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

Mis à jour le 19/12/2023

S'inscrire

Formation OpenShift Avancé : La Sécurité de Kubernetes

3 jours (21 heures)

Présentation

Le logiciel libre Kubernetes (communément appelé « K8s ») est désormais le standard en terme d'orchestration de conteneurs. Cet outil vous permettra d'entrer dans l'ère "Cloud Native" et d'exposer à grande échelle vos applications de manière sûre, reproductible et flexible.

Vous apprendrez également à faire évoluer vos applications vers le standard micro-service, modulaire et scalable. Plébiscité par les géants de la Silicon Valley, K8s est géré par une gouvernance responsable liée à Cloud Native Computing Foundation (une entité de la Fondation Linux).

Kubernetes fournit une « plateforme pour automatiser le déploiement, la mise à l'échelle et la mise en production de conteneurs d'applications sur des grappes de serveurs ». Il supporte de multiples moteurs d'exécution de conteneurs dont Docker, Rocket et Singularity.

Cette formation couvre les aspects avancés de la sécurité dans l'écosystème Kubernetes en se concentrant sur l'exemple concret d'OpenShift, une des distributions phares de Kubernetes, développée par RedHat. Elle aborde les stratégies de sécurité, les bonnes pratiques et fournit des études de cas spécifiques à OpenShift pour une compréhension approfondie de la sécurisation des clusters Kubernetes.

Cette formation vous présentera la toute dernière version de Kubernetes (à la date de rédaction de l'article : Kubernetes 1.29).

Objectifs

- Sécurisation de Bout en Bout : Comprendre les meilleures pratiques pour sécuriser chaque composant du cycle de vie, depuis le développement du code jusqu'à l'utilisateur final

- Identification des Points Stratégiques : Analyser les points cruciaux à sécuriser au sein d'un cluster Kubernetes, en mettant l'accent sur les zones stratégiques qui peuvent être des points d'attaque potentiels
- Compréhension du Fonctionnement Interne : Acquérir une compréhension approfondie du fonctionnement interne de Kubernetes, y compris ses mécanismes de sécurité inhérents
- Détection des Vulnérabilités : Apprendre à identifier les failles potentielles au sein d'un cluster Kubernetes, en mettant l'accent sur les techniques de détection proactives
- Solutions Pertinentes : Acquérir les compétences nécessaires pour appliquer des solutions de sécurité pertinentes et efficaces en réponse aux vulnérabilités identifiées
- Sécurisation des Données et de la Charge Applicative : Mettre en œuvre des stratégies avancées pour sécuriser les données sensibles et garantir la protection de la charge applicative dans un environnement Kubernetes
- Études de Cas OpenShift : Appliquer les concepts appris à des études de cas spécifiques à OpenShift, en comprenant comment adapter les mesures de sécurité en fonction des caractéristiques particulières de cette plateforme

Public visé

- Développeurs
- RSSI
- **Experts en sécurité**
- Administrateurs systèmes
- DevOps
- Architectes

Pré-requis

Bonne connaissance d'un système Unix, de l'API standard de Kubernetes et des conteneurs Linux.

Programme de notre formation OpenShift Avancé

Administration de Kubernetes en Production

- Fonctionnement interne du Control-Plane Kubernetes/OpenShift
- Configuration avancée de Kubernetes/OpenShift pour la production, avec un accent sur la sécurité des pods.
- Configuration semi-automatisée d'un cluster Kubernetes On-Premise
- Haute disponibilité et Rolling Upgrade du Control-Plane
- L'opérateur OpenShift Machine API et le ClusterAutoscaler

Architecture de Kubernetes

- Les composants du Control Plane et des nœuds de travail
- Fonctionnement de la boucle de réconciliation et du Controller Kubernetes
- Fonctionnement de etcd en mode haute-disponibilité

- Fonctionnement interne de l’API server: authentification, autorisation et Admission Control
- Les contrôleurs d'admission (MutatingWebhook et ValidatingWebhook)
- Description de l’algorithme du Scheduler Kubernetes, prédicats et priorités
- Configuration déclarative
- Cinématique de création d’un Pod à partir d’un Deployment
- Kube-proxy : fonctionnement avancé du réseau virtuel des Services
- Service discovery avec CoreDNS
- Description de la structure interne d’un Pod et du conteneur d'infrastructure

Sécurisation du serveur d'API

- Authentification : ServiceAccount, certificats, tokens, et Dex
- Paramétrage du fichier Kubeconfig avec les Configuration Contexts
- Sécurisation de l'API Kubernetes : authentification, autorisation et Admission Control. Mise en perspective avec la configuration OpenShift
- Droits d'accès à l'API avec RBAC: Role And ClusterRole, RoleBinding And ClusterRoleBinding
- Cas pratiques

Sécurité système

- Sécurisation de l'exécution des processus Unix dans les Pods (SecurityContex)
- Industrialisation de la sécurisation des Pods avecPodSecurity et/ou OPA GateKeeper.
- Niveaux de sécurité par défaut : Kubernetes vs OpenShift (SecurityContextConstraints)
- Distroless et rootless containers

Sécurité réseau

- Choix d'un plug-in réseau CNI sécurisé et efficace
- Industrialisation de la sécurité réseau (L4) avec les NetworkPolicies (ingress et egress) et TLS

Qualité de réseau

- Utilisation optimale des ressources matérielles grâce aux Requests et Limits, ResourceQuota et LimitRanges
- Classes de QoS: Guaranteed, Burstable et BestEffort
- Configuration du scheduler Kubernetes avec les Taints et les Affinities

Cas pratiques

- Etude de cas de pentesting Kubernetes.
- Gestion sécurisée des applications, avec une CI/CD orientée GitOps
- Gestion sécurisée du stockage (PersistentVolume, PersistentVolumesClaim, StorageClass), et provisionnement dynamique de volumes.
- Présentation des fonctionnalités avancées de Sysdig et/ou Calico (en option)

Monitoring

- Objectifs de surveillance et de journalisation
- Automatiser le monitoring avec l'opérateur Prometheus
- Obtenir et agréger les métriques de votre cluster et de vos applications
- AlertManager: gestion et routage des alertes
- Visualiser et interagir avec vos données avec Grafana

Module complémentaire (+1 jour)

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.