Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

EXAMEN PROFESSIONNEL D'INGENIEUR PRINCIPAL DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

- SESSION 2016 -

Epreuve écrite d'admissibilité

Mardi 15 mars 2016

SUJET N° 2

Etude de cas à partir de deux dossiers techniques de trente pages maximum, soumis au choix du candidat le jour de l'épreuve écrite, permettant de vérifier les capacités d'analyse et de synthèse du candidat ainsi que son aptitude à dégager des solutions appropriées.

(Durée : 4 heures – Coefficient 1)

Le dossier documentaire comporte 28 pages.

L'usage de la calculatrice est interdit

IMPORTANT

IL EST RAPPELE AUX CANDIDATS QU'AUCUN SIGNE DISTINCTIF NE DOIT APPARAITRE NI SUR LA COPIE NI SUR LES INTERCALAIRES.

SUJET :

Vous êtes responsable du service des SIC en préfecture de Région et le préfet, lors de sa réunion mensuelle au ministère, a été informé de la mise en place à l'échelon national d'un Cloud ministériel.
Fort de son intérêt sur le sujet, il vous demande de lui présenter les concepts du Cloud, et d'évaluer dans quel(s) cas les services de l'Etat pourraient utiliser cette solution. De plus, il s'interroge sur la sécurité des données et la position de la CNIL sur cette technologie.

Vous lui présenterez dans une note :

1) les principes du Cloud, les liens avec le Big Data, et les différents niveaux de service associés.
2) les solutions possibles pour garantir la sécurité des données.
3) Dans quel(s) contexte(s) cette solution peut s'avérer utile.
4) les avantages et inconvénients de votre proposition en termes de sécurité, de rapidité, de fiabilité.
5) les impacts financiers et RH.

Dossier documentaire :

Document 1	Comment le Cloud accélère la valorisation de vos données dans un environnement Big Data ? Source:https://www.numergy.com	Pages : 1 - 3
Document 2	Cloud et Big Data- Pourquoi et comment ? Source : http://www.virtualscale.fr	Pages : 4 - 5
Document 3	Extrait Livre Blanc sur la sécurité du cloud Source: http://www.syntec-numerique.fr/	Pages : 6 - 15
Document 4	Cloud privé- le beurre et l'argent du beurre pour la direction financière. Source: http://www.kyriba.fr	Pages : 16 - 18
Document 5	Organisation territoriale de l'état.	Page 19
Document 6	Les niveaux de services offerts par le Cloud. Source : http://www.universalis.fr	Pages : 20 - 22
Document 7	Passer à la vitesse supérieure grâce au CLOUD. Source : intranet.mi	Page 23
Document 8	Extrait « Note – Réforme de l'organisation territoriale de l'État : intégration des opportunités du numérique et impact sur le système d'information ».	Pages : 24 - 28

Comment le Cloud accélère la valorisation de vos données dans un environnement Big Data ?

Comment gérer et traiter des quantités impressionnantes de données structurées et surtout non structurées (données issues du web, de la messagerie, des réseaux sociaux, etc.) dans les entreprises ? Tel est le défi des services informatiques dans les entreprises. Ces grands volumes de données, plus connus sous le nom de Big Data, n'ont peu ou pas encore été pris en compte par la majorité des entreprises mais les besoins se font ressentir car cette gestion des données est devenue vitale pour leur business. Quelques projets Big Data sont déjà en production et en expérimentation dans certaines entreprises spécialisées dans le retail, les telcos ou encore la banque/assurance. Ces secteurs, très concurrentiels, doivent se différencier en proposant de nouveaux services pour leur clientèle. Ils utilisent donc des solutions Big Data dotées d'équipements matériels de pointe, de bases de données ultra-performantes et d'algorithmes puissants capables de collecter, de trier et d'analyser des quantités très importantes de données. Les projets émanent d'ailleurs souvent des directions marketing.

L'intérêt des Big Data est donc de croiser, de traiter et d'analyser en temps réel ou très rapidement des données produites en entreprise mais aussi des données publiques, des données issues du web et des données créées et partagées par des citoyens (crowdsourcing) afin de générer des applications riches en valeur ajoutée. Et pour satisfaire à ces besoins et à ces exigences, les décideurs IT dans les entreprises n'ont pas d'autre choix que de disposer d'un système d'information agile capable de prendre en compte toutes ces demandes. Mais aujourd'hui sur le terrain, et même si elles se développent rapidement, rares sont encore les infrastructures de stockage liées au Big Data capables de satisfaire à ces besoins. Plusieurs facteurs expliquent ce constat :

Une diversité technologique accrue et une volumétrie des données qui explose

Depuis 20 ans, des solutions hétérogènes se sont développées. Résultat : la diversité technologique est devenue difficile à gérer et à administrer correctement. Ensuite, la volumétrie a explosé. A ce titre, le cabinet IDC estime que le volume des données sera multiplié par 10 en 2020 (44 Zo d'ici à 2020 contre 4,4 Zo en 2013). L'augmentation effrénée des volumes de données est à mettre en parallèle avec l'explosion de la data mobile (usage intensif des smartphones), des usages convergents et multi-terminaux en entreprise. Fort de ce constat, on comprend mieux le phénomène du Big Data. Mais cette croissance exponentielle des données interpelle sur la gestion de leur cycle de vie, leur qualité, leur sécurité et leur traitement.

Des données majoritairement non structurées

Il y a 15 ans, les données étaient à 80 % structurées pour 20 % d'informations non structurées. Aujourd'hui, c'est l'inverse, 80 % de ce volume concerne désormais des données non structurées. Et face à ces dernières, les entreprises sont confrontées aux limites des systèmes existants de base de données relationnelles qui ne sont plus à même de les traiter et de les analyser de manière optimale. Le datawarehouse ne peut donc pas se risquer de s'isoler de plus des 3/4 des données produites. De plus, le poids de la donnée non structurée est extrêmement important, ce qui dégrade d'autant les performances.

Des équipements technologiquement peu adaptés

Dans l'entreprise, la vétusté des équipements et le manque de solutions adaptées ne permettent plus de réaliser, en toute simplicité et en toute sécurité, des sauvegardes régulières et une hiérarchisation intelligente du stockage. Les espaces disques sont ainsi souvent sous-exploités avec un taux d'occupation inférieur à 50 %. De ce fait, une majorité d'entreprises est toujours dans cette phase d'ajouter des baies et des contrôleurs supplémentaires pour faire face à la volumétrie. De plus, les solutions actuelles déployées dans les entreprises ne sont pas forcément adaptées à hiérarchiser toutes ces données et à les traiter en temps réel ou presque.

Une pénurie de compétences

Parallèlement, les entreprises font aussi face à un déficit en compétences nécessaires (appelées datascientists) pour exploiter les possibilités qu'offre le croisement des « Big Data » avec l'analyse de données.

Il faut dire que les opérations à réaliser (chargement de données, extraction, transformation, traitement, etc.) réclament une certaine expertise dans ce domaine. Enfin, la gouvernance dans la gestion des données doit être repensée en prenant en compte tout type de données. L'objectif est donc de reconsidérer le cycle de vie de la donnée et de sa valeur à long terme.

La solution : le Cloud, un accélérateur dans la valorisation des données

Face aux constats précédemment cités, les entreprises ont-elles encore les moyens financiers et les possibilités techniques et humaines de transformer leur infrastructure pour répondre aux exigences des Big Data ? Une chose est sûre, pour relever le défi du Big Data, il faut un changement radical et aller vers des outils et des environnements adaptés. Le Cloud représente ainsi le moyen qui peut faciliter l'accès aux Big Data pour les entreprises en s'affranchissant de toutes ces contraintes, techniques et humaines, tout en maîtrisant leur budget.

En effet, le Cloud permet de disposer d'une mise à jour permanente des solutions et des équipements et de répondre aux problématiques de sécurité et de respect des données sensibles grâce aux garanties offertes. L'objectif du Cloud est d'offrir aux entreprises les processus, les méthodologies et les solutions capables de rassembler des informations, de leur donner du sens et de les présenter pour qu'elles soient utiles à la prise de décision. Bref, le Cloud se doit d'accompagner les entreprises dans leurs projets Big Data en leur offrant un véritable outil d'aide à la décision.

Une mise à disposition d'outils de dernière génération pour créer une véritable banque de données de proximité

En exploitant le Cloud, les entreprises bénéficient de briques spécifiques à la gestion des Big Data pour collecter et centraliser au mieux les données quelle que soit leur source, d'en faire une analyse plus fine et leur donner ainsi plus de valeur. Cela passe donc par l'utilisation de nouveaux modèles de base de données exploitant notamment des approches mixtes entre bases de données relationnelles et non-relationnelles (NoSQL) et par des services d'import pour collecter des grands volumes de données.

Cela passe aussi par une architecture distribuée au niveau du traitement des données non structurées, c'est-à-dire le besoin de répartir la charge sur un grand nombre de serveurs (cluster de serveurs) grâce à une abstraction totale des mécanismes de parallélisation sous-jacents (principe d'Hadoop), puis par l'adoption de systèmes de stockage basés sur la technologie flash ou de type « In Memory » pour obtenir un niveau de service optimal (gros débit et faible latence).

Enfin, cela passe par la virtualisation, l'automatisation et l'orchestration pour simplifier la gestion des données. Cette couche de virtualisation est architecturée en respectant les principes de base d'Hadoop, notamment le principe de localisation, ceci afin d'offrir les meilleures performances.

Une qualité d'accès aux données

A l'heure des Big Data qui réclament des débits très importants et une garantie sur la qualité des accès aux données, bâtir un réseau de stockage de type SAN en interne, n'est pas un choix vraiment judicieux. Il est plutôt préférable de se tourner vers une infrastructure spécifique combinant les avantages d'un DAS (technologie de stockage distribuée en attachement direct aux machines virtuelles), d'un traitement optimisé en cluster via un Hadoop mutualisé. Cette configuration apporte non seulement des performances (temps de traitement divisé par deux en passant d'un SAN à un DAS mutualisé et par 8 après l'optimisation du Cluster) mais aussi une faible latence. Résultat : les débits sont réellement garantis (fini les goulots d'étranglement d'un SAN indépendant d'une infrastructure serveur).

Une gestion de la volumétrie et une sécurité des données

Pour faire face à l'augmentation effrénée des données dans les environnements Big Data, le Cloud sait répondre rapidement aux besoins de ressources supplémentaires sans coûts jugés extravagants (prix souvent basé sur le volume des données et la durée d'utilisation). Cette mise à disposition des ressources doit se faire dans les minutes après la demande.

L'objectif étant pour les entreprises d'avoir une perception de capacité infinie, une perception d'une disponibilité non-stop et une élasticité, afin de déployer des nouveaux services dans les plus brefs délais pour mieux cibler leurs clients et créer ainsi de nouvelles opportunités de business. De plus, le Cloud apporte aujourd'hui plus de sécurité pour prévenir et protéger des menaces externes et internes et sait répondre aux problématiques de respect des données sensibles et de réversibilité grâce aux garanties prévues dans les contrats des fournisseurs. D'autre part, les entreprises ont tendance à privilégier un Cloud « made in France » afin de connaître le lieu où sont stockées les données.

Un délai de livraison fortement réduit

La mise en place d'un projet Big Data peut s'avérer complexe en interne. Suivant les projets, entre le déploiement et les phases d'expérimentation et de production, il peut s'écouler des semaines voire des mois pour qu'un environnement soit vraiment opérationnel. Le Cloud permet de simplifier et d'accélérer tous ces cycles pour une mise sur le marché (time to market) dans les plus brefs délais. Avec le Cloud, l'entreprise a donc la possibilité de tester une mise en production d'un environnement à moindre coût grâce au paiement à l'usage. Cette flexibilité financière permet d'ailleurs de monter rapidement des architectures pour exécuter plusieurs mises en production.

Une simplification des processus pour les entreprises

En optant pour le Cloud pour démarrer un projet Big Data, les entreprises simplifient leurs processus (déport de la complexité vers leur fournisseur) et créent ainsi les conditions d'une collaboration constructive entre les décideurs IT, les métiers et les équipes de leur fournisseur de services.

Ces conditions favorables permettent ainsi de mieux réfléchir aux besoins du projet Big Data et de son évolution, d'optimiser les coûts, d'améliorer la visibilité et la conformité du projet et surtout de profiter de la compétence accrue des équipes des fournisseurs de services Cloud.

Cloud et Big Data : pourquoi et comment ?
Big Data et Cloud Computing, cousins éloignés ou frères siamois ? L'exemple de Hadoop et de l'Infrastructure as a Service.

Parmi les révolutions technologiques du moment, deux sortent particulièrement du lot : le Cloud Computing et le Big Data. A juste titre, d'ailleurs, car l'une comme l'autre constituent une réelle disruption qui, en tant que telle, va remettre en cause les métiers existants et en créer de nouveaux. Mais quelles sont les relations entre Cloud Computing et Big Data ? Une infrastructure de Cloud est-elle nécessaire pour faire fonctionner une
plateforme de Big Data ? Les technologies de Big Data sont-elles, par nature, de la famille du Cloud Computing ?

Bien sûr, on peut parfaitement « faire du Big Data » sans Cloud. Que ce soit dans le monde de l'open source (par exemple en montant un cluster Hadoop [1] directement sur son infrastructure physique) ou bien dans le monde des solutions propriétaires, d'Oracle à EMC Greenplum. A l'inverse, les offres Cloud existantes n'incorporent pas nécessairement de solution de Big Data. D'où vient, alors, cette confusion entre les deux technologies ?

Le fait que certains acteurs soient à l'origine de ces deux phénomènes (Google, Yahoo !) ou qu'on retrouve les mêmes types d'entreprises (des géants de l'Internet grand public : Amazon pour le Cloud public, Facebook pour le Big Data) peut contribuer à cette confusion. Mais il y a également des raisons technologiques : la contrainte de scalabilité, dès lors qu'on traite des volumes de données considérables (c'est-à-dire la nécessité de se doter d'un système capable de supporter la croissance virtuellement infinie des charges de travail), va naturellement poser la question d'un hébergement sur une infrastructure de Cloud. Les offreurs de référence de l'Infrastructure as a Service [2] ou du Platform as a Service [3], d'Amazon à Microsoft Azure, en passant par Google, ne s'y sont pas trompés, et proposent une solution Hadoop ou de Map/Reduce as a Service. En outre, remarquons qu'il n'existe pas, pour l'instant, de version multiutilisateur de Hadoop, ce qui contraint à passer par le Cloud pour en construire une.

Or, que se passe-t-il quand on fait fonctionner Hadoop sur le Cloud ? Hadoop est conçu pour reposer nativement sur un cluster de machines standard (commodity hardware). Il tire principalement sa performance de sa capacité à éclater les problèmes en traitements simples et à exécuter ceux-ci sur le noeud portant les données. En d'autres termes, le code s'exécute au plus près du disque physique. C'est le principe de localisation. Hadoop sur le Cloud se heurte donc à plusieurs contraintes :

- Pour traiter des données stockées dans le Cloud, il faut qu'elles soient présentes sur un jeu de serveurs virtuels Hadoop. Donc, il faut soit les y charger, ce qui peut être très long quand on parle de volumes de données important, soit les y laisser à demeure, ce qui va engendrer des coûts importants puisqu'on ne peut pas éteindre les machines virtuelles [4] ;
- Par ailleurs, l'exploitation de clusters Hadoop qui ont une durée de vie courte dans le Cloud ne correspond pas nécessairement aux besoins des entreprises utilisatrices ;
- La performance de Hadoop est moindre sur une infrastructure de Cloud que directement sur des serveurs physiques, à cause de la surcouche de virtualisation et du stockage en réseau (SAN) qui ne permet pas de bénéficier totalement de l'optimisation native à Hadoop.

Pour toutes ces raisons, nous avons la conviction que la « bonne » place d'un système Hadoop est à côté d'un Cloud, et non au-dessus.

Datazoomr est ainsi une plateforme « Hadoop as a Service » qui utilise le stockage HDFS [5] comme du stockage long terme, afin de permettre :

- D'éviter les transferts de données coûteux ;
- D'avoir les données toujours présentes, en ligne, prêtes pour une interrogation à la volée ;
- D'éviter une duplication supplémentaire et inutile des espaces de stockage ;
- Et surtout, de permettre la mise en place des processus d'alimentations permanents.

Néanmoins, il reste nécessaire d'utiliser une infrastructure de virtualisation afin de garantir l'étanchéité entre les différents clients qui utiliseront cette plateforme. Mais cette couche de virtualisation est architecturée en respectant les principes de base d'Hadoop, notamment le principe de localisation, ceci afin d'offrir les meilleures performances.

Par ailleurs, une infrastructure de Cloud sera présente, en parallèle, afin d'héberger les applications complémentaires nécessaires à un usage étendu du cluster : fonctions avancées (sémantique ou traitement de l'image, par exemple), applications de data-visualisation, interfaces métiers spécifiques, ... Ceci que ces applications soient fournies par des partie tierce, développées spécifiquement par les clients, ou provenant du monde Open Source.

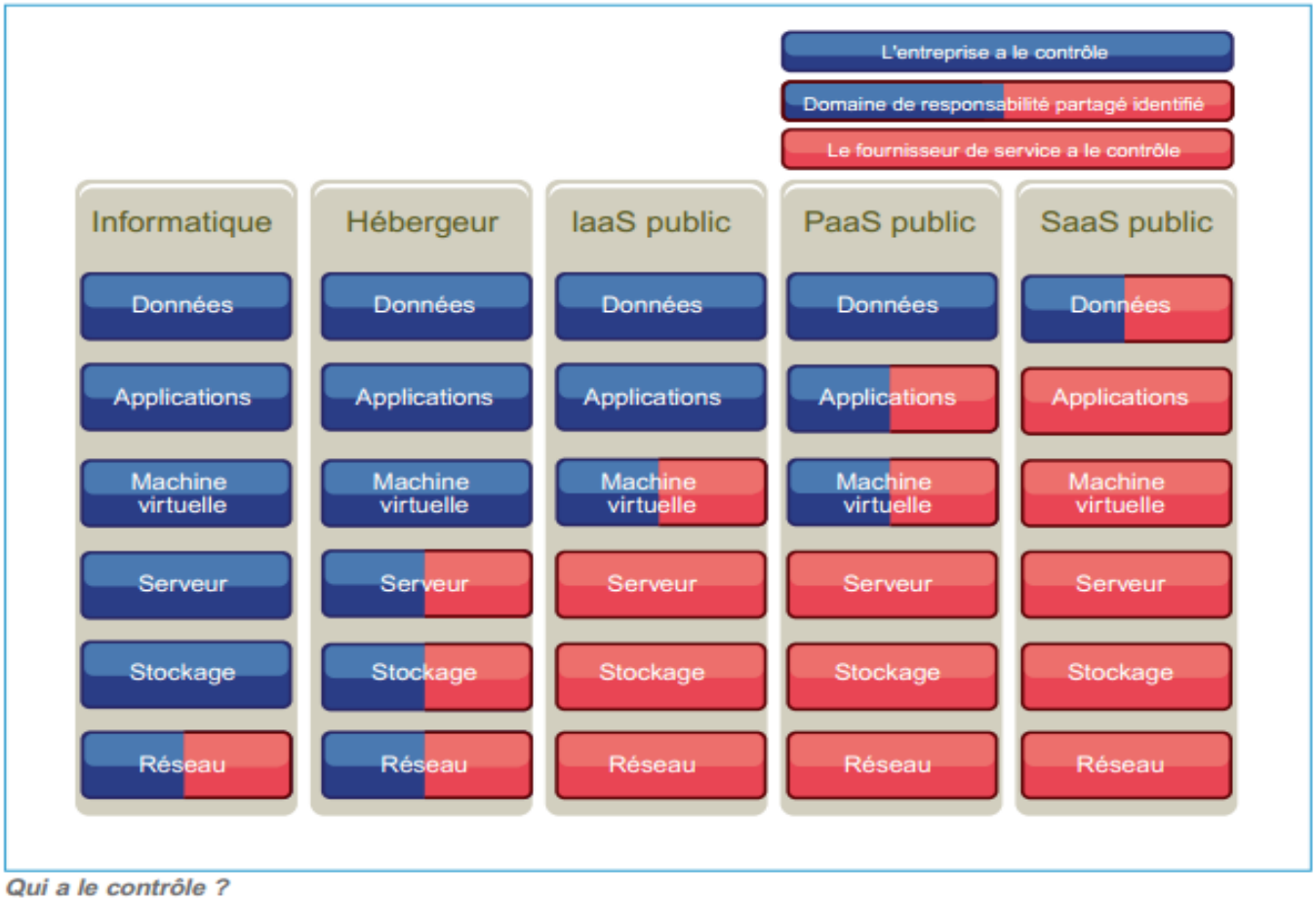
[1] La solution open source de référence pour la parallélisations du traitement des données très volumineuses, basée sur un algorithme nommé Map/Reduce
[2] IaaS, solution d'infrastructure de type Cloud, permettant de provisionner en ligne des serveurs et de les payer à l'usage
[3] PaaS, solution de Cloud permettant de recréer à distance un environnement de programmation complet
[4] http://grandlogic.blogspot.fr/2012/02/native-multi-tenant-hadoop-big-data-20.html
[5] Hadoop Distributed File System, Système de fichier distribué intégré nativement au framework Hadoop

DOCUMENT 3

LE LIVRE BLANC SÉCURITÉ DU CLOUD COMPUTING

LES PROBLÉMATIQUES SÉCURITAIRES ASSOCIÉES AU CLOUD COMPUTING

La « sécurité » est souvent citée comme le frein principal à l'adoption des services Cloud. Qu'en est-il réellement ?
L'accès aux données hébergées dans le Cloud présente en général un haut niveau de sécurité en raison des mécanismes d'authentification mis en place par les fournisseurs de service. Ces mécanismes peuvent d'ailleurs être renforcés par les solutions Corporate clients, de gestion d'identités, qui sont alors placées en amont d'un lien unique avec le fournisseur de solutions Cloud ; notons cependant que certains fournisseurs seulement acceptent une telle architecture.
Les entreprises clientes doivent toutefois considérer les points suivants :
- Quels types d'informations sont accessibles dans le Cloud ? Qui peut y accéder et comment sont elles isolées des éléments non sécurisés ?
- Qui dispose de droits pour envoyer et recevoir des données sensibles en dehors du périmètre de l'entreprise ?
- Quels sont les mécanismes de sécurité qui garantissent la confidentialité des données de l'entreprise au sein du cloud public ?
- Comment les données sensibles doivent-elles être envoyées et comment sont-elles accessibles? En clair ou en cryptant certaines d'entre elles ?
D'autres problèmes spécifiques au Cloud restent posés, notamment :
- Difficulté d'obtenir que certaines données restent localisées dans un pays désigné, le Cloud ne connaît pas de frontières ! Il faut alors être prêt à ce que le fournisseur doive se conformer à des réglementations comme la directive Européenne de Protection des Données ou le USA Patriot Act,



Qui a le contrôle ?

qui peuvent autoriser les autorités locales à prendre connaissance des données (cette possibilité est toutefois largement théorique)

- Impossibilité d'assurer la traçabilité des données, par exemple en vue des certifications SAS 70, Sarbanes Oxley ou autres, qui doivent garantir que nul n'a pu modifier des données sans qu'il en reste une trace. A noter : certains prestataires de services Cloud sont d'ores et déjà certifiés SAS 70 (type II).
Ces problèmes peuvent être en partie contournés par des architectures applicatives adaptées (encryption ou occultation de la propriété des données, et ségrégation des données contractuellement auditables).

ANALYSE DES RISQUES

L'inventaire des menaces et une analyse de risques sont préalables à tout projet informatique. Cela permet de mieux appréhender le contexte d'utilisation du système d'information mis en oeuvre. Si l'apport du Cloud est indéniable, notamment en terme de flexibilité d'accès à des ressources informatiques, la concentration accrue des données et le transfert de certaines responsabilités nécessitent d'analyser les grandes familles de risques induits. On peut ainsi définir quatre catégories de risques à évaluer :
- les risques spécifiques liés aux aspects organisationnels, techniques et juridiques du Cloud
- les autres risques qui ne sont pas spécifiques au Cloud mais qui se retrouvent dans tout projet informatique.
Lors d'une analyse de risques, et à plus forte raison dans le cadre du Cloud, il faut avoir à l'esprit trois éléments de contexte :
- un risque doit toujours être analysé dans un contexte global. Le risque pouvant être contrebalancé par d'autres enjeux (économies, gains, délais...)
- le niveau de risque peut varier de façon significative selon le type d'architecture de Cloud pris en considération
- lorsque les risques sont transférés à un prestataire de service de Cloud, la prise en compte de ces risques par le prestataire, sous forme de service à valeur ajoutée, doit être intégrée dans le contrat.

NEUF PRINCIPAUX RISQUES IDENTIFIÉS

Les risques liés à l'utilisation du Cloud Computing doivent être pris en considération comparativement aux risques encourus par les environnements « traditionnels ».

RISQUE 1 : LA PERTE DE MAÎTRISE ET/OU DE GOUVERNANCE
Criticité : ***
Concerne : Cloud externe
Comme dans toute externalisation informatique traditionnelle, l'utilisation de services d'un prestataire Cloud se traduit d'une certaine manière par :
• un renoncement au contrôle sur son infrastructure
• la perte de la maîtrise directe du système d'information
• une gestion et une exploitation opaques.

RISQUE 2 : DES DÉFICIENCES AU NIVEAU DES INTERFACES ET DES APIs
Criticité : *
Concerne : Cloud interne et Cloud externe
Le niveau de portabilité actuel des services, des applications et surtout des données est encore peu probante : il y a peu de garanties sur les outils, les procédures, les formats de données et les interfaces de services. En cas de réversibilité ou de migration vers un autre fournisseur de services Cloud, les opérations peuvent être rendues très complexes, longues et coûteuses. En cas d'impossibilité de pouvoir revenir en arrière, le risque est élevé de se trouver captif d'une offre particulière.
D'autre part, le manque de clarté des spécifications des interfaces de programmation (APIs), leur pauvreté et le peu de contrôle à portée des clients sont autant de facteurs de risques supplémentaires. Les risques de compromissions liés à un dysfonctionnement des interfaces ou à des altérations de données sont donc à prendre en considération.

Les fournisseurs de services du Cloud proposent un ensemble d'API dont les clients se servent pour gérer et interagir entre leur SI et les services dans le Cloud. L'approvisionnement, la gestion, l'orchestration et le contrôle sont tous réalisés par le biais de ces interfaces.
La sécurité et la disponibilité des services du Cloud dépendent de la sécurité de ces APIs et de la qualité de l'intégration.
Toute API implique un risque potentiel de sécurité et même de rupture. Un problème au niveau de ces interfaces conduit à une perte totale ou partielle de service pour le client.
Ceci est vrai pour les Cloud publics et hybrides, car le SI de l'entreprise est à la fois en interne et dans le Cloud.

RISQUE 3 : CONFORMITÉ(S) ET MAINTIEN DE LA CONFORMITÉ
Criticité : **
Concerne : Cloud externe
Le contexte protéiforme du Cloud génère de nombreuses questions liées aux aspects règlementaires et juridiques.
Et notamment :
• la responsabilité des données et des traitements
• la coopération avec les entités légales et de justice (des différents pays)
• la traçabilité de l'accès aux données aussi bien dans le Cloud, que lorsque ces données sont sauvegardées ou archivées
• la possibilité de réaliser des contrôles et des audits sur le respect des modes opératoires et des procédures
• le respect d'exigences réglementaires métiers.
De plus, lorsque des investissements initiaux ont été réalisés, lorsque des certifications ont été acquises ou des seuils de conformité atteints avant le passage sur le Cloud, toute dérive doit être détectée et une remise en conformité doit être recherchée. L'impossibilité d'effectuer des contrôles, voire des audits formels (ou leur non réalisation) risque alors de devenir problématique.
De plus, certains types d'infrastructure rendent impossible le respect de critères normatifs (PCI DSS et Cloud public).

RISQUE 4 : LOCALISATION DES DONNÉES
Criticité : ***
Concerne : Cloud externe
La dématérialisation des données sur des sites physiques de stockage différents peut conduire à un éclatement des données et une répartition dans différents pays. Un manque de maîtrise de cette répartition géographique est susceptible de provoquer le non-respect de contraintes réglementaires liées à la localisation des données sur le territoire d'un Etat.

RISQUE 5 : SÉGRÉGATION / ISOLEMENT DES ENVIRONNEMENTS ET DES DONNÉES
Criticité : ***
Concerne : Cloud externe
La mutualisation des moyens est l'une des caractéristiques fondamentale du Cloud. Mais les risques afférents sont nombreux, souvent liés aux mécanismes de séparation :
• L'étanchéité entre différents environnements utilisateurs ou clients est une condition sine qua non afin de garantir, a minima, la confidentialité des traitements
• L'isolation des données sous leurs différentes formes (stockage, mémoire, transmission et routage, ...) : elle est réalisée au moyen de différents services de sécurité ou techniques de sécurisation, telles que le contrôle d'accès et le chiffrement
• L'allocation des ressources : la monopolisation de ressources matérielles par un environnement utilisateur ou client ne doit pas être possible au détriment de la disponibilité ou, à moindre échelles, de la diminution des performances des environnements voisins.
Dans le cas d'un environnement partagé entre plusieurs "clients locataires", deux sortes d'attaque sont possibles, de type "guest-hopping" et contre les hyperviseurs.

LES VERTUS DE LA CERTIFICATION SAS 70

Créée par l'American Institute of Certified Public Accountants, la norme SAS 70 concerne les entreprises qui font appel à des fournisseurs spécialisés pour externaliser leurs services. Elle se caractérise par des audits indépendants réalisés par des tiers et des vérifications des processus sur site.
SAS 70 comporte deux niveaux (Type I et type II). Le premier porte sur la description des activités de la société et sur la pertinence des contrôles. Le deuxième niveau évalue leur efficacité à travers des tests dont les résultats sont publiés dans le rapport SAS 70 (type II).

Avantage-clé pour le fournisseur : éviter de multiples audits réalisés régulièrement par ses différents clients. C'est également un moyen important de différenciation commerciale.
Pour les entreprises-clientes, et en particulier celles soumises à la loi Sarbanes-Oxley, la certification SAS 70 garantit notamment la conformité et le « bon ordre » de leurs fournisseurs. (Source : Wikipedia)

RISQUE 6 : PERTE ET DESTRUCTION MAÎTRISÉE DE DONNÉES
Criticité : ***
Concerne : Cloud externe
Les pertes de données ne sont pas spécifiquement liées au Cloud, et les deux grandes familles de risques sont :
• les pertes liées à des problèmes lors de l'exploitation et la gestion du Cloud ;
• un défaut de sauvegarde des données gérées dans le Cloud.
S'ajoutent des risques liés à la non suppression de données (celles à ne pas conserver). En effet, une donnée peut exister logiquement sous les quatre formes suivantes – et bien plus au niveau physique – : les données en ligne (on-line) ou hors ligne (off-line), et les données sauvegardées (souvent en plusieurs versions) ou archivées (parfois en plusieurs versions).
Lorsqu'une demande de suppression d'une donnée située dans le Cloud est émise, cela doit se traduire par une suppression réelle, mais pas nécessairement sous toutes ses formes. En revanche, lorsqu'une demande de suppression définitive d'une donnée est émise, suite à une rupture contractuelle par exemple, ou pour des raisons légales, la suppression doit être effectuée sur toutes les formes que peut prendre cette donnée. Avec la répartition/dissémination des données il est nécessaire de retrouver toutes les instances de cette donnée, ce qui peut s'avérer être une tâche complexe dans le cas de multiples localisations et de la réutilisation des ressources matérielles. Lors d'une suppression sur disque, les données doivent être non seulement désallouées, mais aussi nettoyées (écrasement par motif), ceci afin de ne pas révéler ces anciennes données en les rendant accessibles au suivant à la prochain réallocation de disques au sein du Cloud.

RISQUE 7 : RÉCUPÉRATION DES DONNÉES
Criticité : *
Concerne : Cloud externe, Cloud interne
Il est indispensable d'avoir la garantie de disposer des moyens pour la récupération de données en cas de problèmes autres que les cas de non-disponibilité. La récupération doit pouvoir s'effectuer dans conditions de délais respectant les contraintes exprimées et les besoins métiers. La dissémination des données doit toutefois être effectuée de façon transparente pour l'utilisateur du Cloud.

RISQUE 8 : MALVEILLANCE DANS L'UTILISATION
Criticité : **
Concerne : Cloud externe, Cloud interne
Les architectures de type Cloud sont gérées et exploitées par des personnes disposant de privilèges élevés et qui sont donc à risque élevé. Des dommages peuvent être causés par ces spécialistes techniques. Les risques d'accès non-autorisés aux données ou d'utilisation abusive doivent être pris anticipés. Les dommages causés par des administrateurs système du Cloud - même s'ils sont rares - s'avèrent plus dévastateurs que dans un environnement informatique classique. Des procédures et des moyens sont nécessaires tant pour les phases de prévention et de détection, que pour les phases de protection et de réaction.

RISQUE 9 : USURPATION
Criticité : ***
Concerne : Cloud externe, Cloud interne
Les risques d'usurpation d'identité sont de deux natures :
• L'usurpation de service offert par l'architecture Cloud : il peut s'agir de services similaires, voire identiques, offerts par d'autres offreurs ou en d'autres points du Cloud pour d'autres clients. A l'extrême, on peut se retrouver confronté à des problématiques telles que celle du phishing (hameçonnage).
• L'usurpation d'identité d'utilisateurs ou de clients des services du Cloud : il peut s'agir d'attaques liées au vol de l'identité d'utilisateurs de services suite à des déficiences dans les mécanismes d'authentification. De faux clients utiliseraient de façon indue des ressources, voire accèderaient aux données des clients légitimes.
Dans les deux cas, la faiblesse de l'identification et de l'authentification laisserait la porte ouverte à ces attaques.

LIMITES DU TRANSFERT DE RISQUE
Le transfert de risque du client au prestataire de services de type Cloud ne peut pas être total. Si un risque conduit à la disparition d'une entreprise, à des atteintes sérieuses à sa réputation ou à des conséquences juridiques graves, il sera difficile voire impossible, pour quelque partie que ce soit, de compenser ces dommages. En définitive, on peut déléguer la responsabilité mais pas s'en décharger complètement.

SECURITE LOGIQUE

SÉCURITÉ DES SERVEURS VIRTUELS
Le Cloud Computing s'appuie fortement sur les technologies d'abstraction de services.
Dans le cadre d'un modèle IaaS, c'est la virtualisation de serveurs qui fournit cette abstraction; l'élément de base, visible ou non, étant une machine virtuelle (VM) sur un hyperviseur.
L'hyperviseur héberge également une VM particulière que nous appellerons de manière générique la « partition de gestion » (le vocabulaire varie selon le fournisseur). Elle permet d'administrer l'hyperviseur, de gérer le matériel et les ressources virtualisées.
Généralement on discerne les bonnes pratiques de sécurité liées à la virtualisation en deux familles.
En premier lieu, il s'agit de sécuriser les systèmes en assurant une gestion des mises à jour de sécurité. La mise à jour de l'hyperviseur et de la partition de gestion, a priori à la charge de l'hébergeur, conduit dans la plupart des cas à un redémarrage du serveur. Pour éviter que les VM soient indisponibles durant l'opération, un mécanisme de déplacement automatique des VM vers un autre serveur est possible, voire recommandé.

La sécurisation des systèmes suppose également la réduction des surfaces d'attaque, en fixant au strict minimum les services de la « partition de gestion ». On protège également les fichiers des disques virtuels par du contrôle d'accès, de l'audit, voire du chiffrement. Idéalement, on agit conformément aux recommandations des fournisseurs de l'hyperviseur (configuration des disques virtuels, installation de composants d'intégration dans les VM, etc.) et des OS, en mettant en place un contrôle de conformité automatisé.

La seconde famille de bonnes pratiques concerne la notion d'isolation : isolation des flux réseaux, isolation des VM par niveau de sécurité, délégation de l'administration, affectation de quotas d'usage des ressources par les VM. L'infrastructure de type cloud - pour être efficace et rentable - doit automatiser la plupart des contraintes évoquées précédemment, en plus des processus liées à l'administration, la supervision et l'allocation automatique de ressources.

BONNES PRATIQUES DE CONFIGURATION DES MACHINES VIRTUELLES
• L'entreprise cliente sera attentive au fait que le Cloud provider devra :
• Utiliser des disques durs virtuels de taille fixe
• Protéger les disques durs virtuels et les snapshots par des ACL sur le disque
• Décider de la mémoire allouée à chaque machine virtuelle
• Imposer des limites sur l'utilisation du processeur

• Concevoir le réseau virtuel de façon à isoler le trafic réseau en fonction des besoins
• Limiter le nombre de disques durs virtuels en fonction des besoins
• Sécuriser le système d'exploitation des machines virtuelles selon les recommandations de l'éditeur
• Configurer les antivirus, pare-feu et logiciels de détection d'intrusion dans les machines virtuelles
en fonction de leur rôle
• S'assurer que, avant sa (re)mise en production, une machine virtuelle est à jour en termes de versions et de mises à jour de sécurité de tous les composants logiciels qu'elle héberge
• Installer les composants d'intégration de l'hyperviseur, de façon notamment à s'assurer que les machines virtuelles ont une horloge juste (pour les audits)

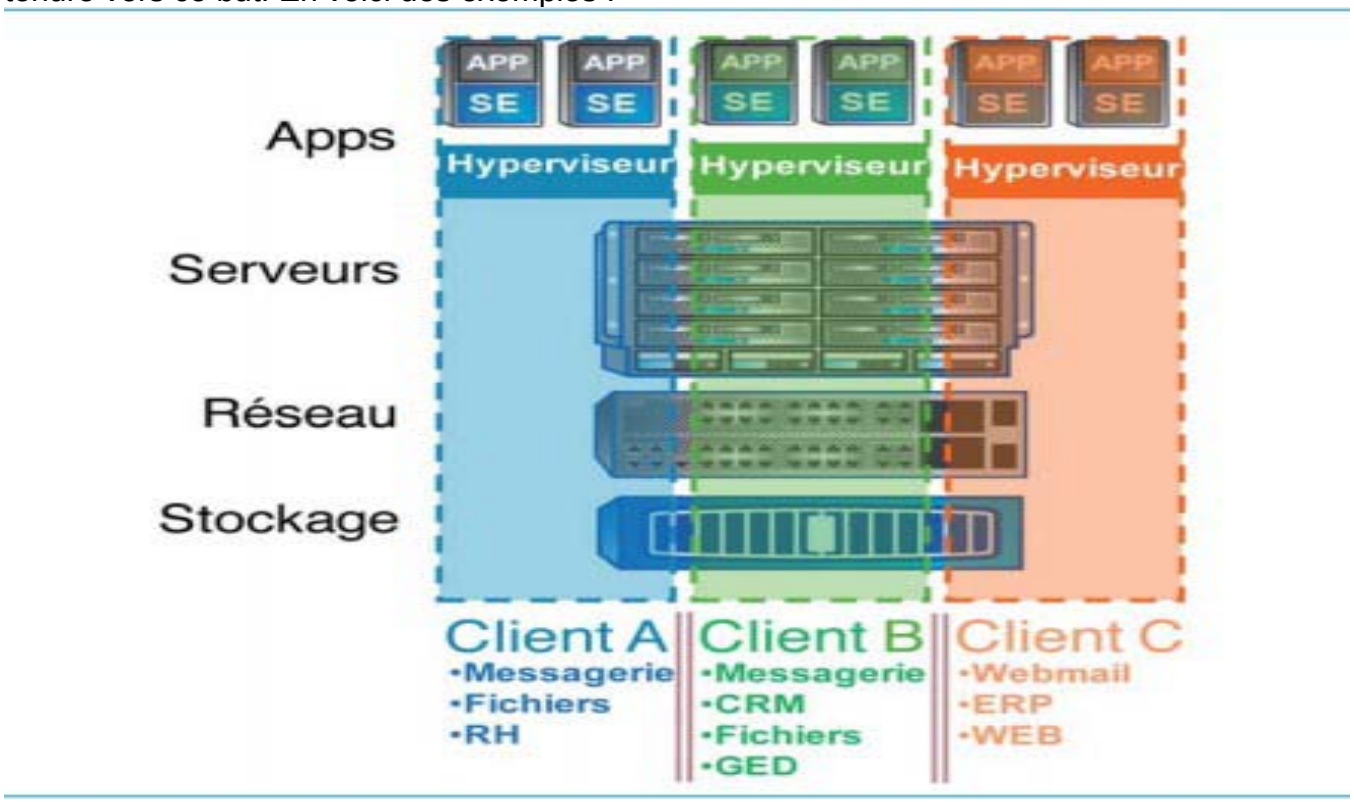
LA COLOCATION SÉCURISÉE

La colocation sécurisée consiste en l'hébergement sur le Cloud des applications et données de multiples clients (sociétés, organisations, entités métier…) au sein d'une seule et unique infrastructure physique, mutualisée, tout en respectant la sécurité, notamment au sens de la confidentialité.

A juste titre, les sociétés-clientes du Cloud veulent être rassurées sur le fait que leurs données et traitements seront bien isolés et protégés des autres environnements hébergés sur l'infrastructure partagée. C'est souvent une obligation légale, par exemple lorsqu'une société stocke des numéros de cartes bancaires ou des données personnelles, médicales…

Comment essayer de satisfaire ces deux impératifs de confidentialité et d'efficacité pour les infrastructures Cloud, et à tous les niveaux : machines virtuelles, serveurs hôte, réseaux (Ethernet et SAN) et stockage ?

En plus d'appliquer rigoureusement les bases de la sécurité d'un système d'information mutualisé (planification rigoureuse des droits d'accès, des privilèges administrateurs, sécurisation des mots de passe, etc.…), certaines techniques ou architectures permettent de tendre vers ce but. En voici des exemples :



Le chiffrement

Le chiffrement est a priori séduisant, notamment la méthode classique à base de clé publique/clé privée : seul le destinataire de l'information peut déchiffrer la donnée qui lui est destinée avec sa clé privée, connue de lui seul, mais pas du fournisseur de la solution Cloud et moins encore d'un autre colocataire. C'est une méthode très sécurisée (selon la taille de la clé) et sélective car on peut choisir de ne chiffrer que ce qui le nécessite.

Toutefois le chiffrement impose certaines réflexions quant à son implémentation. Notamment dans le cas où des traitements sont nécessaires (calcul, indexation, sauvegarde), pouvant obliger à la manipulation de données décryptées.

Solutions d'étanchéité logiques

Faire appel à des solutions d'étanchéité logiques permet de fournir les ressources à des groupes différents d'utilisateurs en toute sécurité.

Au niveau des VM, on peut utiliser un firewall virtuel sur la machine hôte qui cloisonne les VMS ; les VLANs permettent de cloisonner le trafic réseau sur Ethernet ; des partitions virtuelles de stockage apportent l'étanchéité dans la baie de stockage.

Différentes approches sont possibles : on peut retenir la solution la plus pertinente et mature sur chaque couche (selon une approche « best of breed » : la meilleure de sa catégorie), ce qui assure une certaine indépendance dans le choix de chaque solution, mais nécessite d'être certain de la qualité de l'intégration des différentes solutions de sécurisation de chaque couche. Comme souvent, ce n'est pas parce que chaque couche est sécurisée que l'ensemble le sera (attention au maillon faible et à l'interfaçage entre les différentes couches).

Une autre approche consiste à retenir une solution d'infrastructure sur étagère, proposée par un fournisseur unique ou un ensemble de fournisseurs. On perd en indépendance, car les différents composants (serveur, réseau, stockage) sont imposés, mais on gagne en intégration et en sécurisation. En effet, pour simplifier les déploiements de solutions mutualisées et pour en améliorer la confidentialité, certaines sociétés se sont alliés, ont co-réalisé et co-validé des solutions « tout-en-un » et/ou des guides de conception complets qu'ils mettent à disposition des fournisseurs de solution Cloud.

Avantage de cette dernière approche : l'étanchéité est assurée logiquement et de bout en bout, de l'application (la VM) aux disques (la baie de stockage mutualisée, cloisonnée en partitions virtuelles étanches), en passant par le réseau, afin de ne jamais mettre en danger les informations sensibles.

SEGMENTATION RÉSEAU

La segmentation réseau des machines virtuelles (VM) doit parer aux risques classiques de tout serveur, mais également à des risques liés à la colocation dans le cas d'un Cloud public.

Les risques classiques

Il faut appliquer les mêmes règles dans la virtualisation que dans une architecture physique :

• Cloisonner les différents rôles (serveurs frontaux, données, applications, pré-production …) sur des VMdifférentes via des VLAN différents (réseau dédié à une VM ou a un rôle) entre le serveur physique et l'infrastructure du client

• Mettre en place des briques de sécurité (firewall, reverse proxy …) qui assurent les rôles de :

- Routage inter-VLAN : pour que les VM communiquent sur des ports applicatifs spécifiés
- Filtrage (analyse port source/destination)
- Sécurité applicative (vérification protocolaire)

Administrer ses VM via un réseau dédié pour superviser, mettre à jour et ainsi ne pas passer par le réseau frontal/public.

La politique de sécurité mise en place dans l'architecture Cloud doit être appliquée sur la durée avec un contrôle permanent et une mise en oeuvre de bonnes pratiques au quotidien : procédures d'exploitation, tests d'intrusion …

Les risques accentués par le Cloud, liés à la multi-location :

La colocation et le partage de l'infrastructure entre plusieurs clients engendrent des risques accrus et nécessitent un renforcement de la politique de sécurité.

Chiffrer les sauvegardes : alors qu'il est naturel de penser à l'implémentation des protocoles de production chiffrés comme le passage en HTTPS pour les sites Web ou Intranet, il est moins commun de penser à la protection des tâches de plus bas niveau Conflits et usurpation d'adressage : les machines étant virtuelles, il est plus facile dans ce contexte de générer des conflits d'adressage.

Ainsi, une attention particulière doit être portée à la liste des personnes ayant un droit d'administration sur le Cloud. Cloner une instance déjà présente sans prendre en compte ces considérations peut être une source de problème

SÉCURITÉ DE L'INTERFACE D'ADMINISTRATION

L'accessibilité aux interfaces d'administration via une vulnérabilité applicative expose aux risques d'une coupure partielle ou totale du service ou à une perte irrémédiable des données. Par cet accès, l'introduction de virus ou de vers peut également détériorer les applications, faciliter la corruption des données ou nuire à l'image de marque du service.
Les solutions préventives consistent en la mise en place d'équipements de filtrage (pare-feu, proxy, sondes IPS/IDS…) et de solutions antivirus afin de contrôler la légitimité des requêtes entrantes et ainsi garantir l'intégrité des données hébergées. La planification de tests de vulnérabilités et d'intrusions doit être régulière et fréquente.
Le développement des applications doit être soumis à des audits de codes réguliers, et à l'implémentation de règles et contrôles des données.

Authentification

L'accès aux interfaces d'administration du Cloud Computing pourrait permettre à une personne mal intentionnée de provoquer une coupure de service ou de corrompre les données hébergées.
Si l'accès authentifié n'est pas clairement identifié, alors il sera impossible de pouvoir tracer la connexion et la modification des données ou du service qui en résulte. L'authentification doitapporter une preuve de l'identité si on veut pouvoir enquêter sur d'éventuels accès suspects.
Une vulnérabilité provenant d'erreur, de faille « humaine » ou «d'hameçonnage» dans le processus d'authentification peut aussi être exploitée. Celle-ci pourrait donner des accès de type «administrateur » à l'architecture Cloud Computing et entraîner une corruption de la plate-forme.
Les bonnes pratiques en la matière sont :
• La mise en place de mécanismes d'authentification forte (reposant sur deux facteurs ou plus) : identifiant, mot de passe, accès par jeton, certificat électronique, contrôle biométrique ...
• L'identification de l'authentification afin de disposer d'une traçabilité des accès
• La journalisation des authentifications réussies ou échouées
• La stricte application d'une politique de sécurité : changement des mots de passe tous les mois, politique de mots de passe complexes, formation du personnel…

Sécurisation des accès

Pour maitriser la sécurité de bout en bout, il faut sécuriser les éléments constituant la plate-forme Cloud, mais également l'accès à cette plate-forme.
Dans le cas d'un accès aux services hébergés sur le cloud par internet, le serveur (VM) est nativement vulnérable puisqu'il est directement exposé sur la Toile. Deux solutions de sécurisation peuvent être appliquées :
• inclure des briques de sécurité type Firewall (ouvre les ports applicatifs nécessaire), IPS ou IDS (détection et protection d'intrusion) entre l'infrastructure cloud et le client mais aussi éventuellement au sein de l'architecture serveur, entre serveurs front office et serveurs back office.
(cette dernière solution n'est possible que dans les environnements de cloud privés dans lesquels les serveurs n'ont pas d'adresse IP publique)
• sécuriser chaque serveur virtuel par un firewall applicatif installé sur l'OS (ou IPS, IDS applicatif). Cela suppose néanmoins une gestion lourde des règles d'accès avec internet et entre serveurs virtuels.
Ce type d'accès n'est envisageable que pour des serveurs hébergeant des données publiques (serveur FTP public, site web …) peu sensibles pour l'entreprise.
Si le serveur héberge des services privés de l'entreprise (ERP, CRM, intranet …) et constitue alors une extension du SI, le serveur ne doit pas être visible d'internet et des solutions de connexions dédiées doivent impérativement être envisagées, telles que :

• Connexion VPN privée : l'accès aux serveurs du cloud se fait via des liaisons dédiées (fibre, xDSL, multi-opérateur …) entre le cloud et l'utilisateur
• Connexion VPN internet : l'accès aux serveurs du cloud se fait via une connexion sécurisée par des mécanismes de chiffrement et d'identification (IPSEC ou TLS) montée entre le cloud et l'utilisateur, via le transit internet.

Accessibilité
Quel que soit le type de connexion au cloud, dédiée ou via Internet, il faut s'assurer que le service hébergé reste joignable par les utilisateurs. L'accessibilité aux serveurs doit être ajustée au niveau de disponibilité de ceux-ci. Tout comme la redondance offerte par les offres cloud, la joignabilité de ceux-ci doit donc être renforcée par une redondance à tous niveaux. En effet, une infrastructure cloud ultra-disponible ne sert à rien si l'accès ne l'est pas :
• Pour des connexions via internet :
- Il faut s'assurer que le fournisseur de l'offre cloud dispose d'une présence internet redondée sur plusieurs sites
- Et que ces accès internet sont fournis par plusieurs opérateurs ou points de peering
• Pour des connexions dédiées :
- Il faut privilégier une connexion multi-opérateur qui permet de basculer d'un opérateur à l'autre en cas de défaillance
- Idéalement, chaque lien devrait être supporté par une technologie différente xDSL, fibre, BLR …
- La collecte des flux doit se faire sur au moins deux data center : en cas de défaillance du premier, l'accès aux machines est toujours assuré par le data center secondaire.

Les briques de sécurité (firewall de constructeurs différents par exemple …) doivent être également redondées. Il en va de même pour les briques de publication de services (répartition de charge, …) .
Les administrateurs du Cloud Computing doivent être certains de se connecter sur les bons serveurs pour exécuter leurs taches d'administration, sans quoi des informations sur la sécurité de l'infrastructure pourraient être récupérées et utilisées à mauvais escient. Pour se prémunir de ces risques, il convient de :

- Mettre en place d'un protocole de sécurisation du transport des données avec un chiffrage de celles-ci (ex : TLS)
- Instaurer un procédé d'identification du serveur (ex : certificat électronique)
- Filtrer les accès, par un équipement de sécurité type pare-feu à inspection de paquets.
- Rédiger une charte d'utilisation du système informatique (ex : prise de conscience de l'outil informatique comme un point d'entrée dans l'entreprise)
- Appliquer une politique de contrôle stricte des utilisateurs (ex : contrôle de l'installation de logiciel tiers sur la plate-forme, surveillance des accès, journalisation des actions ...).
- La performance des VM peut être altérée si les équipements saturent à cause d'un utilisateur, impactant aussi sur les autres utilisateurs.

Pour éviter cela, il faut adapter le dimensionnent nominal des environnements sur le Cloud. Si l'application peut dès le début supporter une croissance horizontale, c'est-à-dire une multiplication des machines qui traitent le flux (comme de la répartition de charge par exemple) alors il est préférable d'avoir dès le début deux petites machines plutôt qu'une grosse. Ces instances ne seront probablement jamais sur un même socle physique. Ainsi, si un pic de charge local dans le cloud vient affecter une instance, la seconde sera la plupart du temps épargnée. Par ailleurs cette topologie permettra - en cas de forte charge - de multiplier les instances en fonction du besoin. Les prestataires proposent ici des solutions de publication des applications clefs en main.

Adaptabilité aux pics de charge
Une forte charge non prévue sur un des services hébergés sur l'infrastructure Cloud Computing risque d'entraîner une dégradation des performances de ce service. Pour éviter cela, on met en oeuvre un mécanisme de flexibilité des ressources permettant d'adapter la plate-forme aux besoins en un minimum de temps et d'efforts.

Impact de la gestion des mises à jour de sécurité sur la certification

La gestion des mises à jour de sécurité est nécessaire pour certains types de certification. Ne pas les installer équivaudrait plutôt à perdre une telle certification. Par exemple, les solutions d'IaaS privées incluent obligatoirement une gestion automatisée des mises à jour. De même, un des avantages des offres de SaaS publics est justement de déléguer au fournisseur la gestion des mises à jour, et celui-ci doit s'engager sur cette gestion et les délais d'application des mises à jour.

Toute modification du socle technique sur lequel repose la solution Cloud doit être communiquée aux clients, pas forcément en temps réel mais avec une périodicité bien établie.

En cas de modification majeure d'un élément logiciel (remplacement d'une brique par une autre), l'homologation doit être repassée. En revanche, en cas de montée de version ou d'installation de patch, sur une solution logicielle donnée, cette opération ne nous semble pas obligatoire.

Rappelons quand même qu'une homologation est généralement accordée pour une durée bien précise. Le client vérifiera que son fournisseur reste bien à jour de ses homologations.

DOCUMENT 4

Cloud privé, le beurre et l'argent du beurre pour la direction financière

Économies, flexibilité, rapidité.... Les vertus du Cloud ne sont plus à démontrer, même si de nombreuses entreprises hésitent encore à sauter le pas, en particulier dans les fonctions sensibles comme la finance - et la trésorerie. Pour des raisons le plus souvent liées à la sécurité, qu'elle soit opérationnelle, ou qu'elle porte sur la confidentialité de certaines données, elles préfèrent conserver leurs propres infrastructures et ressources. Alternative possible, la privatisation du Cloud permet de bénéficier, pour un surcoût minime par rapport au Cloud public, du meilleur des deux mondes.

Le Cloud Computing a le vent en poupe, c'est indéniable. En quelques années, ce modèle à la fois technique et économique, qui permet de payer des ressources à l'utilisation - qu'il s'agisse de puissance de calcul, de bande passante réseau, de capacité de stockage mais aussi de progiciels en mode SaaS - a conquis de nombreuses entreprises. À l'intérieur desquelles la direction financière n'est pas la dernière à s'intéresser à cette alternative économique, par rapport au couteux TCO d'infrastructures possédées en interne, toujours difficiles à faire évoluer, et jamais à temps.

Mais ces mêmes directions financières se montrent en revanche rétives à l'utilisation, pour leur propre compte, de ces solutions de Cloud Computing. Elles ne manquent pourtant pas sur le marché, qu'il s'agisse de versions de PGI (progiciel de gestion intégré) ou même d'outils plus spécialisés, par exemple pour les trésoriers. Selon Markess International, le domaine Finance (comptabilité, trésorerie…) arrive tout de même en troisième position en termes de pénétration du SaaS dans les entreprises, derrière les domaines Communication d'entreprise et Ressources Humaines. On constate tout de même que les applications ERP et de Business Intelligence ne sont encore que rarement concernées.

Une des raisons de ce retard à l'allumage, provient certainement de la manipulation potentielle de données critiques - soit sur le plan opérationnel (puis-je prendre le risque d'une indisponibilité du système au moment d'une clôture de bilan), soit sur celui de la confidentialité. On arguera ici, et ceci peut aussi permettre de convaincre les directions générales de sauter le pas, que les Datacenter (grands centres de traitement de données) des prestataires de SaaS sont de bien meilleurs bastions que les systèmes d'information de la plupart des entreprises.

Cloud privé = maîtrise de la gouvernance de ses ressources informatiques

Mais il existe une piste encore plus prometteuse : celle du Cloud dit privé **(*)**. Il s'agit, ni plus ni moins, que de privatiser un Cloud public - tout ou partie -, ou de faire construire, par un prestataire de type société de services, un Cloud à l'intérieur de bâtiments propriétaires ou encore, de le construire soi-même pour en utiliser les fondements techniques - virtualisation des serveurs notamment. Selon le choix retenu, les gains économiques seront plus ou moins importants. Dans les trois cas, l'entreprise client du Cloud privé, a les moyens d'imposer sa propre gouvernance des ressources informatiques, en particulier ses règles de sécurité concernant les données les plus critiques.

Les métiers - et par exemple les trésoriers d'entreprise qui sont déjà enclins à utiliser des solutions en mode SaaS mais ne dédaigneraient pas se rassurer sur le plan de la confidentialité des données manipulées - peuvent trouver un allié de choix dans ce mouvement vers le "tout Cloud privé "ou un "mix public - privé ". Il s'agit naturellement de la DSI. En effet, selon une enquête récente de Pierre Audoin Consultants, le Cloud privé est aujourd'hui le modèle privilégié par les DSI. Sur son panel de 200 décideurs informatiques, 71% préfèrent investir dans une solution Cloud de type privé, contre 13% en faveur d'une infrastructure hybride, et seulement 7% pour le Cloud public. Un plébiscite qui prend tout son sens si l'on considère que les DSI sont massivement à l'origine des projets de Cloud Computing dans les entreprises (67%), devançant leur direction générale dans ce type de décision (18%). Il faut dire que l'exemple de certaines entreprises, qui ont divisé par 20 leur nombre de serveurs - donc également les factures d'électricité, de loyer, etc. - a de quoi les faire réfléchir.

Les consultants voient plusieurs avantages au modèle dit privatif.

Premier avantage, cité par Syntec informatique, l'association des éditeurs et sociétés de services dans une étude réalisée sur ce thème, c'est la capacité d'ouverture de ce type d'infrastructure : elle peut facilement devenir communautaire, et par exemple accueillir les applications des partenaires de l'entreprise. Ce qui ne manquera pas de séduire doublement les spécialistes du domaine finance. Car cela facilite la construction de solutions "intégrées", structurées autour des échanges avec ces partenaires d'une part; Et qu'ils gardent la maîtrise technique totale de ces applications tierces d'autre part, grâce à la "recette" effectuée par leur DSI.

Le meilleur respect des règles de la gouvernance d'entreprise, notamment en ce qui concerne la politique de confidentialité. C'est l'avantage le plus évident. Mais attention ! Il s'agit d'une potentialité. Il ne faut pas imaginer que la seule existence d'un Cloud privé dans l'entreprise va faire naître une politique de sécurité et surtout son respect. Aux métiers de définir les priorités et de former.

Sur le plan juridique, le fait que le lieu des données/applications de l'entreprise soit connu de l'entreprise (et généralement à proximité), limitera considérablement les risques juridiques qu'au contraire, un Cloud public peut faire courir lorsque les serveurs du prestataire ne sont pas localisables - ou localisés.... dans un autre pays.

La réduction des délais de déploiement, la flexibilité et la consommation à la demande mieux maîtrisée viennent aussi renforcer la colonne atouts du Cloud privé

Mais quelques désavantages...

Reste tout de même des écueils, à connaître pour opérer le meilleur choix possible.

Le premier concerne l'investissement initial. Créer une infrastructure de Cloud privé, nécessite des dépenses de démarrage, que le client d'un Cloud public n'a pas à faire. On tempèrera tout de même cet argument pour le trésorier d'entreprise. Au moment où il se décide à opter pour tel ou tel type de Cloud dans une approche de type SaaS, l'essentiel de l'investissement en infrastructures est déjà réalisé par la DSI. L'impact financier de son choix peut donc être regardé comme marginal.

La réversibilité peut proposer d'autres problèmes. Dès lors qu'on externalise des données, même sur un Cloud privé géré par un prestataire de services, la question de leur récupération peut se poser. Car les fournisseurs de services appliquent des normes, et se servent d'outils qui ne font pas preuve de neutralité. Autrement dit, et parfois sans le savoir, car les métiers considèrent implicitement que le concept de Cloud privé est porteur d'une maîtrise technique totale, les données financières par exemple, peuvent devenir difficile d'accès. Paradoxal !!

Sans minimiser ces inconvénients, force est de constater que l'option Cloud privé, s'il ne faut pas la choisir automatiquement, mérite à tout coup qu'on s'y arrête un instant. Ne serait-ce, concernant le trésorier, que parce que les spécialistes convergent pour prédire que les grands ERP et solutions CRM finiront majoritairement sur ce type d'infrastructures. Il pourra donc s'avérer intelligent d'y être aussi, puisque son progiciel de trésorerie a des interactions fréquentes avec les dits grands progiciels de gestion. De toute façon, il parait loin le temps où les utilisateurs, même ceux de la fonction finance, manquaient de répondant face aux délais imposés par la DSI pour déployer telle ou telle solution, telle ou telle fonctionnalité. Avec "l'informatique dans le nuage", dans toutes ses versions y compris hybrides, c'est paradoxalement l'horizon qui s'éclaircit pour la mise en œuvre rapide des solutions nécessaires au business.

(*) *Définition : Le Cloud privé (interne ou privatif) consiste à mettre en place un réseau informatique propriétaire ou un centre de données fournissant des services hébergés pour un nombre restreint d'utilisateurs. Les applications virtualisées « privées » sont soit administrées directement par l'entreprise (qui gère seule son infrastructure), soit mutualisées (un prestataire de confiance prend en charge une partie des services externalisés). Ce modèle est censé apporter les avantages du Cloud Computing « public » (ex : baisse des coûts liés à la virtualisation des applications dans le cas d'une infrastructure mutualisée) sans en présenter les inconvénients : en mettant l'accent sur la sécurité des données, sur le respect de la gouvernance d'entreprise et sur la fiabilité des services fournis. Les pplications/infrastructures hébergées restent disponibles en «libre-service », sont évolutives et modulables grâce à la proximité entre l'entreprise et son prestataire.*

Organisation territoriale de l'Etat

Mise à jour : 22 décembre 2015

Aux termes de la charte de déconcentration, la circonscription régionale est l'échelon territorial :

1° De l'animation et de la coordination des politiques de l'État ;

2° De la mise en oeuvre des politiques nationales et de l'Union européenne en matière d'emploi, d'innovation, de recherche, de culture, de statistiques publiques, de développement économique et social, et d'aménagement durable du territoire ;

3° De la coordination des actions de toute nature intéressant plusieurs départements de la région ;

4° De la conduite d'actions de modernisation des services déconcentrés dans les domaines de la simplification de leur activité administrative et de l'amélioration de leurs relations avec les usagers ;

5° De la définition du cadre stratégique de la politique immobilière des services déconcentrés de l'Etat.

Elle constitue également un échelon de programmation et de répartition des crédits de l'État ainsi que de contractualisation des programmes pluriannuels entre l'État et les collectivités locales.

L'administration régionale de l'Etat en « Région » est organisée autour de 8 structures :

- la direction régionale de l'environnement de l'aménagement et du logement (DREAL),
- la direction régionale de l'alimentation de l'agriculture et de la forêt (DRAAF),
- la direction régionale des entreprises, de la concurrence, de la consommation, du travail et de l'emploi (DIRECCTE),
- la direction régionale de la jeunesse des sports et de la cohésion sociale (DRJSCS)
- la direction régionale des affaires culturelles (DRAC)

placées sous l'autorité du préfet de région,

et :

- le rectorat ,
- la direction régionale des finances publiques (DRFiP)
- l'Agence Régionale de Santé (ARS).

A ces services s'ajoute un certain nombre d'agences ou d'établissements publics nationaux ayant une représentation territoriale ou qui concourent à la mise en oeuvre des politiques publiques au niveau territorial et dont la charte de déconcentration prévoit qu'ils conduisent leur action, sous la coordination du préfet, en cohérence avec celle des services déconcentrés des administrations civiles de l'Etat.

Sauf disposition législative contraire ou exception prévue par décret en Conseil d'Etat, la circonscription départementale, placée sous l'autorité du préfet de département, est l'échelon territorial de mise en oeuvre des politiques nationales et de l'Union européenne.

L'arrondissement est le cadre territorial de l'animation du développement local et de l'action administrative locale de l'Etat. Le sous-préfet d'arrondissement est le délégué du préfet de département dans l'arrondissement.

Les niveaux de service offerts par le cloud computing

Les services offerts à l'utilisateur ou à l'entreprise par le cloud sont extrêmement divers et répondent à des niveaux d'exigence très différents. Ceux-ci peuvent aller de la simple consultation de courriel depuis un poste distant de l'entreprise à l'utilisation intensive d'un groupe réservé de machines distantes pour exécuter une application distribuée (c'est-à-dire s'exécutant en parallèle sur plusieurs ordinateurs) demandant une puissance de calcul très importante (mesurée en giga/téra/péta flops) ainsi qu'un espace de stockage considérable (mesuré en téraoctets). Les solutions de cloud sont modulaires et permettent de définir très clairement la frontière entre les couches logicielles du modèle client-serveur que le client cloud (l'entreprise) souhaite conserver à sa charge et celles qu'il souhaite confier au prestataire de cloud.

De manière schématique, on peut distinguer trois niveaux de service (fig. 1) dans ce modèle en couches, qui fixent la frontière d'intervention du prestataire du cloud : le niveau 1 – où le client délègue tous les services au prestataire cloud – avec le logiciel en tant que service (Software as a Service, SaaS) ou les données en tant que service (Data as a Service, DaaS) ; le niveau 2 – où le client délègue la gestion des machines et des environnements de développement tout en conservant la maîtrise de la conception des applications – avec la plate-forme en tant que service (Platform as a Service, PaaS) ; et, enfin, le niveau 3 – où le client ne délègue que la gestion des machines – avec l'infrastructure en tant que service (Infrastructure as a Service, IaaS). La famille as a Service (aaS) représente la mise en connexion transparente d'un produit avec un utilisateur, quelle que soit la distance qui les sépare. Ce produit peut être un logiciel, une base de données, un système préconfiguré pour exécuter des applications internes ou directement le matériel au travers du mécanisme de virtualisation.

Le SaaS, un service de niveau 1

Le logiciel en tant que service (SaaS) est le modèle économique le plus utilisé aujourd'hui. Il fournit au client une solution complète et homogène. Le fournisseur de services propose d'accéder à des applications logicielles configurées, toujours dans leur version la plus récente. Les utilisateurs clients ne possèdent plus les applications mais s'y abonnent, selon le principe d'une facturation par utilisation. Ainsi, la société Microsoft propose une version cloud de sa suite bureautique *Office* pour quelques euros par utilisateur et par mois, à comparer au prix net du logiciel acheté (500 euros) dans une version donnée, beaucoup moins évolutive.

Depuis 2007, le marché des SaaS est en très forte croissance dans les entreprises. Avec la délocalisation des solutions informatiques proposées par le cloud, le coût pour l'entreprise englobe celui des licences des applications logicielles, de la maintenance du système et de l'infrastructure matérielle. Il est généralement moindre que celui qui est issu de l'acquisition des licences et d'un déploiement en interne. Cette réduction des frais s'accompagne de trois autres avantages : la rapidité de déploiement des solutions logicielles, la flexibilité (possibilité de passer d'une solution logicielle à une autre sans heurt) et l'adaptation à des demandes spécifiques (localisation, personnalisation d'une application propre à l'entreprise), et enfin la consommation électrique réduite puisqu'elle est répartie entre les utilisateurs.

Le SaaS présente toutefois des inconvénients majeurs. Le fait de délocaliser les données sur des machines appartenant à un prestataire de services entraîne par nature des soucis de confidentialité et de sécurité supplémentaires. Les protocoles d'authentification des utilisateurs vis-à-vis des serveurs distants font ainsi aujourd'hui l'objet de nombreuses recherches et des milliards d'euros sont dépensés pour garantir la sécurité des systèmes et en faire des systèmes de confiance.

Le DaaS, un service de niveau 1

Le Data as a Service (DaaS) est le service du cloud qui permet aux entreprises d'accéder à des bases de données distantes pour y lire et écrire des données. Le DaaS est un service de stockage de données qui offre aux utilisateurs de très fortes garanties d'intégrité (aucune perte ou altération de données ; politiques de sauvegarde quotidienne, hebdomadaire mensuelle et annuelle, sur supports persistants). Comme il peut s'agir de quantités de données énormes (plusieurs giga/téraoctets), les fournisseurs DaaS (quelques centaines à travers le monde) appliquent des tarifs de location fondés sur le volume, le type des données transférées, la politique et la fréquence des archivages. Dans certains cas, les clients sont facturés en fonction de la quantité de données qu'ils utilisent, en consultation comme en stockage. Dans d'autres, les données sont classées par type (financier, organisationnel, historique, géographique, etc.) et une valeur marchande est associée à chaque type. Les prestataires de service DaaS imposent souvent des quotas de transfert ainsi que des tailles d'espace de stockage. Le DaaS souffre des mêmes inconvénients que le SaaS et repose sur la capacité du prestataire cloud à offrir une qualité de service irréprochable (absence de pannes, débit de données suffisant, cohérence des bases de données, archivage, etc.). Une autre critique souvent formulée à l'encontre du DaaS est la nécessité de télécharger à chaque session de travail des données qui pourraient être facilement stockées sur la machine locale une fois pour toutes, mais qui courent le risque de devenir à la longue incohérentes avec la base de données de référence qui est, par nature, perpétuellement mise à jour sur le serveur distant.

Le PaaS, un service de niveau 2

La PaaS (Platform as a Service) est le service de cloud qui permet à l'entreprise de profiter des systèmes informatiques performants, configurés et maintenus par le prestataire cloud, pour y développer ses propres applications métier. La maintenance de ces applications est laissée à la charge de l'entreprise et le prestataire cloud gère la plate-forme (le système d'exploitation et sa sécurité, les bases de données, les applications serveur, les environnements de développement, etc.). Pour l'entreprise, PaaS revient à mettre à sa disposition un environnement totalement configuré mais dont l'infrastructure matérielle (le type d'ordinateur, de processeur, de quantité mémoire disponible, etc.) est masquée aux utilisateurs. Les services PaaS profitent amplement des progrès réalisés dans le domaine des systèmes d'exploitation qui rendent possible la virtualisation des machines, c'est-à-dire la possibilité de pouvoir faire cohabiter simultanément plusieurs systèmes d'exploitation sur la même machine physique et de partager les ressources matérielles coûteuses (processeur, mémoire, disque, périphériques, etc.). La virtualisation est une technologie matérielle et logicielle innovante permettant de mutualiser l'ordinateur physique. Elle fait l'objet de constantes améliorations.

Le IaaS, un service de niveau 3

L'infrastructure en tant que service ou IaaS (Infrastructure as a Service) est le modèle de cloud où le client prend à sa charge la majeure partie des services informatiques et ne fait que louer l'utilisation du matériel informatique. Le client développe les applications logicielles, les couches hautes (après virtualisation) des systèmes d'exploitation, les bases de données, les logiciels serveurs, etc. Le rôle du prestataire cloud IaaS est de proposer à ses clients un matériel virtuel le plus modulaire possible : les serveurs de calcul, les serveurs de stockage, les réseaux, les sauvegardes, etc. Les techniques de virtualisation permettent à l'entreprise cliente de disposer d'une infrastructure informatique (serveurs, stockage, réseau) localisée physiquement chez le prestataire. L'entreprise a accès à ces ressources matérielles comme si celles-ci faisaient partie de ses propres ressources. Elle se libère ainsi des contraintes d'occupation de surface, de climatisation et de dimensionnement électrique.

Cette mise à disposition quasi transparente du matériel au client est paradoxalement plus complexe à mettre en œuvre pour le prestataire cloud. Les degrés de liberté offerts aux clients impliquent en effet des contraintes de robustesse, de tolérance aux pannes et la nécessité de pouvoir répondre de manière ajustée à des sollicitations de diverse nature et sur plusieurs couches du modèle client-serveur. C'est tout l'inverse d'une solution cloud de niveau 1 où le prestataire de cloud maîtrise toute l'architecture logicielle et où l'interface avec le client ne se fait que dans la couche supérieure

DOCUMENT 7

Passer à la vitesse supérieure grâce au Cloud

Publication : 5 janvier 2016

La DSIC privilégie une nouvelle méthode de réalisation des applications, beaucoup plus réactive.
En quelques mois, de toute fin 2014 à novembre 2015, il a été ainsi possible de réaliser le logiciel traduisant la dernière réforme européenne du droit d'asile.
L'approche traditionnelle condamnait l'administration à ne pouvoir fournir une application qu'après plusieurs années de travaux, de réunions de pilotage associant tous les services concernés, de mois nécessaires pour passer des marchés... Entre temps, le besoin avait souvent déjà évolué ! Une nouvelle façon de travailler permet de réduire à quelques mois le temps de réalisation d'une application ? Voyons comment.

Une équipe intégrée MOA/MOE

L'équipe intégrée est composée de tous les métiers des systèmes d'information, maîtrise d'ouvrage (MOA) et maîtrise d'oeuvre (MOE). Elle associe ainsi urbanistes, architectes, développeurs et exploitants. Portée par le sens de l'engagement collectif, l'équipe intégrée travaille en mode collaboratif pour développer, valider et livrer des lots de fonctionnalités (valeur) en mode continu.
L'organisation se fonde sur une approche opérationnelle pour délivrer rapidement des fonctionnalités au « métier » (autrement dit la direction cliente). Le découpage des travaux entre de multiples équipes et les difficultés de coordination inhérentes sont ainsi évités.
Le développement de l'application est réalisé sur le modèle AGILE/DevOps, en phases itératives de 4 semaines contenant un lot de fonctionnalités à développer pour produire un sous-ensemble d'un produit fini, sur une infrastructure extensible prête à l'usage (CloudMI). Chaque phase nécessite un arbitrage des priorités par l'équipe intégrée pour livrer de la valeur au métier le plus rapidement possible. Ainsi, on évite les effets tunnel anxiogènes pour le métier tout en élevant le niveau de confiance par le partage régulier des résultats et de la proximité des acteurs du projet.

Automatiser au maximum

Avec le Cloud, la quasi-totalité des équipements et des services nécessaires au fonctionnement d'une salle machine peut maintenant être obtenu sur un simple clic. Ainsi la mise à disposition de machines est instantanée. Or tout cela passait il y a peu encore par une commande, l'attente de la livraison des équipements puis de leur installation par des équipes techniques partageant leur temps entre de multiples demandes. Il est même possible d'organiser la fourniture d'un service logiciel complet – un système collaboratif de type Wikipédia par exemple, ou encore une forge de développement – selon la même logique, en automatisant entièrement l'allocation des machines, l'installation des logiciels et leur paramétrage pour disposer sans délai du service souhaité.

La DSIC intègre cette technologie dans ses savoir-faire en l'adaptant aux contraintes des missions du service public. Cela devrait permettre à terme de déporter les grandes applications réglementaires vers des services logiciels de ce type, ouvrant la possibilité de configurer des machines à la demande pour, par exemple, pouvoir armer plus de guichets dédiés à une fonction (immatriculation des véhicules, titres de séjour...) lors des pics d'activité.

Ce mode de travail collaboratif est adopté de plus en plus largement par les entreprises, et bientôt les institutions, pour réaliser les systèmes d'information. Il y a dans la démarche apportée par le Cloud un véritable changement culturel qui bouscule nos habitudes. Désormais, les directions métier passent d'une logique de consommation d'un système réalisé par d'autres à celle de contributeur actif d'une application où elles sont pleinement investies. Les directions informatiques adaptent leurs compétences et leurs procédures pour devenir plus réactives et s'inscrire dans des projets pilotés par les besoins du métier.

DOCUMENT 8

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

SECRÉTARIAT GÉNÉRAL POUR LA MODERNISATION DE L'ACTION PUBLIQUE

DIRECTION INTERMINISTÉRIELLE DU NUMERIQUE ET DU SYSTEME D'INFORMATION ET DE COMMUNICATION DE L'ETAT

39/43 Quai André Citroën

75015 PARIS

Affaire suivie par : Xavier ALBOUY

Téléphone : 01 40 15 72 11

Mél. : xavier.albouy@modernisation.gouv.fr

REF : MICORE/SGN/BC/2015-242

Paris, le 22 décembre 2015

NOTE

à

MM. les préfets préfigurateurs des nouvelles régions

Objet : Réforme de l'organisation territoriale de l'Etat : intégration des opportunités du numérique et impact sur le système d'information de l'Etat

La réforme de l'organisation territoriale de l'Etat, dont les principes ont fait l'objet d'une communication gouvernementale le 31 juillet 2015, induit des transformations majeures dans le fonctionnement des structures actuelles, porteuses d'opportunité pour la performance de l'action publique, et nécessitant des mesures d'accompagnement ambitieuses.

A ce titre, l'évolution du système d'information de l'Etat et des offres d'outils numériques qu'il permet constitue un enjeu majeur. A minima, la continuité de l'action publique nécessite de décliner dans les outils et les organisations informatiques les changements d'organisation prévus dans les services déconcentrés de l'Etat. Par ailleurs, la future implantation sur plusieurs sites géographiques de la plupart des services régionaux nécessite, en complément de l'évolution des pratiques managériales, de développer les outils numériques favorisant le travail collaboratif en multi-site.

Les acteurs du Système d'Information et de Communication de l'Etat, sous la coordination de la Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'Etat (DINSIC), et en lien avec la mission de coordination de la réforme des services déconcentrés de l'Etat (MICORE) se sont mobilisés afin de définir une stratégie d'adaptation du système d'information et de communication de l'Etat à la réforme de l'Etat et permettre sa mise en œuvre.

Des travaux approfondis ont été conduits avec les équipes de préfiguration de Bourgogne-Franche-Comté, chargées par le Premier ministre d'expérimenter les nouvelles méthodes et nouveaux outils, afin d'aligner au mieux les travaux menés par les acteurs nationaux sur les besoins ressentis par les acteurs régionaux, et de permettre un enrichissement mutuel des démarches conduites.

24

Les travaux sont menés avec les principes directeurs suivants :

1. Parmi tous les besoins et idées identifiés, donner la priorité aux actions assurant la continuité de service et à celles ayant le plus d'impact sur la facilitation du travail dans des services multi-sites.
2. Laisser la place à l'expérimentation locale dans le cadre d'une stratégie nationale pilotée.
3. Engager une démarche d'amélioration progressive, se poursuivant au-delà du 1er janvier 2016, mais en permettant aux acteurs régionaux de disposer dès les premiers mois de 2016 d'un premier périmètre de solutions (qu'elles soient nouvelles, ou déjà existantes, en utilisant le levier de la mutualisation interministérielle)

Vous trouverez, annexé au présent courrier, un état des lieux de l'accompagnement « SI » de la réforme de l'organisation territoriale. Ce document s'adresse à tous les acteurs du système d'information de chaque service régional ; certains passages traitant de questions technique s'adressent plus spécifiquement aux services SI. Les orientations principales sont synthétisées dans des encadrés.

Le document présente, pour chaque domaine d'évolution du système d'information, des informations générales sur les orientations prises, les outils qui peuvent être mobilisés, leurs modalités de mise en œuvre, l'identification des interlocuteurs au sein des administrations centrales.

S'agissant d'un état de lieux de travaux qui se poursuivront dans les prochains mois, le contenu de ce document a naturellement vocation à évoluer, se compléter et se préciser. Des informations mises à jour seront rendues disponibles sur l'espace intranet dédié à la réforme territoriale : https://dsaf.pm.ader.gouv.fr/portail/reforme-territoriale.

Nous vous invitons à prendre connaissance de ces informations, à veiller à leur diffusion auprès des acteurs concernés dans les services régionaux, et à les utiliser pour mobiliser les leviers du numérique dès qu'ils pourront être mis au service des transformations organisationnelles et managériales que vous menez dans le cadre de la réforme territoriale.

Le coordonnateur national de la réforme des services déconcentrés de l'Etat

Jean-Luc NEVACHE

La secrétaire générale de la modernisation de l'action publique

Laure de la BRETECHE

Copies :
- M. le Directeur des services administratifs et financiers, Services du Premier Ministre
- M. le Directeur Général de l'administration et de la fonction publique
- M. le Secrétaire Général des ministères économiques et financiers
- M. le Secrétaire Général du ministère de l'intérieur
- M. le Secrétaire Général des ministères chargés des affaires sociales
- M. le Secrétaire Général du ministère de la culture et de la communication
- M. le Secrétaire Général du ministère de l'écologie, du développement durable et de l'énergie
- M. le Secrétaire Général du ministère de l'agriculture, de l'agroalimentaire et de la forêt
- M. le Secrétaire Général du ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche

2. Les outils numériques de partage d'information

Synthèse

Plusieurs types d'outils peuvent venir accompagner la mise en place des nouvelles organisations de services régionaux :

En matière d'outils de travail collaboratif : l'offre de chaque ministère et les perspectives d'offres interministérielles sont cartographiées. La mise en œuvre des outils doit nécessairement se faire dans le cadre plus large de projets d'évolution du management du travail collaboratif au sein des services régionaux.

Les solutions ministérielles de gestion électronique de courrier, quand elles existent, sont cartographiées ; une expérimentation est lancée pour évaluer l'opportunité et les modalités d'une solution interministérielle.

S'agissant des serveurs de partage de fichier, les modalités de décloisonnement des serveurs des anciennes régions fusionnées sont précisées ministère par ministère, afin de guider l'action des équipes techniques locales

Les offres ministérielles d'outils de partage de fichiers volumineux sont également cartographiées.

Hormis la visio-conférence et la web-conférence, d'autres outils numériques peuvent faciliter le travail entre agents d'un même service régional réparti géographiquement sur plusieurs sites :

Outils de travail collaboratif

Encore plus que dans le cas de la visio-conférence, une logique de développement du travail collaboratif axée uniquement sur la dimension « outil informatique » ne permet pas de tirer pleinement parti des opportunités liées au numérique, et génère un risque d'échec des projets correspondants. Les acteurs locaux sont donc invités à engager une réflexion sur l'évolution des pratiques de management du travail collaboratif, et de traiter ces évolutions comme des projets, dans le cadre desquels les outils décrits ci-dessous pourront être mis à profit.

Ces outils, accessibles via des navigateurs Internet, permettent le travail collaboratif sur des documents, leur partage, et son enrichis de fonction de collaboration (gestion de communautés, forums…)

Pour les besoins de travail collaboratif au sein d'un même ministère, les solutions suivantes sont déjà proposées au niveau national :

Ministère	Offre d'outils collaboratifs	Modalités d'accès à l'offre	Interlocuteurs
MCAS	SHARE POINT	Joindre le correspondant régional désigné au niveau de la direction concernée. Il est chargé d'assurer le relais et l'appui aux utilisateurs sur les outils collaboratifs.	Christian LIN : christian.lin@sg.social.gouv.fr Olivier THEBAUD : olivier.thebaud@sg.social.gouv.fr
MCC	Alfresco (expérimentation)	Offre de service sur la base du volontariat, dans le cadre d'une expérimentation.	Nicolas Joron nicolas.joron@culture.gouv.fr

MAAF	Sur base NUXEO, le ministère offre trois services : 1/ GEDSI : espace GED ouvert sur le RIE 2/ GEDNet : espace GED ouvert sur le RIE et sur Internet	Pour GEDSI: compte Agricoll actif indispensable, habilitation applicative requise, accès via RIE uniquement Pour GEDNet : Idem + Accès possible par internet + accès possible avec compte BDNU en alternative au compte Agricoll	Anthony Louis, anthony.louis@agriculture.gouv.fr
MEDDE	Alfresco MEDDE	Un formulaire à remplir sur l'intranet. Ouverture du site en 24h Toutes les informations sont publiées sur l'Intranet : http://intra.pssi.sg.e2.rie.gouv.fr/travail-collaboratif-alfresco-share-au-spssi-a3410.html	Gabor JABER : Psi1.Psi.Spssi.Sg@developpement-durable.gouv.fr
MEFI	Pas de solution actuellement disponible dans les DR. Travail lancé pour décloisonner l'accès aux applis directionnelles et centrales (RSP et outils collaboratifs).		Laure Patas d'Illiers (SG/DSI) pour mise en contact : laure.patas-dilliers@finances.gouv.fr
MI	OCMI	Une fiche détaillée de l'offre peut être demandée à la DSIC/SDI/BUA	Jean-Luc DAVID : jean-luc.david@interieur.gouv.fr

Pour les besoins d'échanges interministériels, la perspective accessible à court terme est d'étendre la solution proposée pour le niveau départemental au niveau régional, et qu'elle puisse être utilisée pour le travail interministériel. Cette solution procurée par le MEDDE est basée sur le produit Alfresco. Les services régionaux sont invités à lancer des expérimentations sur la base de ce produit, et à partager les retours d'expériences avec les acteurs nationaux du SI de l'Etat (DINSIC et DSI ministérielles) et les autres régions.

Gestion électronique de courrier

Le développement d'outils de gestion électronique de courrier est un besoin identifié récemment dans le cadre de la réforme de la carte territoriale. L'objectif exprimé par les acteurs locaux, est de permettre une circulation dématérialisée des courriers reçus et des projets de courriers à envoyer, dans le cadre du fonctionnement des services régionaux en multi-sites.

Certains les ministères disposent aujourd'hui d'une solution nationale de gestion électronique de courrier :

Ministères	Solutions disponibles	Modalités d'accès	Interlocuteurs
MAAF	GEDCourrier : espace GED ouvert sur RIE spécialisé dans la gestion de courriers entrants/sortants d'un service hiérarchisé	Compte Agricoll actif, solution accessible uniquement depuis le RIE	Anthony Louis anthony.louis@agriculture.gouv.fr
MCAS	Néant	-	-
MEFI	Pas de solution actuellement disponible dans les DR. Cependant le ministère travaille à décloisonner l'accès aux applis directionnelles et centrales (GEC)		Laure Patas d'Illiers (SG/DSI) pour mise en contact laure.patas-dilliers@finances.gouv.fr
MCC	Expérimentation pour la GEC (MAARCH à partir de la solution	Offre de service sur la base du volontariat dans le cadre de	Nicolas Joron nicolas.joron@culture.gou

	déployée en administration centrale), la solution e-parapheur est en cours d'élaboration chez l'éditeur.	l'expérimentation GEC.	v.fr
MEDDE	Ces services ne sont pas encore généralisé au sein du ministère	-	Psi1.Psi.Spssi.Sg@developpement-durable.gouv.fr
MI	MAARCH	La solution a fait l'objet récemment d'une généralisation dans toutes les préfectures dans le cadre de la mise en œuvre de l'ordonnance 2014-1330 « saisine par voie électronique », et dont les modalités de mise en œuvre ont été explicitées par le courrier n° 15-021819-D du 15 octobre 2015.	Odile FRASCHINI odile.fraschini@interieur.gouv.fr

La région Bourgogne-Franche-Comté débute une expérimentation d'utilisation d'une solution de gestion de courrier commune aux différents services déconcentrés, dans le contexte des implantations multi-sites des nouvelles directions régionales. Le retour d'expérience alimentera les réflexions sur l'opportunité, et les modalités d'une solution nationale.

Serveurs de partage de fichier

Ces serveurs (usuellement installés en Windows ou Linux, s'appuyant sur des annuaires Active Directory ou Samba) permettent de partager des fichiers au sein d'un même service. La fusion de services dans le cadre de la réforme territoriale pose la question de la mise en place de périmètres de partages plus étendus qu'auparavant.

Elle se pose à deux échelles : au sein d'un même ministère et en interministériel.

1) Comment permettre à des agents localisés sur plusieurs sites, ou aux services régionaux multi-sites, d'accéder et partager les mêmes fichiers partagés, en interministériel ?

Ce chantier complexe à traiter n'est aujourd'hui pas ouvert. En effet, les besoins d'échanges interministériels ont vocation à être couverts par les outils collaboratifs, abordés ci-dessus.

2) Comment permettre à des agents d'un même ministère localisés sur plusieurs sites, ou aux services régionaux multi-sites, d'accéder et partager les mêmes fichiers, en intra-ministériel ?

Techniquement parlant, cela nécessite potentiellement de traiter la fusion des domaines Active Directory ou Samba (ou la mise en place de relations d'approbation entre domaines) pour étendre les autorisations d'accès (entre régions fusionnées), la convergence des serveurs de fichiers des régions fusionnées ou leur réplication. Les évolutions nécessaires seront mises en œuvre par chaque DSI ministérielle pour son périmètre.