Red Hat System Administrator II (RH134)

Modality: Virtual Classroom

Duration: 5 Days

About this course:

This course has been designed to preparing you for the Red Hat Certified System Administrator exam (EX200). Taking both the courses, Red Hat System Administration I and Red Hat System Administration II will be beneficial for your preparation for the certification exam.

Learning objectives:

The course has the following learning objectives:

- Knowing how to install using Kickstart
- Regulating filesystems and logical volumes
- Regulating scheduled jobs
- Approaching network filesystems
- Regulating SELinux
- Administering the firewalling procedure
- Troubleshooting

Audience:

This course is specifically designed for students who have finished their training of the course Red Hat System Administration I (RH124). The topics included in this course are not appropriate in the way that the course RH134 is used as a curriculum beginning step. It will be better if the students who do not have the training of the former Red Hat course take either System Administration I, if they have no expertise in Linux, or the RHCSA Fast Track course (RH200) if they have sufficient knowledge and experience of enterprise Linux administration.

Requirements:

It is important that the students have previously taken the Red Hat System Administration I (RH124) course.

Course Outline:

Automate installation with Kickstart
Automate the installation of Red Hat Enterprise Linux systems with Kickstart.
Use regular expressions with grep
Write regular expressions that, when partnered with grep, will allow you to quickly isolate or locate content within text files.
Create and Edit text files with vim

Introduce the vim text editor, with which you can open, edit, and save text files.

Schedule future Linux tasks

Schedule tasks to automatically execute in the future.

Manage priority of Linux processes

Influence the relative priorities at which Linux processes run.

Control access to files with access control lists (ACL)

Manage file security using POSIX access control lists.

Manage SELinux security

Manage the Security Enhanced Linux (SELinux) behavior of a system to keep it secure in case of a network service compromise.

Connect to network-defined users and groups

Configure systems to use central identity management services.

Add disks, partitions, and file systems to a Linux system

Manage simple partitions and file systems.

Manage logical volume management (LVM) storage

Manage logical volumes from the command line.

Access networked attached storage with network file system (NFS)

Access (secure) NFS shares.

Access networked storage with SMB

Use autofs and the command line to mount and unmount SMB file systems.

Control and troubleshoot the Red Hat Enterprise Linux boot process

Limit network communication with firewall

Configure a basic firewall.

Comprehensive review

Practice and demonstrate knowledge and skills learned in this course.
