thalesgroup.com

THALES

HySIO Flex : le cloud de Thales
Une expérience de dix ans riche d'enseignements

Préambule

Ce livre blanc présente le retour d'expérience de Thales dans la conception, la mise en œuvre et l'opération de son cloud privé mutualisé, HySIO Flex, développé sur une base Opensource (Openstack) et utilisé depuis plus de six ans dans le cadre de ses activités d'infogérance au bénéfice de ses clients les plus exigeants.

Trois exemples pour illustrer ce propos :

- Thales opère pour le compte d'une grande entreprise publique de transport urbain ses applications clients après les avoir transformées en profondeur et migrées sur son cloud, en mode micro-services «conteneurisés» et déployés automatiquement.
- Thales a également migré sur son cloud une grande partie du système d'information d'une entreprise industrielle importante pour l'opérer en mode hybride avec des systèmes traditionnels et le fournir au client en mode service (paiement à l'utilisateur).
- Enfin, pour un autre grand industriel de l'aéronautique, nous avons mis en place il y a plus de quatre ans une instance privée afin de migrer et opérer deux cents applications critiques en mode cloud.

Ce livre blanc se présente sous forme d'une discussion entre différentes parties qui ont chacune joué un rôle dans cette aventure. C'est une confrontation de points de vue opérationnels entre Alexandre, Concepteur à l'initiative du projet ; Julien, Chef de produit qui l'a fait évoluer ; Cédric, Développeur qui a contribué à son éclosion ; Pascal et Mickael, Architectes Cloud qui conçoivent les solutions pour les clients; Nathalie et Yoann, Responsables des équipes qui l'exploitent au quotidien.

Ce dialogue met en évidence des perceptions qui diffèrent selon le rôle de chacun sur les succès, les points d'amélioration, la suite à donner, et des points de convergence qui font l'unanimité.

Ce qui ressort de façon évidente c'est que cette expérience de près de dix années, qui s'appuie sur de nombreux projets menés avec des clients exigeants, a profondément modifié nos pratiques d'infogérant et plus largement l'ensemble de nos activités de conception de Systèmes d'Information, de développement d'application et de cybersécurité.

A l'heure où la plupart des entreprises privées et des organismes publics adoptent résolument une stratégie orientée vers le cloud et le multicloud pour soutenir leur transformation numérique, nous avons pensé que notre expérience et ses impacts sur notre activité d'infogérant pouvait être une contribution utile à leur réflexion, en apportant modestement un éclairage pratique et concret sur un cas d'usage, ce qui a bien fonctionné et ce qui aurait pu mieux fonctionner.

Editorial

Le cloud est devenu une composante naturelle et essentielle à nos activités de développement et d'infogérance, qui apporte à nos clients la flexibilité, la compétitivité économique et les niveaux de service dont ils ont besoin pour servir leurs métiers et contribuer à leur transformation numérique.

Avec notre offre d'infogérance hybride multicloud (HySIO™), nous apportons à nos clients des réponses pragmatiques pour les accompagner dans leur transformation numérique et mieux servir leurs métiers.

L'offre HySIO™ permet une gestion efficace des systèmes d'information par une répartition optimisée des applications sur les infrastructures les mieux adaptées (dédiées/legacy, cloud privé et public). Notre capacité à transformer et gérer les systèmes d'information hybrides et multicloud résulte d'un long chemin parcouru par nos équipes et dont l'origine remonte à 2009.

Dès 2009, convaincu que le Cloud n'était pas juste un effet de mode, Thales a décidé de lancer le projet de conception d'un cloud privé et mutualisé afin d'accompagner ses clients et de moderniser ses activités d'infogérance.

Le cahier des charges était le suivant : prise en compte d'applications sensibles par une solution mutualisée, multi-cients et sécurisée, capable de s'hybrider facilement avec d'autres infrastructures non cloud et cloud, performante, agile, évolutive et compétitive. A l'époque, cette décision fait suite à trois années d'expérimentation sur le cloud menées par notre laboratoire de recherche, qui nous ont permis de mieux en appréhender les possibilités et les enjeux.

En résumé notre ambition : être capable de délivrer des services sur cette plateforme de Cloud dans les mêmes conditions de sécurité et de performance que sur les plateformes dédiées, et pouvoir prendre les mêmes engagements vis-à-vis de nos clients.

Début 2013, après deux années de conception et de construction, la solution HySIO Flex est mise en production. Depuis plus de six ans maintenant, Thales migre, développe les applications critiques de ses clients et les opère avec des conditions économiques nettement améliorées (de l'ordre de 30% en fonction du contexte) tout en respectant des engagements uniques de performance, de disponibilité et de sécurité.

L'offre HySIO™ d'infogérance hybride sécurisée est devenue pour nos clients une réalité concrète. Elle permet une transformation en profondeur des systèmes d'information pour les rendre plus flexibles, agiles et améliorer leurs performances tout en réduisant les coûts.
L'expérience acquise avec notre cloud privé a été un tremplin vers une hybridation sur des solutions de cloud publics telles que AWS, Azure ou OVH. Elle nous a aussi permis d'intégrer une réelle pratique DevSecOps généralisée à tous nos projets. En effet, grâce à la maturité de nos équipes sur le cloud, nous avons développé une approche agile, mis en place des équipes mixtes DevSecOps (Développement, Sécurité et Opérations) et conçu une usine de développement logiciel multicloud, ATHENA, entièrement basée sur des briques Opensource. Elle permet de développer des applications natives cloud performantes et sécurisées, facilite et sécurise la transformation des applications existantes de nos clients pour profiter des avantages du cloud.

Joël Derrien
Directeur Général Délégué
Thales Services

Alexandre, tu as été à l'origine d'HySIO Flex.

Quelles ont été les motivations pour démarrer ce projet de cloud ?

En 2009, avec la direction de Thales et les responsables de l'activité infogérance, nous observions depuis quelques temps l'évolution du concept de Cloud Computing et sa concrétisation sur le marché avec l'arrivée de nouveaux acteurs tels qu'AWS et Rackspace par exemple.

Par ailleurs, nous avions les premiers retours d'expérience cloud grâce à notre laboratoire de recherche qui travaillait depuis 2006 sur ce concept dans le cadre de grands projets européens tels que « RESERVOIR » qui s'appuyaient sur les toutes premières solutions Opensource de l'époque (Eucalyptus, OpenNebula).

Nous étions convaincus que le Cloud Computing deviendrait un élément indispensable de l'informatique des entreprises notamment pour la flexibilité et la réactivité qu'il apportait. Par contre, nos clients ayant des exigences fortes de performance et de sécurité regardaient cette évolution de l'informatique avec une méfiance certaine. Pour réussir, nous devions donc proposer une solution maîtrisée alliant les principaux avantages du cloud (flexibilité, automatisation, mutualisation, paiement à l'usage, …) à un engagement fort de notre part vis-à-vis de nos clients sur l'opération d'applications critiques en production.

Quelles ont été les critères qui ont mené au choix d'Openstack ?

En premier lieu, nous avons choisi l'Opensource parce qu'il nous permet de maîtriser totalement nos solutions et leurs évolutions dans le temps, au service de nos clients, et en particulier sur l'aspect primordial de la sécurité.
Par ailleurs nous étions convaincus que l'offre libre de l'époque avait le potentiel d'évolutivité pour intégrer, dans le temps, les fonctions que nous jugions nécessaires. Thales a une culture fortement ancrée dans l'Opensource (voir le livre blanc « La transformation numérique annonce le second âge de l'Open Source » - Septembre 2018) et par ailleurs, depuis plusieurs années, toutes les solutions « digitales » (Cloud, Big Data, IA, …) sont principalement tirées sur le marché par des technologies Opensource.

Le choix d'Openstack a donné lieu à un grand débat interne. Openstack était naissant alors que d'autres solutions Opensource existaient depuis quelques années et nous les connaissions pour les avoir testées. Nous avons donc mené une étude de risque portant sur les aspects techniques des solutions et sur la gouvernance des communautés.

Du point de vue technique, Openstack était loin d'être mature mais, à la suite de nos tests opérationnels, les modules existants nous ont semblé de bonne qualité. Nous sentions aussi qu'il y avait un fort potentiel de développement, en particulier grâce à la communauté créée autour de contributeurs solides dont les deux premiers, la NASA et Rackspace. La roadmap des versions était bien gérée tout en étant ambitieuse. L'animation technique de la communauté était de bonne qualité et le support bien organisé.

Nous avons également été séduits par la gouvernance affichée de la communauté. La ségrégation claire entre l'organisation technique et l'organisation de gestion/financement était un élément essentiel de différentiation qui garantissait l'indépendance technique. Nous sommes ainsi devenus un des tout premiers contributeurs techniques européens dans la communauté tout en étant membre de la fondation (contributeur financier) sans qu'il y ait mélange des genres.

Avec le temps, nous pouvons considérer d'une part que ce pari s'est avéré être le bon et d'autre part que notre choix a été fait pour les bonnes raisons.

Pour toi, Nathalie en tant que Directrice des opérations de l'activité infogérance.

Quels sont les avantages et inconvénients de l'Opensource pour le cloud ?

Les avantages sont assez évidents. Il y a d'une part la richesse des fonctionnalités et la rapidité des développements. En quelques années, Openstack est passé de deux services de base à plus d'une soixantaine. D'autre part, le support et la réactivité de la communauté sont de vrais avantages lorsque l'on est responsable de la disponibilité de la plate-forme. La culture profondément Opensource de Thales facilite également la prise en compte de la solution par les équipes.

A cela s'ajoutent deux points : la gratuité du logiciel, qui ne veut cependant pas dire que cela ne coûte rien et l'indépendance vis-à-vis d'un éditeur dont on sait que la stratégie peut être versatile et réserver des surprises, notamment sur le plan économique.

En contrepartie, l'Opensource nécessite un investissement interne dans la durée. Pour intégrer, adapter, faire évoluer et maintenir la solution, il est indispensable de constituer et former une équipe pluridisciplinaire (Directeur et chefs de projet, architectes, développeurs, intégrateurs/testeurs, responsables de production) avec un niveau d'expertise suffisant et qui, en fonction de l'ampleur du projet, peut être composée de plusieurs dizaines de personnes. Cette équipe doit aussi assurer la conduite du changement et la formation en interne, qui sont clés pour que chacun s'approprie la solution et pour permettre à l'entreprise d'atteindre petit à petit le bon niveau de maturité.

Yoann,

Responsable du pôle delivery cloud

J'ajouterais que nous devons disposer en interne de compétences qui nous garantissent l'autonomie de fonctionnement dont nous avons besoin. La rareté des compétences et la compétition sur le marché pour intégrer et fidéliser les ressources clés est également une problématique constante à ne pas sous-estimer. Au début du projet les compétences n'existaient tout simplement pas, aujourd'hui elles sont rares et fortement demandées.

Mickael,

Lead Technical Architect

Oui, Openstack repose sur des standards ouverts, des API très bien implémentées dans de nombreux outils (Terraform – Ansible - …), au même titre que celles des grands cloud publics que sont AWS, Azure, ou Google.

Les fournisseurs de Cloud publics offrent d'ailleurs souvent eux-mêmes des API Openstack. Il faut cependant comprendre que chaque acteur implémente les composants Openstack avec des modules et des versions potentiellement différents. Il est donc indispensable de vérifier à chaque fois le bon fonctionnement des API.
Autre richesse de la solution, il est généralement possible de remplacer des services Openstack par des services autres. Par exemple Neutron dispose d'un « Load balancer as a Service » mais cette fonction est souvent remplacée par des solutions tierces comme par exemple HAProxy ou F5 LTM.

Julien,

Responsable de l'ingénierie des Service Managés Cloud

Pour moi, l'Open source favorise le support de standards ouverts et la capacité à instancier notre propre roadmap, donc notre indépendance pour créer et maintenir une solution qui nous correspond.
Par ailleurs, l'Open source est une boite à outils qui nous laisse une très grande liberté pour réaliser nos adaptations et prendre en compte nos besoins spécifiques. Enfin, concernant plus spécifiquement Openstack, la communauté est très active et la solution est très ouverte sur le reste du monde grâce à ses APIs (Application Program Interface) qui sont devenues de facto des standards du marché. La réussite nécessite cependant la constitution dans la durée d'une équipe de spécialistes pouvant assurer l'ingénierie, le support de la solution et l'intégration de nouveaux clients. Depuis le lancement du projet, plusieurs dizaines de personnes sont affectées à ces missions.

Pascal,
Architecte Cloud

Effectivement, la richesse des composants est très importante et grâce aux API, ils interagissent parfaitement entre eux. Suivant le besoin, certains composants peuvent être échangés avec d'autres plus récents, on peut utiliser des back-end différents apportant de nouvelles « fonctionnalités » (back-end de stockage, de réseau, d'annuaire..), voir remplacer certains composants par des solutions propriétaires ou même hardware (SDN type nuage, Load Balancer , firewall..). C'est donc une solution très modulaire que l'on peut adapter précisément aux besoins.

Même si depuis quelques versions la fondation OpenStack a œuvré pour rendre la solution plus stable, les composants restent hétérogènes, aussi bien dans leur architecture que dans leur degré de maturité.

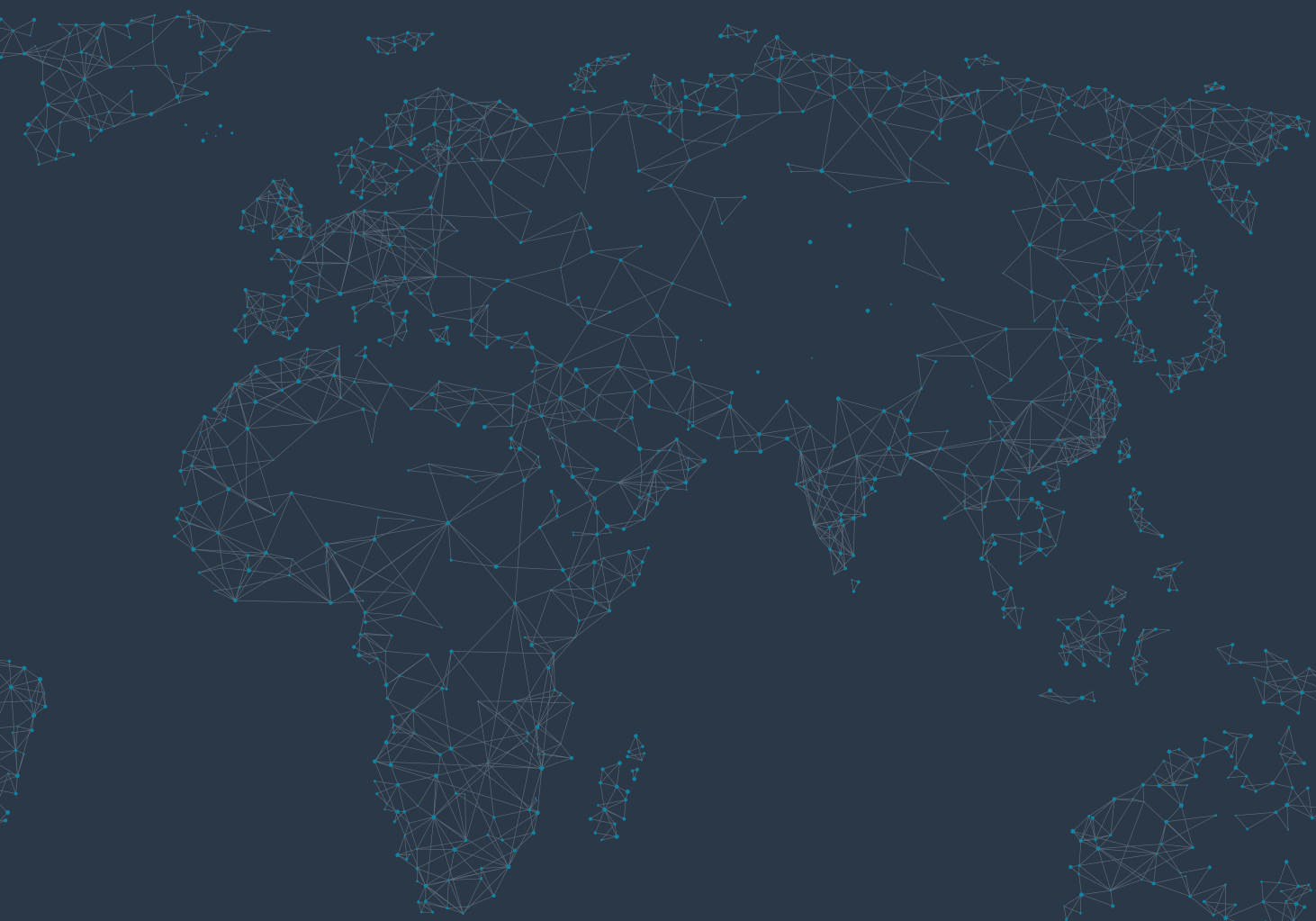
Il est indispensable de bien étudier des critères comme la qualité du code, la taille et la diversité de la communauté, la courbe d'évolution, les autres composants concurrents et la tendance IT avant de les choisir pour éviter de se retrouver au bout de quelques mois dans une impasse.

Au final, la solution est une sorte de lego qu'il n'est pas si facile à maintenir en production : En clair, il faut s'organiser pour être à même de l'exploiter efficacement.

Cedric,
Développeur
expert Openstack

Puisque nous parlons d'hétérogénéité, certains composants sont très ouverts (par exemple Neutron) et s'adaptent facilement aux spécificités. D'autres sont plus fermés (par exemple NOVA) et moins adaptables. L'approche des deux types de composants est très différente. En l'occurrence, Neutron propose un cœur de fonctionnalités et chacun peut l'adapter assez librement. NOVA développe un cœur fermé et stable dans lequel il est couteux de faire entrer des spécificités métier. C'est à nous de nous adapter à cette réalité, module par module.

La communauté est très dynamique et met sur le marché une nouvelle version tous les six mois. C'est très bien du point de vue agilité, évolution et enrichissement des fonctions. Par contre la durée de support des versions est courte par rapport aux habitudes dans l'Opensource (18 mois contre 3 à 5 ans). Elle oblige à suivre plus rapidement les évolutions avec les risques que cela implique en production.



Cédric pour toi qui a largement contribué au développement d'HySIO Flex,

Quels sont les points forts de notre solution ?

Nous avons une longue expérience sur Openstack, une des plus longues du marché, en particulier en France.

Notre solution est opérationnelle, en production depuis début 2013 avec des applications critiques en production, des volumes significatifs (plusieurs milliers de VM actuellement en production), et des performances élevées.
Ainsi nous pouvons assurer des niveaux de disponibilité de 99,95% grâce en particulier à notre instanciation en deux zones de disponibilité et aux mécanismes de synchronisation mis en place.

La solution va au-delà du IaaS. Les fonctions d'hybridation permettent d'intégrer des composants spécifiques (appliances, FW, serveur non cloudifiables tels qu'Oracle ou les AS 400) très simplement et de façon sécurisée.

Les composants que nous avons ajoutés sont faiblement couplés et donc facilement réutilisables sur une autre distribution ou une autre version Open source d'Openstack. C'est important en termes d'évolutivité de la solution et aussi pour son interopérabilité avec d'autres Cloud Openstack (OVH par exemple).

Julien

La vraie mesure du succès de notre projet c'est d'avoir une solution Openstack opérationnelle mutualisée entre plusieurs dizaines de clients exigeants, qui supporte des environnements critiques en production avec des volumétries significatives (plusieurs milliers de machines virtuelles).

Nos développements renforcent la sécurité du cloud pour répondre aux exigences de nos clients. Je pense en particulier à l'authentification forte par défaut, à la séparation native des réseaux d'administration et de production ou aux APIs (Application Program Interface) sécurisées.

Nous avons également travaillé à faciliter les opérations en production. Openstack est conçu par des développeurs dont la première préoccupation est de permettre l'exécution d'applications natives cloud. Nos clients attendent de notre part des engagements forts pour la production d'applications qui souvent ne sont pas natives cloud. Pour cela nous avons travaillé sur le développement de fonctions de gestion industrielle du cloud qui nous permettent d'assurer des niveaux de service élevés aussi bien sur les applications migrées que sur les applications natives cloud.

Enfin, l'intégration avec notre éco système d'infogérance, c'est-à-dire l'ensemble de nos outils de production, notre suite ITSM (IT Service Management) qui intègre en particulier la CMDB (Configuration Management DataBase), la supervision, la gestion des incidents, la facturation, le back-up, ... Cette intégration est indispensable pour fiabiliser la production, la tenue de nos engagements, la bonne information de nos clients.

Alexandre

Oui, nous avons fait ce qui était indispensable pour atteindre notre objectif d'infogérance de SI critiques sur un cloud mutualisé.

Les fonctions de sécurité dont parle Julien, auxquelles j'ajouterai la gestion des DNS (Domain Name System) ou la gestion des réseaux, ont été particulièrement importantes pour permettre la mutualisation entre nos clients tout en respectant la tenue de nos engagements.

Yoann

Du point de vue de la production, la solution propose aussi une fonction unique qui permet de mixer très librement deux types d' hyperviseur (KVM et Vmware) dans un même projet. C'est un gros avantage pour nos clients qui pour beaucoup utilisent Vmware et ne souhaitent pas en changer.

Nous pouvons gérer en même temps des applications plus anciennes que nous migrons en confiant à l'infrastructure (Vmware) la charge d'assurer leur résilience et des applications nouvelles, souvent développées sur l'hyperviseur KVM et qui, parce qu'elles sont natives cloud, gèrent elles-mêmes leur haute disponibilité.

Dans le même ordre d'idée, nous pouvons adapter le niveau de mutualisation aux besoins d'isolation des applications du client, grâce à la possibilité de mixer dans un même projet des serveurs physiques (hyperviseurs) mutualisés et dédiés. Cette possibilité s'avère très utile en particulier pour les fonctions les plus sensibles de nos clients dont ils ne veulent pas qu'elles soient installées sur des machines mutualisées.

Nathalie

Oui, de plus, la tenue de nos engagements de SLAs exige une très forte réactivité. Notre maitrise de la solution, le fait que nous ayons un accès direct au code et que nous le connaissions bien, nous permet d'être très rapide pour corriger les problèmes, notamment lorsqu'ils se trouvent aux bornes de la solution, par exemple entre l'architecture matérielle et Openstack. De ce point de vue, la dépendance vis-à-vis d'un éditeur nous ralentirait.

Par ailleurs, notre expérience de près de dix ans nous donne une compétence solide pour intégrer et gérer d'autres solutions de cloud, dédiées (hyperconvergées) ou publiques.

Mickael

Pour nos projets de migration vers le cloud ou de développements natifs cloud, nous avons conçu et développé une usine logicielle (Athena), également basée sur des briques Opensource et implémentée sur Openstack. C'est la base technologique de notre approche DevSecOps. Elle apporte beaucoup aux équipes de développement et de migration en termes d'agilité, de fiabilité et d'automatisation. Aujourd'hui, Athena est la solution de l'ensemble des équipes pour tout nouveau projet. Les chiffres sont en augmentation constante et rapide avec à ce jour plus de 1600 personnes qui l'utilisent chez Thales et une quarantaine de projets actifs. Elle est déployée sur notre Cloud Openstack et également sur AWS et OVH. Cette usine multicloud permet de déployer et gérer une application automatiquement, indépendamment du cloud sous-jacent. Elle intègre des fonctions telles que « l'autoscalling » et « l'autorepair » indépendantes d'Openstack, AWS, Azure, ou de toute autre solution de cloud. La dimension métier des projets est prise en compte en particulier grâce à l'intégration dans Athena de la solution HySio Watch de monitoring des services multi plates-formes.

Et aujourd'hui

Quelles limites voyez-vous à la solution Thales ?

Nathalie

En tant qu'opérateur le choix d'une distribution du marché plutôt qu'une solution Open source aurait un côté rassurant et nous faciliterait un peu la vie. Par contre, comme je l'ai dit précédemment, nous n'aurions pas la même réactivité. La bonne nouvelle c'est que la solution est stable en production et qu'il n'y a pas eu de gros problème purement lié à Openstack depuis son lancement.

La gestion des montées de versions structurantes est une vraie difficulté. C'est vrai pour tous les utilisateurs d'Openstack car elles nécessitent généralement un arrêt de service. La réponse à cela est d'avoir une « road map » interne structurée, de bien étudier la stratégie d'évolution à chaque montée de version pour limiter les perturbations au strict minimum. L'autre réponse est technique et consiste à conteneuriser Openstack et automatiser au maximum son déploiement.

Pascal

La communauté est importante et très agile. Elle avance vite. Cependant la pérennité des développements n'est pas garantie.

Par exemple le module « Magnum » est petit à petit rendu obsolète par d'autres modules qui offrent les mêmes fonctions et cannibalisent les contributeurs.

D'où l'importance de bien étudier chaque module avant de l'adopter, et pas uniquement d'un point de vue technique. En cas de mauvais choix, le risque de devoir migrer est non négligeable.

Julien

Contrairement à ce que l'on peut penser à priori, l'Open source n'est pas gratuit. Il nécessite soit de s'appuyer sur une distribution payante du marché, soit un investissement interne important qui doit perdurer dans le temps pour faire évoluer régulièrement la solution. Nous avons fait le choix de la seconde option et, en conséquence, nous devons nous organiser pour être indépendants et combler nos éventuels manques internes.

Yoann

De façon très pratique, à l'heure actuelle je vois plus particulièrement un point qui permettrait d'améliorer notre solution, c'est la mise en œuvre d'une solution de SDN (Software Define Network).

Elle nous permettra de gagner en agilité, en sureté de fonctionnement et aussi en scalabilité.

Nous sommes un peu victimes du succès de la plate-forme dans la mesure où, avec notre technologie Vlan actuelle, nous arrivons en limite de capacité.

Cédric

En tant que développeur Openstack, j'ajouterai que nous avons adapté la solution plutôt que de nous adapter à elle. Cette approche se justifie par la nécessité de répondre à l'attente principale de nos clients qui est d'abord de migrer leurs applications existantes en conservant un haut niveau de qualité de service et de sécurité.

En faisant ces adaptations, nous avons veillé à limiter les forks mais nous n'avons pas pu les éliminer totalement. La maintenance en est un peu alourdie et de fait nous perdons en agilité d'évolution.

Alexandre, avec le recul,

Quelles leçons retires-tu de notre expérience Openstack ?

Nous avons perçu dès le début trois difficultés que nous avons adressées à travers notre organisation et nos choix :

- Comment bien gérer l'Open source et sa richesse, choisir les bons modules en fonction de leur maturité, de leur roadmap, du dynamisme des contributeurs.
- Comment adapter une solution quand les objectifs à court terme de la communauté ne correspondent pas tout à fait aux nôtres. La cible Openstack était « l'infrastructure as a code », les instances privées de Cloud et l'hébergement d'applications natives Cloud. Notre cible était un cloud privé mutualisé, hautement sécurisé, pour gérer principalement, au moins dans un premier temps, des applications de gestion migrées et qui s'appuient sur des infrastructures plus « intelligentes », capables en particulier de prendre en compte la disponibilité.
- Comment bien gérer les modifications apportées à Openstack d'une part, pour qu'elles soient facilement portables sur les nouvelles versions, d'autre part, pour que nous puissions les remplacer par les fonctions standards au fur et à mesure de leur disponibilité.

Certains développements internes qui pallient des manques fonctionnels de la solution doivent être abandonnés lorsqu'un module standard est rendu disponible.
La difficulté est d'analyser objectivement la situation pour migrer vers la solution de la communauté au meilleur moment. Nous avons connu cette situation à plusieurs reprises. Par exemple, nous avons développé une interface utilisateur qui n'existait pas. Lorsque le module Horizon est arrivé pour remplir cette fonction, la décision de remplacer notre développement et du bon timing de migration a été difficile à prendre de façon totalement objective et rationnelle.

Enfin, la conduite du changement auprès des équipes de production et de développement est un élément clé de la réussite du projet. Il est indispensable qu'elles prennent la solution à leur compte et se l'approprient. De ce point de vue, notre approche qui a consisté à créer une équipe projet mêlant des personnes du laboratoire de Recherche et développement de Thales, des équipes de développement et des équipes de production a été un succès.

Julien

Comme beaucoup nous étions très optimistes sur le rythme d'adoption du cloud et de développement d'applications natives. Nous pensions qu'en conséquence la répartition entre les ressources sous KVM et sous Vmware serait plus équilibrée.

Dans les faits, nous gérons beaucoup plus d'applications migrées sur le cloud sous Vmware que de nouvelles applications natives cloud sous KVM.

Nathalie

Nous avons eu l'audace de rentrer tôt dans Openstack et d'en faire une solution opérationnelle, mutualisée et sécurisée. Cela a été possible parce que nous avons géré la solution comme un produit avec une vraie roadmap et l'intégration d'une équipe incluant des architectes système, technique, des développeurs et les opérations.

Si nous devions construire un cloud aujourd'hui, nous nous y prendrions sans doute autrement. Compte tenu de l'évolution du marché du IaaS et de sa maturité actuelle, nous choisirions sans doute une solution éditeur pour gagner en vitesse et surtout pour nous concentrer sur les nouveaux enjeux dont le niveau de maturité et d'industrialisation sur le marché sont encore faibles, à savoir la gestion multicloud et d'usine logicielle indépendante. Deux sujets étroitement liés.

Pascal

Dans la réflexion que je mène avec mon client sur l'architecture, nous apportons une attention particulière aux adaptations pour qu'elles ne mettent pas en cause la capacité à suivre les versions d'Openstack. Cette problématique a fait l'objet d'une étude et nous avons choisi avec le client de ne réaliser que le strict minimum des adaptations indispensables. De plus, nous utilisons la conteneurisation pour être en mesure d'évoluer brique par brique et pouvoir faire fonctionner les versions en parallèle pendant une période de temps.

Autre leçon importante, la vitesse d'évolution engendre de l'instabilité, incompatible avec les enjeux de la production. Il est indispensable de gérer rigoureusement sa roadmap interne, en choisissant en particulier d'adopter un rythme d'évolution plus lent (par exemple tous les 12 ou 18 mois plutôt que tous les 6 mois) pour éviter cet écueil.

Avec cette expérience nous avons appris en marchant. Personne chez nous ou sur le marché n'avait à l'époque le recul pour nous conseiller utilement sur nos choix et nous montrer la trajectoire. La maturité est venue petit à petit sur le cloud lui-même et aussi sur les aspects applicatifs. Pour réussir la transformation de son SI le client doit aussi acquérir le niveau de maturité nécessaire. Aujourd'hui, il peut se faire aider pour accélérer le processus.

Pour passer d'une infrastructure classique au cloud et encore plus au multicloud, il faut avoir une vision de l'architecture finale et avancer étape par étape dans la transformation des applications. Les étapes peuvent être par exemple : la virtualisation, puis l'automatisation des déploiements, la migration vers du stockage objet, l'éclatement de l'application en micro services, la conteneurisation, etc. En sachant que toutes les applications n'ont pas vocation à aller jusqu'au bout de la démarche.

Notre retour d'expérience d'utilisation d'un cloud en production nous a permis à partir de 2016 de mettre le pied dans une démarche DevSecOps opérationnelle très rapidement et de la généraliser au sein des équipes de développement et de production.

Nous sommes aujourd'hui bien avancés sur le sujet, nos équipes de production sont maintenant confortables avec les démarches d'automatisation, l'utilisation des API Rest, la notion de SDDC (Software Define Data Center), … Grâce à cela, nous accélérons le temps de mise sur le marché (Time to Market) et améliorons sensiblement la qualité de notre production. Par exemple, pour un client, nous avons pu gagner 80% sur le temps de mise en production de ses applications migrées sur le cloud et réduit de 90% le nombre d'incidents liés à ces mises en production, tout en réduisant ses coûts de plus de 15%.

Forts de notre expérience, nous avons aussi pu nous approprier et maîtriser très rapidement les technologies hyperconvergées et celles du cloud public, ce qui nous ouvre un panel de solutions très large pour mieux répondre aux problématiques de nos clients.

Et maintenant,

Quelles sont les évolutions sur lesquelles nous travaillons ?

Alexandre

Les enjeux du cloud sont en train d'évoluer sur plusieurs plans. Les solutions de IaaS, qu'elles soient publiques ou privées, sont désormais matures mais d'autres défis doivent être relevés.

En particulier :
La gestion multicloud devient une préoccupation majeure.
Les organisations savent maintenant qu'elles vont mixer des solutions de cloud multiples (privé, public, IaaS, PaaS et SaaS) et les hybrider avec leur infrastructure classique qui a vocation à subsister pour une part au moins. Gérer de façon industrielle et sécurisée le multicloud est une nouvelle complexité à prendre en compte pour laquelle le niveau de maturité sur le marché est encore faible.

Le PaaS se développe rapidement car il permet le développement d'applications natives c'est-à-dire d'applications véritablement élastiques et qui intègrent elles-mêmes leur propre mécanisme de résilience en s'appuyant notamment sur des services Cloud de persistance de données hautement disponibles. On peut le considérer comme une évolution naturelle du IaaS qui pose cependant de façon plus prégnante la question de la dépendance au fournisseur de cloud. Dans une stratégie multicloud, le PaaS peut être un frein ou au contraire un facilitateur. L'enjeu pour nous est de construire avec Athena un PaaS qui donne la plus grande indépendance possible vis-à-vis des différents IaaS.

Julien

Oui, je suis totalement d'accord. Nous travaillons sur la gestion multicloud et l'orchestration des conteneurs. Ces deux besoins se rejoignent car le conteneur permet non seulement de supporter les nouvelles applications natives cloud (Microservices) mais aussi d'assurer la portabilité et une plus grande indépendance vis-à-vis des différents cloud, en particulier grâce à une solution comme Kubernetes. Une solution de CaaS (Container as a Service) basée sur Kubernetes et intégrée à notre usine logicielle Athena nous permettra d'assurer l'indépendance vis-à-vis des cloud. La mise en œuvre d'une CMP permet de porter cette vision multicloud et d'avoir une approche industrielle. La difficulté aujourd'hui est de trouver une solution assez mature et qui réponde à tous nos enjeux de gestion multi-tenants et de tenue des engagements de performance et de sécurité.

Nathalie

Pour nous, aux opérations, les prochaines étapes concernent principalement trois points :

- Le renforcement de la sécurité des données, avec en particulier les capacités de chiffrement, d'anonymisation et de sauvegarde pour répondre aux exigences de plus en plus fortes de nos clients et au renforcement régulier des normes telles que HDS (Hébergeur de Données de Santé).
- Les Services autour de la ressource, VM/Containers, données et applications, dans un contexte multicloud : sécurisation, monitoring, sauvegarde, tenue des performances.
- L'automatisation de la réversibilité. L'évolution vers le multicloud rend indispensable de garantir l'indépendance vis-à-vis des solutions et des fournisseurs.

Yoann

Je vais renforcer ce qui a déjà été dit, nous devons être le plus agnostique possible vis-à-vis des solutions de cloud. Nous connaissons très bien Openstack, les solutions du marché (Vmware, VXRail, Nutanix) et de cloud public.

Nous devons désormais monter d'un niveau d'abstraction, renforcer notre usine logicielle, Athena, avec des fonctions avancées pour les développeurs, une sécurité toujours plus intégrée et l'intégration d'une solution CaaS (Container as a Service) pour amener nos clients vers un PaaS indépendant des infrastructures sous-jacente.

C'est sur ce terrain que se joue dans les années qui viennent la transformation vers le cloud des systèmes d'information.

Cédric

Oui. J'ajouterai l'intégration d'une solution de SDN (Software Define Network) que nous avons prévue. C'est un sujet important pour résoudre les limites actuelles de scalabilité et pour mettre en place la notion de «service chaining» qui permettra une vraie rupture en termes d'agilité et de fiabilité.

Conclusion

Cette conversation et ces différents points de vue montrent qu'un projet de cloud n'est pas juste de la consommation à la demande de ressources informatiques, faciles à obtenir à coût réduit. Bien entendu, notre projet est particulier parce que nous opérons les Systèmes d'Information de nos clients avec des contraintes spécifiques et aussi parce que nous avons commencé très tôt lorsque le niveau de maturité des solutions et des personnes était faible. Ceci étant, nous sommes convaincus qu'une grande part des points que nous avons évoqués ici est à prendre en compte peu ou prou dans tout projet de cloud.

Des « quick-win » peuvent être obtenus, qui nécessitent peu de temps et d'investissement. Cependant, pour obtenir les vrais bénéfices du cloud, il faut du temps, acquérir un minimum de maturité sur le sujet et que le projet soit étudié, planifié, exécuté étape par étape. La conduite du changement auprès de toutes les parties prenantes (production, développement, utilisateurs, management, acheteurs, financiers, …) est également un facteur clé de succès.

Avec l'expérience nous avons acquis quelques convictions fortes, en particulier :

- Le cloud de type IaaS est la base indispensable mais elle ne suffit pas à tirer les vrais bénéfices du cloud.
- Il faut construire par-dessus le IaaS des capacités d'hybridation vers les infrastructures classiques (legacy) et vers d'autres cloud pour que le SI puisse être géré efficacement.
- Les fonctions de PaaS sont le complément indispensable aux IaaS. On peut utiliser avantageusement les solutions proposées par les grands cloud publics ou, si l'organisation souhaite conserver une certaine liberté à travers une stratégie multicloud, utiliser une usine logicielle multicloud indépendante.
- La sécurité n'est pas une option dans le monde du numérique. Pas d'économie numérique sans confiance, pas de confiance sans cybersécurité.
- Les développements nouveaux et la transformation des applications existantes doivent s'appuyer sur des organisations, méthodes et des outils DevSecOps, gages de qualité, d'agilité et de sécurité.

A la suite du développement d'HySIO Flex et fort de cette expérience, nous avons donc mis en œuvre des équipes DevSecOps pour assurer les nouveaux développements et pour la transformation des applications existantes, qui s'appuient sur une usine logicielle multicloud, Athena. Athena est une plateforme de développement, d'intégration continue, de tests automatiques (fonctionnels et de sécurité) et de déploiement continu en production. Elle est basée sur un ensemble d'outils Opensource que nous avons intégré, industrialisé et sécurisé depuis bientôt quatre ans.

Nous développons aussi une plateforme sécurisée de BigData et d'IA, également multicloud et qui intègre, industrialise et sécurise toutes les briques logicielles nécessaires pour développer en mode DevSecOps des projets de BigData associés à de l'intelligence artificielle.

Nous avons vocation à aider nos clients à mettre en œuvre leur propre projet, à gagner du temps et à réduire les risques.

Notre implication peut se faire à différents niveaux :

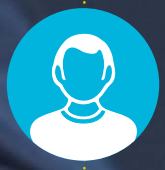
- Conseil pour la conception et la mise en œuvre d'une stratégie cloud.
- Transformation d'une application existante pour la migrer sur un cloud public ou privé.
- Conception, développement et opération d'une application native cloud.
- Migration vers une application en mode SaaS et son opération.
- Conception, mise en œuvre et opération d'une plateforme multi-cloud intégrant et sécurisant un cloud dédié ou privé avec plusieurs solutions de cloud public.
- Mise en œuvre d'une méthodologie DevSecOps, d'une usine logicielle multicloud de type Athena ou d'une plateforme Big-Data et IA clé en main.
- Transformation et infogérance sécurisée de votre SI.

HySIO Flex : le cloud de Thales
Une expérience de dix ans riche d'enseignements

Bio Express

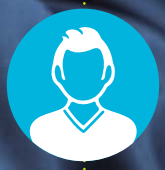
Nathalie S.

2 années dans la direction des opérations d'infogérance de services critiques sécurisés en partie appuyés sur une plaque de cloud privé openstack hybridée et sur les clouds publics.
5 années dans la construction d'un opérateur de cloud public national 100% openstack en dual DC. Lancement d'une offre service managée basée sur un Cloud Openstack mondial sur 4 Datacenter Europe & Asie Pacifique.
15 années en DSI pour un opérateur de transport aérien.



Julien M-F

Je travaille sur le Cloud depuis plus de 10 ans déjà, en premier lieu au travers de projets de recherche européens (comme le projet FP7 Reservoir), puis plus opérationnellement pour nos services d'infogérance en tant qu'Architecte Cloud et Product Owner de notre solution de IaaS. Aujourd'hui, je me focalise sur l'implémentation et la mise en œuvre de nouveaux services comme le Container-as-a-Service et la Cloud Management Platform.

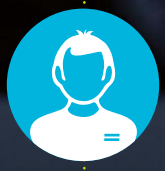


Yoann S.

Intrapreneur, Leader avant d'être manager, passionné par le Cloud et le Chaos Engineering mais avec les pieds sur terre et la tête sur les épaules.
Editeur de logiciel, Startup, Cloud Service Provider Français et Multinationale sont mes terrains de jeu.
J'anime chez THALES des équipes révolutionnaires pour fournir des solutions Cloud à nos clients.
#OpenStack #Kubernetes #python #restful
Mon Motto ? La créativité c'est penser à de nouvelles choses. L'innovation c'est faire de nouvelles choses et une personne qui n'a jamais commis d'erreurs n'a jamais tenté d'innover.

Pascal P.

Architecte cloud OpenStack, responsable de l'architecture des plateformes Cloud interministerielles de la Direction Générale des Finances Publiques, plateforme de « cloud interne » du 1er cercle définit dans la stratégie du cloud computing de l'Etat.
J'ai débuté en tant qu'administrateur système Unix, puis rapidement je me suis occupé de l'intégration des projets de divers clients avant de prendre un poste d'architecte projet à la DGFIP et depuis 3 ans la responsabilité de l'architecture de ses plateformes cloud. J'étends mon expérience cloud avec des formations AWS et AZURE.



Mickael R.

Tombé dans la marmite à l'âge de 10 ans et passionné de logiciels libres depuis toujours, je n'ai jamais cessé de m'intéresser aux différentes évolutions de l'IT. Du développement, aux systèmes et infrastructures, mon parcours hétéroclite me permet aujourd'hui d'avoir une vision d'ensemble des sujets DevOps et Cloud qui allie un mélange des différents métiers de l'IT. Ma connaissance des différents cloud publics et privés me permet d'apporter à mes clients une vision éclairée et pragmatique au regard de leurs besoins.

Cédric B

Touche à tout dans le monde de l'informatique (dev, système, automatisation).
Il y a 10 ans, j'ai découvert (sans le savoir) le cloud, au travers de projets de recherche européens (FP7 Reservoir, ITEA3 EASI-CLOUDS).
Maintenant je suis architecte/expert Cloud/DevOps sur notre solution de IaaS après avoir été core-developer Neutron dans la communauté OpenStack.
J'accompagne le développement de notre solution et nos clients sur des sujets en pointe.

Alexandre B

Après une expérience de développeur puis de chef de projet dans le monde de la cryptographie, j'ai pu prendre la responsabilité de projets d'intégration Infrastructure et d'opération de SI avec des contraintes toujours très fortes en termes de disponibilité, performance et sécurité.
Passionné de nouvelles technologies, j'ai eu la chance de diriger le projet visant à doter THALES de sa propre solution maitrisée de cloud privé pour ses services d'infogérance de Systèmes d'Information critiques. La phase de démarrage projet a été extrêmement enrichissante car située dans un contexte marché avec une très faible maturité.

THALES

22 rue Grange Dame Rose
78140 Vélizy-Villacoublay
France
+33 (0)1 73 32 00 00

> thalesgroup.com <