Un marché concurrentiel pour le cloud computing

Comment les solutions multi-cloud profitent aux entreprises et aux administrations

Roland Berger

IEF

Introduction

Le World Wide Web fête ses trente ans cette année. Mais le concept de « cloud computing », le partage de serveurs ou d'espaces de stockages informatiques, existait déjà avant l'invention d'internet. Les premières vagues de numérisation massive furent liées aux PC et aux technologies sur site pour les entreprises : de même, nous sommes aujourd'hui prêts pour l'ère du cloud computing grâce à des progrès énormes en matière de connectivité, de capacité et de performance de calcul. Une large gamme de produits et de services peut être mise à disposition par le biais du cloud, ce qui a abouti à la création d'un grand marché en croissance rapide.

La présente étude montre que le « cloud » a plusieurs définitions, qu'il s'applique à plusieurs niveaux et qu'il permet d'offrir aux clients potentiels des applications diverses –de la mise à disposition d'infrastructures à des applications logicielles. Qu'un client opte pour une solution mono-cloud, multi-cloud ou hybride, la tendance est inéluctable pour les entreprises mais aussi pour les administrations publiques.

Comme nous l'avons montré dans notre étude sur le fair play dans le monde du numérique *(Fairplay in der digitalen Arena)*, l'économie numérique peut donner naissance à des acteurs de portée mondiale en un claquement de doigt (en apparence) mais peut aussi permettre à une poignée d'entreprises d'accéder à des positions dominantes sur le marché. Dans certains cas, comme pour les moteurs de recherche ou les systèmes d'exploitation mobiles, cela peut aboutir à des « goulots d'étranglements » critiques, ou à des abus de position dominante. Avec l'hyper-croissance et la dynamique forte du marché du cloud, la tendance est aujourd'hui à l'émergence d'acteurs peu nombreux et très dominants. Ce nouveau marché aboutira-t-il aussi à la suprématie de quelques-uns et à la création d'un duopole, voire même d'un monopole ?

Cette étude vise à faire la lumière sur l'écosystème du cloud computing et sur les interactions entre les prestataires de cloud d'une part et les entreprises et institutions publiques d'autre part. Comment les gouvernements peuvent-ils éviter toute dépendance stratégique et défendre leur résilience face aux cyber-attaques tout en encourageant l'innovation et la concurrence ? Comment le secteur public peut-il utiliser au mieux ces technologies notamment au vu des tâches diverses qui attendent les administrations en matière de sécurité des données ?

Nous souhaitons remercier ici ORACLE pour le soutien qui nous a été fourni lors de cette étude, et espérons qu'elle pourra aider à alimenter un débat sur les conséquences du cloud computing. Nous espérons ainsi que les célébrations du 40ème anniversaire de la création d'internet ne seront pas ternies par le regret de n'avoir pas fait davantage pour garantir la concurrence pendant les « années folles » du cloud computing.

Prof. Dr.
Friedbert Pflüger
Président
Internet Economy
Foundation

Clark Parsons
Directeur
Internet Economy
Foundation

SIX LEVIERS POUR L'INNOVATION ET LA DIVERSITÉ DU CLOUD COMPUTING. LES POUVOIRS PUBLICS DOIVENT POSER LES BASES D'UNE CONCURRENCE ÉQUITABLE DANS LE CLOUD EN TANT QUE CLIENTS ET EN TANT QUE RÉGULATEURS.

EN TANT QUE CLIENT, L'ÉTAT DOIT ...

1 ... adapter l'utilisation du cloud à ses objectifs stratégiques

2 ... réduire l'effet lock-in en utilisant des solutions multi-cloud

3 ... imposer contractuellement l'interopérabilité et la portabilité

EN TANT QUE RÉGULATEUR, L'ÉTAT DOIT ...

1 ... encourager le développement de normes de sécurité européennes pour le cloud computing

2 ... soutenir l'autorégulation des fournisseurs de services de cloud

3 ... en dernier recours, mettre en place une réglementation légale de l'interopérabilité des services de cloud

Sommaire

1
IL EST TEMPS D'AGIR 6

Pour préserver la concurrence sur le marché du cloud computing

2
UNE TENDANCE À LA CONCENTRATION 10

Le marché du cloud connaît une croissance effrénée et est dominé par une poignée de prestataires

3
DIVERSITÉ ET FLEXIBILITÉ 20

Des solutions multi-cloud pour atténuer les inconvénients de services uniques

4
L'AVENIR DE L'ADMINISTRATION PASSE PAR LE MULTI-CLOUD 34

Des solutions diversifiées pour des besoins complexes

5
CLIENT ET RÉGULATEUR 41

Comment l'État peut agir pour la diversité et la concurrence sur le marché du cloud

1
IL EST TEMPS D'AGIR POUR PRÉSERVER LA CONCURRENCE SUR LE MARCHÉ DU CLOUD COMPUTING

Au-dessus des nuages, le temps est au beau fixe. Depuis 2006 et le début de la commercialisation de solutions de stockage basées sur le cloud par Amazon sous le nom d'Amazon Web Services (AWS), le marché du cloud connaît une croissance fulgurante. Le volume de données traitées par des centres de calcul dans le cloud est aujourd'hui onze fois plus élevé que le volume de données traitées de manière « traditionnelle ». Le rapport devrait être de 19:1 d'ici deux ans. Le marché du cloud est déjà évalué à environ 200 milliards de dollars US actuellement : c'est approximativement deux fois plus qu'il y a seulement quatre ans.

Cette croissance, la technologie la doit surtout à son adaptabilité : les capacités de stockage et de calcul peuvent être mises à disposition et évoluer à court terme, et si les besoins changent, il est possible de réagir avec souplesse à tout instant. Mais le cloud ne concerne pas que la mise à disposition d'infrastructures informatiques décentralisées : il permet aussi l'utilisation de plateformes complètes pour le développement ou l'exploitation de services et d'applications numériques disponibles directement dans le cloud. Il est par exemple possible d'y modifier des fichiers textes sans que l'utilisateur ne doive installer d'application sur son ordinateur local.

La diversité des services disponibles sur le cloud se reflète du côté des prestataires : outre Amazon, des géants du net comme Google, Microsoft et IBM proposent des services de cloud computing. De grands spécialistes comme Salesforce et plusieurs offres de niche s'ajoutent aussi à la liste. Tous cherchent à se tailler une part de ce gâteau, qui grossit de jour en jour. Mais la concurrence, justement, est de plus en plus rude : les parts de marché se concentrent toujours davantage entre une petite quantité de fournisseurs de services de cloud. Dans le domaine des services d'infrastructure et de plateformes, notamment, la domination d'une poignée d'entreprises se renforce. La menace d'une monopolisation, comme celle des marchés des systèmes d'exploitation, du commerce en ligne ou des moteurs de recherche, est bien réelle.

Une monopolisation (sur ce marché comme sur les autres) nuit cependant gravement à la diversité du marché et à la concurrence. Les clients –qu'il s'agisse d'entreprises, d'administrations publiques ou de personnes privées—verraient l'offre se réduire comme peau de chagrin. Un marché moins concurrentiel nuit aussi à l'innovation et au rapport qualité-prix.

La menace d'une monopolisation sur le marché du cloud est bien réelle.

« Je suis convaincue qu'une concurrence réelle et équitable joue un rôle décisif dans l'instauration de la confiance nécessaire pour exploiter tout le potentiel de nos sociétés. »[1)]

Margrethe Vestager
Commissaire européenne à la concurrence

Mais il n'est pas trop tard pour agir ! Le pouvoir de marché n'est pas encore aussi concentré que dans d'autres secteurs du numérique. Il faut noter par ailleurs que dans ces domaines, la domination de Microsoft, Amazon et Google ne s'est pas faite du jour au lendemain, elle s'est développée petit à petit. Aujourd'hui, les autorités de la concurrence ont bien du mal à limiter les conséquences de leur suprématie. Il est nettement plus simple de lutter de manière préventive contre l'apparition d'une telle puissance de marché.

L'État a ici un double rôle à jouer : tout d'abord, les pouvoirs publics représentent une part importante de la demande en matière de services de cloud computing. Ils doivent à ce titre miser sur la création d'un portefeuille de services équilibré dans le cadre d'une stratégie multi-cloud. Il faut donc choisir la solution la plus appropriée pour chaque domaine de compétence. Le pilotage des solutions devient plus exigeant que pour une solution mono-cloud, certes, mais il est ainsi possible de minimiser la dépendance vis-à-vis d'acteurs uniques. La concurrence entre les différents fournisseurs de services de cloud s'en trouve renforcée, et on évite ainsi la domination d'une entreprise en particulier. D'autre part, l'État, en tant que législateur, définit aussi les conditions-cadres du marché. À ce titre, il doit promouvoir des normes européennes sur la sécurité et l'interopérabilité des services de cloud. Des normes de sécurité cohérentes permettront surtout aux petits prestataires de proposer leurs produits dans toute l'Europe, par-delà les frontières. La mise en place de normes industrielles communes dans le cloud computing facilitera aussi la tâche des clients qui souhaitent combiner les services de plusieurs prestataires, ou « emporter » leurs données avec eux lorsqu'ils en changent. Les acteurs eux-mêmes devraient établir des normes communes pour renforcer l'interopérabilité et la portabilité dans le cadre d'une autorégulation autonome. Une réglementation légale sur l'interopérabilité des services dématérialisés doit rester un dernier recours, mais ne peut pas être exclue d'emblée.

La présente étude est un plaidoyer pour la préservation de la concurrence sur le marché du cloud –notamment dans le secteur public. Nous analyserons tout d'abord le marché du cloud, et décrirons la tendance actuelle à la concentration. Nous évoquerons ensuite les avantages et les défis que présente le cloud, et expliquerons pourquoi les entreprises devraient préférer des portefeuilles multi-cloud aux solutions mono-cloud. Nous décrirons ensuite en détail le rôle du secteur public en tant que demandeur de solutions de cloud, et montrerons que les solutions multi-cloud peuvent lui être particulièrement avantageuses. En conclusion, nous formulerons aussi des recommandations stratégiques pour les décideurs politiques et administratifs. La double fonction de l'État, en tant qu'acheteur de services de cloud et en tant que régulateur du marché, prend ici toute son importance. Notre étude se base sur des entretiens avec des utilisateurs et des prestataires de services de cloud et avec des experts des administrations publiques et du monde de l'entreprise. Nous avons également analysé une large gamme de données et d'études.

2
UNE TENDANCE À LA CONCENTRATION

LE MARCHÉ DU CLOUD CONNAÎT UNE CROISSANCE EFFRÉNÉE ET EST DOMINÉ PAR UNE POIGNÉE DE PRESTATAIRES

2
Une tendance à la concentration

Les services de cloud sont aujourd'hui utilisés intensivement. Ils sont devenus un outil informatique standard et stratégique. Dans ce chapitre, nous montrerons à quel point leur utilisation s'est généralisée ces dernières années et nous donnerons un aperçu du paysage de l'offre et de la concentration croissante du marché. Mais avant d'évoquer ce marché, il faut définir ce dont nous parlons, et décrire ce que l'on entend par cloud computing. Quels sont les différents types de modèles de services et de prestations, et les différentes formes de portefeuilles de services que les utilisateurs peuvent constituer ?

Il n'existe aucune définition du cloud reconnue unanimement par les utilisateurs et les experts. Ces derniers utilisent souvent la définition du National Institute of Standards and Technology (NIST), une organisation subsidiaire du Ministère du commerce des États-Unis. Cette définition, également adoptée par l'agence européenne ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information), est la suivante (traduction française du texte original en anglais) :

Le cloud est un modèle permettant un accès réseau permanent, pratique et sur demande à un ensemble partagé de ressources de calcul configurables (ex. réseaux, serveurs, stockage, applications et services) qu'il est possible de fournir et de mettre à disposition en minimisant l'effort de gestion et la quantité d'interaction avec le fournisseur de service. Ce modèle comporte cinq caractéristiques essentielles, trois niveaux de services et quatre modèles de déploiement.

La présente étude se base sur la définition du NIST. Voici les cinq caractéristiques essentielles d'un service de cloud :

1. Le libre accès sur demande
En cas de besoin, un client peut utiliser les ressources automatiquement et sans interaction humaine avec le prestataire (temps de serveur ou espace de stockage en réseau, par exemple).

2. L'accès élargi au réseau
Les services du prestataire sont disponibles en réseau par le biais de mécanismes normalisés, et sont accessibles par différents terminaux.

3. La mutualisation des ressources
Les ressources du prestataire sont mutualisées et peuvent être utilisées par de nombreux clients. Les utilisateurs ne savent pas où se trouvent les ressources, mais peuvent déterminer contractuellement le lieu du stockage des données (région, pays ou centre de données, par exemple)

4. La souplesse et la rapidité
Les services peuvent être mis à disposition rapidement et avec souplesse (adaptabilité à très court terme), parfois automatiquement. Du point de vue de l'utilisateur, les ressources semblent illimitées.

5. Un service adapté
L'utilisation des ressources peut être mesurée et contrôlée, ce qui permet de la piloter et de l'optimiser : la transparence est ainsi garantie pour le fournisseur et pour l'utilisateur.

Quatre méthodes de mise à disposition existent pour les services de cloud : les quatre « modèles de déploiement ».

- Un **cloud privé** est l'exploitation exclusive d'une infrastructure dématérialisée par une institution unique. Elle peut être organisée et pilotée par l'institution elle-même ou par un prestataire externe, et se situer physiquement au sein de l'institution ou chez le prestataire en question.
- Un **cloud public** permet à un prestataire de fournir ses services au grand public ou à un grand groupe.
- Un **cloud communautaire** permet à un groupe d'utilisateurs ayant des intérêts communs de partager une infrastructure. Elle peut être pilotée par un membre du groupe ou par un prestataire externe.
- Enfin un **cloud hybride** est une combinaison de plusieurs infrastructures dématérialisées, qui peuvent être utilisées en commun grâce à des interfaces standardisées

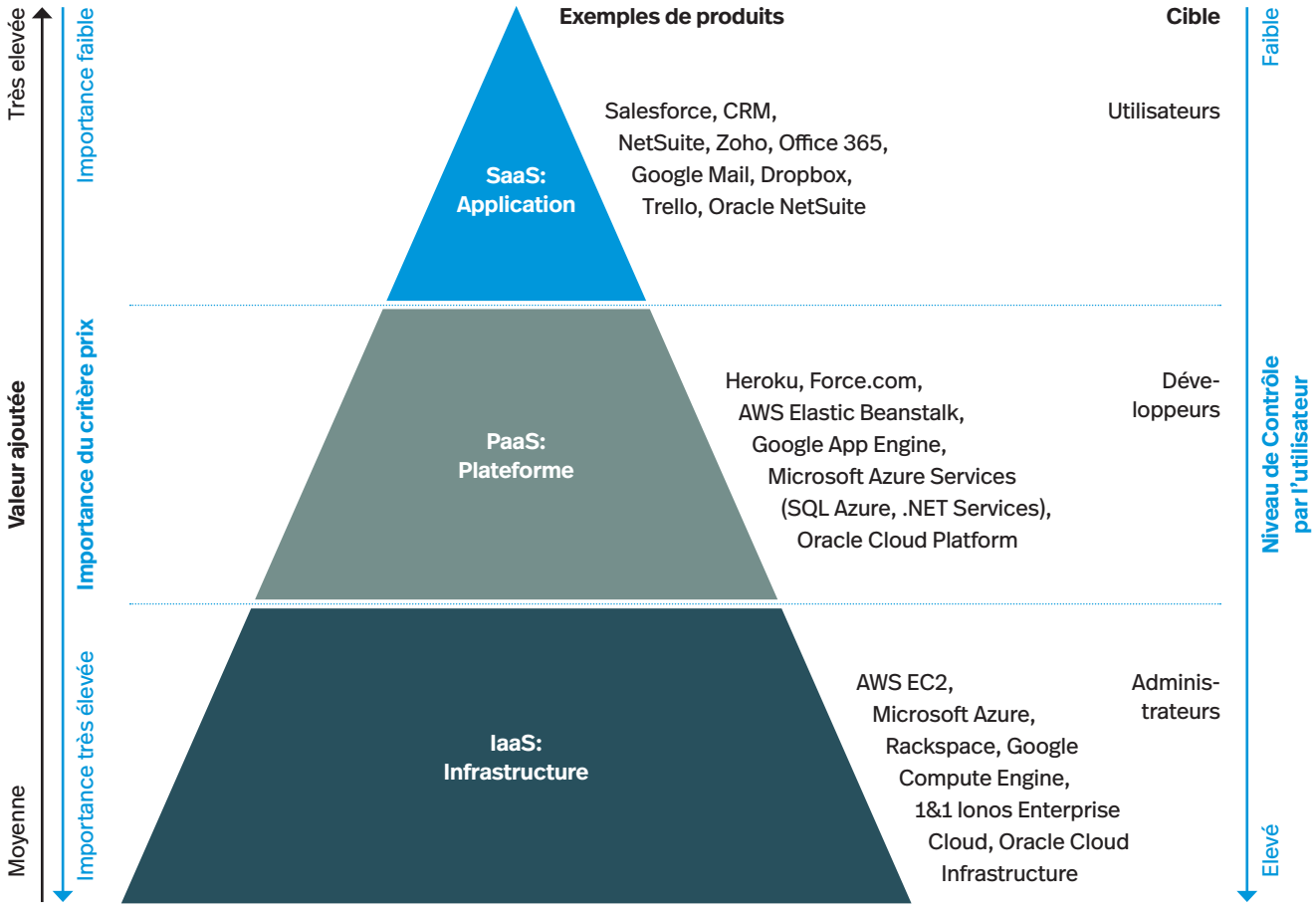
Plusieurs modèles de services sont disponibles dans le cloud. On distingue généralement trois grandes catégories : →A

- Une **Infrastructure en tant que service (IaaS)** met à disposition des ressources informatiques spécifiques en tant que service. Il s'agit généralement de stockage de données, de capacités de calcul ou de réseaux. Le client peut utiliser cette infrastructure pour le fonctionnement de ses propres services (des systèmes d'exploitation ou des logiciels d'application, par exemple). Il bénéficie du fait que la taille de l'infrastructure fournie peut être augmentée rapidement pour s'adapter à ses besoins.
- Le modèle de **Plateforme en tant que service (PaaS)** va plus loin. Il permet au client d'utiliser une infrastructure virtualisée entière en tant que plateforme. Celle-ci inclut des interfaces standardisées et met une gamme d'outils à disposition du client (comme des bases de données ou des langages de programmation par exemple), qu'il peut ensuite utiliser pour ses propres applications.
- Le modèle **Logiciel en tant que service (SaaS)** se concentre sur les applications du prestataire, utilisables par le client via le cloud. L'infrastructure dématérialisée n'est ici qu'un moyen. La gamme d'applications est extrêmement large, et peut aller de l'organisation des données de contact à la gestion de la totalité du système comptable.

Ces trois modèles de services se distinguent par leur prix, la création de valeur impliquée et le niveau de contrôle par l'utilisateur. L'IaaS met une infrastructure à disposition de l'utilisateur ; il peut ensuite l'utiliser selon ses besoins. Le contrôle par l'utilisateur est comparativement haut, et le choix du prestataire est surtout influencé par les capacités physiques et le coût du service. Avec l'augmentation de la valeur ajoutée, le niveau de contrôle du service par l'utilisateur diminue et l'importance du prix comme critère de choix s'accentue. Les services SaaS, par exemple, sont créés sur mesure pour des applications concrètes. Une fois qu'un client a décidé d'opter pour un service SaaS donné, son influence sur la configuration de l'application est limitée. Le prix, en tant que critère décisionnel, est relégué au second plan : l'application doit surtout répondre aux besoins du client.

A Pyramide des services dans le cloud : IaaS, PaaS, SaaS: une augmentation constante de la valeur ajoutée pour l'utilisateur

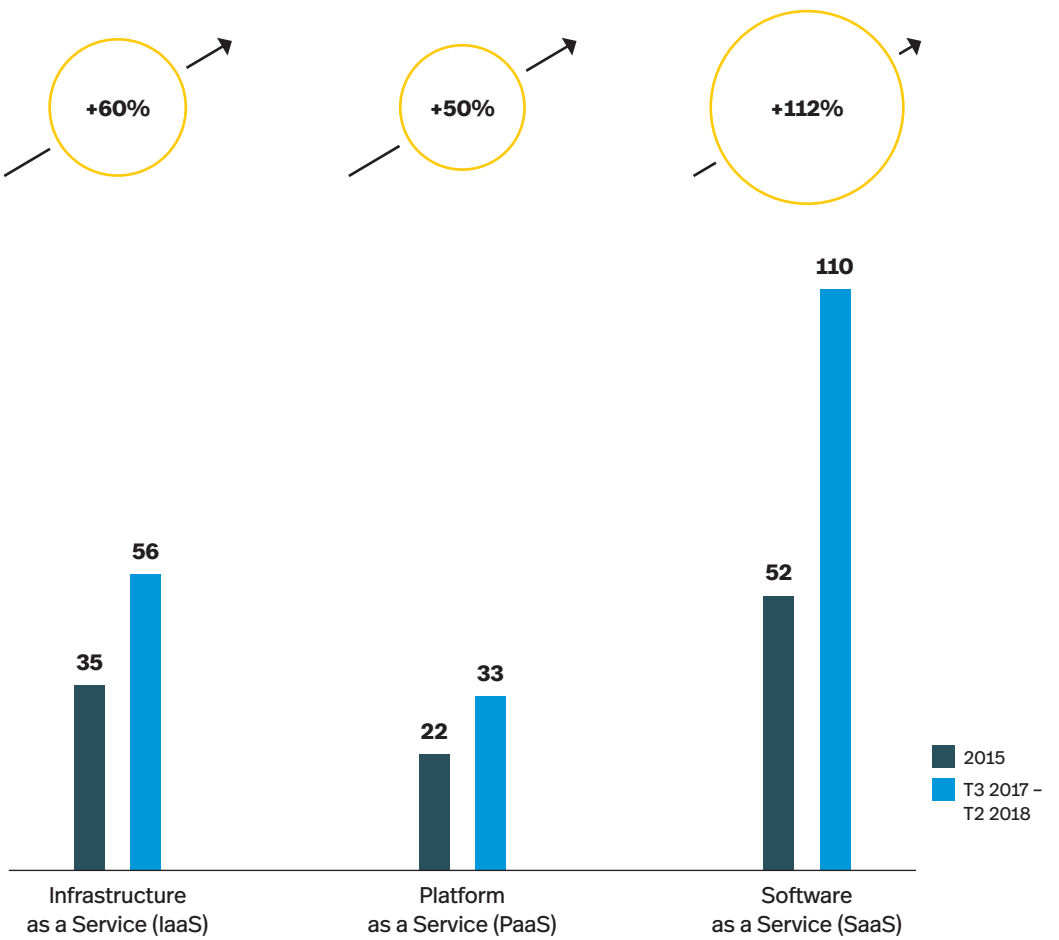
Caractéristiques des différents types de service



Source: Roland Berger

B Le cloud computing comme moteur de la croissance : Une croissance particulièrement forte du logiciel en tant que service

CA mondial du marché du cloud computing selon les segments, 2015-2018 [Mrd. USD]



Sources: ITCandor, Statista

Il est important de distinguer les différents modèles de services pour comprendre le développement des divers segments du marché du cloud et l'évolution des parts de marché des prestataires au sein de ces segments.

Sur la période allant du troisième trimestre 2017 au deuxième trimestre 2018 (soit quatre trimestres), les chiffres d'affaires mondiaux des trois segments (IaaS, PaaS et Saas) étaient de 56, 33 et 110 milliards de dollars US respectivement. →B

Le segment SaaS n'est pas seulement le plus important et de loin, c'est aussi celui qui a connu la plus forte croissance ces dernières années. Cette bonne santé est liée au fait que des fournisseurs de logiciels déjà bien établis se tournent vers des modèles commerciaux basés sur le cloud, et proposent des produits phares en tant qu'application SaaS. Entre 2015 et la période T3 2017 – T2 2018, le marché a enregistré une croissance de 112 % pour les SaaS, 60% pour les IaaS et 50% pour les PaaS.

L'augmentation rapide du chiffre d'affaires sur le marché du cloud reflète deux évolutions. D'une part, le trafic de données géré par les centres de calcul augmente (en tenant compte des flux entre les centres de calcul et les utilisateurs, entre deux centres de calcul et au sein des centres de calcul). Le volume de données stockées dans ces centres augmente lui aussi. Selon le Global Cloud Index publié par Cisco en 2018, le trafic de données géré par des centres de calcul était de 6 819 exaoctets en 2016. Une croissance annuelle de 24,7 % est attendue d'ici 2021, soit un total de 20 555 exaoctets. Un exaoctet correspond à 1 000 milliards de méga-octets, soit 500 000 milliards de pages de texte. Le volume de données stockées dans des centres de calcul

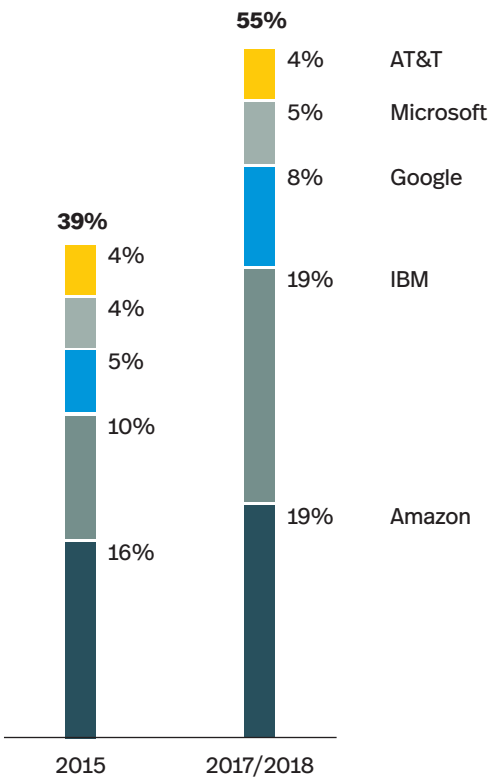
On assiste à un transfert du traitement de données depuis les centres de calcul traditionnels, vers des centres de calcul dématérialisés.

devrait passer de 286 exaoctets en 2016 à 1 327 exaoctets en 2021, soit une augmentation annuelle de 36 %.

D'autre part, on assiste à un transfert du traitement de données depuis les centres de calcul traditionnels (pilotés par les entreprises et les différentes institutions elles-mêmes), vers des centres de calcul dématérialisés. En 2016, le trafic de données traitées par les centres de calcul basés dans le cloud était environ sept fois plus important que le trafic de données traitées par des centres de calcul traditionnels (5 991 contre 828 exaoctets). En 2018, le rapport était déjà de 11:1 (10 606 contre 952 exaoctets) et il devrait être d'environ 19:1 en 2021 (19 509 exaoctets contre 1 046 exaoctets.) Le taux de croissance annuel du volume de données traitées par des centres de calcul basés sur le cloud est d'environ 27 % pour la période 2016 – 2021, contre environ 5% seulement pour le volume de données traitées par des centres de données hors cloud.

C Amazon et IBM devancent la concurrence et dominent le segment IaaS

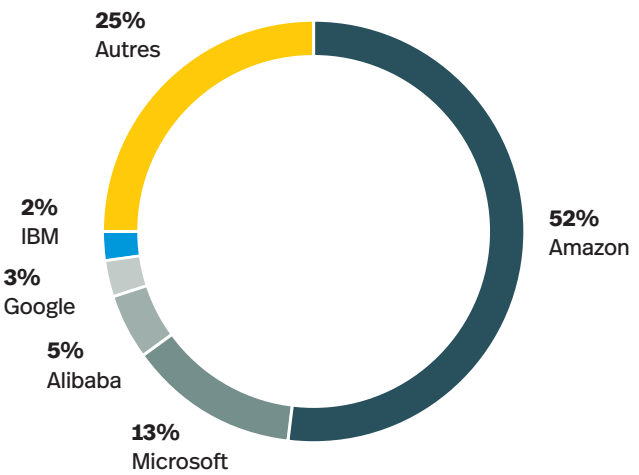
Part de marché mondiale (CA) des 5 plus grands fournisseurs d'IaaS sur le Cloud [%]



Sources: ITCandor, Statista

D Amazon domine : en 2017, l'entreprise engrange plus de la moitié du chiffre d'affaires dans le domaine de l'IaaS sur cloud public

Part de marché mondiale (CA) des 5 plus grands fournisseurs d'IaaS sur cloud public en 2017 [%]



Source: Gartner

Le marché dans son ensemble se partage entre de grands fournisseurs mondiaux comme Amazon, Microsoft ou IBM, et une large gamme de petits prestataires, qui offrent des produits spécialisés sur des marchés limités. Les fournisseurs de solutions de cloud viennent aussi de secteurs divers. On trouve parmi eux des entreprises de télécommunication (comme AT&T, NTT, Vodafone, United Internet), mais aussi des prestataires informatiques (comme IBM, Microsoft, Oracle), des entreprises fondées spécifiquement dans le but de fournir des services dématérialisés (comme Salesforce), ou encore des entreprises de commerce en ligne (Amazon). Les entreprises spécialisées de plus petites tailles sont parfois des dérivées de sociétés informatiques plus importantes. Le prestataire français Outscale, par exemple, est un spin-off de Dassault Systems créé en 2010.

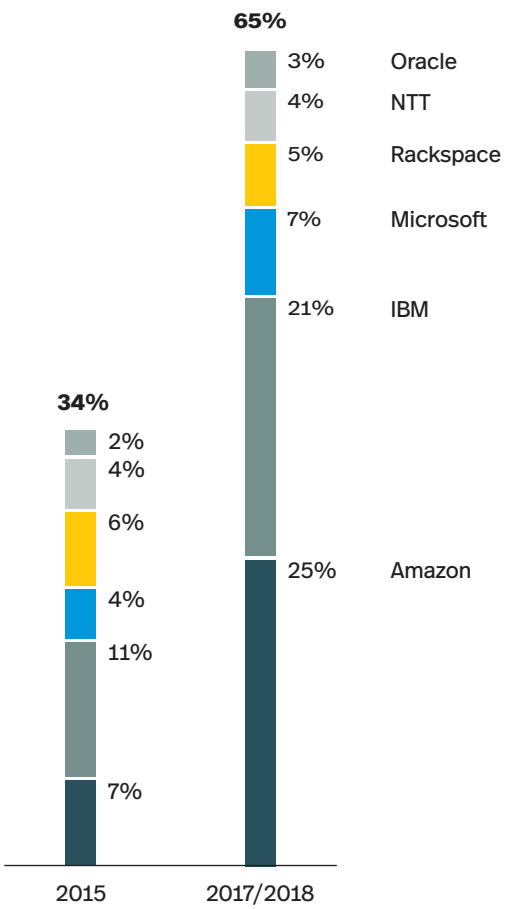
Les grands fournisseurs ont eux aussi leurs points forts. Amazon et Google, par exemple, mettent l'accent sur l'infrastructure, alors que Salesforce se concentre sur l'offre de logiciels et de plateformes via le cloud. Des entreprises comme Microsoft, IBM et Oracle sont plus généralistes et se spécialisent dans des solutions complètes intégrées omni-segments. La spécialisation des entreprises se reflète dans les parts de marché obtenues dans les segments IaaS, PaaS et SaaS.

Infrastructure en tant que service

Sur le segment Infrastructure as a Service (IaaS) Amazon et IBM se taillent la part du lion. Pour les quatre trimestres de la période T3 2017 à T2 2018, ces entreprises engrangent à elles deux près de 38 % du chiffre d'affaires mondial. →C

E Nouvelle victoire : Amazon et IBM dominent aussi le marché des PaaS, Amazon devient numéro un en un temps record

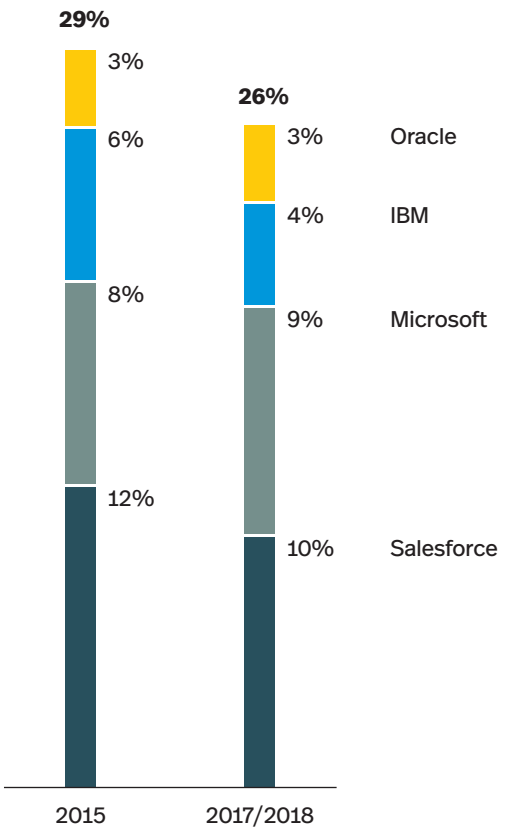
Part de marché mondiale (CA) des six plus grands fournisseurs de PaaS [%]



Sources: ITCandor, Statista

F Une fragmentation très forte : Sur le marché du SaaS en 2018, aucun fournisseur n'obtient de part de marché supérieure à 10%

Part de marché mondiale (CA) des plus grands fournisseurs de SaaS [%]



Sources: ITCandor, Statista

Bien qu'elles aient toutes deux perdu des parts de marché par rapport à 2016, elles restent largement en tête par rapport au numéro trois du marché, Google (7,6%). Sur les places suivantes, on trouve ensuite Microsoft (Microsoft Azure, 5,2%) et AT&T (4,2 %).

La solide position d'Amazon en matière d'IaaS s'explique par son rôle dominant sur le marché de l'IaaS pour cloud public. Plus de la moitié du chiffre d'affaires sur ce segment en 2017 a été généré par Amazon. →D

Plateforme en tant que service

Pour le segment Platform as a Service (PaaS), la situation est similaire à celle du marché de l'IaaS (figure E). Ici encore, Amazon et IBM règnent en maîtres sur une grande partie du marché. Elles ont généré ensemble plus de 46% du chiffre d'affaires sur les quatre trimestres de la période T3 2017 - T2 2018, →E et ont très rapidement distancé leurs concurrents. À titre de comparaison, en 2015, leur part de marché n'était que de 11,3% (IBM) et de 7,3% (Amazon). IBM a récemment perdu des parts de marché (passant de 28,0% en 2016 à 21,3% pour la période T3 2017 - T2 2018), alors qu'Amazon a presque réussi à faire doubler sa part (passant de 13,3% à 25,5%) pour devenir n°1 sur le marché des PaaS.

Software en tant que service

Le segment Software en tant que service (SaaS) est le plus fragmenté. Aucun des concurrents n'a aujourd'hui une part de marché mondiale supérieure à 10%. →F Le plus gros prestataire est Salesforce (9,6 % pour la période T3 2017 - T2 2018), suivi de près par Microsoft

(9,1 %). Suivent, assez loin derrière, IBM (4,0%) puis Oracle (3,3%).

L'analyse du marché confirme les informations des experts avec lesquels nous nous sommes entretenus : le paysage de l'offre reste assez divers, mais on constate une tendance à la concentration, notamment dans les segments IaaS et PaaS.

Ces évolutions pourraient mettre en danger la diversité de l'offre. Dans le pire des cas, une domination totale du marché n'est pas à exclure : les marchés du logiciel (Microsoft), du commerce en ligne (Amazon) ou des moteurs de recherche (Google) en sont victimes depuis longtemps déjà. Le monopole sur le marché du cloud, très porteur, tomberait d'ailleurs aussi entre les mains d'entreprises déjà dominantes dans d'autres secteurs !

Les chapitres suivants montreront que les solutions multi-cloud peuvent contrecarrer cette concentration tout en permettant aux clients de composer la solution la mieux adaptée à leurs besoins. Nous montrerons que l'État, en plus des entreprises, a un rôle important à jouer en tant que client mais aussi en tant que régulateur. Il est en effet beaucoup plus simple de lutter ex ante contre l'émergence d'un monopole sur un marché donné que de tenter ex post de réguler ses conséquences.

Les tendances à la concentration sur le marché du cloud pourraient mettre en danger la diversité de l'offre. Dans le pire des cas, une domination totale du marché n'est pas à exclure.

3
DIVERSITÉ ET FLEXIBILITÉ
DES SOLUTIONS MULTI-CLOUD POUR ATTÉNUER LES IN-CONVÉNIENTS DE SERVICES UNIQUES

L'histoire de l'économie moderne est aussi l'histoire d'une interdépendance croissante entre les entreprises, les domaines d'activités et les régions. Le triomphe des technologies numériques au cours des dix dernières années a provoqué une complexification importante. Le passage au numérique a provoqué le remplacement de chaînes de création de valeur rigides par des réseaux de création de valeur dynamiques. D'un côté, la disponibilité en temps réel de la quasi-totalité des informations pertinentes sur la création de valeur a permis d'améliorer l'efficacité des processus. En récoltant et en analysant les données issues des machines de production, il est par exemple possible de prévoir certaines pannes. La maintenance peut ainsi être mieux planifiée et les arrêts de production évités. Mais l'omniprésence des données n'améliore pas seulement l'efficacité des processus : elle permet aussi de créer des modèles commerciaux totalement nouveaux, alimentés par les données. La création de valeur se base alors exclusivement sur la récolte, la connexion et l'analyse de données. Des moteurs de recherche comme Google ou des plateformes de désintermédiation comme AirBnB sont des exemples réussis de ce type de modèles commerciaux basés exclusivement sur les données.

Les organisations modernes dépendent d'infrastructures performantes pour gérer de grandes quantités de données

Pour que les entreprises puissent tirer avantage de quantités massives de données, elles doivent être en mesure de les stocker et de les traiter. Tous les utilisateurs de données (personnes ou machines) doivent pouvoir accéder aux informations nécessaires à la tâche prévue. Le département logistique, par exemple, doit pouvoir consulter en temps réel l'état du stock, le statut des commandes en cours et les besoins en matériel de la production, voire même être capable d'intégrer ces données directement dans les processus. Ces données sont aussi cruciales au niveau de l'interface client, pour qu'il soit possible d'informer sur les délais de livraison d'un produit avant même qu'une commande ne soit passée. À l'inverse, les données récoltées par l'interface client doivent être intégrées au processus commercial. Il est ainsi possible, par exemple, d'optimiser la production pour s'adapter à des comportements récurrents de la demande.

Les entreprises utilisent des ressources informatiques centralisées depuis longtemps déjà

Des infrastructures haute performances sont nécessaires pour gérer de tels volumes de données. Depuis les années 1950, les entreprises utilisent dans ce cadre des ressources informatiques centralisées, partagées entre plusieurs utilisateurs. Les ordinateurs centraux, les architectures client-serveur dans des réseaux locaux (Local Area Networks) ou encore l'émergence des applications en ligne à la fin de l'année 1999 sont autant d'exemples de partage des capacités informatiques avec accès à distance. Au cours des dix dernières années, le cloud computing est devenu une pierre angulaire de l'informatique d'entreprise, comme le montrent les derniers chiffres d'Eurostat :

- En 2018, un bon quart des entreprises européennes utilisaient des services informatiques dans le cloud, soit une augmentation de 37% par rapport à 2014.

« Les fournisseurs de cloud se sont rendu compte que la sécurité informatique était un argument de vente de plus en plus important pour les utilisateurs afin de réussir à relever les défis du numérique » [2)]

Arne Schönbohm
Président de l'Office fédéral allemand de la sécurité des technologies de l'information (BSI)

- Plus de la moitié (56%) de toutes les grandes entreprises (c'est à dire celles qui comptent plus de 250 salariés) utilisaient des services de cloud en 2018 : une augmentation de 60% par rapport à 2014.
- Le cloud est principalement utilisé pour la communication (courrier électronique) et pour la sauvegarde de données. Ce type de services concerne deux tiers des entreprises utilisant le cloud.

Le cloud permet une adaptabilité des ressources informatiques grâce à des infrastructures externalisées…

Les utilisateurs de technologies de cloud computing bénéficient ainsi de l'externalisation de tout ou partie de leurs services informatiques à des tiers. Ces derniers peuvent, dans certains cas, faire partie de l'organisation, notamment lorsque le département informatique devient centre de profit et offre ses services aux autres départements via un cloud privé. Il est cependant aussi possible d'obtenir des services de cloud auprès de prestataires externes sous forme de clouds publics.

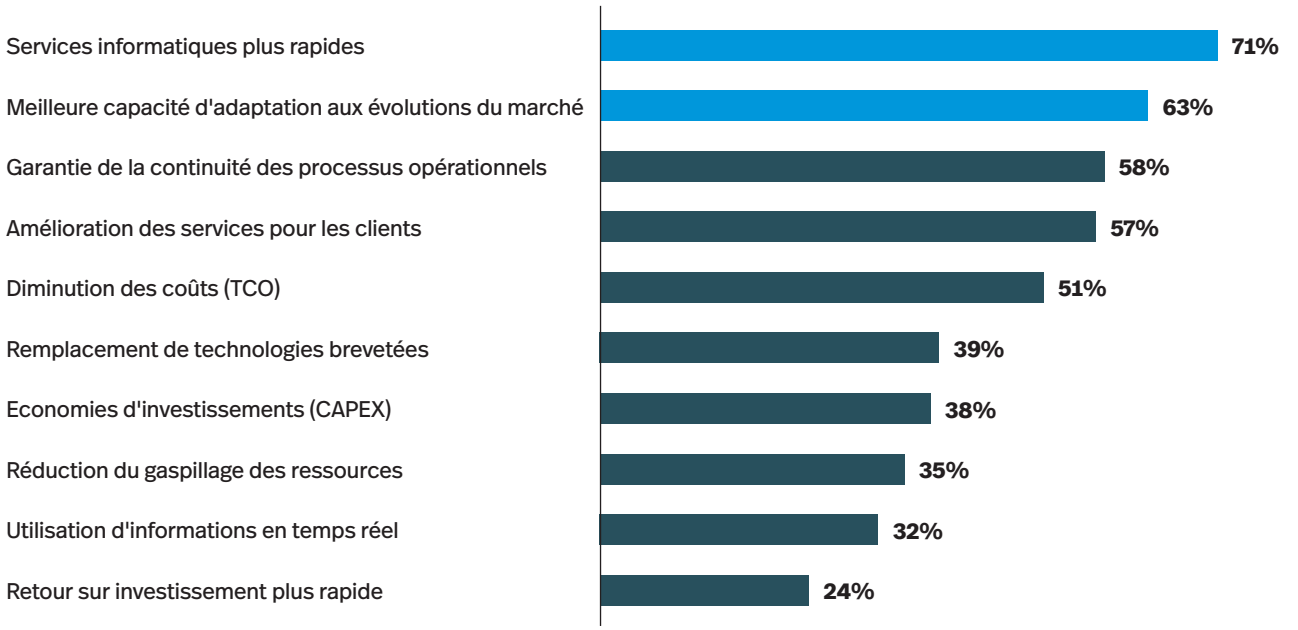
Dans les deux cas, l'infrastructure informatique est externalisée : un achat de service est donc nécessaire pour certains besoins comme le stockage de données, la capacité de calcul ou le courrier électronique. Le paiement dépend ensuite de la prestation utilisée. Le cloud offre ainsi plus de souplesse aux entreprises. Si des ressources informatiques plus importantes sont nécessaires pour gérer un pic d'activité, le cloud peut mettre des capacités supplémentaires à disposition rapidement. Ainsi, les pics de demande peuvent être gérés avec souplesse sans qu'il soit nécessaire d'acheter l'infrastructure nécessaire. Lors des périodes de plus faible demande, les capacités du cloud sont moins utilisées.

C'est un avantage pour le prestataire comme pour l'utilisateur des services de cloud. L'utilisateur n'est pas obligé de se procurer l'infrastructure informatique nécessaire à la gestion de pics d'activité rares : il fait ainsi l'économie de l'investissement initial et des frais d'exploitation. Le prestataire de services dématérialisés peut mettre son infrastructure à disposition d'une large gamme de clients internes ou externes et réguler ainsi son utilisation. La performance et la sécurité du système sont des piliers du modèle commercial des fournisseurs de services de cloud : ces derniers investissent donc continuellement dans leur infrastructure. Les utilisateurs en bénéficient sans avoir besoin d'effectuer eux-mêmes des investissements lourds !

Mais le cloud permet surtout de rendre les entreprises plus agiles lors du développement ou du lancement de nouveaux produits. De nouveaux projets peuvent être entamés sans qu'il soit nécessaire d'obtenir une infrastructure informatique propre. Le cloud permet par exemple à certaines start-up de réagir sans problème à une augmentation soudaine du nombre de leurs clients. Près de 100 millions de photos ont été téléchargées sur le réseau Instagram pendant l'année qui a suivi la création de l'entreprise. Cette croissance explosive n'a été possible que grâce à l'utilisation du cloud, à la souplesse qu'il permet et à son adaptabilité quasi-illimitée. →G

G Rapidité et souplesse : En investissant dans le cloud, les entreprises recherchent surtout plus d'agilité

Objectifs recherchés par les entreprises lors d'un investissement ou d'un projet dans le cloud en 2018 [en pourcentage des personnes interrogées]



Source: IDG Research

… mais comporte des risques liés à la sécurité et aux coûts

En ce qui concerne la sécurité des données, il faut distinguer la sécurité de l'information de la protection des données. Dans le premier cas, il s'agit de protéger les données contre la perte ou les accès non-autorisé. Les fournisseurs de services de cloud, très spécialisés, ont un excellent niveau de sécurité et garantissent une grande fiabilité –leur Monthly uptime percentage est généralement d'au moins 99,5%. La durée possible des pannes mensuelles, avec ce niveau de disponibilité, reste tout de même de 3,5 heures : des disponibilités de 99,9% sont donc aussi proposées. Les fournisseurs de services de cloud peuvent aussi offrir une protection très élevée contre la perte de données grâce à des architec-

tures systèmes redondantes et à la duplication des données dans plusieurs centres de calcul. Le niveau de disponibilité et de sécurité des données offert est donc généralement très élevé : mais des pannes généralisées ne sont pas toujours évitables. En 2017, par exemple, une mauvaise manœuvre d'AWS, le plus grand fournisseur d'infrastructure de cloud, a provoqué une panne chez 54 des 100 plus grands sites mondiaux d'e-commerce.

Au-delà de la disponibilité et de la sécurité des données, la protection des données confidentielles ou personnelles joue aussi un rôle important dans les entreprises. Les utilisateurs qui font appel à des prestataires de services dématérialisés actifs au niveau mondial doivent notamment connaître la juridiction qui s'applique à leurs données. Le Bouclier de protection des données UE-États-Unis permet aux entreprises européennes de transmettre les données personnelles à des entreprises américaines conformément au règlement général sur la protection des données dans la mesure où l'entreprise aux États-Unis dispose d'une certification valide. De même, le « CLOUD Act » permet aux autorités américaines d'accéder aux données de citoyens européens dans le cadre d'enquêtes judiciaires lorsque ces données sont traitées par une entreprise américaine, quel que soit leur lieu de stockage physique. La transmission de données personnelles dans le cadre du CLOUD Act peut cependant aller à l'encontre du règlement général sur la protection des données… Un dilemme pour les fournisseurs de services de cloud basés aux États-Unis, qui ont pour seul choix une infraction au droit américain ou une infraction au droit européen. Les fournisseurs de services de cloud basés en Europe, quant à eux, ne sont pas exposés à ce problème.

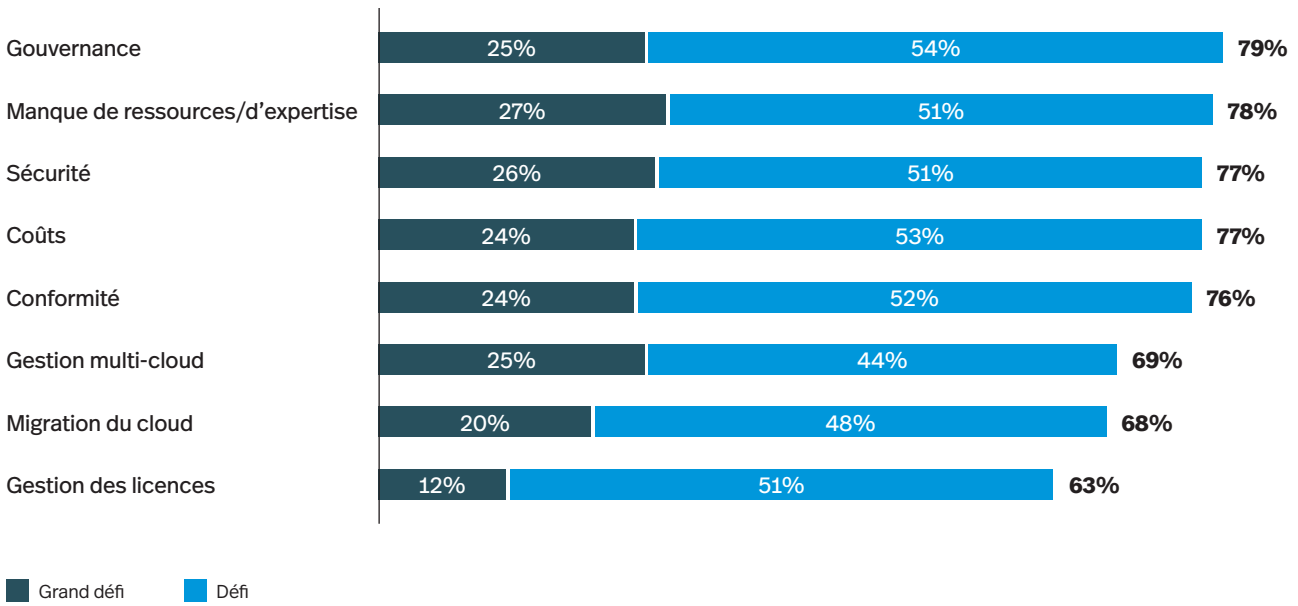
Le coût des services de cloud représente lui aussi un risque. Pour décider de l'utilisation d'un ou plusieurs services de cloud, il faut tenir compte de la durée nécessaire au transfert des applications et des données concernées vers le cloud. Plus cette migration est longue, plus il faut de temps pour commencer à bénéficier des avantages liés au cloud. Au-delà de l'investissement de départ, les frais de fonctionnement constituent le facteur de risque principal. Les ressources du cloud pouvant être obtenues rapidement et sans difficulté, les coûts qu'elles représentent doivent faire l'objet d'un suivi constant. Dans les grandes organisations, où plusieurs départements font appel à des ressources de cloud de manière indépendante, il est souvent assez difficile de déterminer quels sont les coûts effectifs du cloud. Beaucoup ont déjà pris conscience du problème : Selon les entreprises, la maîtrise des coûts est l'un des plus grands défis posés par le cloud. →H

La menace d'un enfermement lié aux écosystèmes mono-cloud intégrés

Au-delà de la protection des données et des coûts, le plus grand danger, lors de l'utilisation de services de cloud, est ce que l'on appelle l'effet « lock-in » (voir encadré page 28). Cet effet d'enfermement se produit lorsqu'un client reste fidèle à un prestataire parce que les obstacles qui s'opposent à un changement sont trop important, et non parce qu'il est satisfait des prestations fournies. On constate ici une similitude entre les mécanismes de marché du cloud computing et des plateformes numériques. Au même titre que Google ou Facebook par exemple, les prestataires de cloud créent des écosystèmes entiers au sein desquels leurs clients peuvent

H Facteurs de risques : Selon les entreprises, les principaux défis sont les ressources humaines, la sécurité et les coûts

Défis rencontrés par les entreprises lors de l'utilisation du cloud computing [2019, %]



Source: RightScale 2019 State of the Cloud Report

accéder à une large gamme de services dématérialisés différents et compatibles les uns avec les autres. Tout comme les plateformes numériques, ces écosystèmes offrent des avantages concrets aux clients, dans la mesure où ils intègrent l'ensemble des applications dématérialisées nécessaires dans un système à guichet unique. Généralement, cet écosystème numérique propose aussi ses propres interfaces avec des applications tierces. Les développements de tiers peuvent ainsi être intégrées à la solution, ce qui augmente l'utilité pour les clients et fait de la plateforme un partenaire incontournable pour les entreprises extérieures. Le désavantage de ce type d'écosystèmes pour le client est l'effet « lock-in » : comme des normes exclusives sont le moyen le plus simple de combiner les différentes applications (bases de données, conteneurs, fonctions de recherche, gestion

de contenu) et données sur le cloud, un client qui souhaite changer de fournisseur de service de cloud pour ses applications et ses données doit faire face à des coûts de migration importants.

À cela s'ajoute le fait que le premier pas dans le cloud est toujours le plus difficile. La migration des applications et des données dans le cloud est l'aboutissement d'un long processus de choix d'une stratégie adaptée. L'idée d'utiliser la même solution pour d'autres applications –notamment des applications totalement nouvelles—est donc très attrayante, même si un prestataire tiers offre une solution mieux adaptée pour les applications concernées. La « gravitation des données » est le phénomène selon lequel une première migration de données vers un cloud spécifique est généralement suivie d'autres données. Les entreprises stockent ainsi rapidement de grandes quantités de données chez des prestataires uniques. Qui souhaite déplacer ces données vers un autre cloud se heurte ensuite rapidement aux limites de la physique. Même en exploitant les capacités maximales d'une connexion à 100 Mo/s, il faut plus de 90 jours ou plus de 13 semaines à une entreprise pour transférer ne serait-ce que 100 téraoctets de données (c'est-à-dire le contenu de 100 ordinateurs portables modernes) d'un cloud vers un autre.

Ces mécanismes poussent les clients à développer des liens étroits avec un prestataire en particulier, ce qui crée une situation de dépendance. Les conséquences peuvent être graves : Si le client n'est plus satisfait de l'offre du prestataire de service en raison de son prix ou de la disponibilité de nouvelles applications, les coûts du changement sont prohibitifs. Il est dès lors possible que le client, effrayé par ces coûts, décide de continuer à travailler avec une solution de cloud non-optimale. La souplesse théorique du cloud est ainsi perdue, tout comme la possibilité de développer et de mettre sur le marché de nouveaux produits rapidement. Dans le pire des cas, l'offre d'applications et les capacités du prestataire peuvent limiter l'innovation et la croissance du client.

Réduire l'effet lock-in avec des solutions multi-cloud

L'utilisation d'une combinaison de solutions de cloud permet d'atténuer nettement les risques évoqués ci-dessus. Les solutions dites « multi-cloud » partent du principe qu'il faut choisir, pour chaque application dans le cloud, le meilleur prestataire du marché. Les applications et les données d'une entreprise sont ainsi réparties entre plusieurs prestataires. Cela permet d'une part de renforcer le niveau de sécurité, étant donné qu'il est possible de choisir une protection plus élevée (donc plus chère) pour les données sensibles que pour les données non sensibles. D'autre part, les stratégies multi-cloud permettent aux entreprises d'éviter l'effet lock-in. Certes, il est possible qu'une dépendance existe malgré tout vis-à-vis de prestataires spécifiques pour des applications hautement spécialisées ; mais l'entreprise dans son ensemble conserve la souplesse nécessaire pour faire appel à différents prestataires pour des applications ou des projets différents. Enfin, les entreprises optant pour une stratégie multi-cloud peuvent aussi mieux profiter de la concurrence tarifaire entre les différents prestataires.

Les solutions multi-cloud ne fonctionnent que lorsque l'utilisateur est capable de gérer la complexité d'une

PRISONNIER DU CLOUD – LES CONSÉQUENCES DE L'EFFET « LOCK-IN DANS LE CLOUD »

L'effet d'enfermement, ou effet « lock-in » se produit lorsqu'une relation très étroite entre un client et un produit crée un obstacle important à l'utilisation d'un produit concurrent. Un lien étroit entre le client et le produit d'un fournisseur donné résulte souvent de l'utilisation de normes exclusives, c'est-à-dire non-ouvertes ou brevetées. C'est notamment le cas des systèmes d'exploitation fermés, facilement utilisables avec les systèmes du même fabricant, mais très difficilement compatibles avec les produits de la concurrence. Les clients voient d'abord les avantages de l'utilisation d'une solution dotée de normes exclusives, notamment en raison de la compatibilité des produits du fabricant entre eux et de la possibilité, avec un mot de passe unique, d'accéder à un service clientèle unique et de profiter d'une expérience utilisateur prévisible. Mais les obstacles au changement permettent au fabricant de pratiquer des tarifs plus élevés, ou de conserver ses clients même si les produits de la concurrence sont meilleurs.

Le cloud n'est pas épargné par ce type d'effets, qui ont pour conséquence le « cloud lock-in » : l'utilisateur décide de ne pas opter pour un produit concurrent moins cher ou plus adapté parce que le coût d'un changement de prestataire est prohibitif. L'utilisateur est donc « enfermé » dans le cloud qu'il avait choisi au départ. L'une des raisons de ce phénomène est l'utilisation de services de cloud brevetés, qui ne prévoient pas d'interface ouverte pour la migration des données vers un autre prestataire.

Le réseau social Instagram a notamment été victime de ce phénomène. L'augmentation soudaine du nombre d'utilisateurs après la fondation de l'entreprise en octobre 2010 a pu être gérée grâce à l'utilisation du cloud. L'entreprise avait opté pour « EC2 », une solution très évolutive d'Amazon Web Services (AWS). Instagram fut ensuite racheté par Facebook, qui souhaita importer les données de l'entreprise vers ses propres centres de calcul. Le manque de standardisation compliqua la manœuvre, et rendit nécessaire l'utilisation d'un cloud privé virtuel d'AWS. La migration dura près d'un an.

Le lock-in peut aussi poser problème en cas de faillite du fournisseur. Le prestataire américain Nirvanix a par exemple cessé ses activités en 2013. Les clients de l'entreprise se sont vu accorder 30 jours seulement pour sécuriser leurs données. Malheureusement, si le volume de données sauvegardées dans le cloud dépasse les 100 téraoctets, le transfert par internet peut prendre plusieurs semaines, et implique la disponibilité d'une autre solution de cloud compatible pour récupérer les données concernées. Le client peut également sauvegarder ses données sur ses propres serveurs, pour autant qu'ils existent, ce qui n'est pas garanti, étant donné que les services de cloud sont utilisés pour éviter l'achat de l'infrastructure en propre.

Ces exemples montrent que ce syndrome d'enfermement n'est pas qu'un problème théorique: il peut induire des difficultés et des coûts supplémentaires bien réels pour les utilisateurs. La portabilité et l'interopérabilité sont très difficiles à mettre en œuvre techniquement, notamment pour les SaaS : les entreprises doivent donc compenser les risques de lock-in grâce à une stratégie multi-cloud. Elles limitent ainsi leur dépendance vis-à-vis d'un prestataire unique.

stratégie de ce type. Le client doit donc, d'une part, avoir une excellente connaissance de l'offre disponible sur un marché donné et des avantages et désavantages respectifs des différentes solutions pour pouvoir choisir le prestataire le plus adapté à ses différentes applications. D'autre part, une solution multi-cloud nécessite des efforts de pilotage conséquents: L'entreprise doit suivre continuellement ses capacités sur le cloud pour éviter que les coûts n'augmentent de manière incontrôlée. Sans ce suivi, plusieurs départements d'une même entreprise pourraient se tourner vers différents prestataires pour des applications similaires, ou conclure des contrats parallèles avec le même prestataire, ce qui implique bien sûr des coûts supplémentaires, mais peut aussi provoquer des problèmes liés à la sécurité : lorsque l'on ne sait pas précisément dans quel cloud se situent les données ni qui y a accès, le risque de perte, d'utilisation abusive des données ou de violation des règles de protection n'est pas à exclure.

La comparaison des avantages et désavantages respectifs des solutions mono- et multi-cloud, au tableau 1, révèle clairement que les solutions multi-cloud sont la meilleure option (toutes choses égales par ailleurs). →I Les solutions mono-cloud ont indéniablement l'avantage d'offrir un écosystème et des applications intégrées, un support unique et un seul mot de passe pour divers services. C'est pourtant ce même caractère écosystémique

I Avantage multi-cloud: bénéfices et risques des solutions mono- et multi-cloud

	Solution mono-cloud	Solution multi-cloud
Chances/ Avantages	• Accès centralisé • Interface unique de support client • Pilotage facile	• Souplesse – solutions optimales pour chaque application • Innovation • Répartition des risques et amélioration du niveau de sécurité • Absence de dépendance vis-à-vis du prestataire • Performance
Risques/ Désavantages	• « Lock-in » auprès d'un seul prestataire • Risque accru lié au stockage de toutes les données chez un seul prestataire • Une solution « à taille unique » ne satisfait pas les besoins de tous les utilisateurs.	• Pilotage complexe

Source: Roland Berger

« Si la transition vers des services basés dans le cloud offre de nombreux avantages concrets, tels que l'efficacité commerciale et la souplesse technique, la migration vers des environnements dé-matérialisés crée aussi un certain nombre de défis du point de vue légal, technique ou sécuritaire. »[3)]

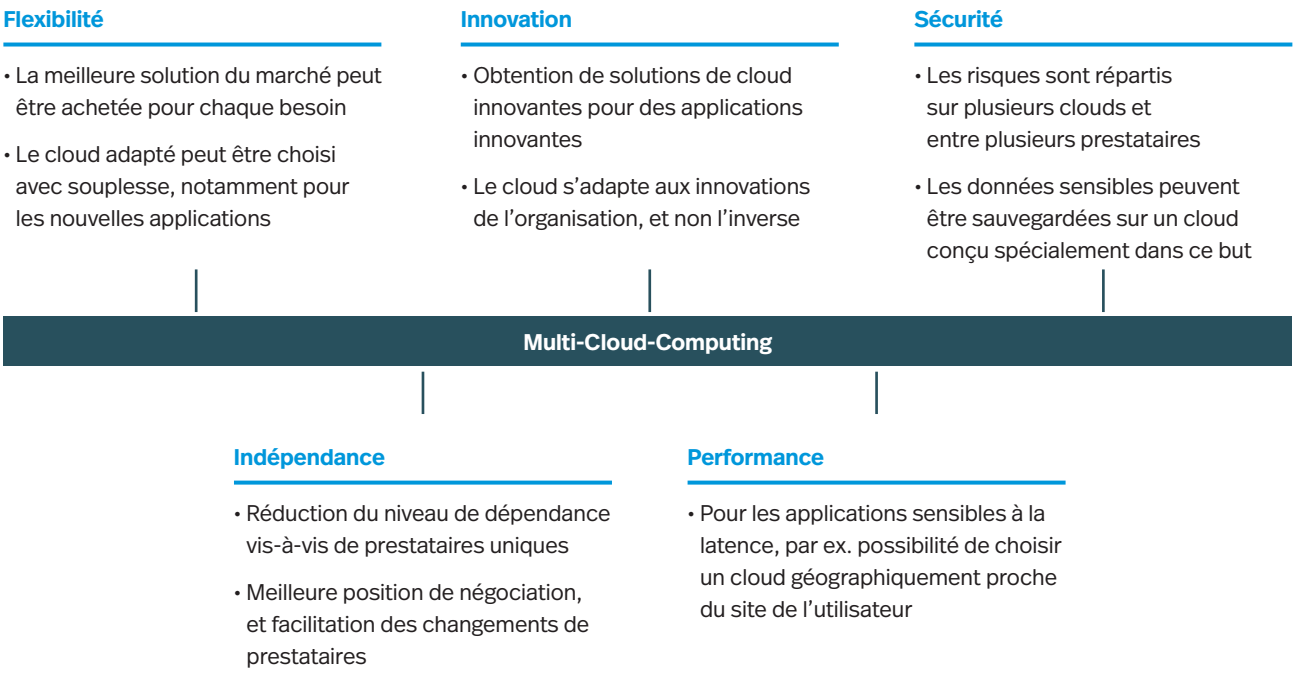
Mariya Gabriel
Commissaire européenne à l'économie
et à la société numériques

qui représente le plus gros désavantage des solutions mono-cloud, car il provoque un effet d'enfermement très fort. Le risque de perte d'informations ou de violation des règles de protection des données augmente également lorsque l'on ne fait appel qu'à un seul prestataire. Enfin, une solution mono-cloud ne peut généralement pas satisfaire tous les besoins d'une entreprise, un désavantage que ne présentent pas les solutions spécialisées.

Les innovations sont plus faciles à mettre en œuvre au sein de solutions multi-cloud

Les solutions multi-cloud gagnent ici des points grâce à des approches de type best of breed : la meilleure solution de cloud possible peut être choisie pour chaque application. Les nouveaux développements et les produits les plus innovants ne sont pas exclus d'emblée

J La diversité fait la force : Les divers avantages des solutions multi-cloud



Source: Roland Berger

en raison du portefeuille limité d'un prestataire mono-cloud. Le développement et la mise en œuvre d'une idée innovante ne doivent pas s'adapter à la solution mono-cloud existante, étant donné qu'une solution de cloud adaptée peut être obtenue pour chaque innovation. →J

Les solutions multi-cloud sont également capables d'améliorer la sécurité des données de l'entreprise. Tout d'abord, avec une solution multi-cloud, le stockage des données est systématiquement distribué entre plusieurs fournisseurs de services. Le risque de perte d'information est donc mieux réparti, ce qui réduit aussi radicalement les chances d'une panne généralisée de toutes les applications dématérialisées. De plus, une solution multi-cloud permet d'accorder aux applications plusieurs niveaux de sécurité. Les applications non-critiques peuvent par exemple fonctionner sur un cloud au niveau de sécurité normal. Pour les applications plus sensibles, celles qui utilisent des données personnelles par exemple, un cloud privé avec un niveau de sécurité élevé peut être mis en place. La souplesse des solutions multi-cloud est également avantageuse en ce qui concerne les performances des différents services de cloud: il est par exemple possible de choisir un cloud haute performance à proximité physique des utilisateurs pour les applications sensibles à la latence.

Les normes ouvertes améliorent la souplesse du cloud computing

L'utilisation de plusieurs clouds permet aussi aux entreprises de diminuer leur dépendance vis-à-vis d'un prestataire unique. Dans ce but, il est important de veiller à éviter l'utilisation d'architectures de cloud brevetées (interfaces, systèmes de base de données ou conteneurs) et leur préférer des normes ouvertes, dans la mesure du possible. L'utilisation d'applications diverses au sein d'un même cloud est facilitée par l'application de normes exclusives, mais celles-ci compliquent le transfert des applications vers un autre cloud. L'utilisation de normes ouvertes facilite ce type de transferts dans un environnement multi-cloud. Les solutions open-source, comme OpenStack par exemple, sont donc de plus en plus attrayantes pour les utilisateurs : la technologie employée leur permet de s'ouvrir aux différentes plateformes et donne ainsi plus de liberté aux utilisateurs.

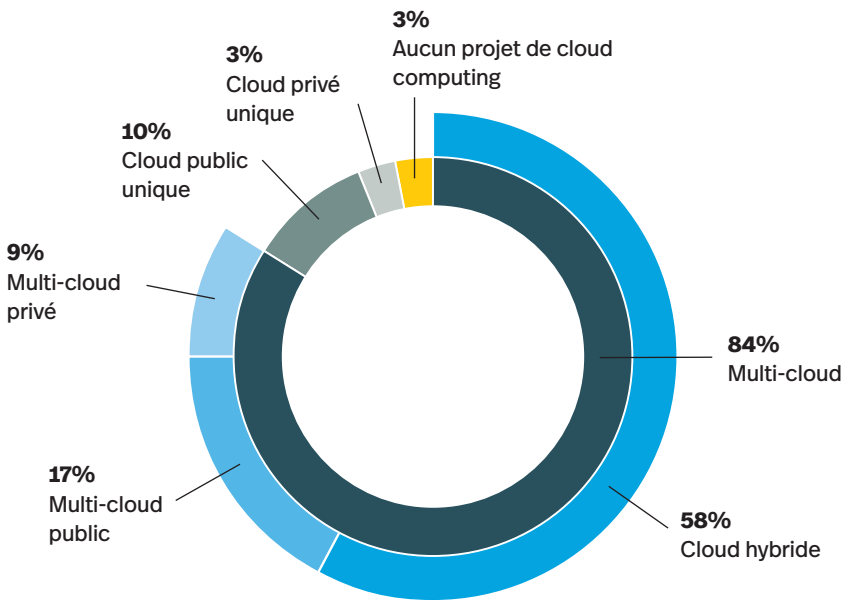
La majorité des entreprises optent pour des solutions multi-cloud

La plupart des entreprises utilisent déjà plusieurs clouds au quotidien. Les enquêtes montrent que seule une petite quantité d'entreprises font appel à des solutions mono-cloud. →K Plus de la moitié des entreprises interrogées préfèrent une combinaison de clouds publics et privés. Une entreprise sur six utilise plusieurs clouds publics, et près d'une sur dix dispose de plusieurs clouds privés.

D'une façon générale, les avantages des stratégies multi-cloud par rapport aux solutions mono-cloud ne sont pas que théoriques : beaucoup d'entreprises reconnaissent aussi leurs avantages pratiques. Certes, l'effet d'enfermement ne peut pas être totalement évité grâce aux solutions multi-cloud, notamment lorsqu'une application cruciale pour l'entreprise utilise des applications

K Le monde de l'entreprise montre l'exemple : 4 entreprises interrogées sur 5 misent sur une stratégie multi-cloud

Stratégies de cloud des entreprises de plus de 1 000 salariés [2019, %]



Source: RightScale 2019 State of the Cloud Report

brevetées provenant d'un prestataire de cloud unique. Mais l'utilisation et le pilotage intelligent de plusieurs clouds peuvent contrecarrer de nombreux désavantages des solutions mono-cloud.

Outre les utilisateurs privés et des entreprises, les administrations publiques se sont elles aussi beaucoup tournées vers le cloud computing ces dernières années. Les services de cloud peuvent être avantageux pour les organisations étatiques dans le contexte de la création de services d'e-Gouvernement. Le chapitre suivant décrit les exigences du secteur public vis-à-vis du cloud, et les solutions offertes par l'utilisation de systèmes multi-cloud.

4

L'AVENIR DE L'ADMINISTRATION PASSE PAR LE MULTI-CLOUD

DES SOLUTIONS DIVERSIFIÉES POUR DES BESOINS COMPLEXES

Les entreprises ne sont pas les seules à produire des milliers de données chaque jour : c'est aussi le cas de l'État et de l'administration publique. Il y a d'une part les dossiers classiques : Au cours de l'année 2016, les tribunaux locaux, en Allemagne, ont traité près de 662 000 procédures pénales –soit plus de 2 600 procédures par jour ouvré. À cela s'ajoutent aussi de plus en plus de données générées par des machines. Les capteurs des systèmes de gestion du trafic ou des stations météorologiques récoltent continuellement des données, qu'il faut ensuite stocker et analyser. Le service météorologique allemand, le DWD, reçoit chaque jour environ 1 000 000 d'alertes de stations terrestres, de navires, d'aéronefs, de stations radars et de satellites météorologiques, par exemple. Le service calcule le volume de ses archives en péta-octets –c'est-à-dire en millions de giga-octets.

Étant donné la quantité de données impliquées, les administrations publiques doivent faire face à des défis au moins aussi grands que les entreprises. Une quantité massive de données doit être stockée, traitée et échangée par les différentes organisations ou départements. Il faut aussi faire face aux obligations légales en matière de documentation. Les avantages du cloud, tels que décrits au chapitre précédent, bénéficient donc aussi aux administrations publiques : l'utilisation de technologies dématérialisées leur permet de mettre à disposition des capacités informatiques importantes avec souplesse.

Il existe cependant des différences non négligeables entre les entreprises et l'administration publique. Le présent chapitre se penche sur les particularités et les défis induits par les besoins des pouvoirs publics en matière de cloud computing :

1. L'administration opère dans un environnement complexe, avec des acteurs politiques, administratifs ou citoyens. Tous ont des besoins différents qu'ils peuvent faire valoir par le biais de l'établissement de normes légales ou de demandes officielles par exemple.

2. Étant donné la diversité des acteurs et des tâches concernées, l'administration publique doit travailler avec des typologies de données très diverses. Certaines doivent être mises à disposition de tous les citoyens, pour satisfaire aux principes de l'Open Data (les données brutes issues des rapports gouvernementaux par exemple). D'un autre point de vue, les autorités publiques travaillent aussi avec des données personnelles et avec des informations confidentielles qui nécessitent dans certains cas un secret absolu.

3. Le système informatique des administrations publiques doit satisfaire à des normes très strictes : il faut garantir à la fois la protection des données personnelles et la sécurité de l'État. Les services de sécurité, notamment, dépendent de ressources informatiques permettant une protection maximale contre les accès non-autorisés –notamment par des États tiers.

Pour satisfaire ces besoins très particuliers, le cloud peut jouer un rôle crucial dans le portefeuille informatique de l'administration publique. Le niveau d'exigence vis-à-vis des solutions de cloud y est plus élevé que dans les entreprises privées ; l'importance de solutions multi-cloud est donc plus grande encore dans le secteur public que dans le secteur privé.

L'administration publique est confrontée à une multitude complexe d'acteurs et de processus

L'administration publique et les différents organismes qui la composent travaillent dans un contexte multi-acteur complexe. L'administration, au sein du pouvoir exécutif, est chargée de missions publiques. Elle doit, à ce titre, répondre au pouvoir législatif, mais aussi aux citoyens, dans le cadre de « l'orientation client ». Les différents organismes sont, quant à eux, soumis au contrôle des autorités de tutelle dans l'exécution de leur mission, mais sont aussi responsables d'autres organismes placés sous leur contrôle. →L De nombreux pays ont par ailleurs une structure étatique fédérale, une structure administrative décentralisée, ou –comme c'est le cas en Allemagne par exemple–les deux. Pour représenter schématiquement les acteurs de l'administration publique dans un État de ce type, il faudrait répliquer le graphique de la figure L pour chaque strate politique. L'administration publique agit donc dans le champ des contraintes de divers acteurs, et doit y effectuer des tâches multiples, qui nécessitent des processus internes (administration du personnel, comptabilité, gestion documentaire, communication interne) et des interfaces externes (information, collecte des demandes, transmission des avis) tout aussi divers.

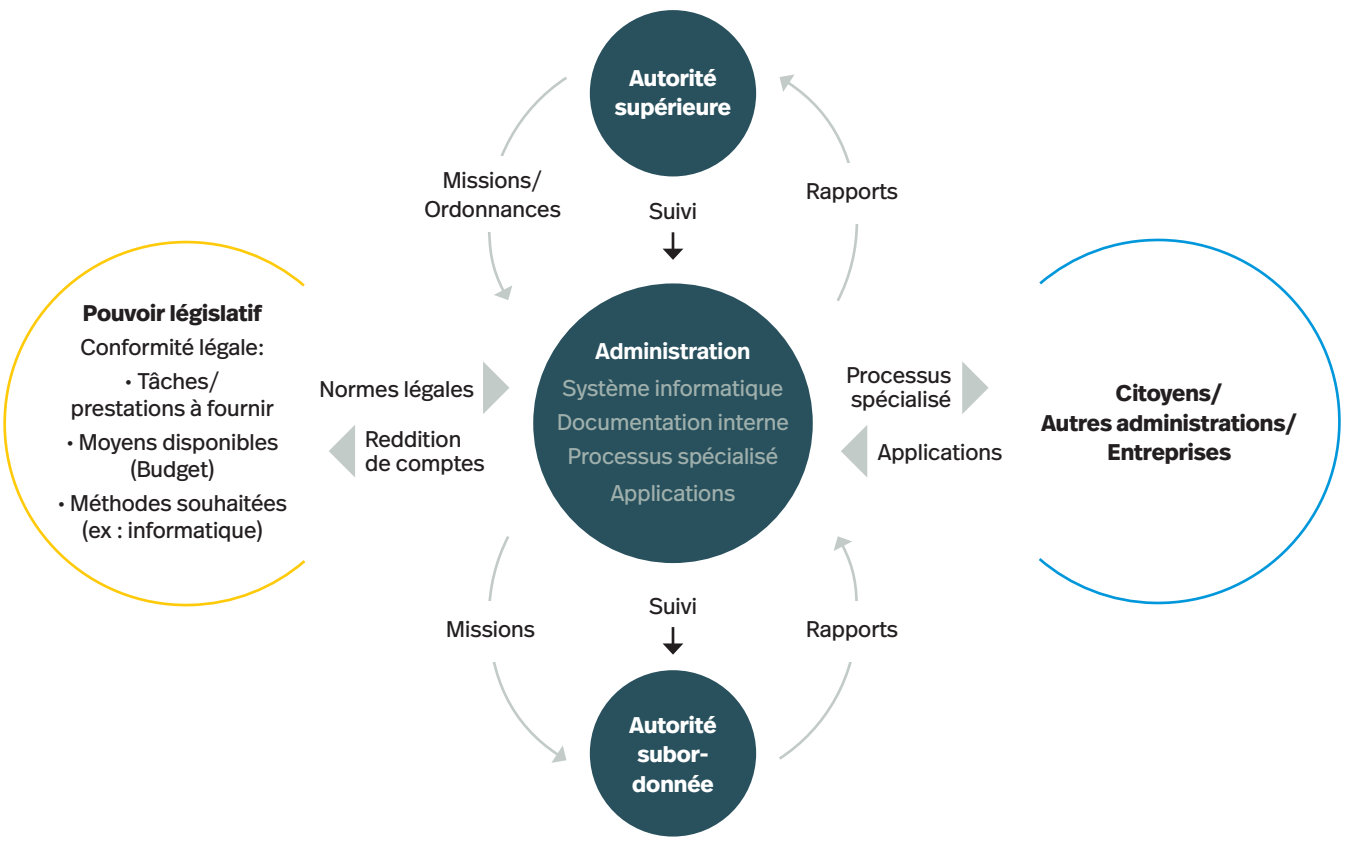
Le système informatique des administrations publiques doit refléter la diversité des acteurs et des processus

Un système informatique fonctionnel doit être capable de refléter cette diversité des processus et des interfaces. Mais les systèmes informatiques des différents organismes doivent aussi respecter des standards uniques pour permettre l'échange de données entre eux et éviter une multiplication des systèmes, source de confusion. L'inventaire des données stockées par l'administration allemande, par exemple, reste cependant très fragmenté pour l'instant. Le bureau allemand des statistiques a identifié 214 bases de données (ou « registres ») au niveau fédéral, régional (Länder) et communal. Cette fragmentation du paysage informatique a des conséquences concrètes : les données concernant les délinquants étrangers, par exemple, sont enregistrées dans le registre central des étrangers, mais aussi dans les systèmes de la police locale concernée. Il peut ainsi arriver qu'une personne soit enregistrée sous plusieurs noms, et qu'il ne soit pas possible de la retrouver dans la base de données en cas d'enquête –ou que des innocents soient suspectés injustement.

L'administration numérique nécessite des interfaces clients innovantes et faciles d'utilisation

Mais les processus et interfaces qu'un système informatique moderne doit pouvoir fournir ne se limitent pas aux relations entre les différents bureaux et départements de l'administration publique. Le passage au numérique de l'administration offre aussi des possibilités nouvelles pour l'interface avec les citoyens et les entreprises : la possibilité de résoudre en ligne toutes les questions administratives liées aux activités privées, bénévoles ou professionnelles faciliterait beaucoup la vie des citoyens, des entreprises et des administrations elles-mêmes. Il ne serait plus nécessaire

L Diversité des acteurs : L'administration publique doit satisfaire des besoins divers



Source: Roland Berger

pour les citoyens de se rendre sur place ou de patienter. Les entreprises pourraient transmettre leurs données et leurs demandes à l'administration plus facilement par le biais d'interfaces standardisées. Les autorités, quant à elles, bénéficieraient d'une automatisation poussée des processus internes –les données et demandes leur parviendraient sous forme numérique, et pourraient ensuite être intégrées au processus spécia-

lisé approprié. Selon la Commission européenne, la mise en place de solution d'e-Gouvernement au niveau européen pourrait aboutir à des économies de plus de 50 milliards d'Euros par an.

L'administration publique a besoin de solutions de cloud de pointe…

L'utilisation de services de cloud est indispensable pour bénéficier au maximum des possibilités offertes par une administration numérique. L'importante adaptabilité des ressources du cloud permet par exemple de garantir des services administratifs en ligne fiables même quand la demande est très forte. L'échange de données entre les autorités ou les différents services est également plus simple et plus rapide grâce aux solutions de cloud.

Mais celles-ci ne peuvent pas se contenter de satisfaire les besoins des nombreux acteurs et des différents processus décrits ici. L'administration publique gère une très large gamme de types des donnée différents, auxquels s'appliquent des réglementations légales différentes. Les réglementations sur l'ouverture des données (Open Data) établissent par exemple que l'administration doit mettre à disposition du public l'ensemble des données brutes qu'elle a collectées, dans la mesure où elles ne contiennent pas de données confidentielles ou personnelles.

Mais les administrations publiques travaillent aussi avec des données personnelles extrêmement sensibles, notamment dans les domaines fiscal ou de la santé. Ces données nécessitent un niveau de sécurité très élevé. La même chose est valable pour les informations classées secrètes, qui pourraient menacer la sécurité et les intérêts de l'État en cas de prise de connaissance par des personnes non-autorisées.

… et nécessite l'utilisation de solutions multi-cloud

Une solution mono-cloud intégrée n'est pas capable de faire face à la diversité des besoins de l'administration publique. Une solution mono-cloud pourrait certes faciliter l'intégration de plusieurs processus spécialisés au sein d'une même plateforme, mais l'ensemble des processus spécialisés devraient s'adapter à l'architecture d'un seul fournisseur. Une stratégie de ce type n'est pas capable de refléter la diversité des processus de manière adéquate : il serait donc systématiquement nécessaire de trouver un compromis entre les composants logiciels du processus et l'architecture du cloud choisi.

Les faiblesses d'une solution mono-cloud peuvent être compensées par la combinaison de plusieurs clouds. Dans le cadre d'une stratégie multi-cloud, il est possible de choisir les solutions les plus adaptées au processus ou au service concerné parmi une offre large. Les bases de données de lutte contre la criminalité, par exemple, nécessitent un accès mobile rapide et à faible latence, pour que les policiers en service extérieur puissent accéder aux informations nécessaires sans délai. Dans l'administration fiscale, par contre, l'accent est mis sur l'adaptabilité de la solution de cloud, qui doit pouvoir gérer les pics de demande autour des échéances liés aux déclarations d'impôts.

Les solutions multi-cloud offrent un haut niveau de sécurité des informations et une solide protection des données

Selon le « Branchenkompass Public Services 2018 » de Sopra Steria Consulting et l'institut F.A.Z, 95% des décideurs, dans les administrations allemandes, considèrent que la sécurité des infrastructures informatiques et des données constituera le défi principal au cours des prochaines années. Une solution multi-cloud offre à l'administration publique un avantage majeur dans la mesure où les différentes solutions individuelles peuvent s'adapter aux impératifs de sécurité de chaque application et des données qu'elles utilisent. Les plateformes d'Open-Data basées sur le cloud, par exemple, doivent être protégées contre la perte de donnée, mais il n'est pas nécessaire de prendre de mesures de sécurité particulière contre le vol de données ou pour garantir le droit au contrôle des données personnelles. Une plateforme de ce type peut donc être mise en place sur un cloud public. Les données des services de sécurité, par contre, doivent être efficacement protégées contre un accès non-autorisé, ce qui est possible grâce à l'utilisation d'un cloud privé, dont l'infrastructure serait située sur le site des services concernés.

Les solutions multi-cloud permettent d'adapter le niveau de sécurité des différents systèmes aux différents types de données traitées, mais aussi d'augmenter le niveau de sécurité dans son ensemble. Un cloud unique offre aussi un niveau de sécurité très élevé, mais ne permet pas d'exclure une panne systémique ou un accès non-autorisé. Même si ce genre de pannes reste rare, avec une solution mono-cloud, un incident lié à la sécurité concerne toutes les données et toutes les applications sauvegardées. Le cloud représente alors ce que l'on appelle un « single point of failure » – un talon d'Achille capable de provoquer l'effondrement du système dans son ensemble.

L'utilisation de plusieurs clouds permet de mieux répartir les risques. Avec une solution multi-cloud, si un système est compromis par une attaque cybernétique, les autres clouds ne sont pas affectés. Une solution de ce type permet donc de mieux répondre au besoin principal de l'administration publique qu'une solution mono-cloud. Si le secteur public souhaite bénéficier des avantages du cloud sans remettre en questions les intérêts et la sécurité de ses citoyens, l'utilisation de solutions multi-cloud doit devenir la référence absolue.

Outre les avantages pour les citoyens et l'administration, l'État génère aussi des externalités importantes en faisant appel à des solutions multi-cloud : En tant qu'acteur crucial sur le marché, il envoie ainsi un message important à l'opinion publique en faveur de la diversité et de la variété sur le marché du cloud. Une administration basée sur des solutions multi-cloud renforce aussi la concurrence entre les différents fournisseurs de services de cloud. Des appels d'offres réguliers pour de nouveaux projets de cloud permettent aussi d'encourager le dynamisme et l'innovation sur le marché. L'État bénéficie ainsi à deux titres de l'utilisation de solutions multi-cloud : L'administration publique peut utiliser le potentiel de la numérisation de manière efficace et sûre, et profite également d'une offre de cloud plus diversifiée et plus innovante.

5
CLIENT ET RÉGULATEUR
COMMENT L'ÉTAT PEUT AGIR POUR LA DIVERSITÉ ET LA CONCURRENCE SUR LE MARCHÉ DU CLOUD

L'utilité du cloud comme solution standard pour la mise à disposition de ressources informatiques sur demande, centralisées, adaptables et facturées selon leur utilisation ne se limite pas aux seules entreprises : elle est aussi de plus en plus souvent plébiscitée par les administrations publiques.

Dans ce secteur en particulier, les nombreux avantages des solutions de cloud font face à des exigences très élevées en matière de sécurité de l'information et de protection des données. À cela s'ajoute le risque d'un enfermement vis-à-vis d'un fournisseur unique lors de l'utilisation de solutions mono-cloud, qui peut mener à une augmentation inutile des coûts et à des performances non-optimales.

Du point de vue macro-économique, l'utilisation de solutions mono-cloud peut renforcer la concentration déjà avancée du marché. À long-terme, on risque ainsi un affaiblissement de la concurrence et un recul de l'innovation dans ce domaine.

Pour garantir le maintien d'une concurrence équitable dans le cloud computing, l'État doit donc agir à la fois en tant que client et en tant que régulateur. →M

En tant que client, il doit soutenir une gamme diverse de fournisseurs et éviter tout effet lock-in en préférant les solutions multi-cloud aux solutions mono-cloud. En tant que régulateur, il doit promouvoir une réglementation « douce », avec des normes et des codes de conduite communs, notamment au niveau européen.

L'État doit agir en tant que client

L'utilisation de solutions de cloud doit faire l'objet d'une décision stratégique et aller dans le sens des objectifs de l'organisation

Les avantages du cloud en ont fait une solution adaptée aux besoins informatiques modernes : il est logiquement devenu une solution standard. Le cloud reste néanmoins un moyen plutôt qu'une fin en soi. Les services publics ont la réputation d'être plus lents que les entreprises privées dans la mise en œuvre d'innovations techniques : ils doivent donc veiller à ne pas tomber dans une logique de « cloud first », qui les pousserait à favoriser le cloud comme solution pour un besoin informatique donné. Plutôt que de réfléchir à la meilleure méthode pour dématérialiser les processus le plus rapidement possible, les organisations doivent déterminer dans quelle mesure une solution de cloud leur permettra d'atteindre un objectif donné plus rapidement, mieux et plus efficacement.

Préférer un portefeuille multi-cloud équilibré à une solution mono-cloud

Les solutions mono-cloud et leurs écosystèmes intégrés ont des avantages réels, mais toutes choses égales par ailleurs, les avantages des solutions multi-cloud sont plus nombreux. Un portefeuille multi-cloud équilibré est particulièrement important pour éviter l'effet d'enfermement. Ce critère est d'une importance particulière pour l'administration publique, qui doit garantir sa capacité d'action à long terme. Mieux vaut donc répartir les risques entre plusieurs fournisseurs pour limiter les conséquences de pannes éventuelles du système.

« Le cloud est l'un des chantiers prioritaires de la transformation numérique de l'État. »[4)]

Mounir Mahjoubi
Ancien Ministre français du numérique

Les contrats conclus avec les fournisseurs de services de cloud doivent tenir compte de la portabilité et de l'interopérabilité des données et des applications

Tous les types de données et d'applications ne sont pas transférables d'un cloud à un autre. Il est donc nécessaire de vérifier les possibilités d'interopérabilité et de portabilité pour toutes les solutions de cloud choisies. L'utilisation de normes industrielles reconnues, comme le format « Open Virtualization » pour les appareils virtuels par exemple, permet d'améliorer l'interopérabilité entre les différents services et solutions de cloud.

L'État doit agir en tant que régulateur

Défendre le développement de standards de sécurité européens pour le cloud

Les standards de sécurité, les certifications et autres schémas de contrôle pour les fournisseurs de service de cloud diffèrent de pays en pays. Même si les normes se ressemblent, leur respect doit être prouvé dans chaque pays selon les systèmes de vérification et de certification locaux. Des normes de sécurité et de contrôle valables dans toute l'Europe pourraient être un facteur décisif pour la création d'un marché unique européen des services de données et de cloud. Les fournisseurs de services de cloud seraient ainsi en compétition au niveau européen, ce qui garantirait la concurrence et l'innovation.

En décembre 2018, la Commission européenne, le Conseil européen et le Parlement européen ont atteint un consensus politique sur un règlement en matière de cyber-sécurité. En mars 2019, le Parlement européen a adopté ce règlement en première lecture. Ce règlement prévoit notamment la mise en place de certifications européennes pour les produits informatiques. Une standardisation de ce type est un objectif particulièrement important dans le domaine du cloud, pour renforcer la concurrence et limiter la concentration progressive du marché. La portabilité, qui fait partie des caractéristiques importantes pour la sécurité des données, doit être prise en compte. Le « Bundesamt für Sicherheit in der Informationstechnik » (Bureau fédéral allemand pour la sécurité informatique), par exemple, précise dans son catalogue « C5 » d'exigences en matière de cloud computing que la portabilité et l'interopérabilité sont des critères d'évaluation de la sécurité des informations offerte par les services de cloud.

L'autorégulation des fournisseurs de services de cloud doit être soutenue et faire l'objet d'une évaluation progressive

Le règlement 2018/1807 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, entré en vigueur à la fin de l'année 2018, prévoit que les acteurs du marché du cloud européen conviennent d'un code de conduite en matière d'interopérabilité en tenant compte des normes ouvertes dans le cadre d'une autorégulation. Cette approche prometteuse doit obtenir un soutien politique et l'accent doit être mis sur le respect du délai de mise en œuvre prévu par le règlement, avant la fin du mois de mai 2020.

Une réglementation légale de l'interopérabilité des services de cloud doit constituer un dernier recours

Les règles de conduite établies par autorégulation devront être évaluées rapidement après leur entrée en

M Client et régulateur : Le double rôle de l'Etat dans la préservation de la concurrence et de l'innovation sur le marché du cloud computing

L'Etat doit agir en tant que…

… client

Utilisation du cloud conforme à une stratégie orientée selon les objectifs de l'organisation/administration

Utilisation préférentielle de portefeuilles multi-cloud équilibrés

Prise en compte contractuelle de la portabilité et de l'interopérabilité

… régulateur

Promotion de normes de sécurité européennes pour le cloud dans le cadre du réglement sur la cyber-sécurité

Soutien à l'autorégulation des fournisseurs de service de cloud avec le développement de codes de conduites sur la portabilité et l'interopérabilité des données

Évaluation de l'autorégulation, le cas échéant réglementation légale

Source: Roland Berger

vigueur –idéalement avant le délai prévu par le règlement, fin-novembre 2022. Si ces règles ne s'avèrent pas suffisamment efficaces pour garantir le degré d'interopérabilité souhaité, il sera nécessaire d'envisager des réglementations légales. Celles-ci doivent cependant rester un dernier recours, pour ne pas freiner les innovations des fournisseurs de service de cloud en leur imposant des normes fixées a priori.

L'innovation et la concurrence sur le marché européen du cloud computing sont des conditions décisives de la réussite du passage au numérique des entreprises et de l'administration. L'État joue un rôle important en la matière en tant que client et en tant que régulateur des solutions de cloud. Il doit utiliser activement cette double fonction pour lutter contre la domination de plus en plus intense de ce marché par une poignée de fournisseurs de service de cloud.

Impressum

Éditeur

Internet Economy Foundation (IE.F)
Uhlandstraße 175
10719 Berlin
www.ie.foundation
Prof. Dr. Friedbert Pflüger
Président

Roland Berger GmbH
Sederanger 1
80538 München
www.rolandberger.com
Stefan Schaible
CEO Germany & Central Europe

Auteures

IE.F
Clark Parsons
c.parsons@ie.foundation
Amelie Drünkler
a.druenkler@ie.foundation

Roland Berger
Klaus Fuest
klaus.fuest@rolandberger.com
Dr. Christian Krys
christian.krys@rolandberger.com
Dr. David Born
david.born@rolandberger.com

Contact

IE.F
Clark Parsons
Directeur général
Internet Economy Foundation (IE.F)
c.parsons@ie.foundation
+49 30 8877 429-400

Roland Berger
Claudia Russo
Attachée de presse
Roland Berger GmbH
claudia.russo@rolandberger.com
+49 89 9230-8190

Date de parution

Mai 2019

Crédits photographiques

Couverture : Zenobillis/iStock; **page 3 :** IE.F; **page 8 :** Jasper Juinen/Bloomberg/Getty Images; **page 10 :** Zenobillis/iStock; **page 20 :** Zenobillis/iStock; **page 22 :** Ulrich Baumgarten/Getty Images; **page 28 :** Zenobillis/iStock; **page 30 :** Emmanuel Dunand/AFP/Getty Images; **page 40 :** Artulina1/iStock; **page 42 :** Joel Saget/AFP/Getty Images

Sources des citations

1) TEDGlobal Talk New York City du 20/09/2017 (Minute 15:06); **2)** Communiqué de presse du Bundesamt für Sicherheit in der Informationstechnik (Office fédéral allemand de la sécurité des technologies de l'information) du 15/08/2017; **3)** Communiqué de presse de la Commission Européenne du 04/09/2018; **4)** Article de Channel Business Partners du 05/07/2018

Avis de non-responsabilité

Cette publication a été préparée à titre indicatif seulement. Le lecteur ne doit pas prendre de décision au regard des informations présentes dans cette publication sans avoir reçu un avis professionnel spécifique. IE.F et Roland Berger GmbH ne peuvent être tenus responsables des dommages résultant de l'utilisation des informations contenues dans cette publication.