

RH363: Red Hat Security: Identity Management and Authentication with Exam

Course Code: RH363

Duration: 4 days

Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

Configure and manage Red Hat Identity Management (IdM)

Red Hat Security: Identity Management and Authentication with Exam (RH363) 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. Red Hat Certified Specialist in Identity Management exam is included in this bundle.

SKILLS 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.

WHO SHOULD ATTEND?

- 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

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)

MODULES

Module 1: Identity Management in Red Hat Enterprise Linux

- Introduce Identity Management in Red Hat Enterprise Linux (IdM) and its high-level architecture

Module 2: Identity Management Core Technologies

- Review the core technologies of Identity Management (IdM) in Red Hat Enterprise Linux

map POSIX attributes to Active Directory users

Module 3: Installing Identity Management in Red Hat Enterprise Linux

- Install Identity Management servers, replicas, and clients on Red Hat Enterprise Linux 9

Module 4: Implementing an Identity Management Topology

- Implement continuous functionality and high availability of IdM services in single-site and geographically distributed topologies

Module 5: Managing the CA and DNS Integrated Services

- Manage the Certificate Authority (CA) and the Domain Name System (DNS) services that are integrated with Identity Management

Module 6: Managing Users and Controlling User Access

- Configure users for authorized access to services and resources

Module 7: Configuring Alternative Authentication Services

- Configure and manage smart card authentication, secrets, and two-factor authentication

Module 8: Integrating Identity Management with Active Directory

- Implement a cross-forest trust between Identity Management and Active Directory, and configure ID views to

Module 9: Integrating Identity Management with Red Hat Utilities

- Integrate an Identity Management deployment with Red Hat Satellite and Red Hat Ansible Automation Platform

Module 10: Troubleshooting and Disaster Recovery Planning for IdM

- Troubleshooting and preparing for disaster recovery with Identity Management

Module 11: Comprehensive Review

- Build a small, resilient Identity Management topology to include multiple replicas and clients, populated with multiple users, credentials, policies, and access rights

END OF PAGE