



## Une banque multinationale atteint la conformité en matière de sécurité grâce à DROPS pour déployer à travers des environnements cloud hybrides isolés.

Une des plus grandes banques internationales prestatrice de services financiers au Canada s'apprête à déployer des applications multi-plateformes en environnement hautement sécurisé.

### Le défi

Le Département IT de la banque opère dans un **paysage informatique diversifié**, incluant IBM i (aussi connu sous les noms iSeries, AS/400) comme serveur de base de données, une application principale en RPG, et une interface utilisateur développée en .NET sur Microsoft Azure.

Le déploiement sur IBM i est lent et laborieux, et les équipes rencontrent des difficultés en l'absence d'outils de gestion des modifications avec une séparation des tâches très fragmentée. Pour des raisons de sécurité, une entreprise externe était chargée de la promotion des packages de versions, tandis qu'un autre groupe d'utilisateurs internes effectuait l'installation. Cette opération externalisée engendrait des coûts élevés et retardait la livraison de nouvelles fonctionnalités.

Pendant ce temps, côté .NET, tout le travail front-end bénéficiait d'un processus CI/CD complet via Azure DevOps.

### Transformation DevOps

L'application bancaire centrale sur IBM i étant hautement stratégique, l'équipe d'architecture a entrepris de moderniser les méthodes et de rationaliser les coûts. L'objectif était d'intégrer le **développement IBM i dans la même méthodologie de pipeline Azure DevOps que les applications front-end**, en utilisant les outils cloud d'Azure pour piloter **tous les déploiements, couvrant à la fois la base de données DB2 i, les objets natifs IBM i, le code .NET, et une application Java résidant dans le système de fichiers IFS** (Integrated File System).

### Cloud hybride et sécurité

Tous les systèmes IBM i de la banque sont hébergés sur site dans le même data center, tandis que le front-end Azure est géré et servi par des ressources basées sur le cloud. Pour respecter les réglementations strictes en matière de sécurité, les environnements privés (développement, test et pré-production) devaient être isolés de l'environnement de production orienté client.

Ainsi, dans une véritable infrastructure cloud hybride, la banque a configuré **deux instances cloud indépendantes et isolées** : un cloud privé de développement et un cloud de production partiellement public. Le serveur de développement IBM i utilise un ensemble d'outils de développement basés sur le cloud, tandis que le serveur de production IBM i présente une interface utilisateur cloud aux clients via une interface publique.

Le serveur de développement IBM i n'a aucune connexion avec le monde extérieur, et aucune communication n'est autorisée entre les deux instances cloud, sauf via un mécanisme d'entreprise strictement contrôlé. Au départ, **cette isolation réseau stricte posait certains défis lors de la phase de déploiement du cycle de vie de l'application**.

### Déploiement entre des environnements cloud « isolés »

La séparation complète des réseaux a été facilitée par DROPS d'ARCAD. Pour déployer de l'environnement cloud de développement vers le

cloud de production, DROPS gère un package de déploiement (dans le cas d'IBM i, des save files) contenant des objets applicatifs testés. DROPS récupère ce package à partir d'Azure Artifacts et l'envoie vers le cloud de production, où il est déployé à la demande depuis Azure vers le serveur de production.

**Aucun outil ne pouvant couvrir à la fois les environnements de développement et de production**, Azure Artifacts est répliqué sur chaque environnement, et un serveur DROPS distinct interagit avec chaque instance d'Azure Artifacts.

Un pipeline Azure automatise la compilation, l'emballage et le déploiement du save files depuis Dev vers QA, en remplissant l'instance Azure Artifacts en Dev. Un second pipeline Azure dans le domaine de production utilise l'instance répliquée d'Azure Artifacts, conjointement avec les connaissances du référentiel de métadonnées ARCAD, pour valider la version entrante et activer le déploiement en production.

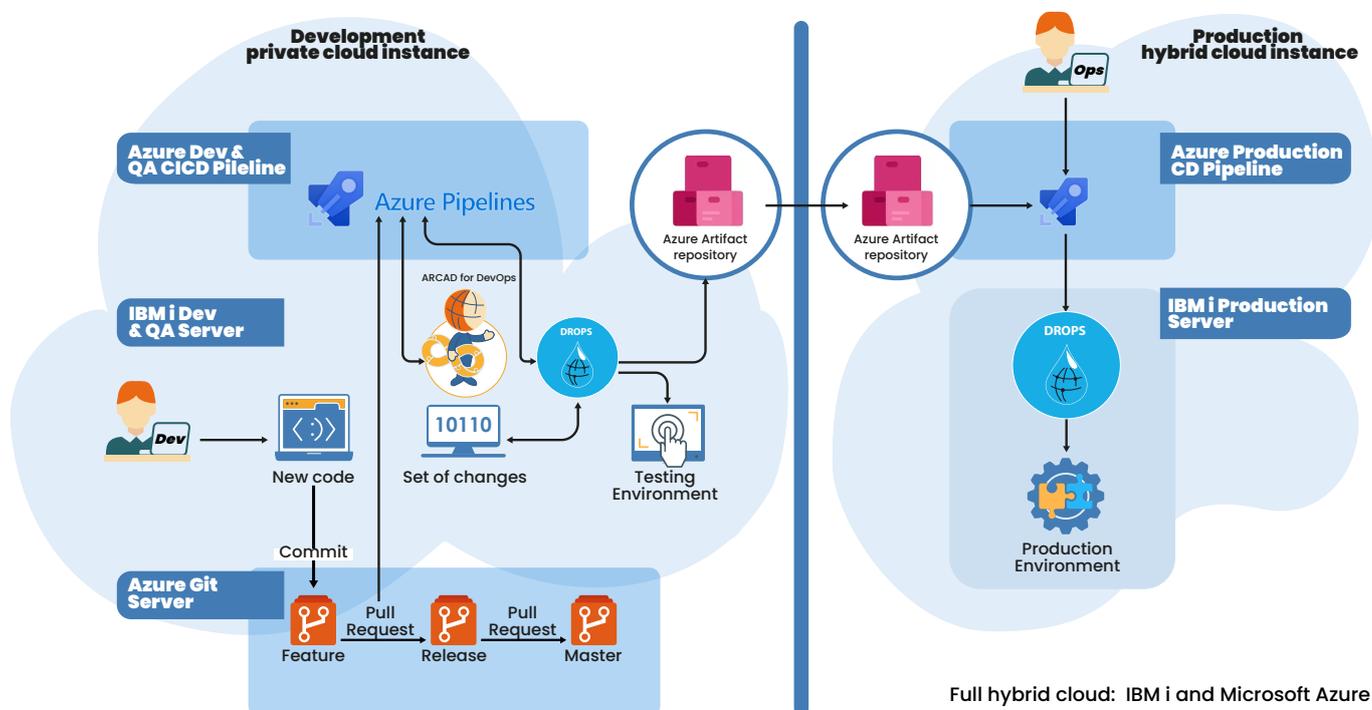
Cela garantit un processus de déploiement universel, sécurisé et conforme : **tous les composants RPG, .NET et Java sont déployés simultanément dans des environnements cloud isolés**, avec une restauration automatique en cas d'erreur.

## Suivi des changements et conformité

Lors de l'intégration d'IBM i dans Azure, un défi majeur était de capturer un package de déploiement et de l'identifier correctement. DROPS capture l'identifiant unique du package externalisé à partir des métadonnées exposées pendant le processus de développement pour garantir que les objets déployés en production sont **exactement les mêmes que ceux testés dans l'environnement QA**. Cet identifiant "voyage" avec les objets modifiés, permettant le suivi des changements tout au long du cycle de vie de l'application jusqu'à la production.

Cela signifie que **tout le cycle de vie peut désormais être suivi depuis Azure DevOps**. Il est facile de voir quel développeur a fait la demande de modification à l'origine, sur quel élément de travail dans Azure Boards, et même quelles lignes de code spécifiques ont été modifiées.

Cela offre un **niveau élevé de transparence** et de responsabilité des modifications, avec une **claire séparation des tâches et une visibilité à tous les niveaux**. Les auditeurs peuvent recevoir des informations complètes sur le cycle de vie des changements effectués même il y a plusieurs mois.



"Les progrès que nous avons réalisés sont incroyables. Les retours de l'équipe sont tous positifs. Nous déployons désormais TOUS les artefacts de manière sécurisée à travers notre environnement cloud hybride. DROPS d'ARCAD a permis des gains de temps et une réduction du travail et des coûts", **Responsable Développement, Banque Numérique**