# Linux Server Administration and System Hardening

5 days | 30 training hours | 08:30 to 16:00 daily | 12 scheduled dates

Linux quietly powers much of the web, cloud and enterprise infrastructure that African organisations rely on. This hands on course builds the practical skills to administer Linux servers confidently and lock them down against attack. Participants work at the command line to manage users, services and storage, then apply hardening steps that reduce the attack surface.

## Course objectives

This programme builds the practical capability to plan, control and evaluate the work it covers, to a standard the delegate's own organisation can rely on. By the end of the 5 days, delegates should be able to:

- Navigate and manage a Linux system from the command line.
- Administer users, permissions and groups securely.
- Install, configure and monitor common services.
- Manage storage, processes and system logs.
- Apply hardening steps that reduce the attack surface.
- Set up updates and backups that keep servers reliable and secure.

## Learning outcomes

On successful completion of the course, delegates will be able to:

- Explain Linux operating system architecture and the role of Linux in enterprise infrastructure.
- Perform essential file and directory administration tasks.
- Configure file ownership, permissions and privileged administrative access.
- Monitor running processes, system resources and server performance.
- Configure basic Linux networking and troubleshoot connectivity problems.
- Implement secure SSH administration and appropriate authentication controls.
- Apply practical Linux system hardening techniques.
- Install security updates and maintain system patching procedures.
- Navigate Linux systems confidently using the command line interface.
- Create, modify, disable and manage Linux user accounts and groups.
- Install, configure and troubleshoot Linux services.
- Manage Linux storage devices, partitions, file systems and mount points.
- Identify unnecessary services, insecure configurations and common server vulnerabilities.
- Configure host based firewalls to restrict unauthorised network access.
- Review system logs and investigate suspicious or abnormal events.
- Configure basic backup and restoration processes.

- Perform a structured server hardening exercise and verify the resulting configuration.
- Prepare basic technical documentation and Linux server maintenance checklists.

## Who should attend

IT professionals responsible for administering, maintaining, supporting or securing Linux based infrastructure, including Linux and IT systems administrators, Windows Server administrators moving to Linux, IT support officers and technicians, network administrators and engineers, server and data centre administrators, IT infrastructure engineers, cybersecurity analysts, information security officers, Security Operations Centre (SOC) personnel, cloud infrastructure administrators, DevOps and platform support engineers, database and application support administrators, ICT officers in government and the public sector, and technical support and IT operations teams. It also suits organisations building internal capacity in secure Linux infrastructure management.

**RECOMMENDED ENTRY LEVEL**

Basic computer and operating system knowledge, familiarity with general IT infrastructure concepts and a basic understanding of IP addressing and networking. Experience in IT support, technical operations or systems administration is an advantage, and basic command line experience helps but is not required. No advanced Linux qualification is needed. Delegates need a laptop with at least 8 GB of RAM (16 GB recommended for local virtual machines), free storage, a terminal or SSH client and virtualisation software or access to a hosted laboratory, with administrative rights to install approved training software. The programme is professional development and does not award vendor certification or a formal occupational qualification.

## Course modules at a glance

| Module | Topic | Main competency |
|---|---|---|
| **01** | Linux Fundamentals and the Command Line | Navigates Linux and performs essential command line administration tasks. |
| **02** | Users, Permissions and Access Management | Manages accounts, enforces permissions and secures administrative access. |
| **03** | Managing Services, Processes, Storage and System Logs | Administers services, manages resources and troubleshoots server problems. |
| **04** | Linux Networking and System Hardening | Configures networking, secures remote access and applies hardening controls. |
| **05** | Updates, Patching, Backups and Recovery | Patches, backs up, restores and verifies a secured Linux server. |

## The 5 day programme

Each training day runs 08:30 to 16:00 with morning and afternoon breaks and a lunch break. Timings can be adjusted to suit an in house group or a client's shift pattern.

## Day 1: Linux operating system foundations

| Time | Session | Key topics | Activity |
|---|---|---|---|
| **08:30 to 10:30** | Module 1: Introduction to Linux server administration, installation and initial configuration | Linux and open source, enterprise adoption, Linux in cloud and data centres, Ubuntu Server, Debian, Red Hat Enterprise Linux and Rocky Linux, kernel, shell and utilities, server roles, installation requirements, virtual machine preparation, hostnames, basic network configuration, root and standard accounts, initial updates, secure deployment practices | Instructor demonstration: server installation |
| **10:30 to 10:45** | Morning tea break | | |
| **10:45 to 12:30** | Module 1: The Linux file system and essential commands | Directory hierarchy including /etc, /home, /var, /usr, /tmp, /boot and /root, absolute and relative paths, creating, copying, moving and deleting files, searching, hidden and configuration files, Bash, command syntax and options, searching and filtering text, redirection, pipelines, shell history, manual pages | Guided command line exercises |
| **12:30 to 13:30** | Lunch break | | |
| **13:30 to 15:00** | Module 1: Working with text editors and Day 1 laboratory | Nano and Vim, safe editing of configuration files, saving and exiting, search and replace, accessing a Linux server, exploring the directory structure, file and directory operations | Practical laboratory |
| **15:00 to 15:15** | Afternoon tea break | | |
| **15:15 to 16:00** | Practical exercises, troubleshooting and daily review | Search and text processing commands, collecting basic system information, review of the day | Daily knowledge check |

**WHAT DELEGATES TAKE AWAY FROM DAY 1**

- Navigate the Linux directory structure with confidence.
- Perform essential file, directory and text processing tasks at the command line.
- Edit configuration files safely with Nano and Vim.

## Day 2: User administration and access security

| Time | Session | Key topics | Activity |
|---|---|---|---|
| **08:30 to 10:30** | Module 2: Linux user account administration and group management | Root, system and standard accounts, creating, modifying, disabling and deleting accounts, home directories, user and group IDs, account expiration and password management, primary and supplementary groups, group based access, role based administrative practices | Instructor demonstration: account and group administration |
| **10:30 to 10:45** | Morning tea break | | |

| Time | Session | Key topics | Activity |
|---|---|---|---|
| **10:45 to 12:30** | Module 2: File ownership, permissions and privileged access management | Read, write and execute permissions, numeric and symbolic modes, chmod, chown and chgrp, umask, SUID, SGID and sticky bits, Access Control Lists, correcting insecure permissions, risks of unrestricted root access, sudo and the sudoers file, least privilege, access reviews | Guided permissions and sudo exercises |
| **12:30 to 13:30** | Lunch break | | |
| **13:30 to 15:00** | Module 2: Linux authentication security and Day 2 laboratory | Password policy, aging and expiration, account lockout, Pluggable Authentication Modules (PAM), SSH key based authentication, failed login review, inactive accounts; creating users and groups, applying permissions, configuring sudo | Practical laboratory |
| **15:00 to 15:15** | Afternoon tea break | | |
| **15:15 to 16:00** | Practical exercises, troubleshooting and daily review | Implementing account security policies, configuring SSH keys, reviewing authentication records, correcting deliberately misconfigured permissions, review of the day | Daily knowledge check |

**WHAT DELEGATES TAKE AWAY FROM DAY 2**

- Create and manage user accounts, groups and group membership.
- Apply correct ownership, permissions and least privilege sudo access.
- Configure SSH key based authentication and review authentication records.

## Day 3: Linux server operations and maintenance

| Time | Session | Key topics | Activity |
|---|---|---|---|
| **08:30 to 10:30** | Module 3: Process management and Linux services | Processes and PIDs, foreground and background jobs, ps and top, priorities and signals, excessive CPU and memory use, unresponsive processes, systemd and systemctl, starting, stopping, enabling and disabling services, units, failed services, service dependencies | Instructor demonstration: service and process management |
| **10:30 to 10:45** | Morning tea break | | |
| **10:45 to 12:30** | Module 3: Software packages and storage administration | APT and DNF, installing and removing packages, repositories, versions and dependencies, secure installation practices, disks and partitions, ext4 and XFS, creating and mounting file systems, /etc/fstab, Logical Volume Management (LVM), disk utilisation | Guided package and storage exercises |
| **12:30 to 13:30** | Lunch break | | |
| **13:30 to 15:00** | Module 3: Performance monitoring, logging and Day 3 laboratory | CPU, memory, swap and disk monitoring, load averages, uptime, bottlenecks, capacity planning, systemd journald and rsyslog, journalctl, authentication and service logs, log rotation, abnormal events; installing and managing a service, monitoring processes | Practical laboratory |

| Time | Session | Key topics | Activity |
|---|---|---|---|
| **15:00 to 15:15** | Afternoon tea break | | |
| **15:15 to 16:00** | Practical exercises, troubleshooting and daily review | Inspecting storage and file systems, configuring a test mount, reviewing system and authentication logs, troubleshooting simulated service failures, review of the day | Daily knowledge check |

**WHAT DELEGATES TAKE AWAY FROM DAY 3**

- Manage services and processes with systemd and standard tools.
- Inspect storage, mount file systems and monitor server resources.
- Use system and authentication logs to troubleshoot server failures.

## Day 4: Network security and hardening controls

| Time | Session | Key topics | Activity |
|---|---|---|---|
| **08:30 to 10:30** | Module 4: Linux networking fundamentals, configuration and troubleshooting | TCP/IP, IP addresses and subnet masks, gateways and routing, interfaces, static and dynamic addressing, DNS and name resolution, ports and protocols, service exposure, the ip command, ping, listening ports with ss, routing tables, DNS troubleshooting, traffic inspection | Instructor demonstration: network inspection |
| **10:30 to 10:45** | Morning tea break | | |
| **10:45 to 12:30** | Module 4: Server hardening principles and securing SSH remote access | Operating system hardening, common Linux threats, risks of default configurations, attack surfaces, defence in depth, least privilege, introduction to CIS Benchmarks, secure configuration baselines, SSH configuration review, restricting root login, key based authentication, limiting access to authorised users, SSH log review | Guided SSH hardening exercise |
| **12:30 to 13:30** | Lunch break | | |
| **13:30 to 15:00** | Module 4: Host based firewalls, additional hardening controls and Day 4 laboratory | UFW and firewalld, rules and access policies, restricting ports, default deny inbound, keeping administrative access during changes, disabling services, removing unused packages, protecting sensitive files, SELinux and AppArmor, secure mount options, auditd, documenting hardening | Practical laboratory |
| **15:00 to 15:15** | Afternoon tea break | | |
| **15:15 to 16:00** | Practical exercises, troubleshooting and daily review | Identifying server weaknesses, applying firewall restrictions, correcting insecure permissions, applying selected hardening controls, verifying server functionality after hardening, review of the day | Daily knowledge check |

**WHAT DELEGATES TAKE AWAY FROM DAY 4**

- Configure and troubleshoot Linux networking and identify listening services.
- Secure SSH remote administration and apply host based firewall rules.
- Apply hardening controls and verify the server still works afterwards.

## Day 5: Security maintenance and final practical assessment

| Time | Session | Key topics | Activity |
|---|---|---|---|
| **08:30 to 10:30** | Module 5: Security updates, patch management and backup administration | Software vulnerabilities, outdated packages, applying updates, repositories, kernel updates, maintenance windows, automated security updates, reboot requirements, patch records, full, incremental and differential backups, RPO and RTO, tar and rsync, scheduled backups, protecting backups, off server and offline copies, backup integrity | Instructor demonstration: patching and backup |
| **10:30 to 10:45** | Morning tea break | | |
| **10:45 to 12:30** | Module 5: System restoration, recovery and preventive maintenance | Recovery procedures, restoring files and configuration, verifying restored data, failed recovery troubleshooting, recovery checklists, performance and authentication reviews, unusual processes, firewall and service checks, scheduled tasks, routine security checks, maintenance schedules | Guided backup and restore exercise |
| **12:30 to 13:30** | Lunch break | | |
| **13:30 to 15:00** | Final practical laboratory: Linux server setup and hardening | Initial configuration, user and group administration, permissions and privileged access, service management, storage and resource checks, network verification, SSH security, firewall rules, disabling unnecessary services, security patching | Integrated practical assessment |
| **15:00 to 15:15** | Afternoon tea break | | |
| **15:15 to 16:00** | Final laboratory completion and programme review | Backup creation and test restoration, log inspection, final security verification, server hardening checklist and technical report, programme review | Final assessment and close |

**WHAT DELEGATES TAKE AWAY FROM DAY 5**

- Apply and verify security updates within a planned maintenance process.
- Create, protect and test restore backups against recovery objectives.
- Administer, harden and verify a complete Linux server and document the result.

## How the course is taught

The programme is run as practical, competency based training rather than a series of presentations, so delegates rehearse the tasks they are expected to perform in their own working environment. Methods used include:

- Instructor led technical presentations
- Live demonstrations
- Hands on practical laboratories in isolated Linux server environments
- Real world technical scenarios
- Security hardening workshops
- Daily knowledge checks
- Final integrated practical assessment
- Approximately 40% theory and demonstrations and 60% practical activity

## How delegates are assessed

### Formative

- Daily practical exercises (40%)
- Technical knowledge checks (20%)

### Practical

- Final server administration and hardening laboratory (40%)

### Certification

- Certificate of Attendance issued by BMC Training to delegates who meet the attendance requirements

## Dates, venues and fees

The programme runs at 12 scheduled dates across the BMC Training network. Every date below is open for registration.

| Dates | Venue | Days | Fee per delegate |
|---|---|---|---|
| **23 to 27 Nov 2026** | Accra | 5 days | US$1,800 |
| **30 Nov to 4 Dec 2026** | Lagos | 5 days | US$1,800 |
| **7 to 11 Dec 2026** | Dubai | 5 days | US$1,800 |
| **22 to 26 Feb 2027** | Harare | 5 days | US$1,800 |
| **2 to 6 Aug 2027** | Pretoria | 5 days | R18,000 |
| **16 to 20 Aug 2027** | Nairobi | 5 days | US$1,800 |
| **23 to 27 Aug 2027** | Dar es Salaam | 5 days | US$1,800 |
| **30 Aug to 3 Sep 2027** | Lusaka | 5 days | US$1,800 |
| **6 to 10 Sep 2027** | Online | 5 days | US$900 |
| **13 to 17 Sep 2027** | Johannesburg | 5 days | R18,000 |
| **27 Sep to 1 Oct 2027** | Cape Town | 5 days | R18,000 |
| **4 to 8 Oct 2027** | Durban | 5 days | R18,000 |

Fees are per delegate. South African venues are priced in rand; other locations and live online in US dollars. Fees exclude 15% VAT where applicable. Group bookings of three or more delegates from the same organisation qualify for a reduced rate. This course is also available as in house training, delivered at your own site on dates that suit your operation.

## To book or request a quotation

Email registration@bmctrainings.org, WhatsApp +27 68 540 3736 or call +27 71 443 2071. Full course details and the live calendar are at www.bmctrainings.org.