Red Hat Single Sign-On Administration Course

Course Duration: 24 Hours **Course code: DO313**

1. Course Overview

This Three-day course focuses on administering, configuring, and managing Red Hat Single Sign-On (RH-SSO) to enable secure authentication and authorization across enterprise applications. You will learn how to implement identity and access management (IAM), configure realms, users, and roles, integrate applications using SSO protocols, and extend RH-SSO functionality using APIs and custom integrations.

2. What you'll learn?

By the end of the course, you will be able to:

- Understand the architecture and components of Red Hat Single Sign-On
- Configure realms, clients, users, groups, and roles
- Implement authentication and authorization mechanisms
- Integrate applications using SAML, OAuth2, and OpenID Connect
- Manage identity brokering and social login integrations
- Configure multi-factor authentication (MFA)
- Use REST APIs for automation and integration
- Monitor, troubleshoot, and secure RH-SSO deployments

3. Target Audience

This course is ideal for:

- System Administrators
- Identity and Access Management (IAM) Professionals
- DevOps Engineers
- Security Engineers

- Application Developers and Integrators

4. Pre-Requisites

Before taking this course, you should have:

- Basic knowledge of Linux system administration
- Understanding of web applications and HTTP/HTTPS
- Familiarity with authentication concepts (LDAP, OAuth, SAML)
- Basic scripting knowledge (optional but recommended)

5. Course content

Module 1: Course Introduction

- Introduction to RH-SSO course and objectives
- Course structure and lab environment overview

Module 2: Overview of Red Hat Single Sign-On

- Introduction to Identity and Access Management (IAM)
- Purpose and benefits of RH-SSO
- RH-SSO architecture and components
- Keycloak fundamentals (upstream project)

Module 3: Installation and Initial Configuration

- RH-SSO installation methods (Standalone & Containerized)
- Server startup and configuration
- Admin console overview
- Configuring initial settings

Module 4: Realms and Tenants

- Understanding realms in RH-SSO
- Creating and managing realms

- Realm settings and configurations
- Multi-tenancy concepts

Module 5: User and Role Management

- Creating and managing users
- User federation (LDAP/AD integration)
- Managing roles (realm roles and client roles)
- Group management and role mapping

Module 6: Authentication and Authorization

- Authentication flows and execution
- Customizing login flows
- Authorization services overview
- Policy-based access control

Module 7: Working with Clients and Protocols

- Creating and configuring clients
- OpenID Connect (OIDC) implementation
- SAML integration
- Securing applications using RH-SSO

Module 8: Identity Brokering and Social Login

- Identity federation concepts
- Configuring identity providers
- Social login integration (Google, GitHub, etc.)
- Single Sign-On and Single Logout (SSO/SLO)

Module 9: Multi-Factor Authentication (MFA)

- Implementing MFA in RH-SSO
- Configuring OTP and authenticator apps

- Adaptive authentication strategies

Module 10: Customization and Extensions

- Custom themes (login UI customization)
- Extending RH-SSO functionality
- Writing custom authenticators
- Using Service Provider Interfaces (SPI)

Module 11: REST APIs and Automation

- Introduction to RH-SSO REST APIs
- Managing users and clients via APIs
- Automating administrative tasks
- Integration with external systems

Module 12: Security and Best Practices

- Securing RH-SSO deployments
- SSL/TLS configuration
- Token management and session handling
- Best practices for IAM security

Module 13: Monitoring, Logging, and Troubleshooting

- Logging configuration and analysis
- Monitoring RH-SSO health
- Troubleshooting authentication issues
- Performance tuning

Module 14: Backup, Migration, and High Availability

- Backup and restore strategies
- Migrating configurations between environments

- High availability and clustering concepts
- Load balancing RH-SSO

Module 15: Integration Use Cases and Hands-on Labs

- Real-world integration scenarios
- Securing web and API applications
- End-to-end SSO implementation
- Practical labs and exercises