

Red Hat Security: Identity Management and Active Directory Integration with Exam

Code:	RH363
Length:	5 days
URL:	View Online

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.

- 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.

Skills Gained

- Create and manage a scalable, resilient Identity Management realm, including both Linux and Microsoft Windows clients and servers.
- Create and manage secure access configurations, including managing and troubleshooting Kerberos, certificate servers, and access control policies.
- Integrate IdM as the back end for other major enterprise tools in the Red Hat portfolio, including Satellite Server and Tower.

Who Can Benefit

- 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

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)

Course Details

Course Outline

- Install Red Hat Identity Management
- Describe and install Red Hat Identity Management (IdM).
- Centralize Identity Management
- Explain the IdM server services, explore IdM clients access methods, and install an IdM client.
- Authenticate identities with Kerberos
- Define the Kerberos protocol and configure services for Kerberos authentication.
- Integrate IdM with Active Directory
- Create a trust relationship with Active Directory.
- Control user access
- Configure users for authorized access to services and resources.
- Manage a public key infrastructure
- Manage certificate authorities, certificates, and storing secrets.
- Maintain IdM operations
- Troubleshoot and recover Identity Management.
- Integrate Red Hat products with IdM
- Configure major services to share the IdM authentication database.
- Install scalable IdM
- Construct a resilient and scalable Identity Management topology.

Download Whitepaper: Accelerate Your Modernization Efforts with a Cloud-Native Strategy

Get Your Free Copy Now