Formation AWS – Compute & Réseau (EC2, VPC, ELB, Auto Scaling)

Informations

Durée : 3 jours (21h.)

Tarif* : Nous consulter

Réf : AWCR

Niveau : Moyen

intra

Mise à jour le 24/03/26

*tarif valable jusqu'au 31/12/2026

Prochaines sessions

Contactez-nous pour connaitre nos futures sessions.

Pré-requis

- Connaissances de base en réseaux (TCP/IP, DNS, routage)
- Expérience en administration systèmes (Linux/Windows)
- Avoir suivi la formation AWS Cloud Practitioner Essentials (recommandé)

Objectifs

Objectifs pédagogiques :

- Découvrir et maîtriser les services de calcul AWS (EC2, AMI, Elastic Load Balancing)
- Comprendre et configurer les réseaux VPC (sous-réseaux, route tables, gateways)
- Mettre en place la haute disponibilité avec Auto Scaling et ELB
- Appliquer les bonnes pratiques de sécurité et d'optimisation des performances

Objectifs opérationnels :

- Concevoir, déployer et administrer une infrastructure AWS de calcul et réseau comprenant : instances EC2 configurées, VPC structuré (subnets, sécurité, routage), Load Balancer pour gestion du trafic, et stratégies de mise à l'échelle automatique (Auto-Scaling) garantissant résilience, performance et optimisation des coûts.

Programme

Jour 1 – Amazon EC2 et Elastic Load Balancing

Amazon EC2

Types d'instances (généralistes, compute-optimized, memory-optimized, GPU)
Gestion des AMI (Amazon Machine Images)
EBS : attachement de volumes, snapshots
Sécurité : key pairs, security groups, NACL

Gestion de la disponibilité et de la scalabilité

Auto Scaling Groups : configuration et politiques de scaling
Elastic Load Balancer (ALB, NLB, GLB)
Stratégies de haute disponibilité
Atelier pratique : lancement d'un cluster d'instances EC2 avec un ALB en front-end et scaling automatique selon la charge

Jour 2 – Réseau et Virtual Private Cloud (VPC)

Concepts fondamentaux du VPC

CIDR, sous-réseaux publics/privés, route tables
Internet Gateway, NAT Gateway, VPC Endpoints

Connexion et interconnexion

Peering VPC
AWS Transit Gateway (aperçu)

Sécurité réseau

ACLs vs Security Groups
Flow Logs et surveillance réseau

Atelier pratique : mise en place d’un VPC complet avec subnets publics/privés, une instance bastion et une application web sécurisée

Jour 3 – Monitoring, optimisation et cas d’usage

Monitoring et logs

CloudWatch : métriques, logs, alarmes
CloudTrail pour l’audit

Optimisation

Choix des bonnes instances et Reserved Instances/Savings Plans
Spot Instances et stratégies d’optimisation des coûts

Études de cas

Déploiement d’une application web scalable et sécurisée
Architecture réseau pour une PME connectant ses bureaux à AWS (VPN site-to-site)
Atelier final : conception et déploiement d’une architecture complète (VPC + EC2 + ALB + Auto Scaling)