Red Hat Security: Linux in Physical, Virtual, and Cloud with Exam (EX415)

Category: Infrastructure & IT Operations | **Vendor:** Red Hat

Duration: 32.00 hours (4 days) **26.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	Red Hat Certified Specialist in Security
Related Exam:	EX415

Course Overview

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. Red Hat Security: Linux in Physical, Virtual, and Cloud (RH415) is designed for security administrators and system administrators who need to manage the secure operation of servers running Red Hat Enterprise Linux, whether deployed on physical hardware, as virtual machines, or as cloud instances. 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. The Red Hat Certified Specialist in Security: Linux Exam (EX415) is included in this offering.

Maintaining the 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.

About This Course

- 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.

Who Should Attend

- 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.

Prerequisites & Entry Requirements

General Prerequisites:

- Take our free assessment to gauge whether this offering is the best fit for your skills.
- Red Hat Certified Engineer (EX294 / RHCE) certification or equivalent Red Hat Enterprise Linux knowledge and experience.

Learning Outcomes

Upon successful completion of this course, participants will be able to:

Impact on the organization

This course is intended to develop the skills that are needed to reduce security risk and to implement, manage, and remediate compliance and security issues in an efficient way at scale. The tools and techniques can help to ensure that systems are configured and deployed in a way that meets security and compliance needs, that they continue to meet those requirements, and that as those requirements are revised, all existing systems can be audited, and remediations and changes consistently applied. This outcome may help the business to efficiently reduce the risk of security breaches, which have a high cost in business disruption, brand erosion, loss of customer and shareholder trust, and financial costs for post-incident remediation. In addition, the organization may be able to use the tools in this course to help demonstrate that the compliance requirements set by customers, auditors, or other stakeholders have been met.

Impact on the individual

- As a result of attending this course, students should be able to use security technologies included in Red Hat Enterprise Linux to manage security risk and help meet compliance requirements
- Analyze and remediate system compliance by using OpenSCAP and SCAP Workbench, and using and customizing baseline policy content that is provided with Red Hat Enterprise Linux
- Monitor security-relevant activity on your systems with the kernel's Audit infrastructure
- Explain and implement advanced SELinux techniques to restrict access by users, processes, and virtual machines
- Confirm the integrity of files and their permissions with AIDE
- Prevent unauthorized USB devices from being used with USBGuard
- Protect data at rest but provide secure automatic decryption at boot by using Network-Bound Device Encryption (NBDE)
- Proactively identify risks and misconfigurations of systems and remediate them with Red Hat Insights
- Analyze and remediate compliance at scale with OpenSCAP, Red Hat Insights, Red Hat Satellite, and Red Hat Ansible Automation Platform

Detailed Course Outline

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.

□□ Certification Path

Red Hat Certified Specialist in Security

Exam: EX415

Skills You Will Learn:

Impact on the organization

This course is intended to develop the skills that are needed to reduce security risk and to implement, manage, and remediate compliance and security issues in an efficient way at scale. The tools and techniques can help to ensure that systems are configured and deployed in a way that meets security and compliance needs, that they continue to meet those requirements, and that as those requirements are revised, all existing systems can be audited, and remediations and changes consistently applied. This outcome may help the business to efficiently reduce the risk of security breaches, which have a high cost in business disruption, brand erosion, loss of customer and shareholder trust, and financial costs for post-incident remediation. In addition, the organization may be able to use the tools in this course to help demonstrate that the compliance requirements set by customers, auditors, or other stakeholders have been met.

Impact on the individual

- As a result of attending this course, students should be able to use security technologies included in Red Hat Enterprise Linux to manage security risk and help meet compliance requirements
- Analyze and remediate system compliance by using OpenSCAP and SCAP Workbench, and using and customizing baseline policy content that is provided with Red Hat Enterprise Linux
- Monitor security-relevant activity on your systems with the kernel's Audit infrastructure
- Explain and implement advanced SELinux techniques to restrict access by users, processes, and virtual machines
- Confirm the integrity of files and their permissions with AIDE
- Prevent unauthorized USB devices from being used with USBGuard
- Protect data at rest but provide secure automatic decryption at boot by using Network-Bound Device Encryption (NBDE)
- Proactively identify risks and misconfigurations of systems and remediate them with Red Hat Insights
- Analyze and remediate compliance at scale with OpenSCAP, Red Hat Insights, Red Hat Satellite, and Red Hat Ansible Automation Platform

Frequently Asked Questions

Q: What delivery options are available for Red Hat Security: Linux in Physical, Virtual, and Cloud with Exam (EX415)?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The Red Hat Security: Linux in Physical, Virtual, and Cloud with Exam (EX415) course helps prepare you for the Red Hat Certified Specialist in Security certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the EX415 official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 4-day Red Hat Security: Linux in Physical, Virtual, and Cloud with Exam (EX415) course provides up to 26.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Red Hat Security: Linux in Physical, Virtual, and Cloud with Exam (EX415) training?

The training takes place over 4 day(s), with each day lasting approximately 32.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Red Hat Security: Linux in Physical, Virtual, and Cloud with Exam (EX415)?

Yes, we provide corporate training, dedicated training, and closed classes for Red Hat Security: Linux in Physical, Virtual, and Cloud with Exam (EX415). Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Red Hat Security: Linux in Physical, Virtual, and Cloud with Exam (EX415), Advanced System Administration, RH416

Q: Why choose Nexus Human for Red Hat Security: Linux in Physical, Virtual, and Cloud with Exam (EX415)?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Red Hat Security: Linux in Physical, Virtual, and Cloud with Exam (EX415) training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)