Red Hat Security: Identity Management and Authentication (RH362)

Duration: 4 Days

Course Description:

Red Hat Security: Identity Management and Authentication (RH362) provides the skills to configure and manage Identity Management (IdM), the comprehensive identity management component bundled with Red Hat Enterprise Linux. This course helps students to gain the skills with this technology most requested by customers.

Some topics covered in this course are central management and provisioning of user accounts; design and installation of IdM server topologies; operation of the integrated DNS and TLS Certificate Authority services; management of two-factor authentication, smart card authentication, and operation as a single-sign on provider; integration and management of two-way trusts with Active Directory; and troubleshooting and disaster recovery planning. Registration of Linux clients to IdM and operation in enterprise environments that use both Linux and Microsoft Windows clients and servers is discussed.

Intended Audience:

Red Hat Certified System Engineers (RHCE) who wish to learn how to provision and configure centralized identity management solutions for Linux clients and how to integrate them with other network services and identity management systems.

- Identity Management specialists or engineers
- Access Management specialists or engineers

Course Outlines:

Identity Management in Red Hat Enterprise Linux

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

Identity Management Core Technologies

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

Installing Identity Management in Red Hat Enterprise Linux

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

Implementing an Identity Management Topology

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

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.

Managing Users and Controlling User Access

- Configure users for authorized access to services and resources.

Configuring Alternative Authentication Services

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

Integrating Identity Management with Active Directory

- Implement a cross-forest trust between Identity Management and Active Directory, and configure ID views to map POSIX attributes to Active Directory users.

Integrating Identity Management with Red Hat Utilities

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

Troubleshooting and Disaster Recovery Planning for IdM

- Troubleshooting and preparing for disaster recovery with Identity Management.

Comprehensive Review

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