Red Hat Security: Identity Management and Authentication (RH362)

Price	Duration	Delivery Methods
$4,280.00	5 Days	VILT, Private Group

This course will empower you with the skills to configure and manage IdM, the comprehensive Identity Management solution bundled with Red Hat® Enterprise Linux. You will master these 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.

Who Should Attend

Identity management specialist or engineer Access management specialist or engineer Web application developer DevOps specialist 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 Objectives

- 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.

Agenda

1 - INSTALL RED HAT IDENTITY MANAGEMENT

- Describe and install Red Hat Identity Management (IdM).

2 - INTRODUCTION TO TROUBLESHOOTING

- Describe a generalized strategy for troubleshooting.

3 - CENTRALIZE IDENTITY MANAGEMENT

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

4 - TAKE PROACTIVE STEPS TO PREVENT SMALL ISSUES

- Prevent small issues from becoming large problems by employing proactive system administration techniques.

5 - AUTHENTICATE IDENTITIES WITH KERBEROS

- Define the Kerberos protocol and configure services for Kerberos authentication.

6 - TROUBLESHOOT BOOT ISSUES

- Identify and resolve issues that can affect a system's ability to boot.

7 - IDENTIFY HARDWARE ISSUES

- Identify hardware problems that can affect a system’s ability to operate.

8 - INTEGRATE IDM WITH ACTIVE DIRECTORY

- Create a trust relationship with Active Directory.

9 - CONTROL USER ACCESS

- Configure users for authorized access to services and resources.

10 - TROUBLESHOOT STORAGE ISSUES

- Identify and fix issues related to storage.

11 - MANAGE A PUBLIC KEY INFRASTRUCTURE

- Manage certificate authorities, certificates, and storing secrets.

12 - TROUBLESHOOT RPM ISSUES

- Identify and fix problems in, and using, the package management subsystem.

13 - MAINTAIN IDM OPERATIONS

- Troubleshoot and recover Identity Management.

14 - TROUBLESHOOT NETWORK ISSUES

- Identify and resolve network connectivity issues.

15 - INTEGRATE RED HAT PRODUCTS WITH IDM

- Configure major services to share the IdM authentication database.

16 - TROUBLESHOOT APPLICATION ISSUES

- Debug application issues.

17 - DEAL WITH SECURITY ISSUES

- Identify and fix issues related to security subsystems.

18 - INSTALL SCALABLE IDM

- Construct a resilient and scalable Identity Management topology.

19 - TROUBLESHOOT KERNEL ISSUES

- Identify kernel issues and assist Red Hat Support in resolving kernel issues.

20 - RED HAT ENTERPRISE LINUX DIAGNOSTICS AND TROUBLESHOOTING COMPREHENSIVE REVIEW

- Practice and demonstrate knowledge and skills learned in Red Hat Enterprise Linux Diagnostics and Troubleshooting.