

## Get live, expert instruction from anywhere.



## Infosec RHCSA Boot Camp

Infosec's RHCSA Boot Camp helps you gain the essential knowledge and hands-on skills needed to leverage Linux for your organizational advantage. You'll learn important facets of Red Hat Enterprise Linux 8, the world's leading enterprise Linux platform.

### Course description

Infosec's five-day Red Hat Certified System Administrator (RHCSA) Boot Camp is a hands-on training covering all-important facets of RHEL 8, the world's leading enterprise Linux platform.

Throughout this boot camp, you gain the essential knowledge and hands-on skills to leverage Linux for your organizational advantage. You learn to create, edit and search Linux files, control permissions and ownership, process and format text data, and use shell scripts to perform multiple tasks.

### Who should attend

- » Experienced Red Hat Enterprise Linux system administrators seeking validation of their skills
- » Students who attended Red Hat System Administration I and II and are on the path to earn RHCSA certification
- » Experienced Linux system administrators who require a certification
- » IT professionals on the path to earn a Red Hat Certified Engineer (RHCE) certification
- » RHCEs who are non-current or who are about to become non-current and wish to re-certify as RHCEs

### Boot camp at a glance



#### Get certified

- ✓ Red Hat Certified System Administrator (RHCSA)



#### Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite



#### Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 5-day boot camp
- ✓ 90-day extended access to all boot camp materials

## The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.



### Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.



### Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.



### Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.



### 700+ IT and security courses

Earn CPEs and build new skills with 100s of additional training courses.

## What's included

- » Five days of expert, live RHCSA training
- » Exam Pass Guarantee
- » Exam voucher
- » Unlimited practice exam attempts
- » 100% Satisfaction Guarantee
- » Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- » 90-day extended access to all boot camp video replays and materials
- » Pre-study learning path
- » Knowledge Transfer Guarantee

### Prerequisites

This Linux boot camp is designed for students who have minimum of one year experience in the Linux computer industry, extensive experience with at least one other operating system and have working knowledge of a UNIX-style editor.

## What you'll learn

An RHCSA is able to perform the following tasks:

- » Understand and use essential tools for handling files, directories, command-line environments and documentation
- » Operate running systems, including booting into different run levels, identifying processes, starting and stopping virtual machines, and controlling services
- » Configure local storage using partitions and logical volumes
- » Create and configure file systems and file system attributes, such as permissions, encryption, access control lists and network file systems
- » Deploy, configure and maintain systems, including software installation, update and core services
- » Manage users and groups, including use of a centralized directory for authentication
- » Manage security, including basic firewall and SELinux configuration

## Hands-on cyber range

You'll build and reinforce your skills as you progress through labs covering a wide range of Linux topics, including basic commands, file and directory operations and attributes, permissions, job scheduling and much more. You'll also learn about managing SELinux, packages, extended file systems, firewalls, and units and control groups.

## Skill up and get certified, guaranteed



### Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.



### 100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.



### Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

# What our students are saying

"I've attended four other workshops like this but Infosec's boot camp is by far the best. I already recommended them to my colleagues and other IT professionals. A student's learning experience is reflective of the teacher's aptitude and knowledge on the subject and the skill to convey the information. Great instructor, great class."

**Timothy M Twyman**  
Department of Defense

---

"Great job keeping the entire class engaged. The knowledge and real-world examples were great in helping me correlate the materials with something I could understand and remember."

**Hollie Perkins**  
Marriott

---

"I have been in this industry for over 10 years, and I have never seen or heard anyone explain complex ideas and systems in such an easy to digest manner."

**Antonio Roberto Garcia**  
GRA Research

---

"Very impressed with Infosec. My instructor did a great job delivering the information strategically and in a way for all to understand. I would definitely take another class/certification prep course."

**Sylvia Swinson**  
Texeltek

---

"The course materials were excellent. The class format was fantastic. The instructor not only prepared us for the examination but also spent a considerable amount of time in learning practical skills for the real world."

**Stephen Field Thomas**  
Compliance Associates, Inc.

# Infosec RHCSA Boot Camp details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

	Day 1	Day 2	Day 3	Day 4	Day 5	After class
Morning session	Introduction Basic file management	The Bash Shell Linux processes and task scheduling	Booting, updating and logging System initialization, message logging and system tuning	Remote file systems Networking, network devices and network connections	The Linux firewall Security Enhanced Linux	Take RHCSA exam at local exam center
Afternoon session	Advanced file management User management	Basic package management Advanced package management	Basic storage partitioning Local file systems and swap	Time synchronization and hostname resolution The secure shell service	Exam review	
Evening session	Optional group & individual study	Optional group & individual study	Optional group & individual study	Optional group & individual study	Optional group & individual study	

*Schedule may vary from class to class*

## Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills, including an in-depth CISSP prep course, the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

## Initial interaction with the system

- » Interact with display manager
- » Overview of Linux Directory Structure
- » Recognize top-level directories
- » Understand command construct
- » Describe and run basic Linux commands
- » Obtain help using multiple native tools and RHEL documentation

## Basic file management

- » Common file types
- » Compress and decompress files
- » Archive and compress files

- » Edit files with vim
- » Create, copy, move, delete files and directories
- » Create links

## Advanced file management

- » Understand ugo/rwx access permissions on files and directories
- » Know symbolic and octal notations of permission allocation
- » Modify permissions for file owner, owning group and others
- » Calculate and set default permissions on new files and directories
- » Comprehend and configure special permission bits: setuid, setgid and sticky
- » Apply sticky bit on public and shared writeable directories
- » Grasp and manage extended access controls for named users and named groups
- » Set default extended access controls on directories

## Basic user management

- » Show who is currently logged in
- » Review history of successful user login attempts and system reboots
- » Review history of failed login attempts
- » Examine user and group information
- » Understand the content and syntax of local user authentication files
- » Analyze user configuration files
- » Add, modify, delete local user accounts with default and custom values
- » Set and modify user passwords
- » Add a user account with no login access

## Advanced user management

- » Configure password aging attributes on local user accounts
- » Lock and unlock user account
- » Understand, create, modify and delete local groups and group memberships
- » Switch into another user account
- » Configure who can execute which privileged commands
- » Identify and manage file owners and owning groups

## The Bash Shell

- » Introduction to the bash shell
- » Internal and external commands
- » Understand, set and unset shell and environment variables
- » Comprehend and use command and variable expansions
- » Grasp and utilize input, output and error redirections
- » Know and use history substitutions, command line editing, tab completion tilde substitution and command aliasing
- » Identify and use metacharacters, wildcard

characters, pipes and pipelines

- » Discover the use of quoting mechanisms and regular expressions
- » Run and control jobs in background and foreground
- » Identify and examine shell startup filescontrols on directories

## Linux processes and task scheduling

- » Identify and display system and user executed processes
- » View process states and priorities
- » Examine and change process niceness and priority
- » Understand signals and their use in controlling processes
- » Review job scheduling Control who can schedule jobs
- » Schedule and manage jobs using at
- » Comprehend crontab and understand the syntax of crontables Schedule and manage jobs using cron
- » Understand anacron and its function

## Basic package management

- » Overview of Red Hat packages, naming and management tools
- » Package dependency and database
- » Query, install, upgrade, freshen, overwrite and remove packages
- » Extract package files from installable package
- » Validate package integrity and authenticity
- » View GPG keys and verify package attributes
- » Manage packages using the rpm command

## Basic package management

- » Overview of Red Hat packages, naming and management tools
- » Package dependency and database
- » Query, install, upgrade, freshen,

- » overwrite and remove packages
- » Extract package files from installable package
- » Validate package integrity and authenticity
- » View GPG keys and verify package attributes
- » Manage packages using the rpm command

## Advanced package management

- » Describe package groups
- » Understand application streams and modules
- » Software repositories and how to access them
- » Review module streams and module profiles
- » Perform software management operations using dnf
- » List, install, update and delete individual packages, package groups and modules
- » Show package information, determine provider and search metadata
- » Exhibit package group and module information
- » Install module from alternative stream

## Booting, updating and logging

- » Linux boot process: firmware, bootloader, kernel and initialization
- » Understand and interact with GRUB2 to boot into different targets
- » Modify GRUB2 configuration
- » Boot system into specific targets
- » Reset lost or forgotten root user password
- » Linux kernel, packages, version anatomy and key directories
- » Download and install a newer kernel version

## System initialization, message logging and system tuning

- » Understand systemd, units and targets
- » Analyze service and target unit configuration files
- » List and view status of running units
- » Manage service units and target units
- » Display and configure default system boot target

- » Switch into non-default targets
- » Analyze system log configuration file
- » Examine log file rotation settings
- » Review boot and system log files
- » Record custom messages in system log file
- » Describe systemd journal service
- » Retrieve and scrutinize messages from journal
- » Store journal information persistently
- » Know system tuning and apply tuning profile

## Basic storage partitioning

- » Master Boot Record vs. GUID Partition Table
- » Identify and understand disk partitions
- » The concept of thin provisioning and its benefits
- » Create and delete partition on MBR disk
- » Create and delete partition on GPT disk
- » Overview of Virtual Data Optimizer and how it conserves storage
- » Create and delete a Virtual Data Optimizer volume

## Local file systems and swap

- » Understand file systems and their benefits, categories and types
- » Review file system types: Ext3/Ext4, XFS, VFAT and ISO9660
- » Know file system administration command set
- » Mount and unmount file systems manually and persistently
- » Determine and use UUID
- » Apply and use file system label
- » Monitor file system and directory usage
- » Create and mount different types of local file systems in partitions
- » Create and mount XFS file system in VDO volume
- » Create, mount, and resize Ext4 and XFS file systems in LVM
- » Create, mount, and expand Stratis file system
- » Understand, create, and activate swap in partitions and LVM



## Remote file systems

- » Overview of Network File System service and key components
- » Network File System benefits and versions
- » Export a share on NFS server
- » Mount the share on NFS client using standard mount method
- » Understand the AutoFS service and its benefits and functioning
- » Analyze AutoFS configuration maps
- » Mount the exported share on NFS client using AutoFS
- » Configure NFS and AutoFS to share and mount user home directories

## Networking, network devices and network connections

- » Overview of basic networking concepts: hostname, IPv4, network classes, subnetting, subnet mask, CIDR, protocol, TCP/ UDP, well-known ports, ICMP, Ethernet address, IPv6, IPv4/ IPv6 differences, consistent device naming, etc.
- » Change hostname of the system
- » Understand the concepts of network device and connection
- » Anatomy of a network connection profile
- » Know network device and connection management tools and techniques
- » Configure network connections by hand and using commands
- » Describe the hosts table
- » Test network connectivity using hostname and IP address

## Time synchronization and hostname resolution

- » Describe time synchronization and the role of Network Time Protocol
- » Comprehend the terms: time source, NTP roles and stratum levels

- » Anatomy of the Chrony service configuration file
- » Configure and verify NTP/ Chrony client service
- » View and set system date and time
- » Overview of Domain Name System and hostname resolution
- » Understand various DNS roles
- » Analyze entries in resolver configuration files
- » Perform name resolution using a variety of lookup tools

## The secure shell service

- » Understand the OpenSSH service, versions and algorithms
- » Overview of encryption techniques and authentication methods
- » Describe OpenSSH administration commands and configuration files
- » Configure private/ public key-based authentication
- » Access OpenSSH server from Windows and other Linux systems
- » Use OpenSSH client tools to transfer files
- » Synchronize files remotely over OpenSSH

## The Linux firewall

- » Describe Linux firewall for host-based security control
- » Overview of the firewalld service
- » Understand the concepts of firewalld zones and services
- » Analyze zone and service configuration files
- » Control access to network services and ports through firewalld
- » Use firewall-cmd command to manage firewall rules



## Security Enhanced Linux

- » Describe Security Enhanced Linux and its terminology
- » Understand SELinux contexts for users, processes, files and ports
- » Copy, move, and archive files with and without SELinux context
- » How domain transitioning works
- » Overview of SELinux Booleans
- » Query and manage SELinux via management tools
- » Modify SELinux contexts for files and ports
- » Add SELinux rules to policy database
- » View and analyze SELinux alerts

## After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

## About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at [infosecinstitute.com](https://infosecinstitute.com).