Linux Administration

3 days; Instructor-Led

Introduction

This three-day instructor-led course is designed to provide students with the necessary skills and abilities to work as a professional Linux system administrator. The course covers how to administer, configure and upgrade Linux systems running one of the three major Linux distribution families: Red Hat, SUSE, Debian/Ubuntu, how to master the tools and concepts you'll need to efficiently build and manage an enterprise Linux infrastructure. It also covers how to use state-of-the-art system administration techniques in real-life scenarios via practical labs. This course prepares the user for the Linux Foundation Certified System Administrator (LFCS) exam, which is also a required component of the MCSA: Linux on Azure Certification.

At Course Completion

After completing this course, students 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, phsyical volumes, ACLs, quotas and clustering.

Audience

This course is intended for students with a basic knowledge of Linux and its most common utilities and text editors. For users with no prior experience we suggest the free 'Introduction to Linux' course available on edx.org.

Prerequisites

Before attending this course, students must have:

- Knowledge of the basic components of Linux.
- Familiarity with text editors.
- Working knowledge of Bash scripting.

Course Outline

Module 1: System Startup and Shutdown

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

Lessons

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

Lab : Chapter Labs

- Boot into non-graphical mode using GRUB
- Add a new startup service with System V
- Add a new startup services with system
- Run Shutdown vs. Halt vs. Reboot

After completing this module, students will be able to:

- Manage startup process in Linux.

- Manage shutdown process in Linux.

Module 2: Linux Filetree System 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
- /dev
- /etc
- /home
- /lib and /lib64
- /media
- /mnt
- /opt
- /proc
- /sys
- /root
- /sbin
- /tmp
- /usr
- /var
- /run

Lab : Chapter Labs

- Change size of the default directories
- Touring the /proc Filesystem

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: 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

Lab : Chapter Labs

- Manipulating system tunables with sysctl.
- Changing the maximum process ID.
- Working with Kernel modules.
- Working with udev

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 4: 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

Lab : Chapter Labs

- Using a file as a disk partition image
- Partioning a Disk Image file
- Using losetup and parted
- Partitioning a real hard disk

After completing this module, students will be able to:

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

Module 5: 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

- Some Notes About Filesystems
- Virtual Filesystem (VFS)
- Filesystem Concepts
- Disk and Filesystem Usage
- Extended Attributes
- ext4
- XFS
- btrfs
- Creating and formatting filesystems
- Checking and Repairing Filesystems
- Mounting filesystems
- Swap
- Filesystem Quotas

Lab : Chapter Labs

- Defragmenting a system.
- Modifying Filesystem parameters using tune2fs.
- Working with file attributes.
- Mounting options.
- Managing swap space.
- Filesystem quotas.
- Working with XFS
- Working with 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 6: RAID and LVM

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

Lessons

- RAID
- RAID Levels
- Software RAID Configuration
- Logical Volume Management (LVM)
- Volumes and Volume Groups

- Working with Logical Volumes
- Resizing Logical Volumes
- LVM Snapshots

Lab : Chapter Labs

- Creating a RAID device
- Creating Logical Volumes

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 7: Processes

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

Lessons

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

Lab : Installing and Configuring Windows 7

- Controlling processes with ulimit
- Using ps and top
- Monitoring process states
- Examining signal priorities and execution

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 8: 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

Lab : Chapter Labs

- Using RPM
- Rebuilding the RPM database
- Using DKPG
- Version control with git

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 9: 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

Lab : Chapter Labs

- Basic yum commands
- Using yum to find information about a package
- Managing groups of packages with yum
- Adding a new yum repository
- Basic zypper commands
- Using zypper to find information about a package
- Basic APT commands
- Using APT to find information about a package
- Managing groups of packages using 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.

Module 10: 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
- PAM (Pluggable Authentication Modules)
- Authentication Process
- Configuring PAM
- LDAP Authentication
- File Permissions and Ownership
- SSH

Lab : Chapter Labs

- Working with user accounts
- Working with groups
- Configuring PAM
- Using chmod

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 11: 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

Lab : Chapter Labs

- Using tar for backup
- Using cpio for backup
- Using rsync for backup

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 12: 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
- Configuring Network Interfaces
- Routing
- Name Resolution
- Network Diagnostics

Lab : Chapter Labs

- Static configuration of a network interface
- Adding a static hostname
- Adding a network interface alias

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.

Module 13: 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

Lab : Chapter Labs

- Installing firewalld
- Examining firewall-cmd
- Adding services to a zone
- Using the firewall GUI

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 14: 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
- Linux Security Modules

Lab : Chapter Labs

- Using SELinux
- Security and mount options
- Using umask
- Usint setuid and scripts

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 15: Basic Troubleshoot 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

Lab : Chapter Labs

- Preparing to use Rescue/Recover media
- Recovering from a corrupted GRUB configuration
- Recovering from a password failure
- Recovering from partition table corruption
- Recovering using the install image

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.

Additional Reading

To help you prepare for this class, review the following resources:
Free 'Introduction to Linux' course available at: https://www.edx.org/course/introduction-linux-linuxfoundationx-lfs101x-2

