MFE-IT

Référence : MFE-AWSEKS

Formation AWS EKS – Kubernetes sur Amazon Elastic Kubernetes Service

Déployer et exploiter Kubernetes sur Amazon EKS

Durée : 3 jours | Volume horaire : 21 h

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

DESCRIPTION

La formation AWS EKS répond à une situation devenue courante : l'équipe maîtrise Kubernetes, mais le faire tourner sur AWS soulève une deuxième série de questions. Qui gère le plan de contrôle ? Comment un pod obtient-il des droits sur un bucket S3 sans qu'on lui colle les clés du compte ? Pourquoi le cluster ne s'agrandit-il pas alors que les pods sont en attente ?

OBJECTIFS PÉDAGOGIQUES

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

- Déployer un cluster Amazon EKS et en comprendre le partage des responsabilités avec AWS.
- Choisir entre groupes de nœuds gérés, nœuds autogérés et AWS Fargate selon la charge.
- Configurer le réseau du cluster (VPC CNI, adressage des pods, politiques réseau).
- Attribuer des droits AWS aux pods sans clés statiques, via IRSA et EKS Pod Identity.
- Mettre en œuvre la mise à l'échelle automatique des pods et des nœuds (HPA, Karpenter).
- Exposer des applications avec l'AWS Load Balancer Controller et gérer les certificats.
- Superviser, durcir et maintenir un cluster EKS en conditions de 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 d'AWS (EC2, VPC, IAM) est également nécessaire. Le niveau de la certification AWS Cloud Practitioner 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 AWS.
- Administrateurs cloud et systèmes en charge de la migration de charges conteneurisées vers EKS.
- Architectes devant arbitrer entre EKS, ECS et les modèles serverless.
- 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 — Cluster EKS et partage des responsabilités

Le partage des responsabilités appliqué à Kubernetes : ce qu'AWS gère (plan de contrôle, etcd, mises à jour) et ce qui reste à votre charge (nœuds, réseau, charges de travail, sécurité). Positionnement d'EKS face à ECS et aux offres serverless : critères de choix honnêtes plutôt que dogme. Création d'un cluster : console, eksctl, infrastructure as code. Authentification kubectl via IAM et l'access entries API. Cycle de vie des versions Kubernetes et stratégie de mise à jour.

Module 2 — Nœuds, Fargate et mises à jour

Trois modèles pour faire tourner vos pods : groupes de nœuds gérés, nœuds autogérés, AWS Fargate — et ce que chacun coûte en argent et en contrôle. Choix des types d'instances, familles ARM Graviton, instances Spot pour les charges tolérantes à l'interruption. Bootstrap des nœuds et AMI optimisées EKS. Mise à jour d'un groupe de nœuds sans interruption : drain, budgets de perturbation, vidage progressif. Lab : mettre à jour un cluster en production sans couper le service.

Module 3 — Réseau du cluster et exposition

Le point qui surprend le plus : avec le VPC CNI, chaque pod reçoit une vraie adresse IP du VPC — conséquences sur le dimensionnement des sous-réseaux et l'épuisement d'adresses. Modes prefix delegation et IPv6. Politiques réseau et isolation entre namespaces. Exposition : Service, Ingress, et l'AWS Load Balancer Controller qui crée de vrais ALB et NLB. Certificats TLS avec ACM. Résolution DNS avec CoreDNS et ExternalDNS.

Module 4 — Identité et accès : IRSA et Pod Identity

Le mauvais réflexe, et pourquoi il coûte cher : injecter des clés d'accès dans un conteneur. La bonne réponse : IRSA (IAM Roles for Service Accounts) et, plus récemment, EKS Pod Identity. Fonctionnement du fournisseur d'identité OIDC du cluster. Association d'un rôle IAM à un service account, au plus juste privilège. Contrôle d'accès Kubernetes : RBAC, rôles et liaisons. Articulation entre RBAC Kubernetes et IAM AWS — deux systèmes distincts qu'il faut faire coïncider.

Module 5 — Mise à l'échelle automatique

Trois niveaux d'élasticité qui ne font pas la même chose. Au niveau du pod : Horizontal Pod Autoscaler sur les métriques CPU, mémoire ou personnalisées ; Vertical Pod Autoscaler et ses limites. Au niveau des nœuds : Cluster Autoscaler, puis Karpenter qui provisionne la bonne instance pour les pods en attente plutôt que d'agrandir un groupe figé. Requests et limits : le paramètre le plus souvent mal réglé, et celui qui décide de tout. 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. Interface CSI et pilotes AWS : EBS CSI pour le stockage bloc attaché à une zone, EFS CSI pour le partagé multi-AZ, S3 pour les objets. PersistentVolume, PersistentVolumeClaim, StorageClass et provisionnement dynamique. Contrainte de zone de disponibilité des volumes EBS et son impact sur la planification des pods. StatefulSets. Sauvegarde et restauration des volumes.

Module 7 — Supervision, durcissement et coûts

Voir ce qui se passe dans le cluster : métriques avec CloudWatch Container Insights et Prometheus, journaux applicatifs et journaux du plan de contrôle, traces distribuées. Durcissement : analyse des images avec Amazon Inspector, secrets chiffrés par KMS, standards de sécurité des pods, restriction de l'accès à l'API du cluster. Gestion des modules complémentaires EKS. Coût d'un cluster et leviers de réduction. 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 AWS (réseau VPC, identités IAM, mise à l'échelle).
- Consacre environ 60 % du temps à la pratique, avec des incidents provoqués volontairement sur le cluster.
- Couvre les briques évaluées par la certification AWS Certified DevOps Engineer – Professional (DOP-C02) sur le volet conteneurs.
- 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