

# Kubernetes – Sécuriser son infrastructure

2 jours (14 heures)

Expertise

Présentiel ou classe à distance

à partir de

**1750 € HT** par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 02/10/2026.

## Objectifs

A l'issue de cette formation, vous serez capable de :

- Identifier les bonnes pratiques de sécurité dans Kubernetes
- Mettre en oeuvre des outils de sécurisation des registres de conteneurs
- Appliquer des outils de conformité dans un environnement Kubernetes
- Déployer des outils de sécurité dynamiques dans un cluster Kubernetes
- Concevoir et intégrer des politiques de sécurité adaptées à vos besoins.

Les compétences visées par cette formation font l'objet d'une évaluation.

## À qui s'adresse cette formation ?

Administrateurs systèmes, DevOps, DevSecOps, développeurs, architectes, SRE.

### Prérequis

Avoir de bonnes connaissances de Linux / Unix, Docker, conteneurs et du réseau SDN. Avoir suivi les formations KUB-ORCH "Kubernetes – Orchestrer ses conteneurs" et KUB-AV "Kubernetes – Pratiques avancées" ou avoir un niveau équivalent.

# Programme

## 1 Pendant votre formation

### Kubernetes – Sécuriser son infrastructure

Jour 1 – Matin

Principes fondamentaux et socles technologiques de sécurité

#### Fondamentaux des conteneurs et de la sécurité

- Evolution vers les architectures basées sur les conteneurs
- Caractéristiques d'un conteneur (immutabilité, portabilité)
- Risques associés (surface d'attaque, isolation insuffisante)

#### Sécurité des technologies sous-jacentes

- Fonctionnement des namespaces (PID, NET, MNT...)
- Control Groups (cgroups) : isolation des ressources
- Rôle du noyau et des OS adaptés aux conteneurs

*Exemples de travaux pratiques (à titre indicatif)*

- Déploiement d'un cluster EKS sur AWS
- Création / configuration d'un utilisateur
- Personnalisation de kubeconfig pour accès sécurisé

Jour 1 – Après-midi

Sécurisation des moteurs de containers et registres

#### Sécurité Docker et OCI

- Configuration sécurisée du daemon Docker
- Bonnes pratiques Dockerfile (USER, COPY, RUN...)
- Sécurité des images : scan automatique, vulnérabilités
- Qu'en dit l'ANSSI ?

#### Ecosystème OCI et évolutions

- Containerd et runc : remplacement de Docker Engine
- Initiative OCI : standardisation des formats
- MicroVM et Unikernels : sécurité renforcée à l'exécution

*Exemples de travaux pratiques (à titre indicatif)*

- Déploiement du registre Harbor
- Découverte des fonctionnalités de sécurité du registre
- Filtrage par worker Kubernetes
- Sécurisation des accès au registre (authentification, rôles)

- Utilisation de Trivy pour scan d'image et détection de CVE

Jour 2 – Matin

Sécurité réseau, RBAC et Service Mesh

### Sécurité dans l'orchestration Kubernetes

- Menaces spécifiques au CaaS (exposition API...)
- Contrôle des accès : utilisateurs, rôles, RoleBinding
- Chiffrement de données sensibles (secrets, etcd)

### Réseau, CNI et Service Mesh

- Politique réseau native (NetworkPolicy)
- Plugins CNI : Calico, Cilium...
- Istio : sécurité, routage dynamique, Mutual TLS
- Visibilité via eBPF

*Exemples de travaux pratiques (à titre indicatif)*

- Déploiement d'une application multipods
- Création de NetworkPolicies pour interdire certains flux
- Intégration d'un microservice dans Istio
- Gestion TLS, routage, jaeger / grafana pour visualisation

Jour 2 – Après-midi

Conformité, sécurité dynamique et politiques avancées

### Ecosystème CNCF et outils de sécurité

- CNCF : Falco, Kyverno, OPA, Kubesplit, Kube-Bench
- Chaîne de sécurité des artefacts (supply chain)
- Cas d'usage : détection, prévention, audit

### Déploiement et gestion de politiques avancées

- Signature et vérification d'image avec Cosign
- Politiques Kyverno : forcer des labels, registres, contraintes
- Sécurité dynamique : règles de surveillance personnalisées

*Exemples de travaux pratiques (à titre indicatif)*

- Déploiement Falco et personnalisation des règles
- Création de politiques Kyverno : forcer un registre, limites CPU / mémoire
- Déploiement de Cosign avec Harbor pour signer et vérifier les images
- Sécurisation du CoreDNS
- Gestion automatisée des secrets et LimitRanges

## Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

## Modalités pédagogiques

Formation délivrée en présentiel ou distanciel\* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode\*\* démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

\* nous consulter pour la faisabilité en distanciel

\*\* ratio variable selon le cours suivi

[Accessibilité aux personnes en situation de handicap](#)

## Détails de la session

Du 2 novembre 2027 au 3 novembre 2027 (2 jours / 14 heures)

**À distance**

Du 2 novembre 2027 au 3 novembre 2027 **À distance**

- 2 novembre 2027 ..... 9h00 – 16h30
- 3 novembre 2027 ..... 9h00 – 16h30