



# 55187- Linux System Administration 16 Level 3 for Windows

Course ID #: 1313-307-16-W

Hours: 28

## Course Content

### Course Description:

This hands-on 4-day Linux System Administration course teaches attendees how to administer, configure and upgrade Linux systems running one of the three major Linux distribution families (Red Hat, SUSE, Debian/Ubuntu). Focused on enterprise environments, it provides Linux system administrators with all the tools and concepts needed to efficiently build and manage a production Linux infrastructure. This course presents state-of-the-art techniques used in the industry and applies them in the context of practical labs.

Linux Foundation Certification Preparation

### At Course Completion:

After completing this course, student will be able to:

- Perform essential Linux commands such as installation, searches and manipulating files.
- Operate running Linux systems by managing the boot process, scheduling jobs, updating the system, monitoring system performance and managing security.
- Manage users and groups by adding/deleting/modifying, configuring LDAP and PAM, modifying user processes and resources.
- Ensure network performance via configuration, monitoring, tunnelling and routing of traffic.
- Configure services such as DNS, shares, SSH and SELinux/AppArmor as well as servers for DHCP and HTTP.
- Manage system storage by using partitions, logical volumes, physical volumes, ACLs, quotas and clustering

### Target Student:

This course is intended for System administrators and users who already have at least some basic exposure to Linux or another UNIX-based operating system constitute the target audience for this class. Anyone who is looking to acquire practical knowledge in the field of system administration in enterprise environments will save significant time by attending this course. It should also be considered a necessary step to be taken by anyone considering more advanced classes in our System Administration curriculum track. The concepts covered provide important building blocks for anyone looking to attend more advanced classes, in particular LFS311: Linux Network Management.



# 55187- Linux System Administration 16 Level 3 for Windows

Course ID #: 1313-307-16-W

Hours: 28

## Prerequisites:

- Knowledge of the basic components of Linux.
- Familiarity with text editors (emacs, VI).
- Working knowledge of Bash scripting.
- Attendees should already have prior exposure to a Linux or UNIX system and practical experience with the command line interface at a level that is equivalent to what is covered in our free LFS101x - Introduction to Linux course (available on edX.org). Basic tools such as text editors, file utilities and basic tasks are assumed to be well-understood prior to this course.

## Topics:

### Module 1: Introduction

This module defines the organization responsible for Linux and explains how it promotes, protects, and advances Linux.

#### Lessons

- Linux Foundation
- Linux Foundation Training
- Linux Foundation Certifications
- Laboratory Exercises, Solutions and Resources
- E-Learning Course: LFS201
- Distribution Details

After completing this module, students will be able to:

- Describe the mission of The Linux Foundation and its role in the Linux and Open Source community.
- Configure the system for safe use via the sudo command.

### Module 2: Linux Filesystem Tree Layout

This module explains how the Linux Filesystem is organized and points out the key directories and their roles.

#### Lessons

- Data Distinctions
- FHS Linux Standard Directory Tree
- root (/) directory
- /bin
- /boot
- /dev
- /etc
- /home
- /lib and /lib64
- /media
- /mnt
- /opt
- /proc
- /sys
- /root
- /sbin
- /srv
- /tmp
- /usr
- /var
- /run



# 55187- Linux System Administration 16 Level 3 for Windows

Course ID #: 1313-307-16-W

Hours: 28

After completing this module, students will be able to:

- Describe how the Linux Filesystem is set up.
- Demonstrate knowledge of how the key directories work.

## Module 3: Processes

This module explains how to work with Linux processes. It begins with an overview of what processes are and how they work before proceeding to illustrate how to create, monitor, prioritize and limit processes.

### Lessons

- Programs and Processes
- Process Limits
- Creating Processes
- Process States
- Execution Modes
- Daemons
- niceness
- Libraries
- Signals

After completing this module, students will be able to:

- Describe the role of processes in Linux and how they relate to programs.
- Identify the different states processes can take.
- Monitor and limit processes.
- Set process priority using niceness values

## Module 4: Package Management Systems

This module explains how to work with the major package management systems used in Linux distributions. Covers both RPM and DKPG as well as the use of version control systems such as git.

### Lessons

- Software Packaging Concepts
- RPM (Red Hat Package Manager)
- DPKG (Debian Package)
- Revision Control Systems

After completing this module, students will be able to:

- Understand the role and function of package management systems.
- Understand and use RPM.
- Understand and use DKPG.
- Understand the role of revision control systems, particularly git.

## Module 5: Package Installers

This module explains how to use the major package installers, including yum, zypper and APT. It also explains the role that package installers play in automating software management and dealing with dependencies.

### Lessons

- Package Installers
- yum
- zypper
- APT

After completing this module, students will be able to:

- Describe the role that package installers play in managing the software update process.
- Demonstrate proficiency with APT, yum and zipper.



# 55187- Linux System Administration 16 Level 3 for Windows

Course ID #: 1313-307-16-W

Hours: 28

## Module 6: System Monitoring

This module explains how to monitor your Linux system and use tools to test it and report any issues.

### Lessons

- System Monitoring
- Process Monitoring
- Memory Monitoring and Tuning
- Network Monitoring
- I/O Monitoring
- I/O Scheduling \*\*
- System Log Files
- sar \*\*

After completing this module, students will be able to:

- Stress your Linux system and monitor results.
- Monitor the performance of drives and file systems.

## Module 7: Linux Filesystems

This module explains how to work with Linux Filesystems, starting with the understanding that Linux treats everything as a file. IT covers Virtual filesystem (VFS), Filesystem Usage and Attributes, Major types (ext4, XFS, btrfs) and how to create, format, mount, swap and repair Filesystems.

### Lessons

- Filesystem Basics
- Virtual Filesystem (VFS)
- Available Filesystems
- Filesystem Concepts
- Disk and Filesystem Usage
- Extended Attributes
- ext4
- XFS \*\*
- btrfs \*\*

After completing this module, students will be able to:

- Create Filesystems.
- Format Filesystems.
- Mount Filesystems.
- Use swap partitions.
- Manage Filesystem quotas.
- Repair Filesystems.

## Module 8: Partitioning and Formatting Disks

This module explains how to work with disks in Linux by naming, partitioning and sizing them.

### Lessons

- Common Disk Types
- Disk Geometry
- Partitioning
- Naming Disk Devices
- Sizing up partitions
- Partition table editors

After completing this module, students will be able to:

- Partition disks.
- Name disk drives.
- Size partitions.
- Edit partition tables.

## Module 9: More on Linux Filesystems

This module expands on Module 8. It explains how to create, format, mount and check filesystems.

### Lessons

- Creating and formatting filesystems
- Checking and Repairing Filesystems
- Mounting filesystems
- automount
- Swap
- Filesystem Quotas \*\*



# 55187- Linux System Administration 16 Level 3 for Windows

Course ID #: 1313-307-16-W

Hours: 28

After completing this module, students will be able to:

- Create and format a filesystem.
- Repair a filesystem.
- Mount/Unmount a filesystem.
- Understand and set up filesystem quotas.

## Module 10: Encrypting Disks

This module explains how to protect filesystems from prying eyes and protect the data they contain.

### Lessons

- Filesystem Encryption
- LUKS
- Using an Encrypted Partition

After completing this module, students will be able to:

- Provide sound reasons for using encryption and know when it is called for.
- Understand how LUKS operates through the use of cryptsetup.
- Be able to set up and use encrypted filesystems and partitions.
- Know how to configure the system to mount encrypted partitions at boot.

## Module 11: LVM and RAID

This module explains how to work with RAID and Logical Volume Management (LVM).

### Lessons

- Logical Volume Management (LVM)
- Volumes and Volume Groups
- Working with Logical Volumes
- Resizing Logical Volumes
- LVM Snapshots \*\*
- RAID \*\*
- RAID Levels \*\*
- Software RAID Configuration \*\*

After completing this module, students will be able to:

- Understand, configure and monitor RAID.
- Create, resize and utilize Logical Volumes.
- Work with LVM snapshots.

## Module 12: Kernel Services and Configuration

This module explains how the Linux Kernel is configured, how the modules and utilities work, the function of sysctl and udev and Device Management.

### Lessons

- Kernel Overview
- Kernel Configuration
- sysctl
- Kernel Modules
- Module Utilities
- Module Configuration
- udev and Device Management

After completing this module, students will be able to:

- Describe how the Linux Kernel is configured.
- Work with Kernel modules.
- Manage devices.
- Work with udev and sysctl.

## Module 13: Virtualization Overview

This module explains Virtualization, gives a brief history, and shows how to create and install a virtual machine.

### Lessons

- Introduction to Virtualization
- Emulation
- Hypervisors
- libvirt
- QEMU
- KVM



# 55187- Linux System Administration 16 Level 3 for Windows

Course ID #: 1313-307-16-W

Hours: 28

After completing this module, students will be able to:

- Create and install a virtual machine.

## Module 14: Containers Overview

This module explains the basics of what a container is, what application virtualization is, and Docker as an example of container technology.

### Lessons

- Containers
- Docker
- Docker Commands

After completing this module, students will be able to:

- Understand the basics of containers and container applications.
- Install and test a Docker application.

## Module 15: User and Group Account Management

This module explains how to work with users and groups in Linux. It also covers how to work with passwords, restricted shells, the root account, Pluggable Authentication Modules (PAM), LDAP and SSH.

### Lessons

- User Accounts
- Management
- Passwords
- Restricted Shells and Accounts \*\*
- The root Account
- Group Management
- SSH
- PAM (Pluggable Authentication Modules)
- Authentication Process
- Configuring PAM
- LDAP Authentication \*\*

- File Permissions and Ownership

After completing this module, students will be able to:

- Manage users and groups by adding/deleting/modifying them.
- Configure and use LDAP.
- Configure on use PAM.
- Modify user processes and resources.
- Appropriately use the root account.
- Use SSH to securely access remote systems.

## Module 16: Networking

This module explains how to conduct basic networking in Linux. It covers IP addresses, Hostnames, Network Interfaces, Routing and Name Resolution.

### Lessons

- IP Addresses
- Hostnames
- Network Devices
- ip and ifconfig
- Network Configuration Files
- Network Manager
- Routing
- DNS and Hostname Resolution
- Network Diagnostics

After completing this module, students will be able to:

- Explain how IP addresses function.
- Manipulate hostnames.
- Configure network interfaces.
- Route traffic persistently and non-persistently.
- Perform network diagnostics.



# 55187- Linux System Administration 16 Level 3 for Windows

Course ID #: 1313-307-16-W

Hours: 28

## Module 17: Firewalls

This module explains how to work with firewalls in Linux. It covers both command line tools and GUI tools as well as firewalld. Zones and source management are discussed, as is service and port management.

### Lessons

- Firewalls
- Interfaces
- firewalld
- Zones
- Source Management
- Service and Port Management

After completing this module, students will be able to:

- Describe the role and function of firewalls.
- Understand the most commonly use tools.
- Describe the function of zones.
- Implement services on zones.

## Module 18: System Startup and Shutdown

This module explains how to manage startup and shutdown processes in Linux.

### Lessons

- Understanding the Boot Sequence
- System Configuration Files in /etc
- Shutting down/Rebooting the System
- The Grand Unified Boot Loader
- GRUB Configuration Files
- The init Process
- systemd
- SysVinit Startup \*\*
- chkconfig and service \*\*
- Upstart \*\*

After completing this module, students will be able to:

- Manage startup process in Linux.
- Manage shutdown process in Linux.

## Module 19: Backup and Recovery Methods

This module explains how to backup data in Linux. It covers the tools that are used for backup and compression as well as for moving and copying files and also for restoring files.

### Lessons

- Backup Basics
- cpio \*\*
- tar
- Compression: gzip, bzip2 and xz and Backups
- dd
- rsync
- dump and restore \*\*
- mt \*\*
- Backup Programs \*\*

After completing this module, students will be able to:

- Describe the benefits of backup up data.
- Demonstrate proficiency with common backup tools.
- Demonstrate proficiency with common compression tools.

## Module 20: Linux Security Modules

This module explains how the Linux kernel enhances security through the use of the Linux Security Modules framework, particularly with the deployment of SELinux.

### Lessons

- Linux Security Modules
- SELinux
- AppArmor

After completing this module, students will be able to:

- Understand enhanced security mode in Linux and its importance in making sure permissions are valid.



# 55187- Linux System Administration 16 Level 3 for Windows

Course ID #: 1313-307-16-W

Hours: 28

- Become familiar with the two most used Linux Security Modules.

## Module 21: Local System Security

This module explains how to secure systems against both internal and external threats. It covers how to identify risks and provides guidance on how to decide what protection is appropriate. Finally, it covers the basic types of security available (physical, filesystem, and security modules e.g. SELinux).

### Lessons

- Local System Security
- Creating a Security Policy
- Updates and Security
- Physical Security
- Filesystem Security

After completing this module, students will be able to:

- Describe the sources of threats to system security.
- Understand the components important to creating a security policy.
- Demonstrate basic familiarity with SELinux.

## Module 22: Basic Troubleshooting and System Rescue

This module explains how to conduct troubleshooting in Linux as well as likely sources of issues. It covers basic concepts in system rescue and recovery and how to identify corrupted filesystems.

### Lessons

- Troubleshooting Overview
- Things to Check: Networking
- Boot Process Failures
- Filesystem Corruption and Recovery
- Virtual Consoles

- Rescue Media and Troubleshooting
- System Rescue and Recovery

After completing this module, students will be able to:

- Describe the common sources of corruption/performance issues.
- Identify the cause of system issues.
- Recover a system after some of the most common types of issues.