RH413 Syllabus

RH 413 course is run on RHEL 6.4 platform. The course aims in training you to secure your Linux servers.

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, and 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.