push
  - pull
  - commit
  - merge
  - branch
  - log
  - init
  - config
- **Files**
  - .gitignore
  - .git/

5.3 Summarize orchestration processes and concepts.

- **Agent**
- **Agentless**
- **Procedures**
- **Attributes**
- **Infrastructure automation**
- **Infrastructure as code**
- **Inventory**
- **Automated configuration management**
- **Build automation**

CompTIA Linux+ Acronyms

The following is a list of acronyms that appear on the CompTIA Linux+ exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

ACRONYM	SPELLED OUT
ACL	Access Control List
ASCII	American Standard for Computer Information Interchange
BASH	Bourne Again Shell
BIOS	Basic Input Output System
CIFS	Common Internet File System
CPU	Central Processing Unit
CUPS	Common Unix Printing System
CVE	Common Vulnerability and Exposures
DHCP	Dynamic Host Configuration Protocol
DTLS	Datagram Transport Layer Security
EFI	Extensible Firmware Interface
EPEL	Extra Packages for Enterprise Linux
FTP	File Transfer Protocol
GCC	GNU Compiler Collection
GPIO	General Purpose Input Output
GPT	GUID Partition Table
GPU	Graphics Processing Unit
GRUB	Grand Unified Bootloader
GUI	Graphical User Interface
GUID	Global Unique Identifier
HBA	Host Bus Adapter
HTTP	Hypertext Transfer Protocol
HTTPd	Hypertext Transfer Protocol daemon
IO	Input Output
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
KDE	K Desktop Environment
LDAP	Lightweight Directory Authentication Protocol
LUKS	Linux Unified Key Setup
LVM	Logical Volume Manager
MBR	Master Boot Record
MD5	Message Digest 5
MOTD	Message of the Day
NAT	Network Address Translation
NFS	Network File System
NTFS	New Technology File System
NTP	Network Time Protocol
OTP	One Time Password
OVA	Open Virtualization Appliance
OVF	Open Virtualization Format
PAM	Pluggable Authentication Module
PCI	Peripheral Component Interconnect
PID	Process ID
PKI	Public Key Infrastructure
PTY	Pseudoterminal
PXE	Pre-execution Boot
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant Array of Independent Disks
RDMA	Remote Direct Memory Access
RPM	RPM Package Manager
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer Systems Interface
SELinux	Security Enhanced Linux
SHA	Secure Hash Algorithm
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
SUID	Set User ID
TACACS+	Terminal Access Controller Access Control System Plus
TAR	Tape Archive
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTY	Terminal Type
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
UTF	Unicode Transformation Format
VM	Virtual Machine
VNC	Virtual Network Computing
VPN	Virtual Private Network
XFS	Extents File System
XRDP	XWindows Remote Desktop Protocol
YAML	Yet Another Markup Language
YUM	Yellowdog Updater Modified

Linux+ Proposed Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the Linux+ exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The bulleted lists below each topic are a sample list and not exhaustive.

EQUIPMENT

- Laptop or desktop that supports virtualization OR access to a cloud service provider
- Network
  - Router
  - Switch
  - Network adapter
- Internet access

SPARE PARTS/HARDWARE

- HDD
- USB OR DVD media

SOFTWARE

- Repository access
- PuTTY or SSH client
- Automation tools (e.g. Ansible, Puppet)
- Git
- Virtualization software

RECOMMENDED DISTRIBUTIONS

- *CentOS
- *Ubuntu
- Fedora
- Debian
- Open SUSE

CompTIA