Développement : y-a-t-il des limites au DevOps et au tout code ?

La démarche DevOps associe étroitement les équipes de développement d'une solution logicielle avec celles chargées de leur exploitation. Cette nouvelle manière agile de produire prend en compte plus rapidement les modifications demandées par les utilisateurs, grâce à des cycles de développement raccourcis et à une mise en production accélérée.

Au début d'un cycle d'amélioration, les équipes de développement planifient le changement à apporter, l'implémentent, vérifient le bon fonctionnement, puis le package et passent la main aux équipes d'exploitation qui vont mettre en route, configurer et monitorer la solution.
Les données de suivi remontent alors chez les développeurs, pour nourrir un nouveau cycle d'amélioration. Voilà pour la version courte.

DevOps ou Biz-SecDevOps with Quality ?

Dans la version longue du DevOps, la phase de planification s'effectue donc, en général, avec les métiers qui font remonter les remarques sur les défauts de la solution, sur la justesse des modifications récemment opérées (y compris en matière de ROI), mais aussi sur les désirs d'évolution. Il faudrait plutôt parler de BizDevOps, car cette approche est orientée métiers.

La qualité est aussi une partie intégrante du cycle opéré par les équipes de développement.
Cette étape, qui peut être largement automatisée, suppose aussi un rapprochement avec d'autres équipes dédiées plus spécifiquement au contrôle qualité. En particulier si la méthodologie DevOps ne s'applique plus à un composant logiciel classique, mais à un produit physique ou dématérialisé, par exemple, un système de freinage d'urgence intelligent intégré à un véhicule, ou une pièce d'avion, lorsque la démarche DevOps s'est infusée au sein des bureaux d'études.

Quality et DevOps sont des termes qui reviennent souvent dans les offres d'emploi, ce qui montre l'importance de cet aspect.

Mais il en existe un autre encore plus stratégique : la sécurité. Avec les modes de développement traditionnels, des équipes dédiées se chargeaient de mettre à l'épreuve des versions de test du produit, avant de le valider, voire de lui attribuer une certification.

Avec des circuits de développement courts et des modifications apportées en continu, cela devient difficile, pour ne pas dire impossible. Les développeurs doivent donc acquérir une certaine hygiène de la sécurité, afin de garder ce sujet à l'esprit lors de leurs travaux, car ils deviennent des acteurs à part entière de la sécurité. Une thématique complète est dérivée de cette problématique, le SecDevOps.

Vers une automatisation totale de l'Ops ?

L'automatisation, au cœur du DevOps, s'appuie, en général, sur des techniques mises en point pour les infrastructures cloud. On parle alors de l'infrastructure « as code » qui définit les besoins matériels, automatise la livraison du logiciel, le provisionnement de l'instance, puis le fonctionnement de l'application à distance depuis les bureaux des développeurs.
Certains prédisent même l'arrivée d'un « everything as code » qui irait encore plus loin en prenant en charge quasiment toute la phase d'exploitation… y compris la commande des serveurs physiques et leur maintenance.

Cette approche pourrait revenir, *in fine*, à ne plus prendre en compte l'expertise de l'opérateur physique chargé de l'exploitation des solutions. Un piège à éviter, car la connaissance du matériel reste essentielle pour les entreprises. Un exemple : dans le cadre de calculs massivement parallèles menés par un établissement bancaire, les GPU sont un atout face aux processeurs classiques en termes de puissance de traitement et d'efficacité énergétique.

Le développeur peut, certes, spécifier ce besoin au sein du code, mais ce sont les équipes chargées de l'exploitation qui doivent choisir les bonnes technologies en fonction des contraintes de leurs datacenters, et saisir les opportunités liées à l'apparition d'une nouvelle offre matérielle.

Si les spécialistes du hardware sont à même de détecter les nouvelles technologies, ils peuvent aussi être forces de proposition. Les applications en conteneur peuvent dorénavant être déployées sur des mainframes : pourquoi ne pas en mettre un au catalogue, puis proposer ces nouveaux services aux métiers et aux développeurs ?

Cette tâche est aujourd'hui entièrement prise en charge par les hyperscalers.
Amazon a mis l'accent sur des instances ARM de nouvelle génération, dont le rapport puissance/coût permet d'ouvrir de nouvelles possibilités à ses clients. Mais dans un cloud privé, qui va apporter ces compétences ? Et il est bon de disposer d'au moins un profil « tech » pour opérer les bons choix sur le cloud public.

Où en serons-nous dans quelques années ? Le groupe SecDevOps devrait s'imposer autour d'équipes resserrées, avec toujours plus d'automatisation par le code. Il sera en prise directe avec le business qu'il dessert. Mais aussi avec la technologie qu'il exploite. Notre sandwich du futur pourrait donc fort ressembler à Biz-SecDevOps-Tech.