Red Hat Certified Specialist in Security: Linux Exam (EX415)

ID EX415 **Price** CHF 557.—(excl. VAT) **Duration** 1 day

Who should attend

These audiences may be interested in becoming a Red Hat Certified Specialist in Security: Linux:

- System administrators responsible for managing large enterprise environments
- System administrators responsible for securing their organization's infrastructure
- Red Hat Certified Engineers interested in pursuing the Red Hat Certified Architect (RHCA) credential

Prerequisites

- Be a Red Hat Certified System Administrator or have comparable work experience and skills (Red Hat Certified Engineer would be even better)
- Review the Red Hat Certified Specialist in Security: Linux exam objectives or have comparable work experience using Red Hat OpenStack Platform.

Preparation

Red Hat encourages all candidates for the Red Hat Certified Specialist in Security: Linux credential to consider taking Red Hat Security: Linux in Physical, Virtual, and Cloud (RH415) to help prepare. Attendance in these classes is not required; students can choose to take just the exam.

While attending Red Hat classes can be an important part of your preparation, attending class does not guarantee success on the exam. Previous experience, practice, and native aptitude are also important determinants of success.

Many books and other resources on system administration for Red Hat products are available. Red Hat does not endorse any of these materials as preparation guides for exams. Nevertheless, you may find additional reading helpful to deepen your understanding.

Course Objectives

To help you study, review the following exam objectives that highlight the task areas you can expect to see covered in the exam. Red Hat reserves the right to add, modify, and remove exam objectives. Such changes will be made public in advance.

Study points for the exam

Use Red Hat Ansible® Engine

- Install Red Hat Ansible Engine on a control node.
- Configure managed nodes.
- Configure simple inventories.
- Perform basic management of systems.
- Run a provided playbook against specified nodes.

Configure intrusion detection

- Install AIDE.
- Configure AIDE to monitor critical system files.

Configure encrypted storage

- Encrypt and decrypt block devices using LUKS.
- Configure encrypted storage persistence using NBDE.
- Change encrypted storage passphrases.

Restrict USB devices

- Install USBGuard.
- Write device policy rules with specific criteria to manage devices.
- Manage administrative policy and daemon configuration.

Manage system login security using pluggable authentication modules (PAMs)

- Configure password quality requirements.
- Configure failed login policy.
- Modify PAM configuration files and parameters.

Configure system auditing

- Write rules to log auditable events.
- Enable prepackaged rules.
- Produce audit reports.

Red Hat Certified Specialist in Security: Linux Exam (EX415)

Configure SELinux

- Enable SELinux on a host running a simple application.
- Interpret SELinux violations and determine remedial action.
- Restrict user activity with SELinux user mappings.
- Analyze and correct existing SELinux configurations.

Enforce security compliance

- Install OpenSCAP and Workbench.
- Use OpenSCAP and Red Hat Insights to scan hosts for security compliance.
- Use OpenSCAP Workbench to tailor policy.
- Use OpenSCAP Workbench to scan an individual host for security compliance.
- Use Red Hat Satellite server to implement an OpenSCAP policy.
- Apply OpenSCAP remediation scripts to hosts.

As with all Red Hat performance-based exams, configurations must persist after reboot without intervention.

Course Content

To help you study, review the following exam objectives that highlight the task areas you can expect to see covered in the exam. Red Hat reserves the right to add, modify, and remove exam objectives. Such changes will be made public in advance.

Use Red Hat Ansible® Engine

- Install Red Hat Ansible Engine on a control node.
- Configure managed nodes.
- Configure simple inventories.
- Perform basic management of systems.
- Run a provided playbook against specified nodes.

Implement access controls for automation controller

- Create and restrict an inventory to an automation controller user
- Restrict a credential and/or a project to an automation controller user
- Be able to create and launch a template as an automation controller user

Configure intrusion detection

- Install AIDE.
- Configure AIDE to monitor critical system files.

Configure encrypted storage

- Encrypt and decrypt block devices using LUKS.
- Configure encrypted storage persistence using NBDE.
- Change encrypted storage passphrases.

Restrict USB devices

- Install USBGuard.
- Write device policy rules with specific criteria to manage devices.
- Manage administrative policy and daemon configuration.

Manage system login security using pluggable authentication modules (PAMs)

- Configure password quality requirements.
- Configure failed login policy.
- Modify PAM configuration files and parameters.

Configure system auditing

- Write rules to log auditable events.
- Enable prepackaged rules.
- Produce audit reports.

Configure SELinux

- Enable SELinux on a host running a simple application.
- Interpret SELinux violations and determine remedial action.
- Restrict user activity with SELinux user mappings.
- Analyze and correct existing SELinux configurations.

Enforce security compliance

- Install OpenSCAP and OpenSCAP Workbench.
- Scan hosts for security compliance
- Tailor security policy
- Scan individual hosts for security compliance
- Generate and apply a playbook from customized XML for remediation of inventory hosts
- As with all Red Hat performance-based exams, configurations must persist after reboot without intervention.

Exam format

This exam is a performance-based evaluation of skills and knowledge required to secure Red Hat Enterprise Linux systems. Candidates work with multiple systems to analyze and implement security measures and are evaluated on whether they have met specific objective criteria. Performance-based testing means that candidates must perform tasks similar to what they perform on the job.

Scores and reporting

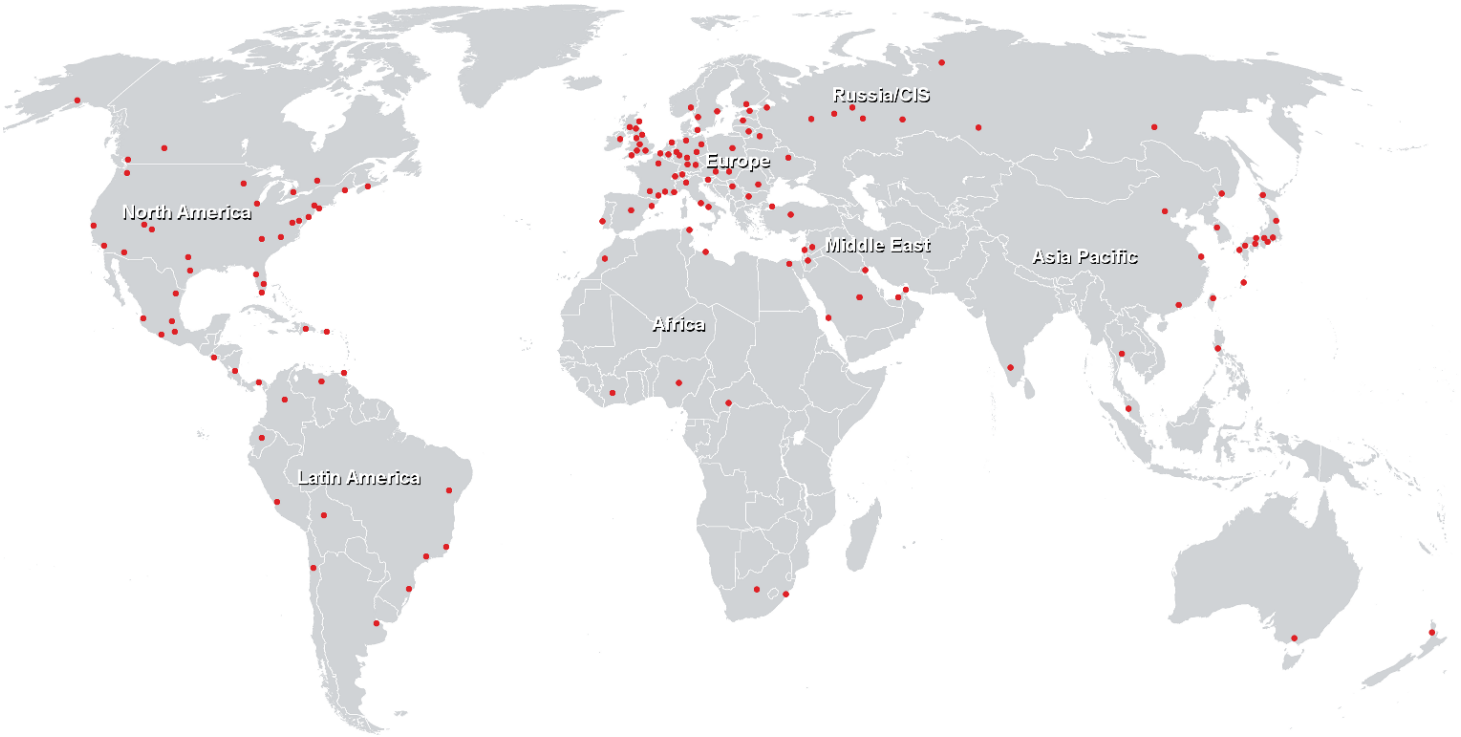
Official scores for exams come exclusively from Red Hat Certification Central. Red Hat does not authorize examiners or training partners to report results to candidates directly. Scores on the exam are usually reported within 3 U.S. business days.

Exam results are reported as total scores. Red Hat does not report performance on individual items, nor will it provide additional information upon request.

You are eligible for one exam retake if you are unsuccessful on your first attempt.

Red Hat Certified Specialist in Security: Linux Exam (EX415)

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch