

TECH/TRENDS

HORS
SÉRIE

NOVEMBRE
2015

PERCEVOIR LE FUTUR

CLOUD



*Préparer
sa migration*

*Sélectionner
son offre*

*Choisir
ses technologies*

we scale
Be a cloud expert

Xebia
SOFTWARE DEVELOPMENT DONE RIGHT

Introduction

Dans le paysage IT actuel, le Cloud Computing est omniprésent. Cependant, même si son adoption progresse au sein des entreprises, la migration de tout ou partie d'un parc applicatif reste bien souvent complexe. Les acteurs de cet écosystème sont de plus en plus nombreux et les offres se multiplient en conséquence. Les décideurs sont confrontés à des choix stratégiques et technologiques difficiles.

L'approche Cloud n'est plus réservée à l'élite des sociétés innovantes et technophiles. Les applications cœur de métier des entreprises basculent progressivement dans les nuages. Avec la montée en compétences des équipes techniques, ce mouvement tend à s'accélérer, à un moment où le time-to-market est devenu un enjeu crucial. Une évolution s'est amorcée avec la diffusion des méthodes agiles : les équipes de développement sont aujourd'hui mieux entraînées pour livrer plus vite des applications ayant davantage de valeur ajoutée. Dans la même dynamique d'éclatement des silos historiques, le mouvement DevOps est apparu, avec ses pratiques de mixité des équipes techniques et ses outils d'automatisation. Beaucoup d'entreprises visent maintenant à dépasser l'intégration continue pour atteindre la livraison continue, voire même le déploiement continu.

Cette accélération des développements, des livraisons et des déploiements fait porter une pression nouvelle sur les besoins en infrastructure. Évaluer l'engouement du public pour votre dernier produit est un art difficile, et y apporter une réponse avec une infrastructure en propre l'est encore plus. Aujourd'hui, une entreprise peut s'appuyer sur des fournisseurs de Cloud, spécialistes de la mise à disposition d'infrastructure et de l'élasticité matérielle. Un nouvel arrivant sur le marché qui tirerait le meilleur parti du Cloud peut, en quelques mois, fonder une plate-forme applicative capable de supporter une affluence exponentielle sans faiblir. Mais ce scénario n'est pas réservé aux entreprises naissantes. L'avantage



*Préparer
sa migration*



*Sélectionner
son offre*



*Choisir ses
technologies*

d'une startup est de ne souffrir d'aucun héritage technique à maintenir, et pourtant, avoir un historique n'exclut pas de profiter de ces nouvelles opportunités. De nombreuses entreprises font évoluer leur infrastructure pour en tirer parti. La diminution des coûts et le besoin d'externaliser certaines responsabilités poussent les entreprises vers le Cloud.

Par ailleurs, les entreprises qui possèdent déjà une infrastructure en propre lancent des réflexions pour améliorer leur outillage et leur gestion, afin de devenir aussi séduisantes qu'un Amazon Web Services auprès de leurs équipes. OpenStack (soutenu par de grands industriels de l'informatique), CloudStack ou Mesos sont autant de solutions pour «cloudifier» les data centers. Dans un contexte ultra-concurrentiel, l'innovation n'est plus un luxe, mais une nécessité. Les bâtisseurs du Cloud sont là pour tous ; les solutions qui profitent aux startups doivent également profiter aux acteurs historiques qui souhaitent évoluer. La question qui se pose aujourd'hui n'est pas de savoir si une entreprise doit migrer vers le Cloud, mais comment. Dois-je aller vers un Cloud public ? Vers un Cloud privé ? Dois-je faire évoluer ou ouvrir mon infrastructure ? Avec quelle stack technologique ? Quelles sont les implications sur mon métier et sur mes équipes ainsi que sur la partie logicielle ? Si vous vous posez au moins l'une de ces questions, bienvenue, vous êtes au bon endroit.



Préparer sa migration



Le Cloud est maintenant ancré

dans le paysage et sa progression quotidienne s'accompagne d'une complexification de l'offre : de nombreux fournisseurs, des modèles variés (public, hybride ou privé), des services à la demande pléthoriques... Ajoutez à cela les changements techniques et métiers induits, et la migration vers le Cloud peut rapidement s'apparenter à la traversée d'une jungle.

POURQUOI MIGRER ?

Passer une partie de ses services ou de son infrastructure d'un hébergement traditionnel au Cloud doit répondre à un besoin concret. Il existe de nombreuses raisons d'adopter les technologies Cloud, parmi lesquelles les plus répandues sont :

- les économies d'échelle,
- la flexibilité,
- la réduction de la durée des cycles de production,
- l'amélioration du taux de disponibilité des applications.

Une migration doit s'accompagner d'améliorations mesurables. Il ne s'agit pas de copier/coller une infrastructure vers le Cloud mais de tirer parti des avantages offerts par les solutions que vous aurez choisies. Le premier élément à déterminer est donc la liste des objectifs que vous voulez atteindre suite au portage de vos applications, services ou infrastructure vers le Cloud.

Il n'existe pas de méthode universelle garantissant le succès des projets. Les systèmes d'information sont hétérogènes ; chacun vient avec son histoire, ses méthodes de travail et ses particularités métier. Il est donc essentiel de définir votre propre chemin, qui répondra à vos attentes et s'adaptera parfaitement à vos spécificités.

Les services à la demande visent à fournir des solutions simples aux problèmes d'infrastructure. Ces offres promettent de libérer les utilisateurs des contraintes techniques en leur donnant la possibilité de se concentrer sur ce qui compte vraiment. Qu'il s'agisse d'un site d'e-commerce, d'une application interne type CRM, voire même d'un jeu en ligne, l'important, du point de vue de l'utilisateur final, est la qualité du service, son ergonomie et son adéquation au besoin. En un mot, le Cloud propose de se concentrer sur l'essentiel, à savoir le produit.

“ Il est essentiel de définir votre propre chemin, qui répondra à vos attentes et s'adaptera parfaitement à vos spécificités. ”

N'OUBLIER PERSONNE !

Le succès d'une migration dépend de nombreux facteurs. D'un point de vue organisationnel, il est essentiel d'impliquer les bonnes personnes. Le but étant de se concentrer sur le produit, les responsables métier doivent pouvoir participer activement dès la genèse d'une migration. Ils seront les garants de l'adéquation entre les réalisations finales et les besoins qu'ils auront exprimés.

Il ne s'agit pas uniquement de métier : les solutions IT nécessitent les compétences d'un grand nombre de profils. Les testeurs, les équipes de développement et les équipes de production font partie de ces acteurs incontournables. Le Cloud impose des changements dans le travail de chacun. Tout d'abord, il est important de réaliser le projet de migration de manière itérative sur des cycles courts. Pour être capable de livrer en production en suivant le rythme des itérations, les Ops aussi sont appelés à participer à l'effort en continu.

Les méthodes agiles, déjà largement établies dans le paysage, favorisent la coopération forte entre les testeurs, les développeurs et les équipes produit. C'est malheureusement insuffisant ! L'adoption de la philosophie « à la demande » du Cloud impacte toute la chaîne de production. Favorisez une approche DevOps, voire BizOps¹ pour faire naître une forte coopération du métier jusqu'à la production.

PRÉPARER L'AVENIR

À l'échelle de l'industrie informatique, les solutions d'hébergement Cloud sont jeunes. Bien que cela puisse apparaître comme un avantage dans un monde IT où les technologies évoluent rapidement, il existe un réel manque de standardisation. Chaque fournisseur adopte des paradigmes qui lui sont propres et propose des services propriétaires qui sont rarement transposables d'une offre à l'autre. Le vendor lock-in est une pratique courante, la stratégie des prestataires de Cloud consistant bien souvent, à créer une dépendance forte à leurs services.

1. Les pratiques BizOps ont pour objectif d'améliorer la rentabilité d'une entreprise via une fluidification des communications entre métier (finance, commerce, marketing, etc.) et opérationnels.



Tout d'abord, les APIs qui permettent d'interagir avec les plates-formes sont fortement hétérogènes. Pour préparer l'avenir et ne pas se retrouver dépendant d'une plate-forme spécifique à moyen terme, veillez à ne pas trop investir sur ces interfaces propriétaires. Certains outils, indépendants des fournisseurs de Cloud, intègrent nativement les APIs des principaux acteurs du marché. C'est le cas de Terraform (Hashicorp) ou de Salt-Cloud pour n'en citer que deux. Les différences entre les solutions Cloud sont fortes et ces outils ne vous masqueront pas intégralement leurs disparités. Ils permettent toutefois de mettre en place une gestion centralisée et unifiée des infrastructures qui facilitera grandement la réversibilité d'une offre à l'autre.

Les APIs ne sont pas les seuls domaines générateurs de dépendances, les services gérés peuvent rapidement devenir les clés de voûte des solutions migrées dans le Cloud. Qu'il s'agisse de bases de données gérées, de messaging, de cache ou de load-balancing, les services sont typiquement spécifiques à la plate-forme. S'ils ont l'avantage de faciliter le démarrage en évitant de se poser trop de questions, ils deviennent vite un point entravant la réversibilité.

La meilleure approche consiste à choisir des technologies standards, déjà établies sur le marché de l'IT. Cette démarche est particulièrement importante pour tout ce qui impacte les développements et les bases de données. Il faut toutefois faire la part des choses entre le coût de portage d'une offre à l'autre et le gain de productivité inhérent aux services gérés. Les load-balancers par exemple, sont aisément portables car ils ne génèrent pas de dépendance forte. Certains fournisseurs font aussi le choix de reposer sur des standards open source pour les caches et le messaging, garantissant ainsi la pérennité des plates-formes.

TRACER LA ROUTE

Définir le périmètre

Afin d'identifier les services dont vous avez besoin, il faut cartographier votre SI, connaître les flux réseau, les services de cache, de load balancing et tout autre service système. L'idée est de faire une « liste de courses » pour se concentrer sur ce qui est nécessaire. Dans une première phase, définissez le périmètre de la migration. En s'appuyant sur les besoins mentionnés précédemment, il est possible d'identifier les lignes de services qui seront

mises en place. Attention, tout le parc applicatif n'est pas candidat à la migration. Il faut prendre en compte les critères de sécurité, d'avantage concurrentiel ou simplement techniques. Par exemple, les bases de données sensibles ou les systèmes critiques connectés à des services propriétaires ne sont pas toujours éligibles à un hébergement en dehors des infrastructures privées.

Vos contraintes réglementaires, financières et administratives doivent évidemment être respectées. Les données ou services peuvent-ils être hébergés en dehors du territoire français ? Est-il possible de rapatrier ou de crypter les données stockées dans le Cloud pour en garantir la confidentialité ? Quels services applicatifs ou systèmes doivent coopérer entre ce nouvel hébergeur et l'existant ? Autant de questions auxquelles il faudra répondre pour fixer le périmètre de la migration. Cette phase de cartographie de l'existant mérite une attention toute particulière, car elle conditionne largement le succès de la migration. Au-delà d'un simple inventaire, l'objectif est de lever toute incertitude et d'éviter de tomber dans l'écueil des découvertes tardives qui pourraient remettre en question l'ensemble du projet.

Dans la seconde phase, il s'agira de dresser cette liste de services et de préparer l'architecture qui sera construite dans le Cloud.

« Comme toute migration, il ne faut pas confondre vitesse et précipitation. »

Démarrer petit, viser grand

Comme toute migration, il ne faut pas confondre vitesse et précipitation. Il est facile de se lancer dans des projets Big Bang qui tendent à englober un périmètre très large, mais il reste très difficile de les faire atterrir sans dommage. Dans le Cloud, les machines et les services ne doivent plus être considérés comme des ressources précieuses appelées à vivre à long terme. Bien au contraire, il faut les considérer comme jetables : les ressources sont destinées à être libérées puis récupérées en fonction des besoins. Ce mode de consommation est favorable à une approche itérative, mettant en avant la notion d'architecture émergente.

Il existe plusieurs approches de migration :

- big bang : migrer l'ensemble du parc applicatif d'un projet en une fois,
- copy/paste : reproduire à l'identique le parc applicatif d'un projet sur le Cloud,
- step by step : migrer les composants les uns à la suite des autres en y apportant des évolutions.

L'approche big bang est à proscrire sauf dans le cas d'une réécriture complète de l'applicatif, ce qui ne constitue finalement pas une migration. Une nouvelle fois, nous pensons que l'approche itérative est la meilleure. Le Cloud favorise la construction de petits composants qui, liés les uns aux autres, couvriront des périmètres à spectre large. Oubliez les solutions monolithiques qui reviendront à créer des ressources critiques ne tirant aucun avantage de ce nouvel hébergement. Attention, les monolithes indispensables au bon fonctionnement d'une solution sont vite des goulets d'étranglement, incompatibles avec la notion de «jetable» citée plus haut.

Si le périmètre de la migration est large, il est indispensable de définir des sous-ensembles cohérents qui pourront être réalisés par itération. Cette méthode a le double avantage de favoriser l'amélioration continue et de limiter les risques d'échec.

“ Si le périmètre de la migration est large, il est indispensable de définir des sous-ensembles cohérents qui pourront être réalisés par itération. ”

Take away Cloud



PRÉPARER SA MIGRATION

- Se poser les bonnes questions : quels bénéfices sont attendus d'une migration ? Quelles briques peut-on améliorer au passage ?
- Impliquer l'ensemble de sa chaîne de production, du métier à la production.
- Penser à la réversibilité, éviter le piège du vendor lock-in.
- Définir clairement le périmètre de la migration et avancer par itérations.

Sélectionner son offre



Vous avez identifié

votre équipe d'explorateurs des nuages, l'objectif est clair pour tout le monde, mais le chemin l'est beaucoup moins. Passons ensemble en revue le panel des solutions et fournisseurs importants à prendre en considération dans la prise d'altitude de votre infrastructure.

CLOUDS PUBLICS

Ce que l'on appelle le Cloud « public » représente un ensemble de ressources de stockage, de puissance de calcul et d'architectures réseaux, toutes pilotables au travers d'outils et d'APIs. Le terme public renvoie à l'ouverture égale des offres tant aux grandes entreprises qu'aux startups ou aux particuliers. Il s'agit là d'offres « self-service », où chaque client va consommer (et être facturé) selon ses besoins.

Les fournisseurs de solutions Cloud se distinguent des hébergeurs historiques de plusieurs façons :

- une extrême flexibilité dans la gestion de leur consommation offerte aux clients,
- une extrême rapidité de mise à disposition des ressources demandées,
- ou encore un outillage permettant de piloter ses ressources via du code.

Ces trois atouts permettent d'utiliser le Cloud pour définir des architectures web élastiques, réagissant de façon quasi organique à la montée en charge, tout en gardant un contrôle permanent sur leur état, via un monitoring efficace. Il est également possible de réaliser des expériences d'architectures de grande envergure, pour des coûts modiques, puisque tout est jetable.

C'est Amazon Web Services qui a tracé le chemin. En 2006, de son expérience en tant que plate-forme e-commerce, est née l'offre que nous connaissons aujourd'hui. Les fournisseurs de services Cloud sont plus nombreux à présent, chacun avec ses points forts et ses axes d'amélioration.

“ Ce que l'on appelle le Cloud « public » représente un ensemble de ressources de stockage, de puissance de calcul et d'architectures réseaux, toutes pilotables au travers d'outils et d'APIs. ”

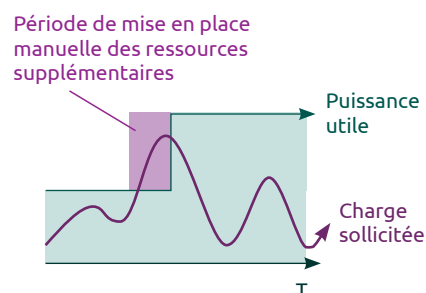
Consommation à la demande

Le premier attrait du Cloud est sa flexibilité. Pour pouvoir supporter un nombre toujours plus grand d'utilisateurs, il faut augmenter la capacité de calcul de son architecture. C'est de ce besoin de maintenir une plate-forme « à l'échelle » de l'usage qu'en font les utilisateurs, qu'est né le terme anglais « scalability ». Le terme est passé en français sous le barbarisme « scalabilité ». Pour la mettre en oeuvre, deux voies sont possibles :

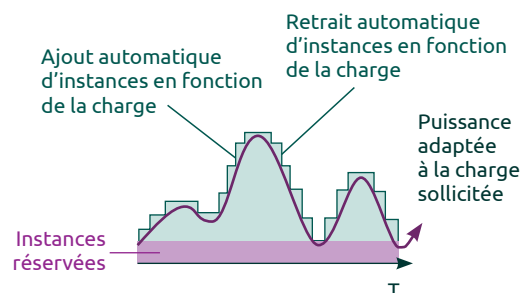
- **scalabilité verticale (scale up)** : il s'agit de changer les serveurs pour des processeurs plus performants ou avec plus de mémoire vive. Il faut toutefois noter que le plafond technique est vite atteint et que les logiciels peinent à tirer le plein parti d'un « super ordinateur ». De plus, ce genre de mise à niveau ne peut s'opérer à chaud, elle nécessite une interruption de service.
- **scalabilité horizontale (scale out)** : au lieu de mettre en place un plus gros serveur, on mise sur l'augmentation du nombre d'instances, de puissance équivalente et une répartition de la charge sur l'ensemble du groupe de machines virtuelles. Ce modèle est préférable car il permet une granularité plus fine de l'offre par rapport aux besoins de puissance. De plus, le démarrage d'une nouvelle machine et le routage d'une partie de flux réseau se font à chaud sans interruption de service.

Dans un cas comme dans l'autre, la scalabilité ne prend son sens que si vous mettez également en place des stratégies de diminution quasi immédiate des ressources consommées par l'infrastructure dans les périodes « calmes ». C'est le réglage fin de vos stratégies de scalabilité, à la hausse comme à la baisse, qui vous donne l'accès à une véritable consommation « à la demande » telle qu'elle est promise par le Cloud.

ON-PREMISE



INFRASTRUCTURE CLOUD



Ressources figées vs Élasticité

Cette scalabilité automatique (ou élasticité) est rendue possible grâce à l'outillage d'APIs et de SDKs apporté par le fournisseur Cloud. Le monitoring d'une plate-forme, couplé à une utilisation intelligente de ces outils, permet de créer des « comportements » pour votre infrastructure :

- allocations de ressources à l'avance, en prévision d'un événement particulier (ventes de Noël, fin de période comptable, etc.),
- scalabilité automatique en fonction de métriques d'usages de ressources : mémoire, processeurs, bande passante, nombre de connexions en cours.

Cette flexibilité technique apporte des bénéfices directs à la dimension financière de vos projets. En plus d'avoir une infrastructure dont le coût est en adéquation avec votre volume d'activité, les coûts glissent de la notion de CAPEX au profit de l'OPEX². Cette nouvelle répartition vous permettra ainsi de tirer bénéfice des trois points suivants :

- une réduction des besoins de financement puisque vous ne serez plus concernés par les coûts parfois exorbitants d'acquisition du matériel,
- une réduction des coûts d'exploitation car vous ne paierez qu'en fonction de la charge et par conséquent de votre consommation,
- une réduction des risques financiers et techniques car vous n'avez pas d'engagement avec le fournisseur (Pay-as-you-go), si bien sûr votre architecture n'est pas fortement couplée aux spécificités de votre fournisseur.

Le TCO, pour « Total Cost of Ownership » (coût total de possession), se calcule en additionnant le prix de tous les éléments qui composent votre infrastructure technique : salle blanche, serveurs, routeurs, électricité, etc. Il faut également additionner les salaires des équipes Ops ainsi que les diverses licences nécessaires pour la virtualisation. Lorsque vous migrez vers un opérateur Cloud, il est plus complexe de faire ce calcul, stratégique pour une entreprise. Sachez que les opérateurs mettent à disposition des outils pour simuler le TCO espéré chez eux, par rapport au TCO actuel de votre infrastructure. Par exemple, vous pouvez calculer le TCO de votre infrastructure chez AWS via l'outil awstccalculator, certifié par une société tierce. Vous aurez ainsi un coût comparatif entre la version on-premise de votre infrastructure et son équivalent Cloud.

2. Les dépenses d'exploitation (OPEX) sont les coûts courants pour exploiter un produit, une entreprise, ou un système. Les dépenses d'investissement de capital (CAPEX), se réfèrent aux coûts de développement ou de fourniture des pièces non-consommables pour le produit ou le système.

Impact organisationnel

Avec la délégation à un fournisseur externe, certaines tâches habituelles de maintenance et d'achats vont être bousculées. C'est pourquoi il est essentiel que l'accompagnement de votre migration technique se fasse de concert avec la redéfinition de ces activités. Cela passera par une montée en compétences des équipes concernées. Les nouvelles activités des Ops seront clairement tournées vers l'orchestration de l'infrastructure :

- la gestion des droits d'accès des développeurs : il faut que chacun ait accès aux ressources nécessaires tout en garantissant l'isolation entre les environnements,
- l'amélioration continue du monitoring et des indicateurs de l'activité de la plate-forme : cela est crucial pour permettre l'optimisation technique et financière.

Pour jouir de toute la souplesse de fonctionnement offerte par le Cloud, il est essentiel de revoir le fonctionnement de certaines procédures internes. Par exemple, inscrivez-vous au plus proche des pratiques BizOps pour tendre vers une communication fluide entre les équipes métiers et les opérationnels en charge de la plate-forme.

Résilience, sécurité et confidentialité

En général, on peut dire sans hésiter que la sécurisation de votre infrastructure chez un fournisseur Cloud est équivalente voire meilleure que celle de votre propre data center. Tous ou presque proposent différentes zones de déploiement, réparties sur le globe, qui permettent de réaliser une architecture hautement disponible et tolérante à la panne. De plus, beaucoup de concepts intrinsèques à la nature des hébergements Cloud apportent une meilleure sécurité que dans un hébergement standard :

- la virtualisation du réseau permet une meilleure séparation et isolation des environnements. La création d'un réseau isolé, dédié pour un projet est une opération triviale chez un opérateur Cloud ;
- le chiffrement des fichiers est aussi une action rapide lorsque l'on met en place des entrepôts de données chez un opérateur dès lors qu'il est configuré dès le début du projet ;
- l'interface de pilotage de votre infrastructure est hautement sécurisée. Si nous prenons l'exemple d'AWS, vous avez la possibilité d'activer le MFA (Multi Factor Authentication) qui sera lié à des périphériques virtuels tels que des smartphones, ou bien physiques de type SecurID RSA Tokens ;



ON-PREMISE



IaaS



PaaS



SaaS

Mon infra dans la vraie vie : à table !

- toute la plate-forme est par défaut monitorée, ce qui vous permet d’avoir une vision unifiée de votre activité. Notez bien que ce monitoring est tout aussi valable pour l’activité technique que pour la consommation de votre budget. Vous pouvez être alerté lorsque la consommation augmente subitement ;
- les fournisseurs Cloud possèdent leur propre outillage et vous alertent de manière proactive lorsqu’ils détectent une activité anormale (publication de clé de sécurité sur GitHub, activité en dehors de votre zone géographique habituelle, etc.).

De plus, les data centers sont régulièrement audités en terme de sécurité d’accès physique aux installations. Tous les fournisseurs montrent patte blanche sur ce sujet puisqu’il en va de leur crédibilité. Vous trouverez sans difficulté une multitude de labels sécurité dans les documentations légales de leur site vitrine.

Concernant la confidentialité, la question est de connaître la juridiction qui s’applique en fonction du fournisseur. La loi stipule que le pays d’origine du fournisseur prévaut sur l’emplacement du data center. Si celui-ci est en France et que votre fournisseur possède son siège aux États-Unis alors vous serez sujet aux lois de ce pays et notamment au fameux Patriot Act. Sans entrer dans les détails de chaque loi, il est indispensable de connaître les trois suivantes :

- **Freedom Act** : évolution du Patriot Act depuis le 1er juin 2015, celui-ci est maintenant moins intrusif que son prédécesseur.
- **Directive européenne 95/46/EC** : cadre légal signé par certains fournisseurs Cloud entre les États-Unis, l’Europe et la Suisse qui permet de protéger l’utilisateur, notamment sur la transmission des données.
- **Loi sur le renseignement** : elle octroie de plus grands pouvoirs d’investigation aux services de renseignement français. Bien que votée courant 2015, le périmètre exact de cette loi est toujours flou.

Mais alors, puis-je migrer mes données sensibles dans le Cloud ? La réponse est positive dans la majorité des cas puisqu’elles seront très certainement davantage sécurisées qu’elles ne le sont à leur emplacement actuel. Il suffit d’observer les services de chiffrement, de disponibilité et de durabilité (99,999999999%) offerts par un acteur tel qu’Amazon Web Services à travers la solution S3. La vraie question se trouve au niveau de votre positionnement stratégique et commercial. Par exemple, si vous êtes un acteur important dans le secteur de la vente en ligne de livres, alors vous n’aurez pas forcément envie d’être hébergé par un de vos concurrents.

Les principaux acteurs

Passons maintenant en revue les fournisseurs à considérer pour faire décoller votre infrastructure vers les nuages.



Après le démarrage d’une première version bêta en 2006, l’offre est ouverte au public depuis 2008. Initiée avec un IaaS seul, elle s’est ensuite étoffée avec une série de services managés, tels que la base de données RDS ou encore les serveurs applicatifs Elastic Beanstalk. Aujourd’hui, AWS possède toujours une avance importante sur ses concurrents. Les analystes ont déterminé qu’Amazon possède aujourd’hui, à lui seul, 10 fois la puissance des 14 autres fournisseurs réunis. Ces ressources gigantesques prennent place dans des data centers qui couvrent l’ensemble des régions du globe.

+	-
<ul style="list-style-type: none"> • Une offre IaaS/PaaS très complète • Une très bonne couverture et puissance des data centers • De nombreux types d’instances 	<ul style="list-style-type: none"> • Soumis aux lois américaines



La plate-forme Microsoft Azure, initialement appelée Windows Azure a été annoncée en 2008 pour une mise à disposition commerciale en 2010. Dans un premier temps, Azure était focalisé à 100% sur l’offre PaaS, correspondant à sa culture intrinsèque d’éditeur logiciel. Après l’arrivée de Satya Nadella, l’offre s’est étoffée avec des solutions IaaS afin d’être au plus proche des problématiques de migration des entreprises. Azure devient un concurrent direct d’AWS de par son offre et sa reconnaissance dans le milieu professionnel via de nombreuses références. Sa plate-forme est par ailleurs disponible en 16 langues, dont le français.

+	-
<ul style="list-style-type: none"> • Une tarification à l’heure • Pay-as-you-go • Une offre IaaS/PaaS/SaaS très complète • De nombreux types d’instances 	<ul style="list-style-type: none"> • Soumis aux lois américaines



Pour répondre à ses propres besoins techniques, Google a depuis longtemps développé en interne ses solutions Cloud. Le géant américain commercialise ses services sous la forme d'offre publique depuis 2008 avec le PaaS AppEngine. La plate-forme Google Cloud s'est étoffée au fil des ans avec Storage et BigQuery, pour finir par l'ouverture tardive de Compute Engine en 2012. Le développement de cette offre est hautement stratégique pour le moteur de recherche qui affiche la volonté de migrer l'ensemble de son infrastructure vers GCP. Google est un challenger d'AWS, avec pour objectif d'être le plus performant et ce au meilleur prix. Dans le Cloud Google, vous bénéficiez de l'infrastructure complète du moteur de recherche avec son réseau privé mondial et sa présence sous forme de point d'accès dans la plupart des pays.

+	-
<ul style="list-style-type: none"> • Une tarification à la minute • Une très bonne couverture des data centers • La performance du service 	<ul style="list-style-type: none"> • Soumis aux lois américaines • Obligation d'avoir, par compte, un email sur un domaine géré par Google



Suite à la volonté de l'état français de voir la création d'un acteur de Cloud souverain, ce sont finalement 2 fournisseurs qui ont vu le jour, Numergy et Cloudwatt. Numergy compte 3 actionnaires (SFR, Bull - racheté par Atos depuis - et la Caisse des Dépôts et Consignations) et propose principalement des offres IaaS en s'appuyant sur un réseau de revendeurs pour leur commercialisation.

Initialement construite sur la plate-forme VMware, Numergy s'appuie depuis l'été 2014 sur OpenStack, et est, par ailleurs, devenu Sponsor Corporate de ce projet.

+	-
<ul style="list-style-type: none"> • Acteur français • L'écosystème OpenStack • De multiples niveaux de certifications sécurité et agrément hébergeur de données de santé 	<ul style="list-style-type: none"> • Un manque de références • Une offre de services encore peu étoffée • Pas de data center à l'étranger



Dans le même élan de l'état français, Cloudwatt a été fondé en septembre 2012 par Orange, Thalès et la Caisse des Dépôts et Consignations. Depuis mars 2015, Orange détient 100% du capital de Cloudwatt. L'une de ses particularités est d'avoir fait le choix de la plate-forme communautaire OpenStack dès son démarrage, afin de pouvoir garantir à ses clients une indépendance technologique et une certaine réversibilité. C'est le fournisseur choisi par l'état français pour les besoins Cloud des ministères.

Aujourd'hui, Cloudwatt est pleinement intégré à l'écosystème professionnel du projet OpenStack. Ils sont Corporate Sponsor, contribuent à l'amélioration du projet et participent à la vie de la communauté. Depuis peu, Cloudwatt propose un ensemble de stacks applicatives One-Clic permettant un démarrage très rapide.

+	-
<ul style="list-style-type: none"> • Acteur français • Une tarification à la minute • L'écosystème OpenStack • Une stack applicative one-clic 	<ul style="list-style-type: none"> • Un data center unique (le 2^e est prévu pour début 2016) • Une offre de services encore peu étoffée



Outscale est une initiative privée qui se démarque de ce fait de ses concurrents Cloudwatt et Numergy. Dassault Systèmes, qui en est à l'origine, le soutient depuis 2010.

Outscale se différencie aussi par son offre dite « multi-souveraine », avec des infrastructures se répartissant sur 3 continents.

Autre facteur différenciant, sur le plan technologique cette fois, Outscale a développé sa propre plate-forme, baptisée TinaOS s'appuyant sur Linux et KVM. La compatibilité de ses APIs avec AWS permet aussi à ses clients de pouvoir basculer « facilement » chez le géant américain.

+	-
<ul style="list-style-type: none"> • De nombreuses références, notamment grâce à Dassault • Des data centers sur 3 continents • La compatibilité avec AWS 	<ul style="list-style-type: none"> • Une offre de services encore peu étoffée • Uniquement sur du IaaS pour le moment



Avec ses 300 000 clients répartis dans 120 pays, Rackspace fait partie du peloton de tête des fournisseurs Cloud d'envergure planétaire. Avec la Nasa, ils sont à l'origine de la création d'OpenStack, solution open source leader à ce jour. Ils sont connus pour la qualité de leur support et se distinguent par une garantie d'accès à leur service de 100%. Rackspace est à la fois fournisseur de Cloud, hébergeur classique sur serveurs dédiés et fournisseur de services pour monter votre Cloud privé dans vos data centers. Il est donc bien placé pour être un interlocuteur unique dans une approche d'hybridation d'infrastructures classiques avec du Cloud.

+	-
<ul style="list-style-type: none">• La qualité du support• La plate-forme multilingue• La performance de son CDN (partenaire Akamai)	<ul style="list-style-type: none">• Les prix plus élevés que la concurrence• Le nombre et la répartition des data centers

Grille de choix

Voici un ensemble de critères notés pour les fournisseurs que nous venons de passer en revue. Ils sont choisis d'un point de vue extérieur, à vous de l'adapter à votre vision des choses en pondérant ces « notes » par un coefficient d'importance de chaque critère.

	AWS	Azure	GCP	Numergy	Cloudwatt	Outscale	Rackspace
Maturité	+++	++	++	+	+	++	++
Outils	+++	++	++	++	++	+	++
Services	+++	+++	++	+	++	+	++
Data centers	+++	+++	+++	+	+	++	++
Licences	+++	+++	++	++	++	+	+
Supervision	+++	++	++	++	++	+	++
Support	++	+++	++	+	+	+	+++

- Les aspects déterminants de votre choix sont :
- **la maturité** : le fournisseur doit avoir des références en production depuis au moins deux ans. Se tourner vers un jeune fournisseur devra se justifier par une offre qui n'existe pas chez la concurrence ;
 - **les outils** : pour pouvoir tirer parti de la plate-forme, vous devez disposer d'une API et de SDKs. Si le fournisseur ne dispose que d'une interface web alors écarter-le de votre sélection sans hésiter ;
 - **les services** : la disponibilité de solutions sur étagères est aussi un point important. Les services gérés vont dans le sens de l'externalisation de responsabilité et permettent de vous focaliser sur votre métier ;
 - **les data centers** : renseignez-vous sur le nombre de régions qui sont couvertes par ses services. Une bonne distribution des data centers permettra de créer une architecture tolérante à la panne et de meilleurs temps de latence ;
 - **les licences** : vérifiez la capacité à héberger les licences de vos produits. Il faut étudier au cas par cas et consulter les éditeurs pour valider la compatibilité avec un hébergement Cloud ;
 - **la supervision** : la fenêtre sur votre infrastructure dans le Cloud devra être propre et la plus large possible. Les outils de monitoring doivent vous permettre d'avoir une vision parfaite de l'activité technique et économique ;
 - **le support/l'accompagnement** : comme chaque migration est unique, il est préférable de pouvoir se faire accompagner pour la préparer et avoir de l'aide en cas de grain de sable dans les rouages.

CLOUDS PRIVÉS

Frontières et motivations

Commençons notre immersion dans le monde des Clouds privés par une précision sémantique. De nombreux fournisseurs Cloud ont dans leur catalogue une offre de Cloud « privé ». Ces offres ne sont pas à notre sens des Clouds privés, mais plutôt des VPCs (Virtual Private Cloud). Il s'agit d'isolation réseau et de réservation de capacité. De notre point de vue, les VPCs doivent plus être vus comme des offres de virtualisation avancée. Il est trivial de monter un VPC au sein d'un Cloud public et certains fournisseurs catégorisés « publics » comme AWS, l'ont également au catalogue. Pour la suite de votre lecture, gardez donc à l'esprit que le terme « Cloud privé » désigne des solutions à mettre en place et maintenir en interne, dans vos infrastructures propres, par vos équipes.

Il est courant d'entendre « pourquoi monter un Cloud privé ? J'ai déjà tout virtualisé, c'est pareil... ». Il ne faut pas confondre virtualisation et Cloud privé. La principale différence réside dans la façon de mettre à disposition les ressources d'infrastructure. La philosophie Cloud se caractérise par une approche orientée « as a Service ». Dans le monde de la virtualisation, les développeurs formulent toujours des demandes aux services en charge de l'infrastructure pour obtenir des ressources, bien souvent via un système de ticketing. Dans une approche Cloud privé, ils peuvent « se servir ». Cette inversion de paradigme réduit fortement les frictions et accélère les projets. Vos équipes d'infra deviennent les « gardiens du temple » de votre infrastructure. Ils ont en charge de maintenir la plate-forme et de garantir la disponibilité des ressources aux équipes projet.

Si vous possédez déjà une infrastructure existante relativement conséquente, le choix de bâtir votre Cloud privé fait sens. Au delà d'une certaine masse critique, gérer vos serveurs de façon unitaire manuellement peut ressembler à la punition de Sisyphe. L'ajout d'une solution logicielle de type Cloud privé apportera plus de flexibilité à votre infrastructure et plus de réactivité à vos équipes.

Le plus gros piège de l'usage des Clouds publics est le vendor lock-in. Pour le Cloud privé, le piège est identique. Si l'on cède aux sirènes commerciales des éditeurs, on se retrouve alors lié à leurs solutions et leurs experts pour un bon nombre d'années. Certaines solutions éditeurs de Clouds privés viennent également avec du hardware dédié ; ajouter du matériel est rarement une bonne initiative quand on cherche à optimiser l'existant. Heureusement, le monde du logiciel open source est là pour nous. Comme dans toutes les bonnes offres, il y a du choix. Pour y voir plus clair, suivez le guide...



Le favori : OpenStack

Le projet OpenStack, démarré en 2005, est clairement le grand leader des solutions de Cloud open source. Il sert aussi bien en Cloud privé (150 000 coeurs CPUs gérés par OpenStack chez Walmart) qu'en Cloud public (RackSpace ou Cloudwatt en sont des exemples). Ce projet est piloté par la fondation OpenStack, qui gère les cycles de livraison, fédère les Users Groups à travers la planète et fait la promotion du projet auprès des communautés techniques et des utilisateurs finaux. La fondation regroupe les différentes entreprises du marché qui s'investissent dans le développement d'OpenStack. Parmi le top 10 des entreprises contributrices de code, on retrouve des noms tels que HP, RedHat, Rackspace, IBM, VMware, Cisco Systems et Intel. La communauté, de plus de 30 000 développeurs, est très vivante et des Users Groups s'organisent en permanence sur tous les continents.

OpenStack est donc en passe de devenir le standard de-facto des solutions Cloud Open Source. Le rayonnement de la fondation et l'énergie de sa communauté apportent un grand choix de formations, de prestataires et de techniciens compétents sur lesquels s'appuyer pour pouvoir rapidement installer et mettre à flot votre propre Cloud privé OpenStack.

OpenStack prend en charge les hyperviseurs KVM, LXC, VMware ESX/ESXi, Xen, PowerVM et Hyper-V.



Le challenger : CloudStack

En face du mastodonte qu'est OpenStack, un autre projet, géré par la fondation Apache, garde la tête haute : CloudStack, issu de la société Cloud.com, rachetée par Citrix en 2011, qui voyait dans leur solution technique une base de travail plus stable que celle du projet OpenStack.

En 2012, Citrix cède le code à la fondation Apache et le projet CloudStack naît. La fondation Apache est orientée vers les contributions personnelles plutôt que vers la mise en avant d'entreprises marraines. Pour cette raison, il est plus difficile de rassembler une liste d'entreprises contributrices. Pourtant, Brocade, Cisco Systems, Juniper Networks, Basho Technologies, Cloudsoft, PuppetLabs ou encore SwiftStack ont des développeurs à temps plein sur le développement de CloudStack.

Quand CloudStack s'est ouvert aux contributions externes, OpenStack avait déjà atteint l'âge de raison et fédérait une grosse communauté. C'est certainement ce qui explique que la communauté soit moins pléthorique que chez le favori. Malgré cela, de nombreuses entreprises lancent leur Cloud privé grâce à ce projet, qui n'est pas prêt de disparaître.

CloudStack prend en charge les hyperviseurs KVM, vSphere et Citrix XenServer.

Au fil des versions livrées, OpenStack et CloudStack occupent chacun à leur tour le haut du pavé sur un aspect ou un autre : performance brute, support du stockage, flexibilité, etc. Même si leur roadmap et leur vision diffèrent légèrement, ce sont bien deux projets de qualité équivalente, qui avancent en parallèle.



L'outsider : Mesos

Le projet Mesos, lui aussi issu de la fondation Apache, est né à Berkeley et a grandi chez Twitter, Airbnb, eBay et Cloudera. Mesos est une solution de mise en commun de ressources (CPU, stockage, réseau), qui se place à un niveau plus élevé qu'OpenStack et CloudStack. Il tourne sur des systèmes Linux, qu'il s'agisse indifféremment de machines physiques ou virtuelles. Il permet donc de faire un Cloud aussi bien sur des serveurs classiques que sur des hyperviseurs, voire même sur les deux à la fois.

Mesos offre une approche « conteneur » depuis ses débuts, avec un format qui lui est propre. Depuis quelques versions, il supporte également le déploiement de conteneurs Docker. La légèreté des conteneurs Docker alliée à la robustesse de Mesos est une combinaison détonante qui pourrait bien faire de l'ombre à ses aînés.

Même si la communauté de curieux, utilisateurs et contributeurs, grossit très vite, l'écosystème de Mesos manque encore d'outils mûrs pour répondre à certaines problématiques telles que le stockage distribué. La société Mesosphere s'est donnée comme mission de combler les manques de cet écosystème. Fin 2014, Docker annonce son partenariat avec Mesosphere et fait confiance à Mesos pour propulser Docker sur des architectures à grande échelle. Les premières versions du projet DCOS (Data Center Operating System) de Mesosphere laissent penser que leur suite d'outils pourrait bien se frayer une place rapidement auprès d'un panel plus large d'entreprises.

Une autre voie

L'objectif d'une stratégie Cloud privé est de pouvoir répartir la puissance de calcul et de stockage d'un parc de machines entre différentes briques applicatives, de façon flexible. Il est envisageable de passer par des solutions Platform as a Service pour atteindre ce but. Des projets comme Cloud Foundry de chez Pivotal ou Stratos de la fondation Apache permettent d'installer directement une solution PaaS open source. Ainsi, la gestion des ressources de votre parc physique ne se placera plus au niveau de l'instanciation de sys-

tèmes complets, mais au niveau du déploiement de vos projets. Selon le type de vos applications, cela peut représenter une surcharge de travail pour réussir à les faire rentrer dans un cadre compatible avec le PaaS choisi, mais c'est malgré tout une option à considérer dans votre réflexion stratégique. Nous reviendrons sur ce sujet plus avant dans ce document.

Adopter n'est pas jouer

Maintenant que nous avons un meilleur aperçu du territoire et des forces en présence, il faut se poser les bonnes questions pour savoir où se placer et tirer le meilleur parti de l'effervescence du monde de l'open source autour du Cloud. Comme nous l'avons précisé dans la première partie, il est important d'impliquer toutes les parties prenantes. Vos équipes techniques ont certainement un avis éclairé sur les choix à faire concernant votre Cloud privé, pensez à les intégrer dans les débats. En premier lieu, faites l'inventaire de votre existant et déterminez sur quelle partie vous comptez appuyer votre Cloud privé. Les contraintes matérielles permettent d'élaguer rapidement certaines options.

Demandez également à vos équipes techniques quelle solution a leur préférence. Une fois en place, votre Cloud privé doit pouvoir vivre et être maintenu pendant plusieurs années. Il faudra pour cela que vos techniciens aient adopté les outils et leur philosophie. De plus, si vous voulez éviter que votre choix technique tombe en poussière par manque de contributions dans les années qui suivent, il faudra investir de l'énergie dans la communauté. Le monde de l'open source professionnel ne peut se constituer uniquement de consommateurs. Sur des composants de cette importance stratégique, il est vital de structurer un véritable plan de participation au projet que vous adoptez. Faire vivre la communauté assure le renouvellement des profils compétents au fil des années. Outre d'éventuels contrats de support auprès de prestataires spécialisés, l'intégration de la communauté est le véritable support de l'open source. Plus vous contribuerez à faire vivre le projet, plus l'intégralité de la communauté sera rapide et dévouée à vous aider lors de besoins futurs.

il est vital de structurer un véritable plan de participation au projet que vous adoptez.

Take away Cloud



SÉLECTIONNER SON OFFRE

- *Élaguer l'arbre de décision en comparant son existant et ses besoins avec les capacités des solutions disponibles.*
- *Réaliser un micro-projet sur chacune des options restantes et mener des rétrospectives pour capitaliser au mieux sur ces expérimentations.*
- *Échanger avec les Users Groups et autres Meetups afin de prendre position en se nourrissant des expériences menées.*
- *Évangéliser : trouver la voie royale d'usage de sa solution Cloud et former toutes les parties prenantes dans le même sens.*

Choisir ses technologies



Quel que soit votre choix

de plate-forme, publique, privée ou un savant mélange, il vous faut pouvoir piloter votre nouvelle infrastructure. Le passage au Cloud est l'occasion d'adopter de nouvelles méthodes et de nouveaux outils pour être plus rapide, plus résilient et maximiser le retour sur l'investissement conséquent qu'est une migration de cette ampleur.

INFRA AS CODE

Que vous ayez fait le choix d'une solution Cloud public ou privé, il faut maintenant l'exploiter efficacement. Chaque plate-forme possède une interface de pilotage Web permettant de créer votre infrastructure. Ne vous y trompez pas : ce n'est là que la partie émergée de l'iceberg, surtout destinée à démontrer les fonctionnalités de l'outil de façon très visuelle. Le véritable intérêt technique des solutions Cloud est l'utilisation d'outils (donc de code) pour gérer son infrastructure. C'est de là que vient le terme « infra as code ».

Dans une approche infra as code, l'intégralité de votre architecture doit être décrite dans un langage destiné à être interprété par une machine. Cette étape de cartographie est indispensable pour pouvoir versionner votre infra et la rendre reproductible. Une fois atteint ce jalon technique, vous pourrez, à volonté, démarrer des environnements complets, réellement iso-production.

Entrent ensuite en scène les outils de provisionning applicatif (ou de gestion de configuration). Ils sont dans le panorama de l'industrie informatique depuis longtemps, la première version du projet CFEngine remontant à 1993. La mouvance DevOps, même si elle prône des changements organisationnels plus que techniques, a donné naissance à une famille d'outils devenus indispensables : Puppet, Chef, Ansible et SaltStack notamment. Tous ces outils ont le même objectif : automatiser et maintenir la configuration d'un serveur, en se basant sur son rôle dans la cartographie de votre parc.

Ces outils permettent de limiter les erreurs manuelles lors d'un déploiement et de diminuer drastiquement le temps nécessaire à la mise en condition opérationnelle d'un serveur. On passe ainsi de quelques heures pour un déploiement manuel à quelques minutes (voire secondes !) dans sa version automatisée. Il est également possible de lancer la même procédure sur de nombreuses machines en parallèle.

Comme ces outils décrivent l'état dans lequel doit être un serveur (et non les actions à faire pour amener un serveur d'un état A à un état B comme dans le cas d'un script shell), ils permettent également de limiter la dérive des configurations au fil du temps.



Le véritable intérêt technique des solutions Cloud est l'utilisation d'outils (donc de code) pour gérer son infrastructure. C'est de là que vient le terme « infra as code ».



Ces outils étant indépendants des fournisseurs de Cloud, il n'est pas nécessaire de ré-écrire le code en cas de changement de fournisseur.

L'utilisation d'un outil de type infra as code permet de reconstruire son infrastructure à partir de zéro rapidement et de la maintenir au fil du temps. Elle assure également une plus grande maintenabilité via des tests automatiques, une plus grande lisibilité via un langage standard et une scalabilité permettant de déployer de nombreuses machines en parallèle.

Toutes les solutions Cloud s'appuient sur des images de serveurs, de la même façon que les systèmes de virtualisation plus connus. Il faut donc, non seulement décrire la topologie de votre parc, mais également préparer ces images de serveurs déployables.

Provisionnement à la volée

Cette méthode consiste à démarrer une image de système minimal et décrire ce que vous souhaitez voir installé dessus, en fonction de sa place et de son rôle dans votre parc. La préparation effective du serveur, de l'installation des paquets système à la configuration finale, est déléguée à l'outil de provisioning que vous aurez choisi. Chacun bénéficie d'une communauté active et d'une entreprise offrant du support. Afin de vous aider à choisir, voici un tableau comportant quelques éléments différenciants :

	Fonctionnement	Support Windows	Support Linux
Puppet	serveur maître + agents ou agents seuls	++	+++
Chef	serveur maître + agents	+	+++
Ansible	serveur maître sans agent (SSH)	++	+++
SaltStack	serveur maître + agents ou agents seuls	++	+++

Infrastructure immuable

Il est des cas d'usages où le provisionning à la volée atteint ses limites. Certaines plates-formes logicielles prennent un temps certain pour s'installer. Dans le cas de machines destinées à des groupes de scalabilité automatique, il serait fâcheux de laisser votre outil de gestion de configuration prendre vingt minutes pour assembler un frontal Web complexe. Le temps de l'assemblage du serveur, le pic de charge peut être déjà passé.

Construire un catalogue d'images pré-provisionnées par votre outil de gestion de configuration est alors une solution à envisager. Des outils comme VMBuilder, Weevee, ImageFactory et Packer vous aideront à gérer le cycle de vie de vos images. Même si cette technique oblige à assurer une plus grande capacité de stockage et un versionnage rigoureux de la bibliothèque d'images, elle présente un réel intérêt opérationnel.

Testabilité

Tout comme n'importe quel code, celui-ci peut (et doit) être testé avant son utilisation en production. Votre architecture est maintenant un livrable versionnable. Le code d'infrastructure devra passer par des environnements de validation afin d'assurer l'absence de régression avant de pousser une modification en production. La reproductibilité de l'architecture permet de détecter au plus tôt des problèmes techniques qui, auparavant, seraient survenus en production.

DOCKER ET SON ÉCOSYSTÈME

La migration vers le Cloud s'accompagne bien souvent de deux questions essentielles : quel packaging utiliser pour livrer les applications ? Comment minimiser l'effort nécessaire à la réversion des solutions ? Docker fournit une réponse simple en définissant un format de packaging et d'exécution utilisable dans tous les environnements Cloud.

Docker est une solution de virtualisation légère fonctionnant sur Linux. Elle est développée par la société éponyme depuis 2012. La technologie Docker permet de packager une application dans ce que l'on appelle un conteneur. À la différence des solutions de virtualisation classiques, un conteneur utilise directement le noyau de la machine hôte. L'isolation est alors garantie non par un hyperviseur, mais directement par les fonctionnalités offertes par le noyau.

Un conteneur Docker contient à la fois l'applicatif et le middleware nécessaire à son fonctionnement. Par exemple, dans le cas d'une application JEE classique, il contiendra à la fois un fichier war, le serveur d'application et la machine virtuelle Java. L'idée est donc de créer un paquet cohérent embarquant l'ensemble des

outils nécessaires à l'exécution de l'application. Le conteneur devient alors le nouveau format unique de livraison pour chacun des composants de la solution.

Qu'il s'agisse de l'environnement de développement, de recette ou de production, l'exécution du conteneur garantit un fonctionnement identique de l'application livrée. L'application, la configuration et le middleware seront toujours les mêmes, tout en bénéficiant des ressources supplémentaires offertes par les environnements s'échelonnant du développement à la production. Si l'on fait l'impasse sur les capacités matérielles, Docker permet de construire des environnements iso-production à chaque niveau.

Les avantages des solutions orientées conteneurs sont nombreux. Au-delà des livraisons garanties identiques d'une machine à une autre, Docker enrichit la sécurité des systèmes en isolant les processus et permet de s'abstraire définitivement de l'infrastructure. Tous ces avantages ne viennent pas sans contrepartie. Il reste aujourd'hui trois points difficiles à adresser pour bâtir des solutions complètes avec Docker :

- la communication réseau entre les conteneurs,
- la gestion du stockage sur disque,
- la mise en cluster d'un ensemble de conteneurs.

Pour adresser ces nouvelles problématiques, une véritable galaxie de projets s'est développée autour de Docker. Tous ces outils visent à faciliter autant la vie des développeurs que celle des opérationnels. Depuis un an, l'engouement autour du projet est tel que les fournisseurs de Cloud l'ont adopté unanimement. Tant et si bien qu'une offre de Cloud sans support Docker fait aujourd'hui figure d'exception.

Les solutions Docker

La société Docker développe maintenant un ensemble d'outils visant à simplifier la création de solutions complexes à base de conteneurs.

- **Docker Compose** permet de décrire à travers un fichier YAML³ un ensemble de conteneurs constituant l'ensemble des composants d'une application (base de données, serveur web, serveur d'application, etc.). Ce fichier peut ensuite être utilisé pour lancer l'application sur un cluster.
- **Docker Machine** permet d'installer et de configurer automatiquement Docker et Swarm sur un système fraîchement installé.
- **Docker Swarm** est l'outil d'orchestration des clusters Docker. Il choisit en

fonction des ressources disponibles sur chaque serveur et des différentes contraintes que vous allez exprimer (type de disque dur, cpu, mémoire, etc.), celui qui sera le plus approprié pour déployer votre conteneur.

Les solutions CoreOS

CoreOS est une distribution Linux basée sur ChromeOS et conçue spécifiquement pour gérer des conteneurs. Cette distribution se démarque des autres par sa légèreté. En effet, elle ne possède pas de gestionnaire de paquets. La seule fonctionnalité offerte par cette distribution est l'exécution de conteneurs. CoreOS est livrée avec trois outils qui lui permettent d'en faciliter la gestion :

- **Etcd** est une base de données de type clef/valeur distribuée. Elle est installée sur chacun des nœuds du cluster CoreOS. Elle peut être utilisée par les conteneurs pour gérer de la configuration, mais elle est aussi utilisée par CoreOS pour stocker l'état du cluster et propager l'état des différents conteneurs.
- **Fleet** est pensé comme une surcouche à Systemd, le mécanisme d'initialisation de nombreuses distributions Linux. Il permet à la fois de gérer le lancement des conteneurs, mais aussi de renseigner etcd sur les nouveaux conteneurs sur le réseau.
- **Flannel** permet à deux conteneurs situés sur deux machines hôtes différentes de communiquer comme s'ils étaient sur le même réseau. Chaque conteneur dispose de sa propre adresse IP et le Daemon⁴ s'occupe de ré-écrire les trames réseau afin de router les paquets en direction du bon conteneur. Il repose sur la base de données etcd pour connaître la topologie réseau de chaque serveur.

Les solutions tierces

- **Weave** est une alternative à Flannel conçue par la société Weaveworks. Il permet de créer un réseau virtuel entre les différents hôtes du cluster. Weave propose également la possibilité d'encrypter l'ensemble des trames réseau échangées entre les différents conteneurs.
- **Flocker** : Docker peut stocker des données en dehors du conteneur, en s'appuyant sur la notion de volume. Cependant, en cas de migration de votre conteneur sur un hôte différent, il faut également migrer les volumes qu'il utilise. Flocker permet de lier les volumes à un conteneur, et donc de les déplacer en même temps que celui-ci. Il fonctionne avec différents systèmes de stockage dont AWS EBS, Rackspace ou EMC ScaleIO.

3- YAML : YAML Ain't Markup Language, format de représentation de données, moins verbeux que JSON ou XML

4- Daemon : type de programme s'exécutant en arrière-plan



PLATFORM AS A SERVICE

Platform as a Service (plus communément appelé PaaS) est une catégorie de services Cloud. Les PaaS fournissent la plate-forme applicative qui se charge de configurer et d'exécuter l'ensemble des services nécessaires au bon fonctionnement d'une application. La promesse des PaaS est donc de n'avoir plus qu'à livrer une base de code ou un ensemble de conteneurs pouvant faire appel à des services gérés. Outre la base de code proprement dite, les équipes devront fournir des paramètres pour indiquer les middlewares et autres produits consommés par l'application.

Ces plates-formes apparues en 2008 avec la sortie de Google App Engine, supportent nativement la scalabilité horizontale. Les ressources allouées pour l'exécution des applications sont adaptées en fonction de la charge. Un site web hébergé dans un PaaS est donc entièrement infogéré par l'hébergeur s'il s'agit de Cloud public.

Les solutions PaaS se sont construites en ciblant principalement les développeurs. Leur objectif est tout simplement de n'avoir à se concentrer que sur le développement en éliminant les distractions liées à la gestion du système sous-jacent. Elles fournissent des interfaces de haut niveau pour superviser et administrer les applications. Quelques minutes suffisent pour démarrer un projet et le déployer. Le développeur peut alors se concentrer sur son travail principal : le développement.

Chez les hébergeurs, les plates-formes répondent à plusieurs problématiques essentielles du cycle de vie d'une application :

- **le déploiement** est géré par upload de package applicatif ou compilation du code source. Les nouvelles versions peuvent être livrées et mises en service petit à petit. Selon les cas, il est même possible de faire de l'A/B testing entre les versions de l'application ;
- **les logs** sont collectés et centralisés dans une console pour faciliter l'analyse en cas de bug. Ils pourront être exportés vers un stockage Cloud pour réaliser de la BI par exemple ;
- **les middlewares** comme la base de données, les serveurs de cache ou les bus de messages sont des services gérés. L'application consomme ces services à la demande ;
- **les backup et restore** sont normalement garantis. Tous les composants utilisés par l'application sont régulièrement sauvegardés ;

- **la supervision** fait aussi partie des services inclus. La plupart des consoles d'administration affichent des graphiques témoignant des performances de l'application ;
- **la scalabilité horizontale** est la clef de voûte de la plate-forme. Elle est définie en nombre d'instances maximales et minimales. Selon la consommation réseau, CPU ou mémoire, l'application pourra voir son nombre d'instances augmenter ou diminuer.

Chez les fournisseurs Cloud, les PaaS peuvent s'intégrer avec l'ensemble des services disponibles. Vous pourrez par exemple faire communiquer vos applications avec des machines virtuelles qui réaliseront des tâches spécialisées (génération d'images, chiffrement, calculs complexes).

Mais attention, il n'y a pas de magie ! Les applications doivent s'adapter au modèle imposé par les plates-formes. Les développeurs ne manqueront pas d'identifier de nombreuses contraintes à respecter pour pouvoir réaliser des applications adaptées au PaaS. Le portage d'une application existante vers ce type de Cloud nécessite souvent des modifications lourdes dans la base de code.

Tout comme pour les services gérés, les PaaS permettent de décharger les équipes d'exploitation d'une partie de leur travail. Les équipes de développement sont plus autonomes et peuvent se charger des mises en production dont le processus est cadré par la plate-forme. Attention là aussi aux problèmes de production, l'aspect boîte noire de ces solutions rend difficile les analyses. Il est donc essentiel que les équipes soient formées sur les solutions retenues.

Les PaaS publics

Des solutions de PaaS publics existent depuis quelques années déjà. Les trois géants américains sont présents sur ce créneau :

- AWS Elastic Beanstalk pour Amazon,
- Azure pour Microsoft,
- et Google App Engine pour Google.

Des alternatives existent avec des concepts intéressants ; citons Heroku ou encore CleverCloud, une solution « made in France ». Pour ces deux dernières, il suffit simplement de fournir le code source de l'application. La mise à jour du code dans le dépôt de source lance sa compilation dans une usine logicielle. Si la construction se déroule sans problème, la nouvelle version de l'application est déployée.

Les PaaS publics bénéficient de la richesse des services proposés par leur fournisseur. Ils bénéficient aussi bien sûr de leur infrastructure divisée en régions et zones de disponibilité. En matière de Cloud, plus le service est de haut niveau, plus sa tarification est élevée. Les acteurs du marché mettent en avant leur valeur ajoutée pour justifier ces coûts.

Notez bien qu'il n'existe pas de standard en la matière. Adopter le PaaS d'un hébergeur revient bien souvent à lier fortement vos solutions à des APIs et services propriétaires non réversibles. Il s'agit donc à nouveau de choisir des technologies standards pour faciliter la réversibilité de l'application. Dans le Cloud public, les choses vont vite et les évolutions sont légions, vos applications doivent suivre ce rythme pour rester fonctionnelles.

Les PaaS privés

Plusieurs éditeurs se sont lancés dans la construction de PaaS privés. Ces solutions ont le principal avantage d'être réversibles. En effet, il s'agit au final de paquets logiciel à installer sur des machines physiques ou virtuelles. Vos applications peuvent donc reposer sur une solution que vous pourrez transposer vers un autre fournisseur sans impact pour les développements.

De plus, ces solutions sont souvent personnalisables. Elles permettent par exemple de choisir les middlewares et langages qui seront supportés par la plate-forme. La personnalisation peut parfois consister à définir des configurations spécifiques pour répondre à vos besoins. Attention, tous les PaaS privés ne supportent pas nativement ce type d'adaptation. Si vos besoins nécessitent ce type de spécialisation, tournez-vous vers une solution open source extensible. Ce dernier point doit toutefois être modéré par le support des conteneurs Docker dont nous avons déjà parlé dans cet ouvrage.

L'utilisation d'un PaaS privé fournissant le support de Docker semble être le meilleur choix à ce jour. Bien sûr le choix d'une solution privée n'est pas celui de la facilité. Le travail à fournir par les équipes d'exploitation pour l'installation et le maintien en condition opérationnelle est bien plus important que sur des solutions gérées. Pensez au préalable à vérifier la liste des middlewares déjà supportés par la plate-forme.

Parmi les solutions actuellement disponibles sur le marché nous retiendrons :

- **Cloud Foundry** développée par Pivotal sous licence Apache 2. Cette solution propose un ensemble de briques pour composer son PaaS. Elle repose sur Bosh pour la gestion de configuration, Lattice pour créer des modules d'exécutions et Diego pour l'orchestration de clusters. Il existe aussi une distribution packagée pour les entreprises : Pivotal Cloud Foundry.
- **OpenShift** est le PaaS développé par Redhat. Il existe dans une version communautaire et entreprise. Le projet est développé en opensource et, pour sa dernière version, repose sur Docker, Kubernetes et Atomic.
- **Stratos** : en 2013, WSO2 a versé sa solution PaaS à la fondation Apache, créant ainsi le projet Stratos. La société continue de développer la plate-forme dans le projet Apache. Le support de Docker est en cours de développement.

Take away Cloud



CHOISIR SES TECHNOLOGIES

- *Automatiser : il est vital de maîtriser au moins un outil d'infrastructure as Code.*
- *Reproduire régulièrement des environnements iso-production pour ses développeurs et testeurs afin de détecter au plus tôt les soucis éventuels.*
- *Tester des idées d'amélioration de son architecture ou de nouveaux outils et faire des tests de charges dans son intégration continue.*
- *Effectuer une veille sur les tendances et évolutions majeures permettant d'évoluer et faire évoluer son infrastructure au bon moment.*

Conclusion

En quelques années, le Cloud est devenu incontournable. Encore récemment, il était utilisé pour créer de nouveaux produits, en faisant table rase de l'historique. La plupart des grandes startups du Web se sont d'ailleurs bâties entièrement dans le Cloud. Avec le temps et une adoption de plus en plus massive, les services se sont étoffés pour répondre à des besoins de plus en plus spécifiques. Grâce à des investissements colossaux dans la construction de data centers et en innovation, les 33/37 fournisseurs ne cessent d'élargir leur gamme de services. Il est d'ores et déjà possible de migrer tout ou partie de son IT vers de l'hébergement à la demande.

Le Cloud change la façon d'envisager l'informatique. Il n'est plus question de gérer des plannings de capacité, et donc d'attendre plusieurs semaines avant la mise à disposition d'une machine sur laquelle opérer. De la même façon, nul besoin de réaliser des investissements matériels lourds pour lancer un nouveau service avant de connaître l'ampleur de son adoption. Le Cloud est un espace de liberté, ouvert à l'innovation rapide et efficace. Cette révolution n'est pas seulement technique car elle prend sa source dans les méthodes issues de l'industrie comme le Lean.

Pour adopter cette nouvelle façon de consommer l'IT, il faut changer ses méthodes de travail en abattant les murs entre les différents silos de production, du métier à l'exploitation. Une migration vers le Cloud ne se prend pas à la légère. Il faut identifier le ou les fournisseurs qui hébergeront la solution future. L'impact est aussi technique, car, non seulement les ressources disponibles sont maintenant jetables, mais aussi le réseau et le stockage qui sont différents des modèles historiques. Il convient donc de choisir des stacks technologiques cohérentes, s'adaptant parfaitement à cet environnement et surtout à vos besoins.

L'hybridation des infrastructures est sur la route de votre réussite dans le Cloud. N'hésitez pas à l'intégrer en usant par exemple des services gérés. Qu'il s'agisse de bases de données, d'envoi de mails, de monitoring, de systèmes d'alertes, de répartition de charge ou encore de stockage, les briques de services sont nombreuses et facilitent grandement la réalisation de produits performants et flexibles. La fusion à travers des liens dédiés ou d'un VPN ou via internet ou des hébergements en dur et à la demande permet de créer une véritable osmose. Ce nouvel ensemble garantit la sécurité et la

résilience de vos services tout en générant une flexibilité nouvelle. L'hybridation favorise également le débord de capacité pour répondre à de fortes charges prévisibles (pic de vente, événement mondial, opération marketing de grande ampleur, etc). Quels que soient vos besoins, pensez à utiliser des produits standards bénéficiant d'une large communauté d'utilisateurs et d'un support de qualité.

Depuis quelques temps, de nouveaux métiers dédiés à la pratique du Cloud apparaissent. Les Clouds brokers se positionnent en intermédiaires pour faciliter la vie de leurs clients. Les administrateurs ayant une expérience DevOps sont très recherchés. Les développeurs sachant tirer parti de l'élasticité le sont tout autant. Une grande portion de la communauté technique planétaire tente d'unifier l'accès aux différents fournisseurs pour arriver à atteindre la promesse formulée : le Cloud unique. Cette promesse d'une énorme masse de ressources de calcul et de stockage est en pleine maturation.

Sous quelle forme le Cloud arrivera à maturité, nul ne le sait. Ce dont nous sommes convaincus, en revanche, c'est qu'il faut dès aujourd'hui commencer à l'appivoiser, à le dompter, pour demain en faire un outil maîtrisé. Le Cloud est l'évolution naturelle d'Internet.

Take away Cloud



PRÉPARER SA MIGRATION

- *Se poser les bonnes questions : quels bénéfices sont attendus d'une migration ? Quelles briques peut-on améliorer au passage ?*
- *Impliquer l'ensemble de votre chaîne de production, du métier à la production.*
- *Penser à la réversibilité, éviter le piège du vendor lock-in.*
- *Définir clairement le périmètre de la migration et avancer par itérations.*



SÉLECTIONNER SON OFFRE

- *Élaguer l'arbre de décision en comparant son existant et ses besoins avec les capacités des solutions disponibles.*
- *Réaliser un micro-projet sur chacune des options restantes et mener des rétrospectives pour capitaliser au mieux sur ces expérimentations.*
- *Échanger avec les Users Groups et autres Meetups afin de prendre position en se nourrissant des expériences menées.*
- *Évangéliser : trouver la voie royale d'usage de sa solution Cloud et former toutes les parties prenantes dans le même sens.*



CHOISIR SES TECHNOLOGIES

- *Automatiser : il est vital de maîtriser au moins un outil d'infrastructure as Code.*
- *Reproduire régulièrement des environnements iso-production pour ses développeurs et testeurs afin de détecter au plus tôt les soucis éventuels.*
- *Tester des idées d'amélioration de son architecture ou de nouveaux outils et faire des tests de charges dans son intégration continue.*
- *Effectuer une veille sur les tendances et évolutions majeures permettant d'évoluer et faire évoluer son infrastructure au bon moment.*



Merci à

*Anne Beauchart, Léo Carel,
Chloé Desault, Nicolas Jozwiak,
Louis Laroche, Pablo Lopez
et Stéphane Teyssier.*

À lire et à relire



Pour télécharger l'un des techtrends en version pdf, rendez-vous sur le site techtrends.xebia.fr

Pour avoir toujours plus d'information sur le Big Data, le Web, les architectures Java, la mobilité et l'agilité, rendez-vous sur blog.xebia.fr

Pour avoir toujours plus d'information sur le Cloud, rendez-vous sur blog.wescale.fr

Les auteurs



Séven
Le Mesle



Thomas
Cousin



Aurélien
Maury



Gérôme
Egron



Jean-Eudes
Couignoux



Matthieu
Nantern





Be a cloud expert

est une société de conseil IT dédiée aux technologies
Cloud



SOFTWARE DEVELOPMENT **DONE RIGHT**

est une entreprise agile qui délivre des logiciels
de haute qualité

Nous contacter :

156 boulevard Haussmann

75008 Paris

01 53 89 99 99

contact@wescale.fr - info@xebia.fr