CompTIA Linux+ Certification Exam Objectives

EXAM NUMBER: XK0-005

CompTIA

About the Exam

Candidates are encouraged to use this document help prepare for the CompTIA Linux+ XK0-005 certification exam. The CompTIA Linux+ certification exam will verify the successful candidate has the knowledge and skills required configure, manage, operate, and troubleshoot Linux on-premises and cloud-based server environments, while using security best practices, scripting, containerization, and automation.

This is equivalent to at least 12 months of hands-on experience working with Linux servers in a junior Linux support engineer or junior cloud/DevOps support engineer job role.

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 ACCREDITATION

The CompTIA Linux+ exam is accredited by ANSI to show compliance with the ISO 17024 standard and, as such, undergoes regular reviews and updates to the exam objectives.

EXAM DEVELOPMENT

CompTIA exams result from subject-matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an entry-level 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 tomore 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 towhether 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 existing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	XK0-005
Number of questions	Maximum of 90
Types of questions	Multiple-choice and performance-based
Length of test	90 minutes
Recommended experience	12 months of hands-on experience working with Linux servers, as well as A+, Network+, and Server+ or similar certifications and/or knowledge
Passing score	720 (on a scale of 100 to 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 System Management	32%
2.0 Security	21%
3.0 Scripting, Containers, and Automation	19%
4.0 Troubleshooting	28%
Total	**100%**

1.0 System Management

1.1 Summarize Linux fundamentals.

- **Filesystem Hierarchy Standard (FHS)**
  - /boot
  - /proc
  - /sys
  - /var
  - /usr
  - /lib
  - /dev
  - /etc
  - /opt
  - /bin
  - /sbin
  - /home
  - /media
  - /mnt
  - /root
  - /tmp
- **Basic boot process**
  - Basic input/output system (BIOS)
  - Unified Extensible Firmware Interface (UEFI)
  - Commands
    - mkinitrd
    - grub2-install
    - grub2-mkconfig
    - grub2-update
    - dracut
  - initrd.img
  - vmlinuz
  - Grand Unified Bootloader version 2 (GRUB2)
  - Boot sources
    - Preboot eXecution Environment (PXE)
    - Booting from Universal Serial Bus (USB)
    - Booting from ISO
- **Kernel panic**
- **Device types in /dev**
  - Block devices
  - Character devices
  - Special character devices
    - /dev/null
    - /dev/zero
    - /dev/urandom
- **Basic package compilation from source**
  - ./configure
  - make
  - make install
- **Storage concepts**
  - File storage
  - Block storage
  - Object storage
  - Partition typo
    - Master boot record (MBR)
    - GUID [globally unique identifier] Partition Table (GPT)
  - Filesystem in Userspace (FUSE)
  - Redundant Array of Independent (or Inexpensive) Disks (RAID) levels
    - Striping
    - Mirroring
    - Parity
- **Listing hardware information**
  - lspci
  - lsusb
  - dmidecode

1.2 Given a scenario, manage files and directories.

- **File editing**
  - sed
  - awk
  - printf
  - nano
  - vi(m)
- **File compression, archiving, and backup**
  - gzip
  - bzip2
  - zip
  - tar
  - xz
  - cpio
  - dd
- **File metadata**
  - stat
  - file
- **Soft and hard links**
- **Copying files between systems**
  - rsync
  - scp
  - nc
- **File and directory operations**
  - mv
  - cp
  - mkdir
  - rmdir
  - ls
  - pwd
  - rm
  - cd
  - .
  - ..
  - ~
  - tree
  - cat
  - touch

1.3 Given a scenario, configure and manage storage using the appropriate tools.

- **Disk partitioning**
  - Commands
    - fdisk
    - parted
    - partprobe
- **Mounting local and remote devices**
  - systemd.mount
  - /etc/fstab
  - mount
  - Linux Unified Key Setup (LUKS)
  - External devices
- **Filesystem management**
  - XFS tools
  - Ext4 tools
  - Btrfs tools
- **Monitoring storage space and disk usage**
  - df
  - du
- **Creating and modifying volumes using Logical Volume Manager (LVM)**
  - Commands
    - pvs
    - vgs
    - lvs
    - lvchange
    - lvcreate
    - vgcreate
    - lvresize
    - pvcreate
    - vgextend
- **Inspecting RAID implementations**
  - mdadm
  - /proc/mdstat
- **Storage area network (SAN)/ network-attached storage (NAS)**
  - multipathd
  - Network filesystems
    - Network File System (NFS)
    - Server Message Block (SMB)/Common Internet File System (CIFS)
- **Storage hardware**
  - lsscsi
  - lsblk
  - blkid
  - fcstat

1.4 Given a scenario, configure and use the appropriate processes and services.

- **System services**
  - systemctl
    - stop
    - start
    - restart
    - status
    - enable
    - disable
    - mask
- **Scheduling services**
  - cron
  - crontab
  - at
- **Process management**
  - Kill signals
    - SIGTERM
    - SIGKILL
    - SIGHUP
  - Listing processes and open files
    - top
    - ps
    - lsof
    - htop
  - Setting priorities
    - nice
    - renice
  - Process states
    - Zombie
    - Sleeping
    - Running
    - Stopped
  - Job control
    - bg
    - fg
    - jobs
    - Ctrl+Z
    - Ctrl+C
    - Ctrl+D
  - pgrep
  - pkill
  - pidof

1.5 Given a scenario, use the appropriate networking tools or configuration files.

- **Interface management**
  - iproute2 tools
    - ip
    - ss
  - NetworkManager
    - nmcli
  - net-tools
    - ifconfig
    - ifcfg
    - hostname
    - arp
    - route
  - /etc/sysconfig/network-scripts/
- **Name resolution**
  - nsswitch
  - /etc/resolv.conf
  - systemd
    - hostnamectl
    - resolvectl
  - Bind-utils
    - dig
    - nslookup
    - host
  - WHOIS
- **Network monitoring**
  - tcpdump
  - wireshark/tshark
  - netstat
  - traceroute
  - ping
  - mtr
- **Remote networking tools**
  - Secure Shell (SSH)
  - cURL
  - wget
  - nc
  - rsync
  - Secure Copy Protocol (SCP)
  - SSH File Transfer Protocol (SFTP)

1.6 Given a scenario, build and install software.

- **Package management**
  - DNF
  - YUM
  - APT
  - RPM
  - dpkg
  - ZYpp
- **Sandboxed applications**
  - snapd
  - Flatpak
  - AppImage
- **System updates**
  - Kernel updates
  - Package updates

1.7 Given a scenario, manage software configurations.

- **Updating configuration files**
  - Procedures
    - Restart service
    - Reload service
  - .rpmnew
  - .rpmsave

  Repository configuration files
    - /etc/apt.conf
    - /etc/yum.conf
    - /etc/dnf/dnf.conf
    - /etc/yum.repo.d
    - /etc/apt/sources.list.d
- **Configure kernel options**
  - Parameters
    - sysctl
    - /etc/sysctl.conf
  - Modules
    - lsmod
    - imsmod
    - rmmod
    - insmod
    - modprobe
    - modinfo
- **Configure common system services**
  - SSH
  - Network Time Protocol (NTP)
  - Syslog
  - chrony
- **Localization**
  - timedatectl
  - localectl

2.0 Security

2.1 Summarize the purpose and use of security best practices in a Linux environment.

- **Managing public key infrastructure (PKI) certificates**
  - Public key
  - Private key
  - Self-signed certificate
  - Digital signature
  - Wildcard certificate
  - Hashing
  - Certificate authorities
- **Certificate use cases**
  - Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)
  - Certificate authentication
  - Encryption
- **Authentication**
  - Tokens
  - Multifactor authentication (MFA)
  - Pluggable authentication modules (PAM)
  - System Security Services Daemon (SSSD)
  - Lightweight Directory Access Protocol (LDAP)
  - Single sign-on (SSO)
- **Linux hardening**
  - Security scanning
  - Secure boot
    - UEFI
  - System logging configurations
  - Setting default umask
  - Disabling/removing insecure services
  - Enforcing password strength
  - Removing unused packages
  - Tuning kernel parameters
  - Securing service accounts
  - Configuring the host firewall

2.2 Given a scenario, implement identity management.

- **Account creation and deletion**
  - Utilities
    - useradd
    - groupadd
    - userdel
    - groupdel
    - usermod
    - groupmod
    - id
    - who
    - w
  - Default shell
  - Configuration files
    - /etc/passwd
    - /etc/group
    - /etc/shadow
    - /etc/profile
    - /etc/skel
    - .bash_profile
    - .bashrc
- **Account management**
  - passwd
  - chage
  - pam_tally2
  - faillock
  - /etc/login.defs

2.3 Given a scenario, implement and configure firewalls.

- **Firewall use cases**
  - Open and close ports
  - Check current configuration
  - Enable/disable Internet protocol (IP) forwarding
- **Common firewall technologies**
  - firewalld
  - iptables
  - nftables
  - Uncomplicated firewall (UFW)

Key firewall features
- Zones
- Services
- Stateful
- Stateless

2.4 Given a scenario, configure and execute remote connectivity for system management.

- **SSH**
  - Configuration files
    - /etc/ssh/sshd_config
    - /etc/ssh/ssh_config
    - ~/.ssh/known_hosts
    - ~/.ssh/authorized_keys
    - /etc/ssh/sshd_config
    - /etc/ssh/ssh_config
    - ~/.ssh/config
  - Commands
    - ssh-keygen
    - ssh-copy-id
    - ssh-add
  - Tunneling
    - X11 forwarding
    - Port forwarding
    - Dynamic forwarding
- **Executing commands as another user**
  - /etc/sudoers
  - PolicyKit rules
  - Commands
    - sudo
    - visudo
    - su –
    - pkexec

2.5 Given a scenario, apply the appropriate access controls.

- **File permissions**
  - Access control list (ACL)
  - Set user ID (SUID)
  - Set group ID (SGID)
  - Sticky bit
- **Security-enhanced Linux (SELinux)**
  - Context permissions
  - Labels
    - Autorelabel
  - System booleans
  - States
    - Enforcing
    - Permissive
    - Disabled
  - Policy types
    - Targeted
    - Minimum
- **AppArmor**
  - Application permissions
- **Command-line utilities**
  - chown
  - umask
  - chmod
  - getfacl
  - setfacl
  - ls
  - setenforce
  - getenforce
  - chattr
  - lsattr
  - chgrp
  - setsebool
  - getsebool
  - chcon
  - restorecon
  - semanage
  - audit2allow

3.0 Scripting, Containers, and Automation

3.1 Given a scenario, create simple shell scripts to automate common tasks.

- **Shell script elements**
  - Loops
    - while
    - for
    - until
  - Conditionals
    - if
    - switch/case
  - Shell parameter expansion
    - Globbing
    - Brace expansions
  - Comparisons
    - Arithmetic
    - String
    - Boolean
  - Variables
  - Search and replace
  - Regular expressions
  - Standard stream redirection
    - |
    - ||
    - >
    - >>
    - <
    - <<
    - &
    - &&
    - Redirecting
    - stderr
    - stdout
  - Here documents
  - Exit codes
  - Shell built-in commands
    - read
    - echo
    - source
- **Common script utilities**
  - awk
  - sed
  - find
  - xargs
  - grep
  - egrep
  - tee
  - wc
  - cut
  - tr
  - head
  - tail
- **Environment variables**
  - $PATH
  - $SHELL
  - $?
- **Relative and absolute paths**

3.2 Given a scenario, perform basic container operations.

- **Container management**
  - Starting/stopping
  - Inspecting
  - Listing
  - Deploying existing images
  - Connecting to containers
  - Logging
  - Exposing ports
- **Container image operations**
  - build
  - push
  - pull
  - list
  - rmi

3.3 Given a scenario, perform basic version control using Git.

- **clone**
- **push**
- **pull**
- **commit**
- **add**
- **checkout**
- **branch**
- **tag**
- **gitignore**

3.4 Summarize common infrastructure as code technologies.

- **File formats**
  - YAML Ain't Markup Language (YAML)
  - JavaScript Object Notation (JSON)
- **Utilities**
  - Ansible
  - Puppet
  - Chef
  - SaltStack
  - Terraform
- **Continuous integration/ continuous deployment (CI/CD)**
  - Use cases
- **Advanced Git topics**
  - merge
  - rebase
  - Pull requests

3.5 Summarize container, cloud, and orchestration concepts.

- **Kubernetes benefits and application use cases**
  - Pods
  - Sidecars
  - Ambassador containers
- **Single-node, multicontainer use cases**
  - Compose
- **Container persistent storage**
- **Container networks**
  - Overlay networks
  - Bridging
  - Network address translation (NAT)
  - Host
- **Service mesh**
- **Bootstrapping**
  - Cloud-init
- **Container registries**

4.0 Troubleshooting

4.1 Given a scenario, analyze and troubleshoot storage issues.

- **High latency**
  - Input/output (I/O) wait
- **Low throughput**
- **Input/output operations per second (IOPS) scenarios**
  - Low IOPS
- **Capacity issues**
  - Low disk space
  - Inode exhaustion
- **Filesystem issues**
  - Corruption
  - Mismatch
- **I/O scheduler**
- **Device issues**
  - Non-volatile memory express (NVMe)
  - Solid-state drive (SSD)
  - SSD trim
  - RAID
  - LVM
  - I/O errors
- **Mount option problems**

4.2 Given a scenario, analyze and troubleshoot network resource issues.

- **Network configuration issues**
  - Subnet
  - Routing
- **Firewall issues**
- **Interface errors**
  - Dropped packets
  - Collisions
  - Link status
- **Bandwidth limitations**
  - High latency
- **Name resolution issues**
  - Domain Name System (DNS)
- **Testing remote systems**
  - Nmap
  - openssl s_client

4.3 Given a scenario, analyze and troubleshoot central processing unit (CPU) and memory issues.

- **Runaway processes**
- **Zombie processes**
- **High CPU utilization**
- **High load average**
- **High run queues**
- **CPU times**
  - steal
  - user
  - system
  - idle
  - iowait
- **CPU process priorities**
  - nice
  - renice
- **Memory exhaustion**
  - Free memory vs. file cache
- **Out of memory (OOM)**
  - Memory leaks
  - Process killer
- **Swapping**
- **Hardware**
  - lscpu
  - lsmem
  - /proc/cpuinfo
  - /proc/meminfo

4.4 Given a scenario, analyze and troubleshoot user access and file permissions.

- **User login issues**
- **User file access issues**
  - Group
  - Context
  - Permission
  - ACL
  - Attribute
  - Policy/non-policy
- **Password issues**
- **Privilege elevation**
- **Quota issues**

4.5 Given a scenario, use systemd to diagnose and resolve common problems with a Linux system.

- **Unit files**
  - Service
    - Networking services
    - ExecStart/ExecStop
    - Before/after
    - Type
    - User
    - Requires/wants
  - Timer
    - OnCalendar
    - OnBootSec
    - Unit
    - Time expressions
  - Mount
    - Naming conventions
    - What
    - Where
    - Type
    - Options
  - Target
    - Default
    - Multiuser
    - Network-online
    - Graphical
- **Common problems**
  - Name resolution failure
  - Application crash
  - Time-zone configuration
  - Boot issues
  - Journal issues
  - Services not starting on time

Linux+ Acronym List

The following is a list of acronyms that appear on the CompTIA Linux+ XK0-005 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
BIOS	Basic Input/Output System
CI/CD	Continuous Integration/ Continuous Deployment
CIFS	Common Internet File System
CPU	Central Processing Unit
DNS	Domain Name System
FHS	Filesystem Hierarchy Standard
FUSE	Filesystem in Userspace
GPT	GUID (Globally Unique Identifier) Partition Table
GRUB	Grand Unified Bootloader
GUID	Globally Unique Identifier
I/O	Input/Output
IOPS	Input/Ouput Operations Per Second
IP	Internet Protocol
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
LDAP	Lightweight Directory Access Protocol
LUKS	Linux Unified Key Setup
LVM	Logical Volume Manager
MFA	Multifactor Authentication
MBR	Master Boot Record
NAS	Network-attached Storage
NAT	Network Address Translation
NFS	Network File System
NTP	Network Time Protocol
NVMe	Non-volatile Memory Express
OOM	Out of Memory
PAM	Pluggable Authentication Module
PKI	Public Key Infrastructure
PXE	Preboot Execution Environment
RAID	Redundant Array of Independent (or Inexpensive) Disks
SAN	Storage Area Network
SCP	Secure Copy Protocol
SELinux	Security Enhanced Linux
SFTP	Secure File Transfer Protocol
SGID	Set Group ID
SMB	Server Message Block
SSD	Solid-state Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
SSSD	System Security Services Daemon
SUID	Set User ID
TLS	Transport Layer Security
UEFI	Unified Extensible Firmware Interface
UFW	Uncomplicated Firewall
USB	Universal Serial Bus
YAML	YAML Ain't Markup Language

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+ XK0-005 exam. This list may also be helpful for training companies that wish to create a lab component for their training offerings. The bulleted lists below each topic are sample lists and are not exhaustive.

EQUIPMENT

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

SPARE PARTS/HARDWARE

- Hard disk drive
- USB or DVD media

SOFTWARE

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

RECOMMENDED DISTRIBUTIONS

- Ubuntu
- Fedora Linux
- Debian
- openSUSE
- Red Hat Enterprise Linux

CompTIA