

Systèmes, Réseaux et Télécoms

DevOps (72 heures)

26_27_4IRC_08_CYBER_UE7_070_MAJ

ACQUIS

- Comprendre l'origine et l'intérêt de la mouvance DevOps dans les projets informatiques.
- Développer une compréhension approfondie du monde du IaaS (Infrastructure as a Service) et du CaaS (Containers as a Service), leurs différences et leurs points communs.
- Comprendre et appliquer les bonnes pratiques de sécurité dans un système d'exploitation Linux.
- Approfondir le fonctionnement d'un système d'exploitation UNIX/Linux (sécurité, réseau, gestion des ressources).
- Maîtriser un environnement conteneurisé de manière sécurisée et contrôlée.
- Mettre en place un système de monitoring d'infrastructure et d'applications.

CONTENU

- Conteneurs Linux (Open Container Initiative)
- Automatisation de la construction d'images (Continuous Integration) à partir d'un code source (GitLab CI/CD).
- Gestion du cycle de vie des conteneurs (Docker).
- Distribution d'images OCI (Registry Docker, signature et validation des images).
- Mise en place des bonnes pratiques de sécurisation des conteneurs (Dockerfile).
- Infrastructure as Code
- Utilisation d'outils permettant le déploiement automatisé et reproductible d'infrastructures (Continuous Delivery).
- Mise en place d'une infrastructure pour le déploiement de conteneurs Linux sur une plateforme IaaS (Terraform, Ansible).
- Container as a Service (Kubernetes)
- Déploiement industrialisé sur une plateforme CaaS via des outils d'automatisation (ArgoCD).
- Utilisation d'opérateurs Kubernetes pour la gestion avancée des applications.
- Configuration et gestion d'un cluster Kubernetes
- Mise en place d'une configuration permettant à une équipe applicative (fictive) d'utiliser le cluster tout en imposant des restrictions garantissant sa stabilité et celle des applications déployées.
- Intégration d'outils de monitoring du cluster Kubernetes et des applications (Grafana, Prometheus, AlertManager).
- Sécurisation du cluster pour limiter les risques liés à l'exécution de conteneurs de sources inconnues (eBPF, Linux Capabilities, Agent OPA).
- Compréhension et configuration des composants réseau fondamentaux d'un cluster Kubernetes (Kube-Proxy, CNI) afin de permettre le déploiement de load balancers haute disponibilité (L2, ECMP).

PRÉREQUIS

- Maîtrise des concepts clés de la virtualisation et de l'Infrastructure as a Service (IaaS)
- Connaissance des principes fondamentaux de l'administration système sous Linux
- Compréhension des notions de base en réseaux, notamment le modèle OSI
- Connaissance des fondamentaux du développement logiciel, incluant Git et les outils de gestion de packages.

PÉDAGOGIE

ÉVALUATION

BIBLIOGRAPHIE