



BTECH TRAINING

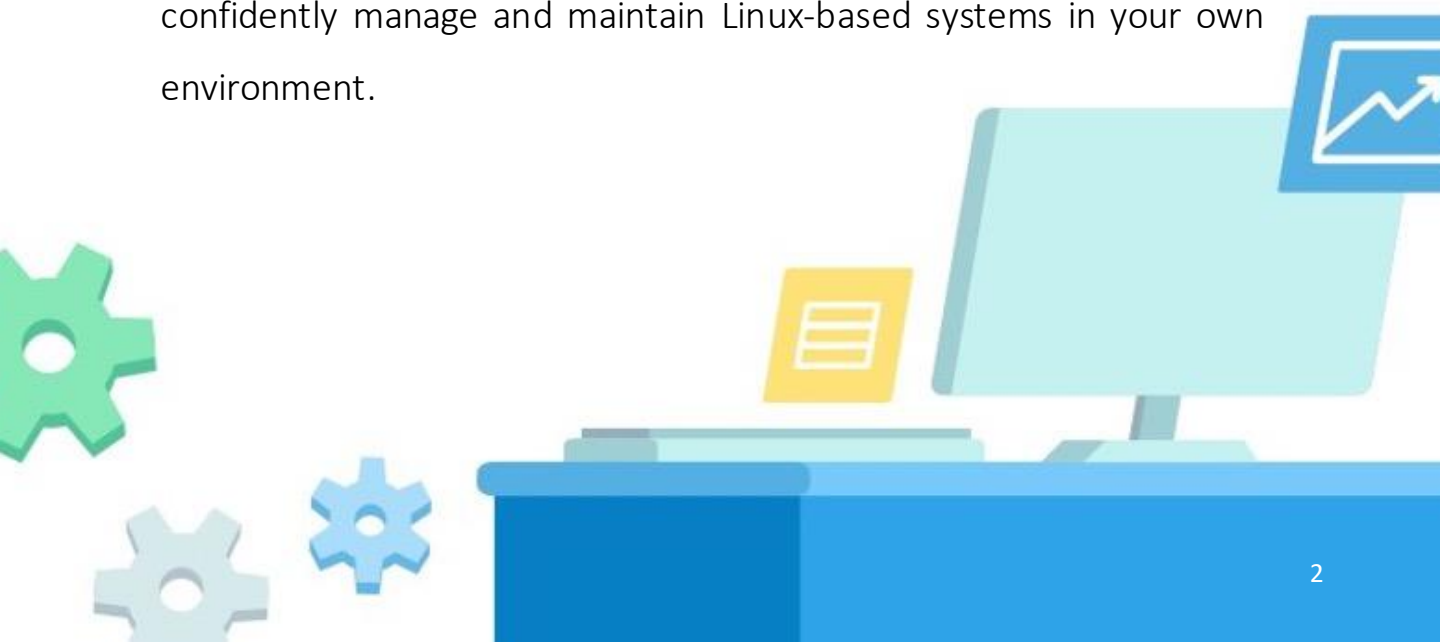
Study Plan Linux System Administration (LF-ADM)



About This Course

This course teaches fundamental concepts and techniques for effectively managing and maintaining Linux-based systems. It covers various topics, including Linux File System Tree Layout, Signal and Processes, Package Management Systems, System Monitoring, Process Monitoring, I/O Tuning and Scheduling, Advanced Storage, Kernel Service and Configuration, User and Group Management, Networking, Security (Firewall), Virtualization and Container Overview. With practical exercises and quizzes, this course offers a comprehensive and hands-on learning experience, allowing students to apply their knowledge and develop their skills.

Upon completion of the course, you will have a solid understanding of Linux system administration concepts and will be able to confidently manage and maintain Linux-based systems in your own environment.



Summary



Training Duration: 32 Hours (4 Days)

Course Main Subjects

- Linux File System Tree Layout
- Signal & Processes
- Package Management Systems
- System Monitoring
- Process Monitoring
- I/O Tuning & Scheduling
- Advanced Storage
- Kernel Service & Configuration
- User & Group Management
- Networking
- Security (Firewall)
- Virtualization & Container Overview
- LFCS Internal Exam



Target Audience

System Administrators, Cloud Administrators, Developers, Site Reliability Engineer.

Prerequisites

Linux IT Associate (LF-ASC)

Learning Output

The learning topics will assist participants in :

1. Solid understanding of Linux system administration concepts and techniques
2. Gain hands-on experience through practical exercises and assignments
3. Manage and maintain Linux-based systems confidently

Requirements

Have a laptop/computer with min. specifications and installed tools:

Operating System	Windows, Linux, or MacOs
Processor	Intel Core i3
Memory	4 GB RAM
SSH Client	Termius / Putty / MobaXTerm
Text Editor	Sublime Text / VSCode
Browser	Chrome and Firefox

Facilities

- Virtual machine (available until H+3 post training)
- Class materials
- Certificate
- Recording (VITL)

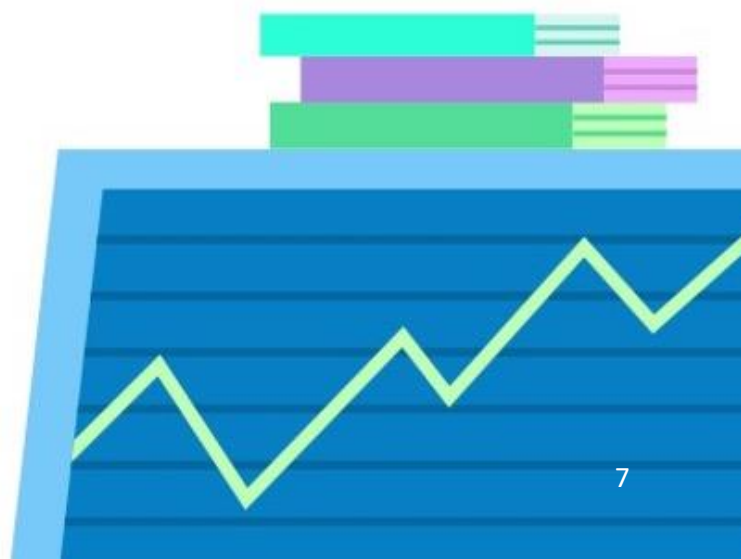
Certification

- Certificate of Course Completion
- Btech Internal Exam (optional)



Learning Strategies

- Theory
- Study Case
- Pre-Test & Post-Test
- Quiz / Internal Exam
- Hands-on Lab



Training Topology



Learning Modules

Training Plan	
Topic	Outcome
1. Course Introduction	<ul style="list-style-type: none"> • Understand the concept of configuring and managing Linux systems for an enterprise environment. • Evaluate the advantages and disadvantages of using command line and graphical interfaces in Linux administration. • Identify and differentiate three main Linux distributions such as RHEL, SUSE, and Debian.
2. Linux Filesystem Tree Layout	<ul style="list-style-type: none"> • Understand the concept of one big filesystem in Linux. • Identify data distinctions within the Linux filesystem, such as user data, system data, and configuration files. • Recognize the FHS (Filesystem Hierarchy Standard) Linux Standard Directory Tree and its purpose in organizing the file system. • Comprehend the purpose of key directories within the Linux file system

3. Process	<ul style="list-style-type: none">• Understand the difference between a program and a process, and identify process attributes such as PID and process state.• Comprehend process resource isolation, control processes with ulimit, and limit resources like CPU time and memory.• Create processes with system calls like fork() and exec(), recognize process states and execution modes, including daemons, and modify process priorities using nice.• Use nice to control CPU usage and prioritize processes.• Recognize shared library versions, use commands like ldd and ldconfig to find shared libraries, and understand the role of static and shared libraries in software development.
4. Signals	<ul style="list-style-type: none">• Understand signals in Linux and their purpose in communicating with processes.• Identify types of signals and their default actions.• Use the kill command to send signals to processes by specifying the PID or process group ID.• Use killall and pkill commands to send signals to processes by name or criteria.• Use signals appropriately to manage processes and understand their potential consequences.

5. Package Management System	<ul style="list-style-type: none">• Understand the purpose of package management systems in Linux and their benefits.• Identify software packaging concepts such as dependencies, versioning, and package types such as source and binary packages.• Recognize available package management systems in Linux, including APT, YUM, DNF, and Zypper, and their differences.• Understand the levels and varieties of packaging tools, such as high-level tools and low-level tools, and their roles in package management.• Recognize package sources, including repositories, packages from the web, and packages from source code.• Create software packages and understand the importance of revision control systems like Git.• Understand how Git works and how it is used in managing software development in Linux.
6. DPKG	<ul style="list-style-type: none">• Understand the essentials of DPKG, the Debian package management system, including package file names and sources.• Use DPKG queries to gather information about installed packages and their dependencies.• Install, upgrade, and uninstall packages using DPKG.• Practice using DPKG through hands-on labs and quizzes.• Develop proficiency in managing packages using DPKG in a Linux environment.

7. APT	<ul style="list-style-type: none">• Recognize the various APT commands such as apt, apt-get, apt-cache, and others, and their purposes.• Use APT queries to gather information about installed packages and their dependencies.• Install, remove, and upgrade packages using APT.• Clean up and manage package dependencies using APT commands.
8. System Monitoring	<ul style="list-style-type: none">• Understand system monitoring and its importance in Linux system administration.• Recognize different system monitoring tools and their purposes.• Learn to use sar, a popular system monitoring tool in Linux, to gather and analyze system performance data.• Understand the significance of log files and their role in system monitoring and troubleshooting.• Use log files to identify system issues, track system events, and perform root cause analysis.
9. I/O Monitoring and Tuning	<ul style="list-style-type: none">• Understand the importance of I/O monitoring and tuning in Linux system administration.• Learn to use iostat to gather and analyze I/O performance data.• Recognize the role of iotop in identifying I/O-intensive processes and ionice in controlling the I/O priority of processes.• Use iostat, iotop, and ionice to troubleshoot and resolve I/O performance issues in a Linux environment.

10. I/O Scheduling	<ul style="list-style-type: none">• Recognize the impact of disk bottlenecks on I/O performance and the need for I/O scheduling.• Understand the different I/O scheduler choices available in Linux and their respective strengths and weaknesses.
11. Linux Filesystems and the VFS	<ul style="list-style-type: none">• Understand the basics of Linux filesystems, including inodes and hard/soft links.• Recognize the role of the Virtual Filesystem (VFS) in providing a unified interface to various filesystems.• Learn about the different filesystem varieties available in Linux, including their advantages and disadvantages.• Understand the concept of journaling filesystems and their benefits for data integrity.• Recognize the role of special filesystems, such as tmpfs and procfs, in providing access to system resources and information.
12. Disk Partitioning	<ul style="list-style-type: none">• Understand the different types of disks available and how disk geometry affects partitioning.• Recognize the importance of partitioning disks and understand the different partitioning schemes available.• Learn how to name disk devices and device nodes using utilities such as blkid and lsblk.• Understand how to size up partitions and back up/restore partition tables using appropriate tools.• Learn how to use partition table editors, such as fdisk, to create, modify, and delete disk partitions.

<p>13. Filesystem Features: Attributes, Creating, Checking, Mounting</p>	<ul style="list-style-type: none">• Setting and modifying filesystem attributes using lsattr and chattr.• Creating a filesystem using mkfs.• Checking and repairing a filesystem with fsck.• Mounting a filesystem using mount and unmounting using umount.• Configuring automatic filesystem mounting, including mounting at boot and with the automount feature, and working with network shares using NFS.
<p>14. Linux Filesystems and the VFS</p>	<ul style="list-style-type: none">• Monitoring disk usage and space with df and disk usage with du• Using swap partition for virtual memory• Setting up and monitoring filesystem quotas• Understanding the purpose of quotacheck and turning quotas on and off• Setting quotas for users or groups on a filesystem.
<p>15. The EXT4 Filesystems</p>	<ul style="list-style-type: none">• Understand the basic concepts and characteristics of the EXT4 filesystem.• Learn about the structure of the ext4 filesystem, including the superblock and block groups.• Know how to use the dumpe2fs tool to view information about an ext4 filesystem.• Learn how to use the tune2fs tool to modify various parameters of an ext4 filesystem.• Be able to apply this knowledge to manage and optimize ext4 filesystems in a Linux environment.

16. The XFS and BTRFS Filesystems	<ul style="list-style-type: none">• Describe the features and benefits of XFS and btrfs as file systems in Linux.• Understand XFS and btrfs as alternatives to traditional file systems and learn about their respective strengths and weaknesses.
17. Encrypting Disks	<ul style="list-style-type: none">• Understand the reasons for using disk encryption.• Know the basics of LUKS and Cryptsetup for setting up encryption.• Learn how to create an encrypted partition.• Learn how to mount an encrypted partition and set it to mount at boot.• Understand the risks and limitations of disk encryption.
18. Logical Volume Management	<ul style="list-style-type: none">• Understand the basics of Logical Volume Management (LVM).• Know how to manage volumes and volume groups using LVM utilities.• Be able to create, display and resize logical volumes.• Understand the concept of LVM snapshots and how to create them.• Understand the benefits and use cases of LVM in managing storage on Linux systems.

19. RAID	<ul style="list-style-type: none">• Understand the concept of RAID and the various RAID levels.• Configure software RAID on Linux systems.• Monitor RAID arrays to ensure their health and availability.• Set up RAID hot spares to ensure high availability and fast recovery in case of disk failures.• Identify and troubleshoot common issues with RAID arrays.
20. Kernel Services and Configuration	<ul style="list-style-type: none">• Understanding the kernel and its role in the operating system.• Modifying kernel parameters through the command line.• Configuring the kernel boot process.• Using Sysctl to view and modify kernel parameters at runtime.• Troubleshooting kernel-related issues.
21. Virtualization Overview	<ul style="list-style-type: none">• Understand the concept and history of virtualization, including the difference between emulation and virtualization.• Learn about the types of virtualization hypervisors, including dedicated hypervisors and hypervisors in the kernel.• Know how to use libvirt to manage virtualization.• Understand the basics of QEMU and third-party hypervisor integration.• Learn how to manage KVM, including creating and managing virtual machines.

22. Containers Overview	<ul style="list-style-type: none">• Understand the basic concept and purpose of containers as a form of application virtualization.• Differentiate between containers and virtual machines, and know when to use each technology.• Be familiar with Docker, including its components and basic commands.• Understand how to build, run and manage Docker containers.• Be familiar with Podman, an alternative container runtime to Docker.
23. User Account Management	<ul style="list-style-type: none">• Understanding user accounts and their attributes.• Creating, modifying, and deleting user accounts using useradd.• Securing user accounts with password management tools, such as chage.• Managing user access through restricted shells and accounts.• Configuring SSH and remote graphical login for secure access to the system.
24. Group Management	<ul style="list-style-type: none">• Understanding the concept of groups and their importance in Linux systems.• Managing groups and group membership using command-line tools.• Creating and managing user private groups to limit access and improve security.• Understanding how users are assigned to groups and how to modify their membership.• Implementing proper group management practices to maintain security and organization in Linux systems.

25. File Permissions and Ownership	<ul style="list-style-type: none">• Understand the concept of ownership and permissions for files and directories.• Learn how to use chmod to set permissions for files and directories.• Understand how to use chown and chgrp to change the ownership of files and directories.• Learn how to use umask to set the default permissions for new files and directories.• Understand the concept of filesystem ACLs and how to use them to set more fine-grained access control for files and directories.
26. Pluggable Authentication Module (PAM)	<ul style="list-style-type: none">• Understand what Pluggable Authentication Modules (PAM) are and their role in authentication.• Understand the PAM configuration files and their functions.• Understand PAM rules and how they are used for authentication.• Understand how to configure LDAP authentication using PAM.• Understand how to troubleshoot PAM issues.
27. Network Adresses	<ul style="list-style-type: none">• Understanding IP Addresses and their purpose in networking.• Recognizing the difference between IPv4 and IPv6 address types and their uses.• Identifying reserved IP addresses and their significance in networking.• Understanding the concept of netmasks and how they are used to determine network boundaries.• Learning how to get and set the hostname of a system for network identification.

28. Network Devices and Configuration	<ul style="list-style-type: none">• Identify common network devices and their functionalities.• Use the "ip" command to manage network devices and configurations.• Configure NICs and predictably name network devices using configuration files.• Utilize Network Manager to manage interfaces and network settings.• Troubleshoot network issues using diagnostic tools like nmtui, nmcli, and DNS resolution.
29. Firewalls	<ul style="list-style-type: none">• Understand what a firewall is and how it works.• Learn about packet filtering and the different generations of firewalls.• Understand firewall interfaces and tools, including firewalld and firewall-cmd.• Learn about zones, source management, service management, and port management in firewalld.• Learn how to manage firewalld zones, including status checks and management examples.
30. System Startup and Shutdown	<ul style="list-style-type: none">• Understand the boot sequence and the role of BIOS in the boot process.• Learn about boot loaders and how to configure them.• Recognize important system configuration files and their functions.• Understand the purpose of the /etc/sysconfig and /etc/default directories.• Know the proper way to shutdown and reboot the system.

31. GRUB	<ul style="list-style-type: none">• Learn about GRUB (Grand Unified Bootloader) and its importance as the default bootloader in most Linux distributions.• Understand the different versions of GRUB and the features they offer.• Learn how to interact with GRUB during boot time to perform various actions, such as selecting a different operating system or booting in different modes.• Know how to install GRUB and the importance of GRUB device nomenclature.• Understand GRUB configuration files and how to configure them, as well as the newer Boot Loader Specification Configuration (BLSCFG) and the <code>/boot/loader/entries</code> directory.
32. System Init: Systemd, Systemv and Upstart	<ul style="list-style-type: none">• Understand the role of the init process in system startup.• Compare and contrast different system startup alternatives: System V, Upstart, and systemd.• Learn the features of systemd, including the use of unit files and targets.• Understand the systemd configuration files, including the use of <code>.service</code>, <code>.target</code>, and <code>.timer</code> files.• Know how to use the <code>systemctl</code> command to manage systemd services, including starting, stopping, and restarting services, viewing the status of services, and enabling or disabling services at boot time.

33. Backup and Recovery Methods	<ul style="list-style-type: none">• Understand the importance of backups and the difference between backup and archive.• Know the different backup methods and backup strategies.• Understand the utilities and programs that can be used for backups, such as tar, rsync, and cpio.• Know how to use tar for backups, restoring files, and incremental backups.• Understand archive compression methods and the use of dd for backups.
34. Basic Troubleshooting	<ul style="list-style-type: none">• Identify troubleshooting levels and when to use them.• Use basic troubleshooting techniques to diagnose and resolve issues.• Troubleshoot networking issues by checking relevant configurations and connectivity.• Check file integrity and use recovery tools to address filesystem corruption.• Understand how to use virtual consoles for troubleshooting and resolving issues with the graphical user interface.
35. System Rescue	<ul style="list-style-type: none">• Understand the importance of system rescue in troubleshooting.• Learn how to create rescue media for troubleshooting.• Explore different system rescue options such as emergency boot media, rescue image, and single-user mode.• Understand how to use rescue media for system recovery and troubleshooting.• Learn how to troubleshoot and recover from common issues such as filesystem corruption and boot process failures.

Thank You

Another Course :

<https://adinusa.id/pro-training>