

Mettre en oeuvre la sécurité par le biais d'un pipeline avec Azure DevOps

Protégez votre code et vos déploiements avec Azure DevOps

 A distance



7 h

Prix inter : 950,00 € HT
Forfait intra : 2.850,00 € HT

Réf.: MSAZ2001

La formation **configurer la structure d'un dépôt pour des pipelines sécurisés** permet de maîtriser les bonnes pratiques de **structuration de dépôts dans Azure Repos** afin de soutenir des **pipelines DevOps** sécurisés et efficaces. Elle guide les participants dans la mise en place d'une architecture adaptée pour gérer le code, les **workflows CI/CD**, la traçabilité et les contrôles de sécurité, tout en assurant une collaboration fluide entre les équipes.

Cette formation est idéale pour structurer des projets DevOps robustes, réduire les risques liés à la sécurité du code et optimiser les performances des pipelines d'intégration et de déploiement continu.

A qui s'adresse cette formation ?



Pour qui

- Développeurs
- Ingénieurs DevOps
- Ingénieurs Sécurité
- Architecte Solutions
- Ingénieur du support
- Analyste des opérations de sécurité



Prérequis

- Connaissance de base d'Azure DevOps
- Connaissance de base des concepts de la sécurité, comme les identités et les autorisations
- Expérience de l'utilisation du portail Azure pour créer des ressources comme Azure Key Vault et définir des autorisations
- **Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !**

Programme

1 - Configurer une structure de projet et de référentiel adaptée aux pipelines sécurisés

- Diviser un projet en sous-projets d'équipe et en dépôts distincts
- Séparer les fichiers sensibles entre plusieurs projets
- Déplacer un dépôt sécurisé en dehors d'un projet
- Attribuer des autorisations aux projets et aux dépôts
- Organiser une structure claire de projets et de dépôts

2 - Mettre en place un accès sécurisé aux ressources utilisées dans les pipelines

- Détecter les menaces de sécurité courantes
- Configurer l'accès aux pipelines via des pools d'agents spécifiques
- Organiser et protéger les variables secrètes et les groupes
- Assurer la sécurité des fichiers et du stockage
- Mettre en place des connexions de service
- Administrer les environnements de manière sécurisée et efficace
- Renforcer la sécurité des référentiels

3 - Gérer les identités liées aux projets, aux pipelines et aux agents

- Mettre en place un pool d'agents hébergé par Microsoft
- Déployer et configurer des agents pour vos projets
- Définir et gérer les identités utilisées par les agents
- Ajuster l'étendue d'une connexion de service
- Convertir en identité managée dans Azure DevOps

4 - Configurer et valider des autorisations

- Définir et contrôler les autorisations utilisateurs
- Configurer et valider les droits d'accès aux pipelines
- Mettre en place et vérifier les règles d'approbation et de gestion des branches
- Superviser et auditer les autorisations dans Azure DevOps

5 - Étendre un pipeline pour utiliser plusieurs modèles

- Concevoir des modèles
- Réécrire le pipeline de déploiement
- Configurer le pipeline et l'application pour générer et utiliser des jetons de manière sécurisée
- Supprimer les secrets en texte brut
- Limiter la journalisation des agents
- Détecter et supprimer conditionnellement les tâches de script dans Azure DevOps

6 - Configurer un accès sécurisé à Azure Repos depuis les pipelines

- Configurer l'accès du pipeline aux packages
- Définir les secrets d'informations d'identification et les secrets pour les services
- Vérifier les secrets stockés dans Azure Key Vault
- Vérifier que les secrets ne s'affichent pas dans les journaux

7 - Configurer les pipelines pour utiliser les variables et paramètres en toute sécurité

- Vérifier que les paramètres et variables conservent leur type
- Limiter l'utilisation non sécurisée des paramètres et variables
- Placer les paramètres dans un fichier YAML sécurisé
- Limiter les variables définies à la mise en file d'attente
- S'assurer que les variables obligatoires sont bien définies dans Azure DevOps

8 - Configurer les pipelines pour utiliser les variables et paramètres en toute sécurité

- Garder le bon type pour les paramètres et les variables
- Éviter l'utilisation non sécurisée des paramètres et variables
- Mettre les paramètres dans un fichier YAML pour les protéger
- Limiter les variables modifiables lors du lancement du pipeline
- Vérifier que les variables obligatoires sont présentes dans Azure DevOps



Les objectifs de la formation

- Configurer une structure de projet et de référentiel sécurisé pour les pipelines Azure DevOps
- Sécuriser l'accès aux ressources de pipeline en utilisant des pools d'agents et des connexions de service
- Gérer les identités pour les projets, pipelines et agents dans Azure DevOps
- Configurer et valider les autorisations utilisateur et les vérifications d'approbation
- Étendre un pipeline en utilisant plusieurs modèles pour améliorer la modularité
- Configurer des pipelines pour utiliser des variables et des paramètres de manière sécurisée



Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.



Les points forts de la formation

- Au cours de cette formation, les participants découvriront comment implémenter la sécurité à chaque étape d'un pipeline DevOps, en intégrant les principes du DevSecOps dans leurs workflows CI/CD
- L'expertise technique et l'expérience de consultants
- Une formation alignée sur les bonnes pratiques de sécurité cloud et DevOps



Dates 2025 - Référence MSAZ2001



Dernières places disponibles



Session garantie

le 8 déc.

- le 8 déc. 9h00 -> 17h00