# Red Hat OpenShift Administration II: Configuring a Production Cluster (DO280) Training

Duration: **4 Day**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

## Overview

**Configure, secure, and manage Red Hat OpenShift clusters for enterprise-grade workloads.**

The {*training} equips system and platform administrators with the skills needed to manage production OpenShift clusters that host multiple applications and development teams.

Participants will learn to configure **authentication and authorization**, **multi-tenancy**, **network and application security**, and to manage **OpenShift add-ons** via Operators. The course also covers enabling **developer self-service**, managing **cluster updates**, and deploying applications that require advanced privileges such as CI/CD pipelines, monitoring agents, and security tools.

> *This course is based on Red Hat OpenShift Container Platform 4.18 and applies to all deployment types, including ROSA, ARO, and OpenShift Container Platform.*

## Who Should Attend

This course is designed for:

**Primary Audience:**

- Platform Engineers
- System Administrators
- Cloud Administrators
- Infrastructure Engineers managing OpenShift environments

**Secondary Audience:**

- Enterprise Architects
- Site Reliability Engineers (SREs)
- DevOps Engineers designing and supporting OpenShift infrastructure

## What You Will Learn

By the end of this {*training}, you will have gained knowledge and skills in the following areas:

- Deploy applications using **manifests, Helm, Kustomize, and templates**.
- Configure **user and application authentication and authorization**.
- Secure internal and external **network traffic** with policies and routes.
- Manage **Kubernetes resources declaratively** for predictable deployments.

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700


- Enable **developer self-service** safely within multi-team environments.
- Manage **Operator and cluster lifecycle updates**.
- Run **privileged or restricted workloads** securely.

## Impact on the Organization

Organizations adopting Red Hat OpenShift benefit from a**secure, reliable, and scalable application platform** built on Kubernetes.

This course enables IT teams to:

- Manage **multi-tenant OpenShift environments** efficiently.
- Standardize operational processes across **cloud and on-premise infrastructures**.
- Strengthen **application security and compliance** with Kubernetes-native tools.
- Collaborate with Red Hat SRE teams when using**managed OpenShift services** (e.g., ROSA, ARO).

By mastering these skills, organizations ensure **consistent performance, improved developer productivity, and operational resilience** across all environments.

## Impact on the Individual

After completing this course, you will be able to:

- Configure authentication, authorization, and role-based access for OpenShift users.
- Manage and secure multi-tenant environments for multiple teams.
- Deploy, monitor, and update applications using OpenShift's declarative resources.
- Configure and maintain Operator-based add-ons for enhanced functionality.
- Secure workloads that require elevated privileges.
- Perform OpenShift cluster upgrades and maintain high availability during updates.

These skills prepare you to perform the**daily responsibilities of an OpenShift cluster administrator** across on-premise, cloud, or managed environments.

# Red Hat OpenShift Administration II: Configuring a Production Cluster (DO280) Training

Duration: **4 Day**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

## Outline

**1. Declarative Resource Management**
Deploy and update applications using parameterized manifests to suit different environments.

**2. Deploy Packaged Applications**
Use templates, Helm charts, and Kustomize to distribute and update reusable application packages.

**3. Authentication and Authorization**
Configure HTPasswd identity provider and define user roles, groups, and access policies.

**4. Network Security**
Protect communication between applications inside and outside the cluster using NetworkPolicies and secure routes.

**5. Expose Non-HTTP/SNI Applications**
Configure external access for TCP/UDP applications that do not use traditional HTTP/SNI ingress.

**6. Developer Self-Service**
Enable safe project self-service for development teams or restrict it to administrators when necessary.

**7. Managing Kubernetes Operators**
Install, update, and manage Operators using the Operator Lifecycle Manager (OLM) and Cluster Version Operator (CVO).

**8. Application Security**
Deploy and manage workloads that require elevated privileges or direct host access securely.

**9. OpenShift Cluster Updates**
Perform cluster upgrades while minimizing disruption to running workloads and user access.