Multicloud : comment développer la bonne approche « best of breed »

Après des années de scepticisme suivies par une stratégie de petits pas, les DSI français plongent dans le cloud et passent peu à peu d'un modèle cloud hybride au multicloud.
Fin 2020, IDC estimait que 85 % des entreprises étaient déjà engagées dans une stratégie multicloud et que ce taux atteindrait 90 % en 2024.

Bien souvent, ce sont les métiers qui ont initié cette approche en choisissant les services SaaS répondant à leurs attentes. Désormais, les DSI les plus matures vis-à-vis du cloud se sont engagées dans une stratégie résolument « best of breed » pour choisir leurs services en fonction des capacités de chaque Cloud Services Provider (CSP). On peut choisir Google Cloud Platform (GCP) pour sa technologie Big Query, AWS pour porter des applications Web et, encore, Microsoft Azure pour les outils liés à la workplace.

Principal enjeu : gérer une infrastructure

La présence géographique ou la réglementation de certains pays obligent aussi les DSI à chercher d'autres CSP pour couvrir leurs besoins.
« Les entreprises ont besoin d'aller vers des usages multicloud en fonction de leurs besoins fonctionnels ou dans une recherche de meilleure couverture géographique. Nous avons suivi cette évolution en nous appuyant, dans un premier temps, sur AWS, puis sur Microsoft Azure, sur Google Cloud Platform, Alibaba et, enfin, OVH et Croc, en Russie. Nous accompagnons nos clients vers une hybridation multicloud public » raconte Stéphane Aisenberg, cofondateur de Linkbynet.

Celui-ci a constaté l'accroissement de ce besoin de déployer des workloads cloud en Chine, en Russie ou en Amérique du Sud, après les premiers déploiements en Europe et en Amérique du Nord. Ce qui engendre de nouveaux besoins en termes d'expertise et de gouvernance. Les entreprises doivent faire monter en compétences leurs équipes d'exploitation sur ces services cloud qui offrent chacun des outils d'administration différents.

Splunk s'est positionné sur la supervision multicloud avec une plateforme qui dispose de plus de 2 000 intégrations avec de multiples solutions IT et bien évidemment tous les CSP.
« On peut connecter de multiples sources de données, qu'elles soient internes, issues des cloud publics ou d'autres technologies, dont les mainframes, les plateformes blockchain de traçabilité, etc. », explique Stéphane Estevez, directeur produit chez Splunk.

» Superviser l'ensemble de ces briques d'infrastructure, c'est un peu la cour des miracles ! Il faut être capable de monitorer toutes ces briques depuis un seul point et non plus basculer d'un outil à un autre, entre les outils en ligne des fournisseurs cloud, celui d'APM (Application Performance Management) de l'entreprise et les outils de supervision réseau. » poursuit-il.

Cette diversité d'outils entrave l'action des ingénieurs lorsqu'il faut localiser rapidement les problèmes d'exploitation et il faut parfois impliquer plusieurs administrateurs pour y parvenir.

Le Multicloud bouscule les architectures

Le réseau est un aspect souvent négligé dans les projets de migration vers le cloud. Pourtant, dès que les applications stratégiques de l'entreprise prennent le chemin des datacenters des fournisseurs de cloud publics, l'accès devient critique. Les performances et la disponibilité des accès Internet, trop aléatoires, poussent les entreprises à opter pour les solutions de connexion directe aux datacenters des CSP.

Qu'il s'agisse du DirectConnect d'AWS, de l'ExpressRoute de Microsoft Azure ou de l'Express Connect d'Alibaba Cloud, chaque CSP propose une offre de connexion directe avec ses spécificités propres. L'entreprise alors doit apprendre à configurer et à administrer ces liens, ce qui peut rapidement devenir complexe à l'échelle de la planète.

Jérôme Dilouya, CEO d'InterCloud propose de gérer ces infrastructures pour le compte des entreprises : « Notre offre s'adresse aux grandes entreprises internationales, comme Schneider Elctric, des banques et assureurs mondiaux qui n'ont pas deux ou trois datacenters cloud à connecter, mais parfois une cinquantaine dans le monde. Dans de telles conditions, la gestion de chaque lien réseau devient un sac de nœuds. Arrivées à un certain point, les entreprises se tournent vers nous, non plus seulement pour une question d'outsourcing, mais pour ne plus avoir de compétences à acquérir et maintenir sur chacun de ces cloud. »

Selon lui, certains de ses clients sont en train de se débarrasser de leur ancienne infrastructure réseau. Toutes leurs applications prenant désormais le chemin du cloud public, le réseau d'interconnexion de leurs applications entre CSP devient le véritable backbone de l'entreprise.

Faut-il privilégier les services managés

Le choix du DSI de sélectionner les meilleurs services auprès des multiples fournisseurs cloud et plus largement une stratégie « best-of-breed » présente de nombreux avantages, notamment pour mieux servir les métiers. Mais elle expose fortement au risque de « vendor lock-in » et elle pose la problématique de l'homogénéité de l'ensemble.

Ainsi, garantir le même niveau de sécurité entre des applications portées par un cloud A et par un cloud B qui disposent chacun d'outils différents pose de vrais problèmes de conformité.

F5 se positionne aujourd'hui en tant que fournisseur d'outils multicloud qui permettront aux entreprises de s'affranchir des solutions spécifiques des CSP : « Nous proposons des solutions qui peuvent se déployer on-premise ou dans n'importe quel Cloud public », argumente Arnaud Lemaire, directeur technique F5 France.

« Cette approche permet à la DSI de s'abstraire des services applicatifs délivrés par les fournisseurs cloud eux-mêmes, comme les firewalls applicatifs, le chiffrement SSL, etc. Ainsi, le DSI est assuré de la conformité de la sécurité d'un environnement qui peut être très hétérogène, et l'entreprise n'a pas à repenser l'ensemble de ces services liés à la sécurité et à la performance au moment de changer de CSP. »

Pour renforcer cette stratégie cloud, F5 vient de prendre le contrôle de la startup franco-américaine

Volterra. Celle-ci a créé un backbone mondial qui permet à une entreprise de connecter un datacenter, un site distant à son infrastructure Cloud via un nœud sécurisé Volterra.

Kubernetes n'est peut-être pas la réponse magique

Si les experts pointent les dangers de mettre en œuvre des fonctions extrêmement spécifiques à certains fournisseurs cloud, à l'image de la fonction Serverless Lambda d'AWS, l'alternative du conteneur logiciel porté par une infrastructure Kubernetes n'est pas aussi miraculeuse que certains semblent vouloir le faire croire.

Ainsi, pour un grand client international, l'ESN Skale-5 avait développé une application sur GCP qui a dû être portée sur Alibaba Cloud lorsque le client a souhaité déployer l'application sur un deuxième Cloud. Résultat : entre 30 % à 45 % du code a été réécrit, bien que l'application soit portée par Kubernetes. Beaucoup des scripts de déploiement « Infrastructure as Code » ont été réécrits.

Yann Colleu, consultant et architecte cloud chez Skale-5 explique les limites de la portabilité apportée par Kubernetes : « La logique applicative reste la même, mais quand on fait le choix de Kubernetes, on uniformise les API, mais tout ce qui est infra-as-code pour construire le cluster, les types de disques et stockage à mettre en place, le load-balancing, tout cela va changer d'un Cloud provider à un autre. »

Kubernetes ne représente qu'une part de l'infrastructure et, pour le consultant, tenter de s'abstraire de tout lock-in ne doit pas être la priorité dans un projet de conteneurs logiciels.
Pour lui, la conteneurisation est, avant tout un moyen de standardiser au maximum l'infrastructure logicielle, ce qui est une excellente pratique pour aller vers le cloud et simplifier malgré tout les déploiements.

Alain Clapaud