MFE-IT

Référence : MFE-GCPGKE

Formation Google Kubernetes Engine (GKE)

Déployer et exploiter Kubernetes sur Google Cloud

Durée : 3 jours | Volume horaire : 21 h

Distanciel · Sessions garanties dès 1 inscrit · 60 % de pratique

DESCRIPTION

La formation Google Kubernetes Engine s'adresse à ceux qui connaissent Kubernetes et découvrent qu'il ne se comporte pas tout à fait pareil chez Google. C'est logique : Kubernetes vient de chez eux, et GKE en est l'implémentation la plus intégrée du marché — avec des automatismes que les autres n'ont pas, et des choix par défaut qu'il faut comprendre avant de les subir.

OBJECTIFS PÉDAGOGIQUES

À l'issue de cette formation, les participants seront capables de :

- Choisir entre GKE Autopilot et GKE Standard en connaissance de cause, et en assumer les conséquences.
- Déployer un cluster GKE et comprendre le partage des responsabilités avec Google.
- Configurer le réseau du cluster (VPC natif, adressage des pods, politiques réseau).
- Attribuer des droits Google Cloud aux pods sans clés statiques, via Workload Identity.
- Mettre en œuvre la mise à l'échelle automatique des pods et des nœuds.
- Exposer des applications avec Ingress, Gateway API et le load balancing Google.
- Superviser, durcir et maîtriser le coût d'un cluster GKE en production.

PRÉREQUIS

- Une pratique préalable de Kubernetes est indispensable : les notions de pod, deployment, service et namespace doivent vous être familières, et vous devez savoir lire un manifeste YAML. Notre Formation Kubernetes ou une expérience équivalente constitue le point de départ attendu.
- Une première expérience de Google Cloud (projets, IAM, VPC) est également nécessaire. Le niveau de la certification Cloud Digital Leader, ou des bases d'Associate Cloud Engineer, suffit largement.
- Parce que chaque participant est unique, un entretien personnalisé avec notre expert nous permet de concevoir une formation parfaitement alignée avec ses objectifs.

PUBLIC VISÉ

- Ingénieurs DevOps et SRE exploitant ou s'apprêtant à exploiter Kubernetes sur Google Cloud.
- Administrateurs cloud et systèmes en charge de la migration de charges conteneurisées vers GKE.
- Architectes devant arbitrer entre GKE Autopilot, GKE Standard et Cloud Run.
- Développeurs souhaitant comprendre l'environnement d'exécution réel de leurs applications.

PROGRAMME DÉTAILLÉ

La formation alterne apports théoriques et pratique (environ 60 % du temps). Les modules s'articulent autour d'exercices concrets basés sur des cas d'usage métier réels.

Module 1 — GKE Autopilot ou Standard : l'arbitrage fondateur

Kubernetes est né chez Google, et cela se voit. Ce que GKE gère à votre place et ce qu'il vous laisse. Mode Autopilot : Google gère les nœuds, vous ne payez que les pods, et vous perdez une partie du contrôle — une contrainte pour certains, un soulagement pour la plupart. Mode Standard : vous gardez la main sur les nœuds, et la responsabilité qui va avec. Critères de choix honnêtes, et cas où l'on regrette Autopilot. Positionnement face à Cloud Run : quand Kubernetes n'est tout simplement pas nécessaire. Création d'un cluster : console, gcloud, infrastructure as code. Canaux de version et mises à niveau automatiques.

Module 2 — Nœuds, pools et mises à niveau sans interruption

Pools de nœuds : plusieurs profils de machines dans un même cluster, et pourquoi c'est presque toujours nécessaire. Types de machines, familles ARM, et VM Spot pour les charges tolérantes à l'interruption. Provisionnement automatique des nœuds : GKE crée le pool adapté aux pods en attente. Mises à niveau sans interruption : stratégies de surtension et bleu-vert, budgets de perturbation, drain progressif. Lab : mettre à jour un cluster en production sans couper le service.

Module 3 — Réseau du cluster et exposition des applications

Le mode VPC natif : chaque pod reçoit une vraie adresse IP du VPC, via des plages d'adresses secondaires — conséquences sur le dimensionnement des sous-réseaux, et l'épuisement d'adresses qui arrive plus vite qu'on ne croit. Clusters privés et accès au plan de contrôle. Politiques réseau et isolation entre namespaces. Exposition : Service, Ingress qui crée un vrai load balancer Google, et la Gateway API qui remplace progressivement Ingress. Certificats gérés par Google. Cloud DNS et résolution de service.

Module 4 — Identité et contrôle d'accès : Workload Identity

Le mauvais réflexe, et pourquoi il coûte cher : monter une clé de compte de service dans un conteneur. La bonne réponse, et l'une des meilleures intégrations de GKE : Workload Identity, qui associe un compte de service Kubernetes à un compte de service Google Cloud, sans aucune clé à gérer ni à faire tourner. Fonctionnement, mise en place, dépannage. Contrôle d'accès Kubernetes : RBAC, rôles et liaisons. Articulation entre RBAC Kubernetes et IAM Google — deux systèmes distincts qu'il faut faire coïncider.

Module 5 — Mise à l'échelle automatique et dimensionnement

Quatre mécanismes qui ne font pas la même chose, et qu'on confond souvent. Au niveau du pod : Horizontal Pod Autoscaler (CPU, mémoire, métriques personnalisées) et Vertical Pod Autoscaler, qui ajuste les requests à votre place — utile, et redoutable si mal compris. Au niveau du cluster : Cluster Autoscaler et provisionnement automatique des nœuds. Requests et limits : le paramètre le plus souvent mal réglé, et celui qui décide de tout — d'autant plus en Autopilot, où il détermine directement la facture. Lab : diagnostiquer des pods bloqués en Pending et corriger la cause réelle.

Module 6 — Stockage et charges avec état

Faire tourner autre chose que du sans-état. Pilotes CSI Google : Persistent Disk (bloc, attaché à une zone), Filestore (NFS partagé), Cloud Storage FUSE pour les objets. PersistentVolume, PersistentVolumeClaim, StorageClass et provisionnement dynamique. Contrainte de zone des disques et son impact sur la planification des pods. Clusters régionaux contre clusters zonaux : ce que la haute disponibilité coûte réellement. StatefulSets, sauvegarde et restauration.

Module 7 — Supervision, durcissement et maîtrise des coûts

Voir ce qui se passe : Cloud Operations (anciennement Stackdriver) — métriques, journaux, traces, intégration native avec GKE. Prometheus géré. Alertes qui remontent le symptôme visible par l'utilisateur, pas chaque secousse d'un indicateur. Durcissement : Binary Authorization (n'exécuter que des images signées), Artifact Registry et analyse de vulnérabilités, standards de sécurité des pods, GKE Sandbox. Coût d'un cluster : ce qui le fait grimper, et les leviers réels (Autopilot contre Standard, Spot, dimensionnement des requests). Atelier de synthèse : reprendre un cluster mal configuré et le remettre en état de production.

LES PLUS DE CETTE FORMATION

- Traite Kubernetes là où il devient réellement délicat : son intégration dans Google Cloud (VPC natif, Workload Identity, Autopilot).
- Fait trancher dès le premier module l'arbitrage Autopilot / Standard, qui conditionne tout le reste.
- Consacre environ 60 % du temps à la pratique, avec des incidents provoqués volontairement sur le cluster.
- Se déroule en groupe de 1 à 3 participants, ce qui permet de travailler sur vos propres clusters.

MODALITÉS PÉDAGOGIQUES

Format et déroulement

La formation est dispensée à distance via une classe virtuelle interactive. Elle peut également être réalisée sur site, avec un contenu personnalisé selon les besoins de votre projet professionnel. La répartition théorie/pratique est d'environ 40 %/60 %.

Format ultra-personnalisé MFE-IT

Chaque session accueille de 1 à 3 participants, garantissant un accompagnement très individualisé. Un entretien préalable permet d'adapter le contenu au profil de chacun. Les sessions inter-entreprises sont garanties dès 1 seul inscrit (pas de risque de report sauf cas de force majeure).

Évaluation des compétences

Tout au long de la formation, le formateur évalue la progression des participants par des QCM, des mises en situation et des travaux pratiques. À la fin, une attestation de validation des acquis est remise à chaque participant.

Suivi post-formation

Pendant un mois après la formation, chaque participant peut contacter les formateurs MFE-IT pour toute question sur la mise en œuvre des acquis. Une réponse est apportée par e-mail ou téléphone sous 48 heures ouvrées.

Accessibilité

MFE-IT s'engage à accueillir les personnes en situation de handicap. Contact : contact@mfe-it.com.

INFORMATIONS PRATIQUES

Ressources formateur

- Démonstrations structurées alignées sur le programme détaillé
- Énoncés d'exercices et corrigés tout au long de la formation
- Un environnement technique prêt à l'emploi pour les ateliers pratiques
- Validation des acquis par le formateur à la fin de chaque atelier
- Documents de référence numériques

Certification et validation

À l'issue de la formation, une attestation est envoyée par e-mail précisant les objectifs, la nature, la durée et les résultats de l'évaluation. Un certificat de réalisation peut également être fourni sur demande.

Bénéfices pour les participants

- Se former depuis son lieu de travail ou son domicile, sans déplacement
- Bénéficier d'un formateur-consultant expert du sujet
- Profiter d'un format ultra-personnalisé (1 à 3 participants)
- Poursuivre la formation même en cas d'imprévu

Bénéfices pour l'organisation

- Optimiser le budget formation en réduisant déplacements et hébergements
- Offrir une formation de qualité à tous les collaborateurs, où qu'ils soient
- Réduire le temps d'absence lié aux déplacements
- Accompagner la montée en compétences des équipes dans tous les contextes