+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 03/17/2026

Sign up

OpenShift Training for Kubernetes DevOps Engineers

3 days (21 hours)

Overview

Red Hat OpenShift is Red Hat's enterprise Kubernetes platform. It adds a secure PaaS model, an ecosystem of Operators, and native mechanisms to Kubernetes to industrialize the deployment and operation of applications.

In practice, a deployment that works on Kubernetes may fail on OpenShift due to security constraints (SCCs), dynamic user identities, or differences in network exposure via Routes.

This training is intended for Kubernetes DevOps engineers who need to migrate, adapt, and ensure the reliability of workloads on OpenShift: getting started with the cluster, understanding SCCs, adapting Helm charts, advanced on-premises administration, and security best practices.

It also covers industrialization using Tekton and ArgoCD, application lifecycle management via OLM, as well as observability and troubleshooting.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Understand the differences between OpenShift (OCP) and Kubernetes.
- Install and manage an OpenShift cluster (on-premises + cloud).
- Migrate your workloads and Helm charts to OpenShift.
- Package your application as a distributed Operator via OLM.
- Set up monitoring, CI/CD, and security on OpenShift.

Target Audience

- DevOps engineers proficient in Kubernetes (deployments, Helm, RBAC, K8s networking)
- Teams looking to make a solution OpenShift-compatible for a client or ISV context

Prerequisites

- Operational experience with Kubernetes (kubectl, Helm, Pods/Services/Ingress/PV concepts)
- Basic Linux knowledge

OpenShift for Kubernetes DevOps Engineers

[Day 1 - Morning]

OpenShift vs. Kubernetes: The Fundamentals

- OpenShift's Position in the Red Hat/IBM Ecosystem
- OCP Architecture: Control Plane, etcd, CRI-O, HAProxy, internal registry
- Security Differences: SCC vs. PodSecurityPolicy/PSA
- Routes vs. Ingress, NetworkPolicy, and OVN-Kubernetes
- OperatorHub and OLM: the OpenShift App Store
- Extended RBAC and projects (enhanced namespaces)

[Day 1 - Afternoon]

First steps with an OpenShift cluster

- OpenShift Web Console vs. kubectl/oc
- UI Differences: Developer vs. Administrator
- Inspect available SCCs and compare with K8s PSA
- Deploying a custom image: understanding the default failure
- Fix the deployment via SCC or ServiceAccount patch
- Hands-on Workshop: Lab 1: First Steps with OCP + SCC (diagnosis and correction).

On-premises installation and adaptation of K8s workloads

- Assisted Installer vs. IPI vs. UPI
- Prerequisites: DNS, load balancer, certificates, NTP, mirror registry
- Topologies: bare-metal, VMware vSphere, RHV/oVirt
- MCO and MachineConfigPool, certificate rotation, custom ingress cert
- Adapting workloads: Helm porting, non-root images, compatibility checklist (SCC/NetworkPolicy/ImagePullPolicy)
- Hands-on workshop: Lab 2: Simulated installation & post-installation + workload adaptation.

[Day 2 - Morning]

Advanced on-premises administration

- In-depth look at MCO: MachineConfig, MachineConfigPool
- Cluster update: EUS, stable/fast channels, over-the-air update
- etcd: backup/restore, quorum, replacing a master
- Nodes: drain/cordon, labels, taints & tolerations
- Storage: CSI drivers, ODF introduction; internal registry (S3/storage)
- Hands-on workshop: Lab 3: On-premises cluster administration (MC, update, etcd backup, nodes, StorageClass/PVC).

[Day 2 - Afternoon]

OpenShift on the Cloud and multi-cluster with ACM

- ROSA and ARO: architecture, shared responsibilities, SLA
- Differences between cloud and on-premise administration
- ACM: multi-cluster governance, placement rules, ApplicationSets
- ACM policies: compliance, application tests, remediation
- Multi-cluster observability from ACM
- Hands-on workshop: Lab 4: Multi-cluster deployment (ApplicationSet + policies + observability).

Advanced security on OpenShift

- SCC in depth: restricted-v2, anyuid, privileged, custom SCC
- Pod Security Admission vs. SCC: coexistence and migration
- ACS/StackRox: runtime scanning, network graph
- Secrets management: HashiCorp Vault, External Secrets Operator
- Audit & compliance: FIPS, CIS, OCP benchmark

[Day 3 - Morning]

CI/CD, GitOps, and Operators on OpenShift

- OpenShift Pipelines (Tekton): Tasks, Pipelines, Triggers, PipelineRuns
- OpenShift GitOps (ArgoCD): ApplicationSet, App-of-Apps
- Create a Helm-based Operator using the Operator SDK
- Lifecycle via OLM: CatalogSource, Subscription, InstallPlan, upgrades
- Publish to a private CatalogSource and ISV distribution
- Hands-on Workshop: Lab 5: Complete CI/CD Pipeline + Distributed Custom Operator.

[Day 3 - Afternoon]

Monitoring, observability, and troubleshooting

- Enable User Workload Monitoring and create PrometheusRules
- Logging: Loki vs. Elasticsearch, log forwarding to an external SIEM
- Custom metrics: exposing Prometheus from the application
- Troubleshooting: must-gather, sosreport, debug node, oc debug/oc rsh/oc adm inspect
- Common issues: crashloopbackoff, image pull errors, SCC denied
- Hands-on workshop: Lab 6: Application monitoring & troubleshooting (Grafana, log forwarding, scenarios).

Practical Exercise & EX280 Certification

- Full port of an ISV app: “vanilla” Helm K8s? OpenShift
- Identify bottlenecks: SCC, images, network, storage
- Adapt the chart, create the Operator, deploy via OLM
- Set up monitoring + logs + alerting
- Presentation of results by group
- Hands-on workshop: General overview, EX280 certification, resources, and community.

Target Audience

This training is intended for both individuals and companies, large or small, wishing to train their teams in new advanced IT technologies or to acquire specific business knowledge or modern methods.

Assessment upon enrollment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals regarding the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Practical Course: 60% Practical, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical instruction from the instructor—supported by examples and discussion sessions—and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been properly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training program.