

Red Hat OpenShift Administration II

Duration: 4 Days

Description

This training is designed to provide advanced knowledge and competencies required to securely, sustainably, and scalably configure and manage production-level OpenShift clusters in enterprise environments.

Participants gain hands-on experience in critical operational areas such as enabling secure self-service across multiple teams, configuring authentication and authorization, implementing network security controls, managing Operators, and performing cluster updates. By the end of the course, participants will be able to manage production clusters with minimal disruption to running applications.

Within the scope of this training, participants will learn to:

- Enable secure self-service configurations for cluster users with different roles
- Deploy applications that require elevated permissions, such as CI/CD tooling, performance monitoring solutions, and security scanners
- Configure multi-tenancy and OpenShift security features
- Manage Operator-based OpenShift add-ons and extensions

Outline

Declarative Resource Management

- Parameterized manifest structures for different target environments
- Application deployment using resource manifest files
- Application update processes through manifests
- Environment-based configuration management

Deploying Packaged Applications

- Shareable and distributable application packages
- Usage of packaged manifest structures

- Application version upgrade and maintenance processes

Authentication and Authorization

- HTTPBasic identity provider configuration
- User and group management
- Role assignments and access control mechanisms
- RBAC-based authorization management

Network Security

- Securing traffic between applications within the cluster
- Controlling external access to the cluster
- Network policy configuration
- Designing secure communication architectures

Exposing Non-HTTP/SNI Applications

- Publishing applications without using an Ingress Controller
- External access scenarios
- Alternative exposure methods and configurations

Enabling Developer Self-Service

- Secure self-service configuration in multi-team environments
- Project-based authorization models
- Restricting self-service when projects are provisioned by operations teams
- Secure multi-tenancy design

Managing Kubernetes Operators

- Operator Lifecycle Manager (OLM) architecture
- Cluster Version Operator management
- Operator installation and updates
- Operator lifecycle management

Application Security

- Applications requiring elevated privileges
- Host operating system access scenarios
- Kubernetes security policies
- Secure container runtime principles

OpenShift Updates

- OpenShift cluster update strategies
- Version upgrades with minimal disruption
- Operator and component updates
- Update planning in production environments

Prerequisites

Proficiency in fundamental OpenShift and Kubernetes concepts

Basic knowledge of container technologies (Docker/OCI)

Experience using the Linux command line

Completion of OpenShift Administration I or equivalent knowledge level