Préparation à la certification CKAD avec de la pratique

Prix : 2 925 €HT

Durée : 3 jours

Code de Référence : KUBCKAD

Catalogue Cloud Native et DevOps

Objectifs de la formation

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

- Identifier les concepts clés et les ressources essentielles de Kubernetes à maîtriser pour la certification CKAD
- Créer, configurer et déployer des applications Cloud Native avec Kubernetes
- Implémenter des mécanismes de configuration dynamique, de persistance de données, de gestion réseau, de sécurité et d'observabilité dans un cluster Kubernetes
- Utiliser les outils d'automatisation (Helm, CRD, etc.) pour industrialiser les déploiements
- Vous entraîner efficacement à la certification CKAD via des exercices pratiques et des simulations réalistes, notamment à l'aide de la plateforme killer.sh

Public

Cette formation s'adresse aux développeurs d'applications souhaitant concevoir, déployer et maintenir des applications dans un environnement Kubernetes. DevOps, ingénieurs systèmes ou cloud, architectes techniques, ingénieurs SRE ou administrateurs souhaitant valider leur maîtrise de Kubernetes côté développement.

Prérequis

Connaissances de base en administration Linux / Unix, en Docker, en fonctionnement des conteneurs et en réseau SDN. Avoir suivi les formations « KUBORCH » (Kubernetes – Orchestrer

ses conteneurs) et « KUBAV » (Kubernetes – Pratiques avancées) ou disposer de compétences équivalentes.

Programme de la formation

Jour 1 – Matin
Introduction à CKAD & Préparation de l'environnement d'examen

- Présentation des certifications CNCF : CKAD, CKA, CKS + KCNA/KCSA
- Objectifs et compétences évaluées dans le référentiel CKAD
- Organisation de l'examen : durée, interface, outils, notation
- Préparation de l'environnement de travail :
  – Configuration du terminal : autocompletion, alias
  – Navigation dans les namespaces
  – Astuces pour gagner du temps à l'examen

Exemples de travaux pratiques (à titre indicatif) :
Configuration complète de l'environnement d'examen (kubectl, bashrc, alias)
Navigation entre namespaces, inspection de ressources
Utilisation avancée de kubectl avec –dry-run et -o yam

Jour 1 – Après-midi
Déploiement d'applications & Configuration applicative

- Création de Pods, Deployments, ReplicaSets
- Jobs & CronJobs
- DaemonSets
- ConfigMaps & Secrets
- Stratégies de déploiement RollingUpdate, Recreate, Blue/Green et Canary, avec Rollback

Exemples de travaux pratiques (à titre indicatif) :
Création et mise à jour de Deployments
Ajout de ConfigMaps et Secrets à des Pods
Intégration de probes dans un Deployment
Planification d'un CronJob, test d'un Job unitaire
Déploiement d'un Pod avec plusieurs conteneurs (sidecar, initContainer…)

Jour 2 – Matin
Sécurité, limitations, ressources & stockage persistant

- ResourceQuota, LimitRange, QoS, PodPriority
- SecurityContext, ServiceAccount, RBAC
- Volumes, PV, PVC, StorageClass

Exemples de travaux pratiques (à titre indicatif) :
Définition de quotas et de limites mémoire/CPU
Test de comportements QoS : BestEffort, Burstable, Guaranteed
Configuration de SecurityContext (non-root, readOnlyRootFS, etc.)
Création d'un PersistentVolume et d'un PVC, usage dans un Pod

Jour 2 – Après-midi
Observabilité, Troubleshooting Helm & CRDs

- Probes : readiness, liveness, startup
- kubectl describe, logs, debug
- Helm : installation, structure d'un chart, customisation via values.yaml
- Kustomize : bases, overlays et personnalisation de manifestes
- Custom Resource Definition (CRD), controllers et operator pattern

Exemples de travaux pratiques (à titre indicatif) :
Ajout de probes à un Deployment
Analyse de logs et simulation de CrashLoopBackOff
Installation de Helm, déploiement d'un chart officiel, surcharge de valeurs
Création et déploiement d'une CRD (ex : ArgoCD, CertManager), inspection via kubectl

Jour 3 – Matin
Services, Ingress & NetworkPolicy

- Services : ClusterIP, NodePort, LoadBalancer
- Ingress / Gateway API : configuration, règles de routage, hôtes virtuels
- NetworkPolicy : définition, cas d'usage, impact des plugins CNI

Exemples de travaux pratiques (à titre indicatif) :
Déploiement de services de type ClusterIP et NodePort
Installation d'un Ingress Controller (ex : NGINX)
Configuration d'un Ingress avec plusieurs chemins et hôtes
Déploiement de NetworkPolicies limitant les communications inter-namespaces

Jour 3 – Après-midi
Simulation complète de certification sur plateforme killer.sh

- Présentation de la plateforme d'entraînement killer.sh
- Recommandations de stratégie pour l'examen : gestion du temps, priorisation des questions
- Révision rapide des commandes clés et cas récurrents à l'examen
- Débrief collectif et analyse individualisée

Exemples de travaux pratiques (à titre indicatif) :
Lancement d'une simulation complète sur killer.sh
Résolution de cas sur les 7 domaines CKAD :
– Application Design and Build
– Application Deployment
– Application Observability and Maintenance
– Application Environment, Configuration and Security
– Services and Networking

Correction accompagnée et revue des stratégies gagnantes

Certification (en option)
Prévoir l'achat d'un voucher en supplément
Le passage de l'examen se fera ultérieurement
L'examen (en anglais, chinois simplifié ou japonais au choix) s'effectuera en ligne, et durera en moyenne 2h00
La validité de cette certification est de 2 ans

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.