Kubernetes – Pratiques avancées

Prix : 1 750 €HT

Durée : 2 jours

Code de Référence : KUBAV

Catalogue Cloud Native et DevOps

Objectifs de la formation

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

- Expliquer les principes avancés et les dernières évolutions de Kubernetes
- Présenter le cycle de vie d'un cluster Kubernetes
- Déterminer les solutions tierces permettant d'enrichir votre cluster Kubernetes
- Mettre en oeuvre les bonnes pratiques permettant d'optimiser votre efficacité dans la gestion de votre cluster Kubernetes.

Public

Cette formation s'adresse aux Administrateurs systèmes, développeurs, ingénieurs DevOps et architectes Cloud souhaitant aller plus loin dans approfondir leur maîtrise de cette technologie, avec notamment l'intégration de des solutions tierces de l'écosystème Kubernetes.

Prérequis

Avoir suivi la formation KUBORCH « Kubernetes – Orchestrer ses conteneurs » ou avoir les connaissances équivalentes. Avoir des connaissances de base en administration Linux / Unix, sur les conteneurs, sur les principes de fonctionnement des conteneurs ainsi que sur le réseau SDN.

Programme de la formation

Jour 1 – Matin
Rappels sur les fondamentaux de Kubernetes

- Rappel des ressources Kubernetes
- Dernières nouveautés Kubernetes
- Tour d'horizon de l'écosystème Kubernetes
- Gestion des runtimes de conteneurs (containerd, CRI-O) et fin de dockershim

Gestion des volumes avancés

- Volumes avancés avec « StorageClass » et « PersistentVolumeClaims »
- Les « StatefulSets » pour les applications avec état et Headless Services

Exemples de travaux pratiques (à titre indicatif)
Volumes avancés
« StatefulSets »

Jour 1 – Après-midi
Authentification et autorisation

- Les identités dans K8S
- Les méthodes d'authentification
- ServiceAccounts, Tokens et BoundServiceAccountTokenVolume
- Les modèles d'autorisation RBAC, OPA/Gatekeeper

Exemple de travaux pratiques (à titre indicatif)
Gestion de l'authentification et des autorisations

Maîtrise des capacités

- Les capacités du cluster
- Les requests/limits (CPU/RAM)
- Les « LimitRanges »
- Les « ResourceQuotas »
- Les « Quality of Service classes »

Exemple de travaux pratiques (à titre indicatif)
Quotas et limitations des ressources

Jour 2 – Matin
Monitoring

- Principes sur le monitoring
- Prometheus
- Grafana

Exemples de travaux pratiques (à titre indicatif)
Déploiement et configuration du monitoring
Création de dashboard

Gestion des logs

- Production des logs applicatifs
- Les différentes solutions
- Le modèle EFK (Elasticsearch, Fluent Bit / Fluentd et Kibana) et alternatives : Loki, OpenSearch, Vector

Exemple de travaux pratiques (à titre indicatif)
Déploiement et configuration d'une stack de logs

Audit

- Production des logs d'audit Kubernetes
- Analyse des logs

Exemples de travaux pratiques (à titre indicatif)
Mise en place de l'auditing au sein du cluster
Visualisation des logs Kubernetes
Déploiement et utilisation de Harbor (registre d'images)

Jour 2 – Après-midi
Architecture avancée et bonnes pratiques

- Présentation des concepts d'architecture avancée de Kubernetes
- Disponibilité des composants Kubernetes (High Availability et multi-zone)
- Bonnes pratiques
- Optimiser sa gestion du cluster
- Cycle de vie du cluster (upgrade, sauvegarde/restauration)
- Mettre à jour son cluster Kubernetes
- Scheduling avancé (nodeSelector, affinity, anti-affinity, taints/tolerations)
- Stratégies de scaling (HPA, VPA, Cluster Autoscaler)
- Introduction au Networking avancé (Gateway API, network policies, service mesh : Istio ambient, Cilium/eBPF)
- Introduction aux CRDs (Custom Ressource Definition)

Exemple de travaux pratiques (à titre indicatif)
Architecture avancée et cycle de vie du cluster Kubernetes

Packaging applicatif avec Helm

- Présentation des fonctionnalités de packaging de Helm
- Organisation des manifests Kubernetes en charts

Exemple de travaux pratiques (à titre indicatif)
Création d'un package applicatif avec Helm
Des performances tuning (hpa, vpa, analyse de performance…)
Troubleshooting cluster (etcd, API server, networking)

Sécurité et conformité DevSecOps

- Introduction à Trivy, Kyverno, SecurityContext, Pod Security Admission (PSA) et Pod Security Standards (PSS)

Méthodes pédagogiques

- Ce cours se présente sous la forme d'un séminaire ponctué de démonstration afin d'illustrer les concepts théoriques abordés.

- Le formateur tient compte de la situation de chaque apprenant et se base sur les expériences, les connaissances et les questions particulières des participants pour nourrir le groupe de cas concrets et de retours d'expériences ciblées

Les supports de formation seront les suivants :

- Présentation théorique au format pdf

Ces supports seront fournis aux participants au cours de la formation au format PDF.

Méthodes d'évaluation des acquis

Avant la formation :

- Le questionnaire de positionnement et d'auto-évaluation des compétences adapté à la formation :
  - Complété individuellement par chaque stagiaire avant la formation
  - Permet de recueillir et de mettre à disposition du formateur avant la formation

En cours de formation :

- Points d'étapes réguliers par le formateur sur la compréhension des stagiaires, de la réponse de la formation à leurs attentes et à leurs besoins
- Retour d'expérience en fin de journée de formation pour ajustements éventuels de la suite de la formation.

Après la formation « à chaud » :

- Le questionnaire d'auto-évaluation des compétences complété individuellement par chaque stagiaire après la formation et ajusté (si besoin) puis validé par le formateur en fonction des évaluations réalisées en cours de formation.
- Le questionnaire de satisfaction « à chaud » complété individuellement par chaque stagiaire en fin de formation.
- Le compte rendu formateur complété par le formateur.

Après la formation « à froid » :

Le questionnaire de satisfaction « à froid » complété individuelle par chaque stagiaire quelques semaines après la session de formation.

Un certificat de réalisation de fin de formation est remis au stagiaire lui permettant de faire valoir le suivi de la formation.