

Secure RHEL in Physical, Virtual & Cloud Environments

12 – 16 July 2027
Abu Dhabi

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Secure RHEL in Physical, Virtual & Cloud Environments

Ref: 103600402_80886 **Date:** 12 – 16 July 2027 **Location:** Abu Dhabi **Fees:** 4700 Euro

Course Overview:

The **Red Hat Security Exam Prep Course: Mastering EX415 for Secure Linux Systems** is an advanced, hands-on training program that equips IT professionals with the skills required to secure Red Hat Enterprise Linux RHEL systems across physical, virtual, and cloud environments. This course prepares participants for the Red Hat Certified Specialist in Security: Linux EX415 exam and aligns with the RH415 training course. By leveraging critical tools and technologies such as SELinux, AIDE, PAM, OpenSCAP, Red Hat Insights, USBGuard, and the Ansible Automation Platform, learners will gain the competencies to manage and automate system hardening, compliance enforcement, and intrusion prevention.

Participants will work with real-world scenarios to apply Linux system hardening techniques, automate remediation using Red Hat Ansible, monitor systems with Audit and AIDE, and enforce security compliance using SCAP-based tools. The course addresses both proactive and reactive security management, ensuring professionals can safeguard RHEL systems from internal and external threats in physical, virtualized, and cloud-hosted deployments.

Target Audience:

- System Administrators
- Linux Security Engineers
- Cloud Infrastructure Engineers
- IT Compliance Officers
- DevOps Engineers and Automation Architects

Targeted Organizational Departments:

- IT Security & Compliance
- Cloud Infrastructure Management
- Linux Server Administration
- DevOps & Automation Engineering
- Internal Audit & Risk Management

AGILE LEADERS
Training Center

Targeted Industries:

- Government & Defense for compliance and classified environments
- Banking & Financial Services for data protection and auditability
- Healthcare for HIPAA/ISO security needs
- Telecommunications & Tech Services
- Cloud Service Providers and Data Centers

Course Offerings:

By the end of this course, participants will be able to:

- Secure RHEL systems in physical, virtual, and cloud environments
- Use SELinux and AIDE for Linux system hardening
- Implement USBGuard and PAM Configuration for device and access control
- Configure and use OpenSCAP and Red Hat Insights for security compliance
- Automate remediation tasks using Red Hat Ansible Playbooks
- Monitor systems using Audit and manage encrypted storage with LUKS & NBDE
- Prepare thoroughly for the Red Hat EX415 course and exam

Training Methodology:

This course is designed with a practical, scenario-based training approach, combining live demonstrations, guided labs, and interactive simulations. Learners will engage in case studies based on real security threats, configuration challenges, and compliance requirements. Interactive sessions will simulate enterprise-level problems, requiring learners to troubleshoot, analyze, and apply secure configurations using RH415 best practices.

Participants will also experience hands-on labs replicating EX415 tasks, including using Red Hat SELinux and AIDE for intrusion detection, OpenSCAP policy enforcement, Red Hat Insights for proactive risk management, and Ansible for automated compliance. Peer discussions, group problem-solving, and feedback reviews ensure comprehensive understanding.

Course Toolbox:

- Digital course workbook with RH415-aligned exercises
- Ansible Playbook templates for security remediation
- OpenSCAP profiles and checklists
- SELinux user mapping guides
- AIDE monitoring configuration samples
- USBGuard policy examples
- RH415 practice scenarios and review sheets
- Access to virtual lab environment if applicable

AGILE LEADERS
Training Center

Course Agenda:

Day 1: Foundations of Secure RHEL Systems

- **Topic 1:** Introduction to Red Hat Security Certification and EX415
- **Topic 2:** Managing Risk & Security Strategy for Secure RHEL Systems
- **Topic 3:** Basic Ansible for Security Automation in RH415 Training
- **Topic 4:** Using Red Hat Ansible Playbooks for Remediation Tasks
- **Topic 5:** System Configuration Management with RH415 Tools
- **Topic 6:** Troubleshooting Security Automation Errors
- **Reflection & Review:** Key Takeaways from Day 1 and Ansible Lab Summary

Day 2: Authentication and Access Controls

- **Topic 1:** Implementing PAM for Linux Authentication Management
- **Topic 2:** Configuring Password Quality and Login Policies
- **Topic 3:** Session Controls with Pluggable Authentication Modules
- **Topic 4:** Device Access Control with USBGuard in RHEL
- **Topic 5:** Writing and Managing USBGuard Policies
- **Topic 6:** Troubleshooting Authentication and Device Security
- **Reflection & Review:** Review of PAM and USBGuard Configuration Labs

Day 3: Monitoring and Intrusion Detection

- **Topic 1:** Introduction to Linux Audit Subsystem and Use Cases
- **Topic 2:** Writing Audit Rules for Logging Critical Events
- **Topic 3:** Analyzing Audit Logs with ausearch and aureport
- **Topic 4:** File Integrity Monitoring with AIDE Setup and Configuration
- **Topic 5:** Generating and Validating AIDE Reports
- **Topic 6:** Hardening System Logs and Persistence Mechanisms
- **Reflection & Review:** Audit and AIDE System Hardening Recap

Day 4: Data Protection and SELinux Management

- **Topic 1:** Introduction to SELinux Modes and Policies
- **Topic 2:** Enabling and Troubleshooting SELinux Violations
- **Topic 3:** Configuring SELinux User Mappings and Roles
- **Topic 4:** Encrypting Storage with LUKS on RHEL
- **Topic 5:** Implementing NBDE for Encrypted Storage Automation
- **Topic 6:** Managing Disk Keys, Passphrases, and SELinux Policies
- **Reflection & Review:** SELinux and Storage Security Lab Reflections

Day 5: Compliance Enforcement and Certification Prep

- **Topic 1:** Using OpenSCAP Workbench and Profiles for Compliance
- **Topic 2:** Automating Compliance Remediation with Ansible
- **Topic 3:** Vulnerability Scanning with Red Hat Insights
- **Topic 4:** Scaling Compliance Using Red Hat Satellite Integration
- **Topic 5:** Exam Simulation Tasks and EX415 Preparation Strategies
- **Topic 6:** Final Lab: Applying End-to-End RHEL Security
- **Reflection & Review:** Consolidated Review and EX415 Exam Readiness

FAQ:

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

A Red Hat Certified System Administrator RHCSA certification or equivalent hands-on experience is strongly recommended. Familiarity with Red Hat Enterprise Linux command-line operations and basic administration is expected.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day's session is generally structured to last around 4-5 hours, with breaks and interactive activities included. The total course duration spans one week, approximately 20-25 hours of instruction.

What is the role of Ansible in Red Hat Security training?

Ansible is used to automate configuration remediation, apply OpenSCAP-based fixes, and deploy consistent hardening policies across multiple RHEL systems.

AGILE LEADERS
Training Center

How This Course is Different from Other Red Hat Security Certification Courses:

Unlike generic Linux security trainings, this course is tailored specifically to prepare participants for the Red Hat Certified Specialist in Security: Linux EX415 certification using the RH415 training framework. It integrates hands-on exposure to Red Hat-specific security tools like SELinux, AIDE, OpenSCAP, USBGuard, and PAM within real RHEL 9.2 environments.

The course emphasizes automation and compliance management using Red Hat Ansible, Red Hat Satellite, and Red Hat Insights, providing learners with scalable, enterprise-ready approaches to managing Linux system security. This training stands out for its practical simulations, real-world case scenarios, and tightly aligned exam-focused structure based on the most current EX415 objectives. The tools are not physically provided but demonstrated through case-based insights and virtual labs, empowering learners to confidently apply them in enterprise environments.