

Programme de Formation

Déploiement et orchestration d'applications avec Kubernetes : de l'initiation à la production



Organisation

Durée : 21 heures

Mode d'organisation : Présentiel

Contenu pédagogique



Public visé

Administrateurs systèmes, ingénieurs DevOps/SRE, architectes infrastructure, responsables plateformes cloud-native souhaitant maîtriser l'administration et la sécurisation de Kubernetes en production. Formation adaptée aux professionnels devant gérer des clusters critiques et optimiser leur architecture pour la haute disponibilité.



Objectifs pédagogiques

- Maîtriser l'architecture interne de Kubernetes et le fonctionnement de ses composants (Control Plane, Nodes, API Server)
- Déployer et administrer des clusters Kubernetes hautement disponibles en production avec kubeadm - Sécuriser un cluster Kubernetes : RBAC, Pod Security Standards, Network Policies, admission controllers (Kyverno, OPA)
- Optimiser les ressources avec LimitRange, ResourceQuota, QoS et stratégies de scheduling avancées
- Configurer le stockage persistant en production (CSI, StorageClass, OpenEBS)
- Implémenter l'observabilité complète : monitoring (Prometheus), visualisation (Grafana), logging (EFK)
- Gérer les accès réseau avec Ingress Controllers (NGINX) et Gateway API
- Appliquer les principes GitOps et IaC (Helm, Kustomize, ArgoCD)
- Comprendre les extensions Kubernetes : Operators et CustomResourceDefinitions



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 s'adresse aux experts souhaitant mettre en oeuvre et maîtriser des clusters Kubernetes de production, ainsi qu'à toute personne désirant comprendre en détail comment Kubernetes est architecturé, installé et maintenu. Le déploiement d'applications hautement sécurisées sur Kubernetes est également décrit, cette formation s'adresse aussi bien aux ingénieurs systèmes souhaitant mettre en place des clusters Kubernetes sûrs, performants et hautement disponibles qu'aux Devops et développeurs désirant déployer rapidement et simplement leurs applications. Cette formation vous présentera la toute dernière version de Kubernetes (à la date de rédaction de l'article : Kubernetes 1.27+).

Administration de Kubernetes en production

- Configuration avancée de kubeadm
- Mise en place automatisée d'un cluster Kubernetes On-Premise
- Sécurisation d'un cluster Kubernetes On-Premise pour la production
- Mise en place de la haute disponibilité pour le Control-Plane
- Mise à jour automatisée en mode Rolling Update du Control-Plane et des nœuds Kubernetes
- Virtuosité dans l'utilisation de kubectrl pour la CKAD
- Intégration continue dans le Cloud avec kind
- Les runtimes: crictl, Docker et Containerd

Architecture de Kubernetes

- Les composants du Control Plane et des nœuds de travail
- Fonctionnement de la boucle de réconciliation et du Controller Kubernetes
- Fonctionnement d'etcd en mode haute-disponibilité
- Fonctionnement interne de l'API server
- Authentification
- Autorisation
- Admission Control
- Gestion des contrôleurs d'admission
- Extension du cycle de vie du serveur d'API avec les MutatingAdmissionWebhook et les ValidatingAdmissionWebhook
- 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

Gestion des utilisateurs et droits d'accès

- Authentification : certificats, tokens
- Paramétrage du fichier Kubeconfig avec les Configuration Contexts
- Gestion des ServiceAccounts
- Sécuriser le pilotage du cluster avec les autorisations RBAC
- Role, ClusterRole, RoleBinding et ClusterRoleBinding
- Création de RBAC simples et génériques pour piloter un cluster de production
- Infrastructure AS Code, GitOps
- Comprendre l'IaC
- Comprendre le GitOps
- Tour d'horizon des gestionnaires de packages pour Kubernetes Helm, Operator-SDK, Kustomize
- Automatiser les déploiements avec ArgoCD

Réseaux - CNI

- Comprendre le fonctionnement du réseau virtuel des Pods
- Choix d'un Add-On réseau sécurisé et performant: l'exemple de CILIUM et de CALICO
- Monitorer et administrer les flux réseaux

Sécurité

- Sécuriser l'exécution des processus Unix dans les Pods
- Security Context
- Mode privileged
- Linux Capabilities
- Sécurisation des processus Unix
- Industrialiser la sécurité des Pods avec le module Pod Security Admission
- Découvrir le moteur de règles OPA-Gatekeeper
- Industrialiser la sécurité du réseau (L4) avec les NetworkPolicies

Qualité de service

- Utilisation optimale des ressources matérielles grâce aux Requests et Limits
- Classes de QoS
- Guaranteed
- Burstable
- BestEffort
- Contrôle d'allocation des ressources par Namespace avec les ResourceQuota
- Contrôle d'allocation des ressources par Pod avec les LimitRange

Optimisation du Scheduler

- Contrôle de la planification avec les Labels et les Affinités
- NodeSelector, NodeAffinity, PodAffinity, PodAntiAffinity
- Taints and Tolerations

Les Operators

- Présentation des méthodes d'extension de Kubernetes : les Operators
- Comprendre l'utilisation des ressources CRD
- Ajouter des API customisées à Kubernetes: les CustomResourceDefinitions
- Déployer une stack de monitoring avec l'opérateur
- Prometheus/Grafana/AlertManager

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
- Visualiser et interagir avec vos données avec Grafana

Gestion du stockage en production

- Comprendre le stockage hyperconvergé et hautement disponible
- Déploiement de ceph avec rook operator

Operators, HELM & EFK (+1 jour)

- Présentation des méthodes d'extension de Kubernetes : les Operators

- Ajouter des API customisées à Kubernetes: les CustomResourceDefinitions
- Créer ses opérateurs avec l'Operator-Framework et l'Operator-SDK
- Helm 3
- Gestion des logs avec la pile EFK (ElasticSearch, Fluentd, Kibana)

Introduction à ISTIO & LINKERD (+1 jour, uniquement sur demande en équipe)

- Service Mesh
- ISTIO
- LINKERD2 (Conduit)

Modules cloud complémentaires - préparer la production (1 journée)

- Pipeline de CI/CD: théorie et mise en oeuvre (GithubActions/ArgoCD)
- Les Services Mesh: fonctionnement et cas pratique avec Istio
- Ingress: fonctionnement et cas pratique avec nginx-controller

Services de gestion de conteneurs du cloud public ou multi-cloud : les exemples de Google Kubernetes Engine et de Rancher (1/2 journée)

Outils avancés de déploiement pour Kubernetes (1/2 journée)

- Les Operators
- Ajouter des API customisées à Kubernetes: les CustomResourceDefinitions
- Créer ses opérateurs avec l'Operator-Framework et l'Operator-SDK
- Helm: présentation et exemple avec la gestion des logs EFK (ElasticSearch, Fluentd, Kibana)

Accompagnement et conseil sur des cas pratiques proposés par les participants (1/2 journée à 1 jour)



Prérequis

Expérience pratique avec Kubernetes : avoir déjà déployé et géré des applications sur K8s. Maîtrise de Linux et de la ligne de commande. Connaissances en réseau (TCP/IP, DNS, load balancing). Familiarité avec Docker/conteneurs et les concepts DevOps. Compréhension des architectures distribuées et du cloud computing. Pratique de kubectl.



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.
- Équipements/logiciels mis à disposition : accès cluster Kubernetes partagé, machines virtuelles préconfigurées, outils monitoring (Prometheus, Grafana).
- Équipements que les participants devront amener : ordinateur portable (Linux/macOS/Windows), installation d'un 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.