ORIGIN ACADEMY · COURSE SYLLABUS

Linux Administration

Run production Linux: the shell and text tools, users and permissions, systemd and the boot process, networking, storage, containers, automation and troubleshooting.

18 weeks · about 12 hours a week · live cohort of up to 10
Curriculum last updated 19 November 2026

Availability

This course opens soon. Join the waitlist on the course page to hear first about dates and prices.

Before you start

- No Linux experience needed
- Comfortable using a computer and installing software
- English good enough to follow technical documentation and live sessions: about a credit (C6 or better) in WASSCE or NECO English Language, or an equivalent such as KCSE or IGCSE English (roughly CEFR level B1). You don't need the certificate: Phase 0 is free, so you can check for yourself
- A laptop running Linux, macOS, or Windows with WSL

How the course works

- A live cohort of up to 10 students, with a mentor.
- At least half your time is hands-on: every module ends with a lab.
- Live sessions are recorded, so you can rewatch them or catch up.
- Questions between sessions are answered within 24 hours on weekdays.
- A mentor reviews every phase project, like a pull request at work.

Phase 0 is free for everyone, before you enroll.

Curriculum

PHASE 0 · WEEKS 1–2 · FREE

Linux Foundations

The shell, the filesystem hierarchy, files and links, editors and getting help.

- What Linux is: kernel, distributions and the shell
- Navigating the filesystem hierarchy
- Files, links, archives and compression
- Editing files with Vim and nano
- Getting help: man, --help and tldr

You build: Set up and document your own server

PHASE 1 · WEEK 3

Text Processing & Pipelines

Redirects, pipes and the text toolkit: grep, sed, awk, sort, cut and friends.

- stdin, stdout, stderr and redirects
- Pipes and tee
- grep and regular expressions
- sed and awk
- sort, uniq, cut, tr, wc and paste

You build: Log report built from one-line pipelines

PHASE 2 · WEEKS 4–5

Users, Groups & Permissions

Ownership, modes, sudo, ACLs and the principle of least privilege.

- Users and groups
- File permissions and ownership
- sudo and the super user
- ACLs and special permission bits
- Authentication logs and least privilege

You build: Multi-user team server with shared directories

PHASE 3 · WEEKS 6–7

Processes, systemd & Boot

How Linux boots, the process lifecycle, signals, priorities and resource limits, systemd units, timers and journald.

- The boot process: firmware, GRUB, kernel and init
- Processes, forking and job control
- Signals, priorities and ulimits
- systemd units, services and timers
- Logs with journald

You build: Hardened systemd service with log rotation

PHASE 4 · WEEKS 8–9

Networking & Firewalls

TCP/IP, subnetting, DNS and DHCP, routing, ip/ss tools, packet capture, nftables and SSH hardening.

- TCP/IP, IP addressing and subnetting
- DNS and DHCP
- Routing, ip and ss
- ping, traceroute and tcpdump
- Netfilter and nftables
- SSH keys and hardening

You build: Locked-down web server behind a firewall

PHASE 5 · WEEKS 10–11

Storage & Backups

Disks and partitions, filesystems, inodes and mounts, LVM, RAID, swap and tested restores.

- Disks, partitions and filesystems
- Inodes, mounts and fstab
- LVM and RAID
- Swap and memory pressure
- Backups you have actually restored

You build: Backup and disaster-recovery runbook

PHASE 6 · WEEK 12

Containers & cgroups

Namespaces and cgroups, container runtimes, Docker and running containers as services.

- Namespaces and cgroups
- Container runtimes and images
- Docker for administrators
- Containers as systemd services

You build: Containerised app run by systemd with resource limits

PHASE 7 · WEEKS 13–15

Shell Scripting & Automation

Bash scripting, scheduling, Git, and configuration management with Ansible.

- Bash variables, conditionals and loops
- Functions, exit codes and safe scripts
- Scheduling with cron and systemd timers
- Ansible inventories, playbooks and roles

You build: Ansible playbook that builds a server from scratch

PHASE 8 · WEEK 16

Security, Monitoring & Troubleshooting

Patching, auditd, fail2ban and CIS benchmarks, metrics with Prometheus, a method for finding what's wrong, the debugging toolkit, and software licences.

- Patching and package hygiene
- Hardening with CIS benchmarks
- auditd and fail2ban
- Metrics and alerts with Prometheus
- A troubleshooting method: uptime, load, memory, disk, network
- The debugging toolkit: strace, ltrace, gdb, perf and Valgrind
- Open-source licences: what admins need to know

You build: Security audit report on a live system

PHASE 9 · WEEKS 17–18

Capstone

Operate a multi-server environment through planned changes and incidents.

- Environment build-out
- Planned changes with rollback plans
- Incident drills and post-mortems
- Handover and review

You build: Production-style environment with on-call handover

Your certificate

You earn it by doing two things:

- Attend every live session. If you miss one, make it up by watching the recording and submitting that week's lab within 7 days. You can do this up to 2 times per course.
- Score more than 50% on the final evaluation at the end of the course.

Your Enterprise Readiness Rating is separate: it scores your projects, capstone and assessments so employers can see how job-ready you are.

Questions

Email academy@originclouds.io, or see the course online: https://academy.originclouds.io/courses/linux-administration