



Red Hat Security: Identity Management and Active Directory Integration

COURSE OVERVIEW

**Course Modality**

Classroom
+ hands-on labs

**Course Time**

4 days

**Course Level**

Intermediate

**Course Language**

English

Red Hat Security: Identity Management and Active Directory Integration (RH362) provides the skills to configure and manage IdM, the comprehensive Identity Management solution bundled with Red Hat® Enterprise Linux.

This course teaches you skills on the most requested Red Hat Identity Management (IdM) capabilities, including Active Directory trusts, multi-product federation, configuration management with Ansible, integrated certificate management, single sign-on, one-time passwords, and cybersecurity policy conformance.

Prerequisites:

- ✓ Be certified as a Red Hat Certified System Administrator (RHCSA) (required)
- ✓ Be certified as a Red Hat Certified Engineer (RHCE)

(recommended, but not required)

Intended Audience:

Red Hat Certified System Administrator (RHCSA) who wants to learn how to provision and configure IdM technologies across both Linux and Windows applications

- ✓ Identity management specialist or engineer
- ✓ Access management specialist or engineer
- ✓ Web application developer
- ✓ DevOps specialist

Skill Covered:

- ✓ Install Red Hat Identity Management servers, replicas, and clients.
- ✓ Configure and manage Kerberos authentication and secure services.
- ✓ Create and manage a trust relationship with Microsoft Active Directory.
- ✓ Configure highly secure user authentication—local and remote—including two-factor authentication.
- ✓ Manage secrets, vaults, certificates, and keys.

- ✓ Troubleshoot identity management processes.
- ✓ Integrate Satellite 6 with IdM.
- ✓ Integrate Tower with IdM.
- ✓ Configure IdM backup and recovery.

COURSE CURRICULUM

Module 1:

Install Red Hat Identity Management

Describe and install Red Hat Identity Management (IdM).

Module 2:

Centralize Identity Management

Explain the IdM server services, explore IdM clients access methods, and install an IdM client.

Module 3:

Authenticate identities with Kerberos

Define the Kerberos protocol and configure services for Kerberos authentication.

Module 4:

Integrate IdM with Active Directory

Create a trust relationship with Active Directory.

Module 5:

Control user access

Configure users for authorized access to services and resources.

Module 6:

Manage a public key infrastructure

Manage certificate authorities, certificates, and storing secrets.

Module 7:

Maintain IdM operations

Troubleshoot and recover Identity Management.

Module 8:

Integrate Red Hat products with IdM

Configure major services to share the IdM authentication database.

Module 9:

Install scalable IdM

Construct a resilient and scalable Identity Management topology.

RECOMMENDED EXAMS



Red Hat Certified Specialist in Identity Management exam (EX362)

Classroom or Digital | 130 minutes

Red Hat Certified Specialist in Identity Management

Classroom or Digital | 90 minutes