

Le SI de Mutex passe sur AWS

Compte rendu rédigé par ANDSI & Pierre Delort

En bref...

Dominique BOSSARD, DSI du Groupe Mutex, effectuera un retour d'expérience afférent au programme MOPS2020, projet s'inscrivant dans le cadre d'une transformation profonde de cette société. Après une brève présentation de Mutex, il exposera notamment l'organisation et le déroulé du projet, les dispositifs de sécurité retenus ainsi que ses éléments financiers et économiques.

L'Association Nationale des Directeurs des Systèmes d'Information organise des débats et en diffuse des comptes-rendus, les idées restant de la seule responsabilité de leurs auteurs. Elle peut également diffuser les commentaires que suscitent ces documents.

Présentation de Mutex

Mutex est une société d'assurance française créée en 2011, spécialisée en prévoyance et épargne retraite. Emanation de la FNMF et filiale du Groupe VYV, Mutex conçoit des produits et solutions en marque blanche. Son chiffre d'affaires en assurance prévoyance ressort à 1 milliard d'euros. Elle emploie à ce jour environ 600 collaborateurs, dont 100 informaticiens.

Son écosystème se rapporte à AESIO, ADREA, mais également à Chorum, Harmonie Mutuelle ou à la MGEN. Ces deux derniers acteurs correspondent à de véritables piliers du Groupe VYV. Mutex correspond à une assurance et non à une mutuelle, et en tant qu'assurance, Mutex entretiens des relations avec la Banque de France, mais également avec l'Assurance Maladie ou l'ACPR (Agence de Contrôle Prudentiel et de Résolution, le régulateur de l'Assurance).

Cartographie applicative

Mutex dispose d'un SI classique avec des applications liées à des échanges en BtoB, mais également des applications « clé en main » qui sont fournies aux distributeurs. Finance, RH, actuariat, etc., les briques applicatives sont nombreuses.

Le projet MOPS

En termes de contexte, ce projet a pour origine l'arrivée à échéance, en 2019, d'un contrat d'infogérance Atos/Bull qui proposait une prestation de data center. En 2017, le volume hébergé s'établissait principalement à 200 To de stockage actif et 340 VMs/serveurs x86, et plus 80 applications.

Les services achetés auprès de Bull/Atos ne répondaient plus aux attentes en raison d'une offre peu évolutive, d'une faible capacité à accélérer, à une maîtrise des coûts peu lisible en projection, etc. En 2018, un dialogue compétitif a été conduit pendant six mois. Au départ, il s'agissait d'un appel d'offres d'infogérance classique. Rapidement, il est apparu pertinent de passer à une stratégie cloud.

Le seul impératif se rapportait à une nécessaire maîtrise des datas qui devaient demeurer en France. A cette époque Microsoft et Amazon étaient les seuls acteurs capables de proposer un cloud souverain. L'infogéreur devait être en mesure d'intégrer dans son offre du *full cloud*. Atos et Bull n'ont pas été retenus dans la *shortlist*. GFI et Sopra Steria ont montré un savoir-faire sur ces sujets tandis qu'Easy Team se situait dans une logique « disruptive ». Pour finir, GFI a été retenu.

Les enjeux du projet se déclinaient de la sorte :

- dynamiser l'infogérance ;
- améliorer la qualité et la sécurité de l'hébergement ;
- améliorer la disponibilité et la continuité de fonctionnement ;
- bénéficier de la flexibilité offerte par le cloud ainsi que de l'évolutivité des services applicatifs ;
- réduire les coûts d'exploitation et d'hébergement du SI de Mutex.

Périmètre et stratégie de migration

Le périmètre de la migration renvoie à l'intégralité du SI Mutex, applications et dispositifs techniques. En revanche, il a été décidé de ne pas migrer les éléments qui étaient déjà hors data center, à savoir quelques activités ou applications déjà en mode SaaS, la messagerie, etc.

La stratégie initiale se rapportait à 11 lots en mode *sprint*. Celle-ci a été abandonnée afin de préserver les ressources sur des opérations le week-end durant une période de quatre mois. Un découpage en 4 lots macro fonctionnel avait également été envisagé avec une étape de bascule à blanc et une étape de bascule réelle pour chaque lot. Il a finalement été décidé de procéder à un découpage en 9 lots en privilégiant la migration des environnements hors production puis les environnements production en deux week-end, ce qui a bien fonctionné.

Planning

Le dialogue compétitif auprès de quatre sociétés a été conduit en 2017. GFI a été retenu pour une étude préalable. Le démarrage des travaux préparatoires et contractuels (infogérance et éditeurs) a démarré en janvier 2019. A la même période, une négociation est intervenue avec les éditeurs pour les ajustements potentiels des licences. L'ensemble des éditeurs a joué le jeu, à l'exception d'Oracle. L'ACPR a été informée et cette dernière n'a pas relevé de difficulté. Elle a simplement rappelé que Mutex devait lui donner la capacité d'auditer l'infogéreur. AWS a donné des gages, ce qui a rassuré cette autorité. En mai 2019, la *landing zone* AWS était prête. La migration a ensuite débuté à partir de septembre. Le projet s'est terminé à l'été 2020 avec seulement trois mois de retard.

Organisation du projet

Il semblait essentiel que ce projet technique soit porté par le métier et le DG et pas uniquement par les informaticiens. En raison de la complexité de la démarche, des sous-chantiers ont été ouverts. Par exemple, un sujet afférent à la Direction de programme a été mené pour assurer une bonne coordination et une communication adéquate.

Les principaux points déterminants et favorables se déclinent comme suit :

- sponsoring hiérarchique fort ;

- architecture de type IaaS à la source (SI 100 % virtualisé) ;
- cœur réseaux en propre indépendant du cloud et liaisons très hauts débits ;
- Atos et GFI au rendez-vous ;
- intégration d'un sachant/expert cloud au sein du dispositif projet ;
- Directeur de Programme communiquant et coordonnant les différents acteurs SI et Métiers de Mutex.

Pour ce qui est des éléments positifs, il convient de retenir les éléments suivants :

- objectifs atteints : 100 % du SI Mutex basculé sur AWS dans le planning annoncé ;
- absence totale de souci d'ordre technique et stabilité constatée une fois les SI basculés ;
- gains de temps de réponse constatés par les utilisateurs sur les SI migrés ;
- business plan confirmé : 36 % de gains à isopérimètre de l'infogérant en coûts évités et Payback sur trois ans.

Le point d'attention technique principal renvoie à la nécessité de bien connaître le SI. Il importe également de mentionner l'identification des OS inéligibles au IaaS cloud. De surcroît, il convenait d'adapter la stratégie de migration en tenant compte du plan projet Mutex et de la capacité planning et ressources. Enfin, il apparaît indispensable d'opérer un suivi régulier de l'évolution des coûts.

Les dispositifs de sécurité

Un travail a notamment été conduit afin de séparer AWS en plusieurs comptes, mais également une refonte globale des VLANs à travers la notion de VPC à l'intérieur des comptes AWS. En termes de qualité de service, il importe de souligner une augmentation du SLA global à travers les mécanismes intrinsèques d'AWS. De surcroît, un mécanisme de PRA a été défini par la sanctuarisation d'une AZ (Availability Zone) AWS de la région de Paris ou la création d'un compte DR (Disaster Recovery) pour les tests annuels. Enfin, plusieurs travaux sont en cours, à l'instar du chiffrement des données au niveau Infra à travers les services AWS disponible.

Eléments financiers

Ajustement licensing :

- 0,6 million d'euros TTC.

Pour ce qui est du Run (baseline comparée avant/après) les éléments financiers sont les suivants :

- 36 % de gains à isopérimètre de l'infogérant en coûts évités et Payback sur trois ans.

Perspectives

Les prochaines étapes renvoient à des actions FinOps à l'instar de la supervision « AWS Budget » (dispositif d'alerte de dépassement de seuils) ou d'un arrêt des instances non utilisées en période « creuse » (nuit et week-end pour les environnements hors production et les applications de production inutilisées). Il convient également de mentionner une évolution vers des services managés afin de bénéficier de fonctionnalités propres au cloud et de réduction des coûts apportée par les services PaaS, tout en conservant une capacité de réversibilité.

Débat

Int : Je connais mieux GCP, mais il me semble que les dépenses peuvent être cadrées sur AWS.

DB : En effet. Il importe de déterminer un équilibre entre une organisation contraignante et une certaine souplesse pour les utilisateurs. En outre, il convient de vérifier régulièrement la facture AWS.

Int : Une équipe chargée de vérifier les infras a été déployée. Comment cela fonctionne-t-il concrètement ?

DB : Mutex emploie 100 informaticiens. La gouvernance informatique regroupe cinq personnes. Une personne sur FinOps est en lien avec le patron de l'architecture. A ce jour, une interne a la responsabilité du *software asset management*. Des nouveaux métiers ont été constitués, avec GFI en *back up*.

Int : A combien le taux de remise s'établit-il avec ce type de contrat ?

DB : Le taux ressort à 30 %.

Int : Nous avons un cloud privé surdimensionné et notre idée consiste à le réduire.

DB : Ce qui convient à Mutex ne s'applique pas forcément à d'autres structures. AWS est une entreprise américaine qui facture en dollars et qui est sur des contrats luxembourgeois. Enfin, il est impératif que l'informatique de Mutex ne soit pas considérée comme un pollueur. L'engagement environnemental, sociétal et social embarque un volet IT. Le recours à des structures mutualisées permet de moins polluer.

Int : La moitié du coût énergétique renvoie aux Capex. La mutualisation conduit à un meilleur bilan énergétique.

DB : Ce type d'information m'intéresse.

Int : Vous avez soulevé la question des sauvegardes. Le coût de stockage semble raisonnable, ce qui n'est pas le cas de la logistique de gestion des sauvegardes.

DB : Nous ne sommes pas raisonnables s'agissant des volumes que nous conservons. Le potentiel de gains étant réel en la matière, un travail devra être mené sur le sujet.

Int : Amazon propose différents dispositifs de stockage à l'instar de Glacier qui n'est pas onéreux. Le temps de récupération des données varie en fonction du prix du forfait.

Int : Dans le doute, nous sauvegardons tout. Il est intéressant de constater que de grandes sociétés peuvent basculer sur le cloud.

Int : Avez-vous constaté des difficultés avec les équipes infra dans la mesure où elles changent de métier.

DB : A l'occasion de mon arrivée, l'informatique chez Mutex accusait un réel retard technique. Aucune personne à ce jour ne souhaiterait faire marche arrière.

Int : Nous avons opéré ce type de bascule dans une caisse régionale de Groupama. Nous disposons d'un cloud privé. Avez-vous procédé à une recherche d'optimisation sur la gestion des environnements ?

DB : Nous allons désormais rentrer dans ce niveau de sophistication.

Présentation des orateurs

Dominique BOSSARD, après un début de développeur en Allemagne, a travaillé dans les services financiers (Groupe BNPP, CdC) en études et production (CTO) et est le DSI de Mutex (groupe VyV). Il est diplômé du CNAM (Master's degree option IT, réseau et système).