Projet Cloud Sécurisé

Le but de ce projet est de construire un CI/CD permettant un déploiement automatique d'une application sur un serveur de production.

Pour simuler un environnement de production, il vous est demandé de créer une machine virtuelle sur votre poste avec le système d'exploitation de votre choix (fortement conseillé d'utiliser linux ☺ )

Reprenez un de vos projets fait dans votre cursus qui servira d'application métier. C'est celle-ci qui sera manipulée pour l'intégration et le déploiement continu sur le serveur. Si vous n'avez pas de projet à reprendre, vous pouvez partir du projet Git suivant :

- Backend: https://github.com/DavidIMT/Tuto-Web-service.git (soit vous gardez la bdd embarquée h2, soit vous pouvez utiliser une bdd mysql à partir d'une image docker)
- Frontend (facultatif): https://github.com/DavidIMT/Tp_docker_front (une modification devra être apportée dans le fichier App.js -> renseigner l'url du backend sur l'appel à l'API)

Le projet sera à faire en groupe de 4, trois grandes parties sont à réaliser :

- Adaptation du projet métier pour ajouter la configuration de Docker, l'ajout de tests unitaires si besoin, des agents SonarQube etc..
- Création d'une application CI/CD (back et front) qui peut s'exécuter en local sur une de vos machines.
- Création et configuration de la VM avec la connexion de l'application CI/CD à cette dernière pour les déploiements.

Le choix de la technologie utilisée pour la réalisation du projet est libre.

Attendus fonctionnels :

- Un utilisateur pourra se connecter sur le site qui gérera le CI/CD. La connexion se fera via un système d'authentification OAuth2 (système de Google ou Github peut faire l'affaire).
- Des rôles seront affectés aux utilisateurs pour les autoriser à ne faire que certaines actions (travail sur l'aspect sécurité des identités)
- Un pipeline sera affiché sur l'IHM qui permettra de suivre en temps réel le déploiement de l'application étape par étape.
- Un pipeline de déploiement pourra être lancé soit via l'IHM de votre application, soit par un évènement de l'application qui va être déployée (Hook Github sur un push sur la branche main par exemple)
- Le déploiement de l'application sur le serveur de production de la VM sera fait avec Docker.
- Intégration de SonarQube dans le projet pour une analyse de la qualité de code.
- (Facultatif) Mise en place de tests d'intrusions (partie PenTest et red team vu en Cybersécurité)

Points technique demandés dans l'exécution des tâches de la CI/CD :

- Récupération du code hébergé sur GitHub
- Compilation maven/gradle avec run des TU
- Création image docker
- Déploiement avec une connexion SSH sur la VM
- Run de l'image sur un serveur de la VM
- Run des tests d'intrusions
- Analyse sonarQube
- Rollback si erreur
- Plus d'étapes si ça vous semble nécessaire

Bonus : Gestion du déploiement de l'application dans un cluster Kubernetes

Tips :

- Création de la VM : passez par VirtualBox, il s'agit de la façon la plus simple et rapide de créer des VM. Attention, ne fonctionne pas ou mal sur les macs avec les puces non INTEL, une solution serait d'utiliser l'application UTM.
- N'hésitez pas à faire des lots de développement cohérents (finir fonctionnalité par fonctionnalité) au lieu de commencer à travailler sur tous les points du projet en même temps ☺

Évaluation :
Vous serez notés sur le code source du projet et sur une présentation qui aura lieu le vendredi 9 janvier. Lors de cette présentation de 15 minutes max, vous proposerez une démonstration qui servira de fil directeur pour expliquer votre projet, les résultats obtenus, le fonctionnement, les choix techniques, etc.