

RED HAT SERVER HARDENING

DURATION: 4 DAYS

COURSE OVERVIEW

Secure a Red Hat Enterprise Linux system to comply with security policy requirements

Red Hat® Server Hardening (RH413) builds on a student's Red Hat Certified Engineer (RHCE®) certification or equivalent experience to teach 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.

TARGET AUDIENCE

This course is designed for people who:

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

COURSE OBJECTIVES

1. Review errata and apply them to Red Hat Enterprise Linux.
2. Use special permissions and file system access control lists.
3. Manage users and password-aging policy requirements.
4. Install and configure Red Hat Identity Management tools.
5. Understand system auditing.

COURSE CONTENT

Track security updates

Understand how Red Hat Enterprise Linux produces updates and how to use yum to perform queries to identify what errata are available.

Manage software updates

Develop a process for applying updates to systems including verifying properties of the update.

Create file systems

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

Manage file systems

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

Manage special permissions

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

Manage additional file access controls

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

Monitor for file system changes

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

Manage user accounts

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

Manage pluggable authentication modules (PAMs)

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

Secure console access

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

Install central authentication

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

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.

Configure system logging

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

Configure system auditing

Enable and configure system auditing.

Control access to network services

Manage firewall rules to limit connectivity to network services.

COURSE PREREQUISITES

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