Course Code: **CIS309**
Course Name: Red Hat Certified System Administrator
Certification: Red Hat Certified System Administrator RHEL 7 – EX200
Duration: 3 months
Tuition: $1895

Course Overview

This course covers the core system administration skills required in Red Hat Enterprise Linux environments. The course discusses the environment, the command line, administration and permissions, scripting and scheduling, processes, networking, and logging, advanced networking, remote connections and access, files systems and device management, boot process and installation, and introduces virtualization. The course also explores SELinux and troubleshooting.

Course Content

- **Lesson 1** – **The Environment**
  This lesson covers the following topics:
  - use Gnome to run applications, manage virtual workspaces, and use window control buttons
  - configure Gnome menus, panels, and desktop icons, themes, and colors for a better user experience
  - access online help with a web browser or built-in help through Gnome
  - explore the file system using the Gnome file manager
  - copy, move, delete, and rename files and directories using the Gnome file manager
  - create and edit text files from the desktop environment using the Gnome editor
  - login, logoff, lock, and unlock a Gnome session as well as power up and down a system
  - use the two default Gnome mail clients and configure basic settings to send and receive e-mail
  - work with the network-manager to check the network configuration and explore networks from the File Manager
  - describe the roles and differences between Xwindows and the Gnome desktop environment
  - configure system and security settings from the Gnome interface
  - switch users on a multiuser system and run multiple desktops for different users
  - describe a shell, the purpose for shells, and list some of the shells available
  - open, close, set fonts, set colors, resize, and run a command from the Bourne Again Shell (BASH)
  - using autocomplete, and using history with the hist command and arrow keys

  - list, copy, move, and delete files
  - list, create, move, change, and delete directories; and use shortcuts to move around the file system
  - execute GUI applications from the command line, run them in the background, and see diagnostic or debug information in the shell
  - use man and info to get help, and identify or locate help in /usr/share/doc
  - use common commands like less, cat, more, and diff to view and compare file contents
  - describe how relative and absolute paths are used and how shortcuts like ../ and ~/ make directory traversal easier
  - create aliases for commands and make links to files or directories
  - manipulate the BASH prompt and describe how the env and export features can be used
  - use the shell tools echo, cat, and who to create and edit text files
  - explore the Gnome User Interface and run commands from the BASH Shell

- **Lesson 2** – **The Command Line**
  This lesson covers the following topics:
  - use input and output redirection to stdin and stdout to manage output from shell commands
  - use pipes to chain one command to another to alter the output
  - use globbing to select files based on matching filename patterns
  - switch users and shells within a Terminal window; in particular to become the root user to perform administrative tasks
  - switch to and back from TTY consoles in order to execute shell commands
  - use the find command to locate files based on their name or other properties
  - perform actions on files that are returned from a find command
  - identify the path and filename for a command or locate files that have been indexed
  - work with vim to open, do basic edits, and save a text file
  - use features of vim to search text, replace text, and add, remove, or delete lines
  - perform basic file operations and editing using the emacs text editor
  - use a shell text editor to create or edit a text file
  - work with sed to alter the contents of a text file
  - identify a BASH script file and the header specifying the interpreter used for the script
  - create a simple BASH script that can chain multiple commands together to perform an action
  - execute, pause, and run a script in the background and then bring it to the foreground

  - view the shell environment variables and be able to set a shell variable within a script
  - recognize an archived file and the tools necessary to retrieve the contents
  - use the gzip and gunzip commands to compress or decompress a file
  - use bzip2 to compress or decompress a file
  - use the tar command to create, extract, compress, or list the contents of an archive
  - use the star command to create, extract, compress, or list the contents of an archive that supports extended ACLs
  - use gzip and bzip2 with tar directory to compress and decompress in a stream
  - use additional, but not as often used in Linux, compression and decompression tools
  - use scripts to automate the management and archiving of files and directories

- **Lesson 3 – Administration and Permissions**
  This lesson covers the following topics:
  - run the Gnome package manager to view installed and find software
  - install software from the package manager
  - update the current software manually or automatically using the package manager
  - choose appropriate update times, schedules, and mode to update the RHEL 7 system
  - use yum to list, find, and install software packages from the shell
  - update the system software from the shell
  - remove, reinstall, or replace a software package
  - add, remove, or set the software repositories for yum and the Gnome package manager
  - configure a local repository and only allow software packages and updates that have been approved
  - describe how users and groups work and how they are connected
  - add, edit, modify, and delete a user using the Gnome User Manager application
  - change your password through the Gnome interface or from the shell
  - describe the components of the /etc/password file and the purpose of the /etc/shadow file
  - change any users password including the root user
  - add, delete, and edit a user from a shell including how to set the user properties, shell, and home directory
  - modify user properties directly in the /etc/passwd file to fix user problems
  - apply user password ageing and other policies to user accounts
  - add, modify and delete groups
  - add a user to a group or groups

- modify a users default group
- describe the basic file permissions for users and groups and how they relate to file ownership
- identify POSIX file and ownership permissions on files and directories
- change a files owner and group and set file and group permissions
- change a directories owner, group and permissions
- add and edit users, groups and packages as well as configure user permissions on files

- **Lesson 4** – **Scripting and Scheduling**

  This lesson covers the following topics:
  - identify and understand the basic syntax of a regular expression
  - use grep to find patterns in a file based on simple patterns or regular expressions
  - use advanced grep features like recursively finding matching files and ignoring case sensitivity
  - use grep with I/O redirection and pipes to create lists
  - use grep to locate content within a text file
  - get and set discretionary and mandatory Access Control Lists
  - add, edit, and view quotas
  - create a directory that can be shared by multiple users in a common group
  - use read to get input from the user in a BASH script
  - use the if statement and the basic looping construct for
  - use the while and until looping constructs
  - use bash test operators to check for conditions
  - describe the order of expansion when used a script
  - set an exit status and use it from the Shell
  - describe the different job schedulers and how they differ
  - describe the configuration of a crontab file and the different sections for a cron job
  - create a cron job
  - edit and pause cron jobs as well as set jobs for users and root
  - identify the at parameters and commands used for managing jobs
  - schedule a job using at
  - alter, delete, and view at jobs
  - describe a systemD timer unit and the options
  - schedule a systemD timer task
  - convert a cron job to a systemD timer task
  - create a script that will use grep to find files with certain contain and schedule this job to run each day at 2:05 am

- **Lesson 5 – Processes, Networking, and Logging**

  This lesson covers the following topics:
  - list and identify running processes
  - recognize common running processes
  - monitor processes and their resource utilization
  - start and stop processes
  - set or change the priority for a process
  - troubleshoot or identify problem processes
  - start and stop a network service
  - configure a service to start or not start at boot
  - use SystemD to start services
  - work with SystemD to manage running services
  - use SystemD to manage the system
  - describe basic networking terminology and interfaces on Linux
  - identify network devices and their configuration
  - use the Gnome network manager to configure a network device
  - change the hostname, DNS, and other network settings for the host; including deactivating and activing a network device
  - configure a network device entirely from the shell
  - configure the system to use a network time source
  - configure Linux systems with common network scenarios
  - list the location of log files and the purpose of the common logs
  - view and analyze log files and interpret basic values from other journal sources
  - review SystemD journal logs
  - configure SystemD journals to forward system messages to traditional system logging tools
  - store and archive logs
  - configure what is logged to system logs
  - modify the system log settings and retention policies
  - use renice to change a processes priority, change a network adaptors IP Address and check the logs for any unauthorized access attempts

- **Lesson 6 -Advanced Networking**

  This lesson covers the following topics:
  - work with network services through SystemD Services
  - configure a basic bind service
  - configure a basic dhcpd service
  - configure a basic ntpd service
  - configure a system to use Precision Time Protocol
  - configure the logging server to store logs sent from external servers
  - configure a basic smbd service

- use Samba to share a directory with Windows clients
- configure a basic sshd service
- configure a basic web service
- configure a basic telnet service
- configure a basic ftp service
- configure a basic squid proxy service
- configure a basic mail server
- use the Security Level Configuration Tool to manage a basic firewall
- describe the sections of the firewall and the basics of how the firewall rules are configured
- add and delete rules to an iptable configured firewall
- save and restore iptable rulesets
- configure the system to use a set of firewall rules on boot from the shell
- add a rule to allow a network service port through the firewall
- use the advanced features of the firewall manager
- add a limit to the firewall for certain types of traffic
- start a network service add a rule to the firewall to allow external access to the service

- **Lesson 7** – **Remote Connections and Access**

  This lesson covers the following topics:
  - describe the various remote access technologies that are available on Linux
  - use telnet to connect to remote hosts
  - use VNC to connect, or be the host of, a remote connection
  - use ssh to connect to a remote host
  - use scp to transfer a file to and from a host
  - work with ssh tunneling to secure vnc or xdmcp
  - use ssh keys to authenticate rather than user name and password
  - describe the components of the Network File System
  - install, setup and configure NFS
  - recognize the differences in the configuration for running NFS securely
  - mount an external shared NFS partition to the local system
  - add and configure a local NFS share
  - configure an exported share to work on reboot
  - enable and support pNFS on the server
  - mount and unmount remote SMB, or Samba, shares
  - use autofs to mount shares automatically
  - identify the files and setting that must be changed to support an external directory service
  - configure a system to use an LDAP based directory service
  - login to the server using a user account from the LDAP directory service

  - configure and use permissions and settings for the LDAP user on the server
  - configure a system to use MS Active Directory
  - login to the server using a MS Active Directory user account
  - configure MS AD permissions for the user on the server
  - use a Directory Service configured client to mount a remote NFS share that you configure on a remote host

- **Lesson 8** – **File Systems and Device Management**
  This lesson covers the following topics:
  - describe the various supported file systems
  - identify the file systems of mounted and external drives
  - mount and unmount various file systems
  - configure the system to mount a file system at boot
  - use an encrypted file system
  - mount an encrypted file system at boot and using a fully encrypted file system
  - control the automatic mounting of file systems when devices are plugged in and safely unmount file systems
  - add new partitions or additional swap space non-destructively
  - create a file system on a physical disk
  - use tools to create, delete, list and manage MBR based partitions
  - resize a MBR based partition
  - change the label of a partition
  - mount and unmount iSCSI Network Area Storage
  - use tools to create, delete, and list GPT based partitions
  - using and compressing swap partitions or files
  - identify and describe LVM configuration for Volumes
  - use basic LVM commands to create and remove volumes
  - manage free space in a storage pool and allocate space as required
  - assign logical and physical volumes to a volume group
  - use LVM tiered storage to use faster SSDs with HDDs to create fast "hybrid" storage
  - create a snapshot of a volume
  - backup and restore volumes
  - use shell commands to manage LVM storage
  - create and configure a basic RAID 0, 1, and 5 volume
  - resize a RAID volume
  - create an XFS LVM Filesystem and then mount the partition so it will be available even after rebooting

- **Lesson 9** – **Boot Process and Installation**
  This lesson covers the following topics:

- describe the basic boot process and system components involved
- configure the boot loader
- alter the runlevel of the system
- identify, configure, and boot from GPT or MBR
- change the boot target with systems using SystemD
- alter the boot process to gain access to fix problems or diagnose issues
- create boot targets, boot states, and control parallel daemon instantiation with SystemD
- describe Red Hat Enterprise Linux (RHEL) 7 hardware requirements
- describe and be able to select the appropriate installation method
- perform the initial install of RHEL 7 onto a physical system using the graphical installer
- complete the install of RHEL 7 onto a physical system using the graphical installer
- perform a minimal install using the text mode installer
- complete a minimal install using the text mode installer
- describe swap space requirements and how to manage swap space during installation
- recognize issues that can occur with UEFI and some setting that can allow the installation still
- configure kernel setting and limits
- update or modify a kernel to ensure a bootable system
- list, add, remove, and configure kernel modules
- troubleshoot basic boot failures after an installation
- troubleshoot and configure the GRUB boot loader
- fix boot partition issues
- fix mount points that no longer exist
- use modprobe to blacklist modules
- alter kernel settings to solve common system issues
- list the kernel modules, change the runlevel target, and add a second boot option to the grub boot loader in RHEL 7

- **Lesson 10** – **Introduction to Virtualization**
  This lesson covers the following topics:
  - describe the built-in virtualization tools and programs in RHEL 7
  - distinguish between the different virtualization tools used to run guests on RHEL 7
  - describe and use RHEL 7 as a guest running on a Host
  - install RHEL 7 as a guest
  - launch a RHEL 7 guest from the host
  - modify the running RHEL 7 guest to perform well under a host
  - configure keyboard support
  - use tools to detect problems in guests and report them to the host

  - use sVirt to protect guests
  - configure and optimize RHEL 7 to be a host for guests
  - configure settings for hosting guests
  - create and manage virtual machines
  - access a virtual machine's console from the host
  - start, stop, and control guests
  - configure the system to start virtual machines on boot
  - obtain information about a guest
  - throttle I/O for a guest and manage guest resource allocations
  - use kickstart to create an automation script for automated installs
  - investigate booting or installation issues using dracut
  - configure Kickstart to automatically connect to a Directory Service
  - use a kickstart script to do an installation
  - use a kickstart script to install RHEL 7 as a guest
  - use SystemTap to investigate and monitor the activities of the operating system kernel
  - use built-in tools to generate bug and crash reports for diagnosis or sending to Red Hat
  - use kpatch to do dynamic patches to the kernel
  - use RHEL 7 as a Host for VMs and as a Client running on a VM

- **Lesson 11– SELinux and Troubleshooting**
  This lesson covers the following topics:
  - identify and recognize the components and purpose of SELinux
  - configure and choose the applicable SELinux Mode
  - configure SELinux settings
  - identify and recognize the components and purpose of SELinux User contexts
  - use and apply a SELinux Process context
  - use restorecon to restore file security contexts
  - identify role-based access controls (RBAC) in SELinux
  - identify and choose SELinux Policies
  - configure and control SELinux Policies
  - add a new policy rule to be enforced
  - identify and troubleshoot a reported policy violation
  - use SELinux to secure a Network Service
  - troubleshoot common memory issues
  - troubleshoot CPU or Memory intensive processes
  - identify and diagnose file permission issues
  - troubleshoot common file permission security issues
  - troubleshoot common network issues
  - identify locked files or files used by a process

- troubleshoot and repair the XFS file system
- describe the basic tools for repairing a variety of file systems
- debug the XFS file system
- troubleshoot a drive that has failed in either a hot-swap or raid configuration
- troubleshoot using the Red Hat Rescue Environment
- use SELinux to protect a network service and find the processes using the most memory or CPU resources