

Linux System Administration

Intensive 5-Day Bootcamp for CompTIA Linux+ Certification

FA-0291 · 5-Day

DevOps, Cloud & Infrastructure · Automation, RPA & Power Platform

Introduction

Tagline: From Command Line to Certification—Master Linux the Practical Way

In an era where Linux powers the backbone of enterprise servers, cloud infrastructures, and DevOps pipelines, proficiency in Linux system administration is more than a technical skill—it's a career imperative. The CompTIA Linux+ certification (XK0-005) is recognized globally as a benchmark for validating the competencies required of early-career Linux administrators. This intensive 5-day course is meticulously designed to align with the latest CompTIA Linux+ exam objectives, ensuring that participants are well-prepared to excel in the certification and in real-world scenarios. Guided by an instructor with over 30 years of industry experience, the course emphasizes hands-on labs and practical applications over theoretical concepts, providing participants with the tools and confidence to manage Linux systems effectively.

Learning outcomes

By the end of this course, participants will be able to:

- **Filesystem Navigation and Management:** Proficiently navigate and manage the Linux filesystem and directory structures.
- **User and Group Administration:** Administer user and group accounts with a focus on security and efficiency.
- **Permissions and Ownership:** Configure and manage permissions and ownership to safeguard system integrity.
- **Storage Solutions:** Implement and manage storage solutions, including logical volumes and filesystems.
- **System Troubleshooting:** Troubleshoot and resolve common Linux system issues with confidence.

- **Shell Scripting:** Automate routine tasks using shell scripting to enhance operational efficiency.
- **System Security:** Secure Linux systems by applying best practices in authentication, permissions, and firewall configurations.

Prerequisites

Participants should have:

- Strong understanding of computer systems and networking concepts.
- Experience with using a terminal or command-line interface.
- Access to a computer with internet connectivity.

Training outline

1. 1. Introduction to Linux System Administration

- Overview of various Linux distributions and their applications in different environments.
- Understanding the role and responsibilities of a Linux system administrator.
- Efficient navigation of the Linux command line interface.

2. 2. Filesystem Hierarchy and Management

- In-depth exploration of the Filesystem Hierarchy Standard (FHS), including key directories such as /boot, /proc, /sys, /var, /usr, /lib, /dev, /etc, /opt, /home, and /tmp.
- Mounting and unmounting filesystems.
- Managing disk quotas and performing filesystem integrity checks.

3. 3. User and Group Administration

- Creating, modifying, and deleting user accounts.
- Managing group memberships and permissions.
- Implementing password policies and account security measures.
- Utilizing superuser privileges and the sudo mechanism.

4. 4. Permissions and Ownership

- Understanding and configuring file and directory permissions.
- Differentiating between symbolic and numeric permission representations.

- Implementing special permissions: SUID, SGID, and sticky bits.
- Troubleshooting common permission-related issues.

5. 5. Storage Management

- Partitioning disks using tools like fdisk and gdisk.
- Creating and managing logical volumes with LVM.
- Formatting and mounting various filesystem types (ext4, xfs, btrfs).
- Implementing RAID configurations for redundancy and performance.

6. 6. Process and Service Management

- Monitoring active processes and system resource utilization.
- Managing system services using systemd and systemctl.
- Scheduling recurring tasks with cron and at utilities.
- Handling system boot processes and troubleshooting boot issues.

7. 7. Networking Fundamentals

- Configuring network interfaces and understanding IP addressing.
- Managing network services such as SSH, DNS, and DHCP.
- Implementing firewall rules using iptables and firewalld.
- Diagnosing and resolving common network connectivity issues.

8. 8. Package Management and Software Installation

- Utilizing package managers: apt for Debian-based and yum/dnf for Red Hat-based systems.
- Adding and managing third-party repositories.
- Compiling and installing software from source.
- Ensuring system security through regular updates and patches.

9. 9. Shell Scripting and Automation

- Writing and executing basic Bash scripts.
- Utilizing variables, conditionals, loops, and functions in scripts.
- Automating administrative tasks to improve efficiency.
- Debugging and optimizing shell scripts for performance.

10. 10. System Security Practices

- Implementing user authentication mechanisms and configuring PAM.
- Setting up and managing firewalls to control access.
- Applying security updates and patches promptly.
- Conducting regular security audits and vulnerability assessments.

11. 11. Troubleshooting and System Maintenance

- Diagnosing hardware and software issues using system logs.
- Managing system performance and identifying bottlenecks.
- Performing regular backups and restoration procedures.