Programme de Formation

OpenShift avancé : sécurité, haute disponibilité et administration en production

Organisation

Durée : 21 heures

Mode d'organisation : Présentiel

Contenu pédagogique

Public visé

RSSI et experts en sécurité, développeurs, architectes infrastructure, administrateurs systèmes, ingénieurs DevOps/SRE souhaitant maîtriser la sécurisation avancée de Kubernetes en production avec OpenShift. Formation adaptée aux professionnels responsables de la sécurité des clusters critiques et de l'application des bonnes pratiques de sécurité.

Objectifs pédagogiques

- Maîtriser l'architecture interne de Kubernetes/OpenShift et comprendre le fonctionnement du control plane en production
- Déployer et administrer des clusters OpenShift hautement disponibles (IPI vs UPI) avec Machine API et ClusterAutoscaler
- Sécuriser de bout en bout un cluster Kubernetes/OpenShift : authentification (certificats X.509, tokens, OIDC), autorisation RBAC, admission controllers
- Identifier et corriger les vulnérabilités de sécurité : pentesting Kubernetes, détection proactive des failles
- Industrialiser la sécurité système avec SecurityContext, Pod Security Standards, SecurityContextConstraints (SCC), OPA Gatekeeper - Contrôler et isoler les flux réseau avec les Network Policies (L4) et TLS
- Optimiser les ressources avec QoS (Guaranteed, Burstable, BestEffort), ResourceQuota, LimitRange, taints et affinités
- Gérer le stockage sécurisé en production (CSI, PersistentVolume, provisionnement dynamique)
- Mettre en œuvre l'observabilité complète avec Prometheus Operator, AlertManager, Grafana et la console OpenShift
- Appliquer les bonnes pratiques GitOps pour une CI/CD sécurisée

Description

Le logiciel libre Kubernetes (communément appelé « K8s ») est désormais le standard en termes 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 1.31 et et Openshift 4.17).

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
- Techniques d'installation et de mise à jour d'Openshift (IPI vs UPI)
- L'opérateur Openshift Machine API et le ClusterAutoscaler

Architecture de Kubernetes

- Les composants du Control Plane et des noeuds 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
- Kubelet: gestion des noeuds et des conteneurs
- 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
- Introduction aux Kubernetes Operators et à leur mise en oeuvre dans Openshift

Sécurisation du serveur d'API

- Authentification: ServiceAccount, certificats, tokens, OpenID Connect 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 (SecurityContext)
- Industrialisation de la sécurisation des Pods avec PodSecurity et/ou OPA GateKeeper.
- Niveaux de sécurité par défaut: Kubernetes vs Openshift avec les 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 service

- 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

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
- Présentation de la console Openshift

Prérequis

Bonne connaissance d'un système Unix/Linux. Maîtrise de l'API standard de Kubernetes et des conteneurs. Expérience pratique avec Kubernetes et kubectl. Compréhension des concepts réseau (TCP/IP, DNS, TLS). Familiarité avec les architectures distribuées et les principes DevOps recommandée.

Modalités pédagogiques

- Répartition : 8h cours magistraux, 13h de labs et de pratique
- Organisation des Labs : groupes de 15 participants maximum, 1 intervenant
- Présentiel OU à distance (choix selon nombre d'inscrits et préférences)

Moyens et supports pédagogiques

- Supports de cours PDF, scripts et manifests YAML, guide de référence Kubernetes, accès plateforme de TP en ligne, liens vers documentation officielle.
- Equipements/logiciels mis à disposition : Accès cluster OPENSHIFT/Kubernetes partagé, machines virtuelles préconfigurées, outils monitoring (Prometheus, Grafana). Mise en œuvre d'un cluster OPENSHIFT sur le cloud AZURE.
- Équipements que les stagiaires devront amener : Ordinateur portable (Linux/macOS/Windows), installation d'une client SSH, connexion internet stable.

Modalités d'évaluation et de suivi

Un suivi individualisé par des évaluations formatives est assuré. Une attestation de fin de formation est délivrée à la fin du parcours.

Informations sur l'admission

L'admission à cette formation ne fait l'objet d'aucun examen, test ou sélection préalable ; l'inscription est validée après réception du dossier complet et confirmation par l'organisme de formation.

Informations sur l'accessibilité

Notre organisme s'engage à garantir l'accessibilité de ses formations à distance et en présentiel aux personnes en situation de handicap. Un référent handicap est mobilisable afin d'analyser les besoins spécifiques et de mettre en place, lorsque cela est possible, les adaptations pédagogiques, techniques ou organisationnelles nécessaires.