Faysal Aziz

Linux System Administration

A Comprehensive 3-Day Intensive Course leading to CompTIA Linux+ (XK0-005)

FA-0290 · 3-Day

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

---

Introduction

Want to master Linux? This hands-on, 3-day course will get you there. Linux is everywhere these days – from the servers running major companies to the backbone of cloud computing. If you're looking to grow your career in IT, whether as a system administrator, network engineer, or cybersecurity expert, solid Linux skills are essential.

You'll learn from an instructor with three decades of experience who focuses on practical, real-world skills – not just theory. We've designed this course to give you exactly what today's employers are looking for.

Learning outcomes

- Proficiently navigate and manage the Linux filesystem and directory structures.
- Administer user and group accounts with a focus on security and efficiency.
- Configure and manage permissions and ownership to safeguard system integrity.
- Implement and manage storage solutions, including logical volumes and filesystems.
- Troubleshoot and resolve common Linux system issues with confidence.
- Automate routine tasks using shell scripting to enhance operational efficiency.
- Secure Linux systems by applying best practices in authentication, permissions, and firewall configurations.

Prerequisites

- Basic understanding of computer systems and networks.
- Prior experience with command-line interfaces is advantageous but not mandatory.

Training outline

1. Introduction to Linux System Administration

1. Overview of Linux distributions and their applications in various environments.
2. Understanding the role and responsibilities of a Linux system administrator.
3. Navigating the Linux command line interface efficiently.

2. Filesystem Hierarchy and Management

Detailed exploration of the Filesystem Hierarchy Standard (FHS).

1. Key directories: /boot, /proc, /sys, /var, /usr, /lib, /dev, /etc, /opt, /home, /tmp.

2. Mounting and unmounting filesystems.
3. Managing disk quotas and filesystem integrity checks.

3. User and Group Administration

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

4. Permissions and Ownership

1. Understanding and configuring file and directory permissions.
2. Differentiating between symbolic and numeric permission representations.
3. Implementing special permissions: SUID, SGID, and sticky bits.
4. Troubleshooting common permission-related issues.

5. Storage Management

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

6. Process and Service Management

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

7. Networking Fundamentals

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

8. Package Management and Software Installation

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

9. Shell Scripting and Automation

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

10. System Security Practices

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

11. Troubleshooting and System Maintenance

1. Diagnosing hardware and software issues using system logs.

2. Managing system performance and identifying bottlenecks.
3. Performing regular backups and restoration procedures.
4. Developing disaster recovery plans and ensuring system resilience.

This course is designed to provide participants with a robust and practical understanding of Linux system administration, leveraging the extensive industry experience of the instructor to deliver content that is both current and immediately applicable in professional settings.

© 2026 Faysal Aziz · Kuala Lumpur