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

Mis à jour le 04/03/2026

S'inscrire

Formation OpenShift pour ingénieurs DevOps Kubernetes

3 jours (21 heures)

Présentation

Red Hat OpenShift est la plateforme Kubernetes enterprise de Red Hat. Elle ajoute à Kubernetes un modèle PaaS sécurisé, un écosystème d'Operators et des mécanismes natifs pour industrialiser le déploiement et l'exploitation des applications.

Dans la pratique, un déploiement qui fonctionne sur Kubernetes peut échouer sur OpenShift à cause des contraintes de sécurité (SCC), des identités utilisateurs dynamiques, ou des différences d'exposition réseau via Routes.

Cette formation s'adresse aux ingénieurs DevOps Kubernetes qui doivent migrer, adapter et fiabiliser des workloads sur OpenShift : prise en main du cluster, compréhension des SCC, adaptation de charts Helm, administration on-premise avancée et bonnes pratiques de sécurité.

Elle aborde également l'industrialisation via Tekton, ArgoCD et la gestion du cycle de vie applicatif via OLM, ainsi que l'observabilité et le troubleshooting.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre les spécificités OpenShift (OCP) vs Kubernetes.
- Installer et administrer un cluster OpenShift (on-prem + cloud).
- Porter ses workloads et charts Helm sur OpenShift.
- Packager son application en Operator distribué via OLM.
- Mettre en place monitoring, CI/CD et sécurité sur OpenShift.

Public visé

- Ingénieurs DevOps maîtrisant Kubernetes (déploiements, Helm, RBAC, networking K8s)
- Équipes souhaitant rendre une solution compatible OpenShift pour un contexte client / ISV

Pré-requis

- Expérience opérationnelle Kubernetes (kubectl, Helm, concepts Pods/Services/Ingress/PV)
- Connaissances de base Linux

OpenShift pour ingénieurs DevOps Kubernetes

[Jour 1 - Matin]

OpenShift vs Kubernetes : les fondamentaux

- Positionnement d'OpenShift dans l'écosystème Red Hat / IBM
- Architecture OCP : Control Plane, etcd, CRI-O, HAProxy, registry interne
- Différences sécurité : SCC vs PodSecurityPolicy/PSA
- Routes vs Ingress, NetworkPolicy et OVN-Kubernetes
- OperatorHub et OLM : l'App Store OpenShift
- RBAC étendu et projects (namespaces augmentés)

[Jour 1 - Après-midi]

Premier contact avec un cluster OpenShift

- Console Web OpenShift vs kubectl/oc
- Différences UI : Developer vs Administrator
- Inspecter les SCC disponibles et comparer avec PSA K8s
- Déployer une image custom : comprendre l'échec par défaut
- Corriger le déploiement via SCC ou patch de ServiceAccount
- Atelier pratique : Lab 1 : Premier contact OCP + SCC (diagnostic et correction).

Installation on-premise et adaptation des workloads K8s

- Assisted Installer vs IPI vs UPI
- Prérequis : DNS, load-balancer, certificats, NTP, registre miroir
- Topologies : bare-metal, VMware vSphere, RHV/oVirt
- MCO et MachineConfigPool, rotation certificats, ingress cert custom
- Adapter les workloads : portage Helm, images non-root, checklist compat (SCC/NetworkPolicy/ImagePullPolicy)
- Atelier pratique : Lab 2 : Installation simulée & post-install + adaptation workload.

[Jour 2 - Matin]

Administration on-premise avancée

- MCO en profondeur : MachineConfig, MachineConfigPool
- Update du cluster : EUS, canaux stable/fast, over-the-air update
- etcd : backup/restore, quorum, remplacement d'un master
- Nœuds : drain/cordon, labels, taints & tolerations
- Stockage : CSI drivers, intro ODF ; registry interne (S3/stockage)
- Atelier pratique : Lab 3 : Administration cluster on-prem (MC, update, backup etcd, nœuds, StorageClass/PVC).

[Jour 2 - Après-midi]

OpenShift sur le Cloud et multi-cluster avec ACM

- ROSA et ARO : architecture, responsabilités partagées, SLA
- Différences d'administration cloud vs on-premise
- ACM : gouvernance multi-cluster, placement rules, ApplicationSets
- Politiques ACM : compliance, application tests, remédiation
- Observabilité multi-cluster depuis ACM
- Atelier pratique : Lab 4 : Déploiement multi-cluster (ApplicationSet + policies + observabilité).

Sécurité avancée sur OpenShift

- SCC en profondeur : restricted-v2, anyuid, privileged, SCC custom
- Pod Security Admission vs SCC : coexistence et migration
- ACS/StackRox : scanning runtime, network graph
- Secrets management : HashiCorp Vault, External Secrets Operator
- Audit & conformité : FIPS, CIS benchmark OCP

[Jour 3 - Matin]

CI/CD, GitOps et Operators sur OpenShift

- OpenShift Pipelines (Tekton) : Tasks, Pipelines, Triggers, PipelineRuns
- OpenShift GitOps (ArgoCD) : ApplicationSet, App-of-Apps
- Créer un Operator Helm-based via Operator SDK
- Cycle de vie via OLM : CatalogSource, Subscription, InstallPlan, upgrades
- Publier dans un CatalogSource privé et distribution ISV
- Atelier pratique : Lab 5 : Pipeline CI/CD complet + Operator custom distribué.

[Jour 3 - Après-midi]

Monitoring, observabilité et troubleshooting

- Activer User Workload Monitoring et créer des règles PrometheusRule
- Logging : Loki vs Elasticsearch, log forwarding vers SIEM externe
- Métriques custom : exposer Prometheus depuis l'applicatif
- Troubleshooting : must-gather, sosreport, debug node, oc debug/oc rsh/oc adm inspect
- Cas typiques : crashloopbackoff, image pull errors, SCC denied
- Atelier pratique : Lab 6 : Monitoring applicatif & troubleshooting (Grafana, log forwarding, scénarios).

Mise en situation & certification EX280

- Portage complet d'une appli ISV : Helm K8s "vanilla" ? OpenShift
- Identifier les blocages : SCC, images, réseau, stockage
- Adapter le chart, créer l'Operator, déployer via OLM
- Mettre en place monitoring + logs + alerting
- Présentation des résultats par groupe
- Atelier pratique : Synthèse générale, certification EX280, ressource et communauté.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.