

RED HAT SECURITY: LINUX IN PHYSICAL, VIRTUAL, AND CLOUD WITH EXAM (EX415)

DURATION: 4 DAYS

COURSE OVERVIEW

Maintaining security of computing systems is a process of managing risk through the implementation of processes and standards backed by technologies and tools. In this course, you will learn about resources that can be used to help you implement and comply with your security requirements.

TARGET AUDIENCE

System administrators, IT security administrators, IT security engineers, and other professionals responsible for designing, implementing, maintaining, and managing the security of Red Hat Enterprise Linux systems and ensuring their compliance with the organization's security policies.

COURSE OBJECTIVES

1. Manage compliance with Open SCAP.
2. Enable SE Linux on a server from a disabled state, perform basic analysis of the system policy, and mitigate risk with advanced SE Linux techniques.
3. Proactively identify and resolve issues with Red Hat Insights.
4. Monitor activity and changes on a server with Linux Audit and AIDE.
5. Protect data from compromise with USB Guard and storage encryption.
6. Manage authentication controls with PAM.
7. Manually apply provided Ansible Playbooks to automate mitigation of security and compliance issues.
8. Scale Open SCAP and Red Hat Insights management with Red Hat Satellite and Red Hat Ansible Tower.

COURSE CONTENT

Manage security and risk: Define strategies to manage security on Red Hat Enterprise Linux servers.

Automate configuration and remediation with Ansible: Remediate configuration and security issues with Ansible Playbooks.

Protect data with LUKS and NBDE: Encrypt data on storage devices with LUKS and use NBDE to manage automatic decryption when servers are booted.

Restrict USB device access: Protect system from rogue USB device access with USBGuard

.Control authentication with PAM: Manage authentication, authorization, session settings, and password controls by configuring pluggable authentication modules (PAMs).

Record system events with audit: Record and inspect system events relevant to security, using the Linux kernel's audit subsystem and supporting tools.

Monitor file system changes: Detect and analyze changes to a server's file systems and their contents using AIDE.

Mitigate risk with SE Linux: Improve security and confinement between processes by using SE Linux and advanced SE Linux techniques and analyses.

Manage compliance with Opens CAP: Evaluate and remediate a server's compliance with security policies by using Opens CAP.

Automate compliance with Red Hat Satellite: Automate and scale your ability to perform Open SCAP checks and remediate compliance issues using Red Hat Satellite.

Analyze and remediate issues with Red Hat Insights: Identify, detect, and correct common issues and security vulnerabilities with Red Hat Enterprise Linux systems by using Red Hat Insights.

Perform a comprehensive review the content covered in this course by completing hands-on review exercises.

COURSE PREREQUISITES

Be a Red Hat Certified Engineer (RHCE®), or demonstrate equivalent Red Hat Enterprise Linux knowledge and experience

TEST CERTIFICATION

EX415 - Red Hat Certified Specialist in Security: Linux exam.

By passing this exam, you become a Red Hat Certified Specialist: Linux, which also counts toward becoming a Red Hat Certified Architect (RHCA®).

This exam is based on Red Hat Enterprise Linux version 7.5.

FOLLOW ON COURSES

Recommended next exam or course Red Hat Satellite 6 Administration (RH403) Recommended for those interested in learning more about Red Hat Satellite

Automation with Ansible I (DO407) and Automation with Ansible II: Ansible Tower (DO409) Recommended for those who want to use DevOps practices to ensure security