Infrastructures Virtuelles et Conteneurs

Infos pratiques

> **ECTS** : 3.0
> **Nombre d'heures** : 24.0
> **Niveau d'étude** : BAC +4
> **Période de l'année** : Enseignement huitième semestre
> **Méthodes d'enseignement** : En présence
> **Forme d'enseignement** : Cours magistral et Travaux dirigés
> **Composante** : Sciences économiques, gestion, mathématiques et informatique

Objectifs

La puissance actuelle des machines multicœurs permet la création de machines virtuelles dédiées à des applications et de les héberger en concurrence sur une seule et même machine ou sur un cluster de machines ou des clouds tels que AWS d'amazon ou Azure de Microsoft. L'objectif, pour les étudiants, est de maitriser ces outils pour leur permettre le déploiement d'environnements de tests, de pré-productions, ou de productions de manière automatisée, sécuritaire, reproductible, et standardisée pour leurs futures applications.

Approche pédagogique et plan de cours.

Ce module aborde les outils de virtualisation et d'isolation utilisés dans les déploiements sécurisés et automatisés d'environnements et d'applications. Cette technique consiste donc à héberger des machines "invitées" sur une seule machine "hôte". Il existe essentiellement deux types de déploiements automatisés.

Le premier consiste en la création d'un système complet embarquant l'application qui sera considéré comme une machine invitée indépendante du système hôte qui la contient. Il s'agit là d'une machine virtuelle. Ces machines sont gérées par des outils nommés hyperviseurs, les plus connus étant VmWare, VirtualBox et Xen/KVM.

Les seconds outils sont les conteneurs aussi appelés "bacs à sable". Ils sont plus légers que les machines virtuelles et permettent de définir un environnement particulier isolé du reste de la machine hôte. Ces conteneurs permettent de contraindre et limiter l'accès à certaines ressources de la machine hôte par les machines invitées. Les conteneurs les plus connus sont Docker et Systemd.

Ces deux techniques sont très utilisées en DevOps par l'intermédiaire d'outils de gestion de machines virtuelles et de conteneurs ainsi que de scripts de déploiement et de configuration de l'environnement d'accueil. Cela permet ainsi des déploiements automatisés, sécurisés et pré-configurés. Les outils de gestion les plus connus étant Puppet, Ansible, Mesos, Terraform, Salt, Vagrant ou les outils payant de VmWare.

Les services en ligne tel que Azure, AWS, OVH, IBM et Oracle utilisent ce type de service.

Évaluation

Session 1 : Contrôle Continu Intégral (cf. règle par défaut de la section « Modalités spécifiques » des M3C spécifiques)

Session 2 : Règle par défaut décrite dans la section « Modalités de contrôle et examens / Modalités spécifiques »

Pré-requis nécessaires

- Connaissance en système et en réseau
- Connaissance en langage de scripts
- Connaissance basique en sécurité

Compétences visées

- Connaissance de outils de virtualisation
- Connaissance des outils de gestion de déploiement et de configuration
- Connaissance des outils en ligne dans les clouds
- Savoir créer des configurations de virtualisation et de déploiement d'applications
- Savoir sécuriser des configurations de virtualisation et de déploiement

Bibliographie

- Securing DevOps: Security in the Cloud, Julien Vehent, 2018, ISBN 978-1617294136
- The DevOps Handbook: how to create World-Class agility, reliability, and security in technology organizations, Gene Kim et al., IT Revolution Press, 2016, ISBN 978-1942788003
- Learning DevOps, Mikael Krief, Packt Publishing, 2019, ISBN 9781838642730
- Docker in Practice, 2ème édition, Ian Miell, Aidan Hobson Sayers, 2019, ISBN 978-1617294808
- Vagrant: Up and Running, Mitchell Hashimoto, 2013, O'Reilly Media, Inc., ISBN 9781449335830