Red Hat Security: Linux in Physical, Virtual, and Cloud

Duration: 4 Days   Course Code: RH415

Overview:

Maintaining the security of computing systems is a process of managing risk through the implementation of processes and standards backed by technologies and tools.
The "Red Hat Security: Linux in Physical, Virtual, and Cloud" (RH415) course is designed for security and system administration personnel who manage the secure operation of computer systems running Red Hat Enterprise Linux on physical hardware, as virtual machines, or as cloud instances both in private data centers and on public cloud platforms.
Maintaining the security of computing systems is a process of managing risk through the implementation of processes and standards backed by technologies and tools.
You will learn about technologies and tools that can be used to help you implement and comply with your security requirements, including the kernel's Audit subsystem, AIDE, SELinux, OpenSCAP and SCAP Workbench, USBGuard, PAM authentication, and Network-Based Device Encryption.
You will learn to monitor compliance and to proactively identify, prioritize, and resolve issues by using OpenSCAP, Red Hat Insights, Red Hat Satellite, and Red Hat Ansible Automation Platform.
You will have a basic introduction to how Red Hat Ansible Automation Platform automates the deployment of remediation to systems, by using Ansible Playbooks from OpenSCAP or Red Hat Insights.
This course is based on RHEL 9.2, Ansible Core 2.14, Red Hat Ansible Automation Platform 2.4, Satellite 6.14, and OpenSCAP 1.3.7.
***Note:** Starting January 1, 2026, Red Hat introduces RHLS-Course — a flexible subscription model now included with this catalog offering. This replaces the previous direct virtual class enrollment from Global Knowledge.*
When you purchase this item, you'll receive an RHLS subscription at the course level, giving you the freedom to choose the schedule that works best and self-enroll in your selected class.
Your RHLS subscription includes:
• One live, instructor-led virtual session
• 12 months of self-paced learning access
• One certification exam with a free retake
Onsite Classroom-based sessions and closed course options remain unchanged.
Updated Jan2026

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Target Audience:

System Administrator- responsible for supporting the company's physical and virtual infrastructure, systems, and servers IT Security Practitioner / Compliance & Auditor- responsible for ensuring the technology environment is protected from attacks and is in compliance with security/privacy rules and regulations.Automation Architect- Engineer or architect responsible for the company's automation development and optimizing cloud tools and infrastructure to achieve automation goals.

Objectives:

- After this course participants should be able to:
- Manage compliance with OpenSCAP.
- Enable SELinux on a server from a disabled state, perform basic analysis of the system policy, and mitigate risk with advanced SELinux techniques.
- Proactively identify and resolve issues with Red Hat Insights.
- Monitor activity and changes on a server with Linux Audit and AIDE.
- Protect data from compromise with USBGuard and storage encryption.
- Manage authentication controls with PAM.
- Manually apply provided Ansible Playbooks to automate mitigation of security and compliance issues.
- Scale OpenSCAP and Red Hat Insights management with Red Hat Satellite and Red Hat Ansible Automation Platform.

Prerequisites:

- Red Hat Certified Engineer (EX294 / RHCE) certification or equivalent Red Hat Enterprise Linux knowledge and experience.

Take Red Hat free assessment to gauge whether this offering is the best fit for your skills Red Hat Skills Assessment

Testing and Certification

- Red Hat Certified Specialist in Security: Linux exam (EX415)

Follow-on-Courses:

None

Content:

Managing Security and Risk

- Define and implement strategies to manage security on Red Hat Enterprise Linux systems.

Automating Configuration and Remediation with Ansible

- Remediate configuration and security issues automatically with Ansible Playbooks.

Protecting Data with LUKS and NBDE

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

Restricting USB Device Access

- Protect systems from rogue USB device access with USBGuard.

Controlling Authentication with PAM

- Manage authentication, authorization, session settings, and password controls by configuring Pluggable Authentication Modules (PAM).

Recording System Events with Audit

- Record and inspect system events relevant to security by using the Linux kernel's Audit system and supporting tools.

Monitoring File System Changes

- Detect and analyze changes to a server's file systems and their contents by using AIDE.

Mitigating Risk with SELinux

- Improve security and confinement between processes by using SELinux and advanced SELinux techniques and analysis.

Managing Compliance with OpenSCAP

- Evaluate and remediate a server's compliance with security policies by using OpenSCAP.

Analyzing and Remediating 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.

Automating Compliance with Red Hat Satellite

- Automate and scale OpenSCAP compliance checks by using Red Hat Satellite.

Comprehensive Review

- Review tasks from Red Hat Security: Linux in Physical, Virtual, and Cloud.

Additional Information:

Official course book provided to participants

Further Information:

For More information, or to book your course, please call us on Head Office Tel.: +974 40316639

training@globalknowledge.qa

www.globalknowledge.com/en-qa/

Global Knowledge, Qatar Financial Center, Burj Doha,Level 21, P.O.Box 27110, West Bay, Doha, Qatar