Linux-200

1 – Introduction
- About This Course and How to Prepare
- Lab Servers and Following Along

2 - Essential Tools
- Access a Shell Prompt and Issue Commands
- Use InputOutput Redirection
- Use grep and Regular Expressions to Analyze Text
- Access Remote Systems Using SSH
- Log in and Switch Users in Multiuser Targets
- Archive, Compress, Unpack and Uncompress Files Using tar, star, gzip and bzip2
- Create and Edit Text Files
- Create, Delete, Copy and Move Files and Directories
- Create Hard and Soft Links
- List, Set and Change Standard UGORWX Permissions
- List, Set and Change Standard UGORWX Permissions umask
- Locate, Read and Use System Documentation with man, info and usrsharedoc
- Finding Files with Locate and Find

3 - Operate Running Systems
- Boot, Reboot and Shutdown a System
- Boot Systems into Different Targets Manually
- Interrupt the Boot Process to Gain Access to a System
- Identify CPUMemory Intensive Processes, Adjust Process Priority and Kill Processes - Part 1
- Identify CPUMemory Intensive Processes, Adjust Process Priority and Kill Processes - Part 2
- Identify CPUMemory Intensive Processes, Adjust Process Priority and Kill Processes - Part 3
- Identify CPUMemory Intensive Processes, Adjust Process Priority and Kill Processes - Part 4
- Locate and Interpret System Log Files and Journals
- Access a Virtual Machines Console
- Start and Stop Virtual Machines
- Start, Stop and Check the Status of Network Services
- Securely Transfer Files Between Systems

4 - Configure Local Storage
- List, Create and Delete Partitions on MBR and GPT Disks
- Create and Remove Physical Volumes, Assign Physical Volumes to Volume Groups and Create and Delete Logical Volumes
- Configure Systems to Mount File Systems at Boot by UUID or Label
- Add New Partitions and Logical Volumes and Swap to a System Non-Destructively

5 - Create and Configure File Systems
- Create, Mount, Unmount and Use VFAT, EXT4 and XFS File Systems

- Mount and Unmount CIFS and NFS Network File Systems
- Extend Existing Logical Volumes
- Create and Configure Set-GID Directories for Collaboration
- Create and Manage Access Control Lists (ACLs)
- Diagnose and Correct File Permission Problems

6 - Deploy, Configure and Maintain Systems
- Configure Networking and Hostname Resolution Statically or Dynamically Troubleshooting
- Configure Networking and Hostname Resolution Statically or Dynamically Network Manager
- Configure Networking and Hostname Resolution Statically or Dynamically Hostname Configuration
- Schedule Tasks Using at and cron
- Start and Stop Services and Configure Services to Start Automatically at Boot
- Configure Systems to Boot into a Specific Target Automatically
- Install Red Hat Enterprise Linux Automatically Using Kickstart
- Configure a Physical Machine to Host Virtual Guests
- Install Red Hat Enterprise Linux Systems as Virtual Guests
- Configure Systems to Launch Virtual Machines at Boot
- Configure Network Services to Start Automatically at Boot
- Configure a System to Use Time Services
- Install and Update Software Packages from Red Hat Network, a Remote Repository or the Local File System YUM
- Install and Update Software Packages from Red Hat Network, a Remote Repository or the Local File System RPM
- Install and Update Software Packages from Red Hat Network, a Remote Repository or the Local File System Managing Repositories
- Install and Update Software Packages from Red Hat Network, a Remote Repository or the Local File System Configuring a Local Repository
- Update the Kernel Package Appropriately to Ensure a Bootable System
- Modifying the System Bootloader

7 - Manage users and groups
- Create, Delete, and Modify Local User Accounts
- Change Passwords and Adjust Password Aging for Local User Accounts
- Create, Delete, and Modify Local Groups and Group Memberships
- Using set-GID On Directories
- Configure a System to Use an Existing Authentication Service for User and Group Information Using Realmd

8 - Manage security
- Configure Firewall Settings Using firewall-config, firewall-cmd, or iptables
- Configure Key-Based Authentication for SSH
- Introduction to SELinux
- Set enforcing and permissive modes for SELinux

- List and identify SELinux file and process context
- Restore Default File Contexts
- Use Boolean Settings to Modify System SELinux Settings
- Diagnose and Address Routine SELinux Policy Violations

9 - Preparing For The Exam
- How to Practice and Study After Completing the Course
- Best Practices to Remember While Taking the Exam

Linux-300

1 - Introduction to Red Hat Certified Engineer
- Introduction to RHCE
- Course Syllabus
- Registering for the Exam
- Taking the Exam

2 - System configuration and management
- Use Network Teaming or Bonding to Configure Aggregated Network Links Between Two Red Hat Enterprise Linux Systems or Interfaces
- Configure IPv6 Addresses and Perform Basic IPv6 Troubleshooting
- Route IP Traffic and Create Static Routes
- Use procsys and sysctl to Modify and Set Kernel Runtime Parameters
- Configure a System to Authenticate Using Kerberos - KDC Server Setup
- Configure a System to Authenticate Using Kerberos - Client Setup
- Configure a System as Either an iSCSI Target or Initiator That Persistently Mounts an iSCSI Target - Target Setup
- Configure a System as Either an iSCSI Target or Initiator That Persistently Mounts an iSCSI Target - Initiator Setup
- Produce and Deliver Reports on System Utilization (Processor, Memory, Disk, and Network)

3 - Network services
- Section Overview
- Install the Packages Needed to Provide the Service

- Configure SELinux to Support the Service
- Use SELinux Port Labeling to Allow Services to Use Non-Standard Ports
- Configure the Service to Start When the System is Booted
- Configure the Service for Basic Operation
- Configure Host-Based and User-Based Security for the Service

4 - HTTPHTTPS
- Install and Configure Apache
- The Apache Configuration File - A Walk Through
- Configure Private Directories
- Configure Group Managed Content
- Configure a Virtual Host
- Deploy a basic CGI application
- Configure TLS Security - Generating Key Files, CSRs and Self Signed Certificates
- Configure TLS security - Configuring the Virtual Host

5 - DNS
- Configure a Caching-Only Name Server
- Troubleshoot DNS Client Issues

6 - NFS
- Provide Network Shares to Specific Clients - Server Installation and Configuration
- Provide Network Shares to Specific Clients - Client Installation and Configuration
- Provide Network Shares Suitable for Group Collaboration
- Use Kerberos to Control Access to NFS Network Shares - Quick NFS Setup
- Use Kerberos to Control Access to NFS Network Shares - Kerberos NFS Server and Client

7 - SMB
- Provide Network Shares to Specific Clients - Server Installation and Configuration
- Provide Network Shares to Specific Clients - Client Installation and Configuration
- Provide Network Shares Suitable for Group Collaboration

8 - SMTP
- Configure a System to Forward All Email to a Central Mail Server - Setup
- Configure a System to Forward All Email to a Central Mail Server - Client Testing

9 - SSH
- Configure Key-Based Authentication
- Configure Additional Options Described in Documentation

10 - NTP
- Synchronize Time Using Other NTP Peers - Set Up Local Time Server
- Synchronize Time Using Other NTP Peers - Peer with New Time Server

11 - Database services
- Install and Configure MariaDB
- Install and Configure Local and Remote MariaDB Clients
- Create a Simple Database Schema
- Perform Simple SQL Queries Against a Database
- Backup and Restore a Database - Backups
- Backup and Restore a Database - Restore

12 - Preparing For The Exam
- How to Practice and Study After Completing the Course
- Summary and Next Steps