



## Red Hat® Server Hardening (RH413)

Build on your Red Hat Certified Engineer (RHCE®) certification or equivalent experience by learning how to secure a Red Hat Enterprise Linux® system to comply with security policy requirements. Many security policies and standards require systems administrators to address specific user authentication concerns, application of updates, system auditing and logging, file system integrity, and more. Red Hat Server Hardening provides strategies for addressing specific policy and configuration concerns.

### What You'll Learn

- Review errata and apply them to Red Hat Enterprise Linux
- Use special permissions and file system access control lists
- Manage users and password-aging policy requirements
- Install and configure Red Hat Identity Management tools
- System auditing

### Who Needs to Attend

- Those who need technical guidance on how to enhance the security of Red Hat Enterprise Linux systems
- Anyone who is responsible for implementing security policy requirements on Red Hat Enterprise Linux systems consistently and in a reproducible, scalable way
- Those who must be able to demonstrate that systems meet security policy requirements
- Anyone how maintains continued adherence to security requirements, including management of security-critical operating system/software updates

### Who Needs to Attend

- Those who need technical guidance on how to enhance the security of Red Hat Enterprise Linux systems
- Anyone who is responsible for implementing security policy requirements on Red Hat Enterprise Linux systems consistently and in a reproducible, scalable way
- Those who must be able to demonstrate that systems meet security policy requirements
- Anyone how maintains continued adherence to security requirements, including management of security-critical operating system/software updates

### Prerequisites

RHCE certification, Red Hat Certified Systems Administrator (RHCSA®) certification, or equivalent experience required

### Follow-On Courses

- [Red Hat® Enterprise Deployment and Systems Management \(RH401\)](#)
- [Red Hat® Enterprise Performance Tuning \(RH442\)](#)
- [Red Hat® Enterprise Clustering and Storage Management \(RH436\)](#)

### Certification Programs and Certificate Tracks

This course is part of the following programs or tracks:

- [RHCA - Red Hat® Certified Architect](#)

### Course Outline

#### 1. Manage Software Updates

Develop a process for applying updates to systems, including verifying

properties of the update.

## **2. Create File Systems**

Allocate an advanced file system layout, and use file system encryption.

## **3. Manage File Systems**

Adjust file system properties through security-related options and file system attributes.

## **4. Manage Special Permissions**

Work with set user ID (SUID), set group ID (SGID), and sticky (SVTX) permissions, and locate files with these permissions enabled.

## **5. Manage Additional File Access Controls**

Modify default permissions applied to files and directories, and work with file access control lists.

## **6. Monitor for File System Changes**

Configure software to monitor the files on your machine for changes.

## **7. Manage User Accounts**

Set password-aging properties for users; audit user accounts.

## **8. Manage Pluggable Authentication Modules (PAMs)**

Apply changes to PAMs to enforce different types of rules on users.

## **9. Secure Console Access**

Adjust properties for various console services to enable or disable settings based on security.

## **10. Install Central Authentication**

Install and configure a Red Hat Identity Management server and client.

## **11. Manage Central Authentication**

Configure Red Hat Identity Management rules to control both user access to client systems and additional privileges granted to users on those systems.

## **12. Configure System Logging**

Configure remote logging to use transport layer encryption, and manage additional logs generated by remote systems.

## **13. Configure System Auditing**

Enable and configure system auditing.

## **14. Control Access To Network Services**

Manage firewall rules to limit connectivity to network services.

### **Further Information:**

For More information, or to book your course, please Call/Email us on : - +254 713 027 191

[KENYA - training.kenya@clclearningafrica.com](mailto:training.kenya@clclearningafrica.com)

[TANZANIA - training.tanzania@clclearningafrica.com](mailto:training.tanzania@clclearningafrica.com)

[UGANDA - training.uganda@clclearningafrica.com](mailto:training.uganda@clclearningafrica.com)

[RWANDA - training.rwanda@clclearningafrica.com](mailto:training.rwanda@clclearningafrica.com)

[BURUNDI - training.burundi@clclearningafrica.com](mailto:training.burundi@clclearningafrica.com)

[ETHIOPIA - training.ethiopia@clclearningafrica.com](mailto:training.ethiopia@clclearningafrica.com)