DEDICACE

Je dédie ce présent rapport:

- A mon père pour son amour, son soutien aussi bien matériel, moral que financier.
- A tous mes professeurs depuis NOTRE DAME D'AFRIQUE jusqu'à PIGIER via le collège catholique SAINT JEAN BOSCO, merci d'avoir cru en moi, en mon intelligence et à mes potentialités. Par votre abnégation au travail vous m'avez ouvert les portes de la réussite.
- A mes amis et connaissances qui m'ont soutenu de près et de loin.

REMERCIEMENTS

Nos remerciements vont d'abord à l'endroit de :

- Mon père pour ses conseils et sa disponibilité ;
- Mes frères et sœurs ;
- Mes professeurs et personnel de l'école PIGIER-CI pour les efforts considérables fournis lors de ma formation et qui ont conduit à la validation de mes différentes Unités d'Enseignement (UE) en ce qui concerne le Master Génie Informatique et Réseaux.

Toute ma profonde reconnaissance, ensuite, à Mr KOUASSI DADI non seulement pour sa sympathie mais aussi et surtout pour son soutient paternel et professionnel.

Je ne saurai terminer sans adresser des mots de reconnaissance à mes très chers amis qui représentent pour moi une seconde famille.

Enfin, nous tenons à remercier tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce travail.

- Nous tenons de plus à remercier profondément un ami de toutes les batailles, qui nous est cher et qui se reconnaîtra sans doute dans ce passage des *Petits poèmes en prose* de Baudelaire : « *Les chemins bourbeux rendent plus désirable l'aube spirituelle et plus tenace l'exigence d'un idéal* ». C'est grâce à la judicieuse et chaleureuse attention de ce compagnon d'armes que ces mots ont pris du sens et que les épreuves de la vie, si difficiles ou malheureuses qu'elles soient, ont pu se transformer en merveilles. Sans son appui inconditionnel et sa patience, ce mémoire ne serait pas ce qu'il est...

LISTE DES ACRONYMES

TABLE DES FIGURES

AVANT - PROPOS

INTRODUCTION GENERALE

Le développement remarquable du *Cloud Computing*, ces dernières années, suscite de plus en plus l'intérêt des différents utilisateurs de l'internet et de l'informatique qui cherchent à profiter au mieux desservices et des applications disponibles en ligne à travers le web en mode services à la demande et facturation à l'usage. C'est un nouveau modèle économique que le *Cloud Computing* promet pour les TIC.

En effet, le modèle promet un changement dans le mode d'investissement et d'exploitation des ressources IT. Avec le *Cloud Computing* les organisations, institutions et entreprises n'ont plus besoin d'investir lourdement dans des

ressources informatiques, nécessairement limitées, et nécessitant une gestion interne lourde et couteuse. Aujourd'hui elles ont le choix de migrer vers un modèle *CloudComputing* où elles peuvent acheter ou louer des ressources en ligne. Ce modèle leur épargne les coûts de gestion interne, puisque les ressources informatiques sont administrées au niveau du fournisseur du *Cloud Computing*.

La disponibilité des services en ligne donne aussi la possibilité de ne plus s'approprier d'équipements informatiques mais de payer les frais en fonction de l'utilisation des ressources. Ce modèle attire déjà un grand nombre d'entreprises notamment les petites et moyennes entreprises (PME) et les très petites entreprises (TPE).

Le *Cloud Computing* offre également la modularité des ressources informatiques (*hard* et *soft*) et leur disponibilité, en terme de volume et dans le temps, selon les besoins du client et à sa demande.

Dans un contexte économique où les entreprises cherchent à rentabiliser au maximum lesinvestissements et à limiter les coûts d'exploitation, le *Cloud Computing* se présente comme étant la solution de demain.

La Direction Générale du Trésor et de la Comptabilité Publique (DGTCP), donc, soucieuse de son développement ne veut pas être en marge concernant l'adoption de cette solution dite prometteuse.

En la DGTCP possède l'un des réseaux les plus vastes de la Côte d'Ivoire de par ses représentations dans la quasi-totalité des villes. L'augmentation du nombre d'utilisateurs, du trafic, la convergence de la voix et des données ainsi que les éventuelles attaques expliquent la dégradation dudit réseau, mettant à mal l'utilisation des ressources.

Au regard de l'impact négatif que cela engendre sur le rendement sur le rendement et la qualité de service, optimiser son réseau devient donc indispensable. Pour ce faire la DGTCP a décidé de se tourner vers une solution *Cloud Computing*à savoir WINDOWS AZURE.

Quel est l'intérêt de cette solution ? Est-ce une solution adéquate ? Qu'en est-il de la confidentialité et de la sécurité des informations importantes et sensibles ?
Telles sont entre autres les questions auxquelles nous tenterons de répondre durablement au travers du thème qui nous a été soumis à savoir : « **Mise en œuvre d'une solution Cloud Computing avec Windows Azure : Cas de la DGTCP.** »
Dans notre démarche, il sera d'abord question, de faire une étude de l'existant de la DGTCP.
Ensuite d'établir la cartographie des insuffisances techniques afin d'adapter au mieux la solution choisie et enfin de mettre en œuvre ladite solution.

PREMIERE PARTIE

PRESENTATION DE LA DGTCP ET ETUDE DE L'EXISTANT

Introduction

CHAPITRE 1 : PRESENTATION DU CADRE DE TRAVAIL

1.1 Présentation générale de la DGTCP

La Direction Générale du Trésor et de la Comptabilité Publique (DGTCP) est généralement connue sous le nom de « Trésor public ». Il est créé depuis le 1er Janvier 1963 pour assurer le recouvrement des recettes publiques et le paiement des dépenses de l'Etat. Les attributions successives qui lui sont conférées à travers la pluralité des textes qui le réorganisent dont le dernier en date est le décret n°2007-468 du 15 Mai 2007 en font une administration dynamique au service du développement.

La DGTCP est une institution chargée de la centralisation des opérations financières de l'état ivoirien.

1.1.1 Rôles et attributions

- Le recouvrement des recettes
- L'exécution des dépenses publiques
- La gestion financière et comptable des communes et des établissements publics nationaux
- La gestion de la trésorerie de l'Etat et des postes comptables à l'étranger
- La gestion de la dette publique
- La centralisation des dépôts des établissements publics nationaux
- Le recouvrement des créances contentieuses
- La surveillance des marchés financiers et d'assurance.

1.1.2 Organigramme

La Direction Générale du Trésor et de la Comptabilité Publique est actuellement dirigée par Monsieur **KONE Adama**, assisté de deux directeurs généraux adjoints que sont : Messieurs **ASSAHORE Konan Jacques** et **FOFANA Lancina**.

Voir annexe 1 : Organigramme de la DGTCP

1.2 Présentation de la DSI

La Direction des Systèmes d'Information, est dirigée par **M. KABRAN Ekian François.**

1.2.1 Rôles et attributions

La direction des systèmes d'information est chargée :

- De déterminer et suivre la mise en œuvre du plan directeur informatique du Trésor public ;
- Du traitement et de la production des données ;

- De la conception, et de la mise en place des applications informatiques du Trésor public ;
- De la mise en place du réseau informatique du Trésor public.

1.2.2 Organisation

Elle comprend quatre sous-directions :

- Sous-direction des applications spécifiques et de la formation ;
- Sous-direction production ;
- Sous-direction des applications de la comptabilité générale de l'Etat ;
- Sous-direction réseau et support utilisateur, au sein de laquelle se déroule notre stage de fin de cycle.

La sous-direction réseau et support utilisateur se compose de cinq services que sont :

- Le service réseau
- Le service maintenance
- Le service High Tech
- Le service assistance premier niveau
- .0

0Le service support utilisateur.

Le service réseau, service au sein duquel nous exerçons plus précisément, s'occupe des infrastructures réseaux et télécommunication :

- Lien inter-sites (interconnexion) ;
- Equipements actifs (firewall, routeurs, commutateurs…) ;
- Serveurs de communication ;
- Sécurité d'accès au réseau et au système d'information.

Voir annexe 2 : Organigramme de la DSI

CHAPITRE 2 : ETUDE DE L'EXISTANT

2.1 Description du système informatique

2.1.1 Inventaire des ordinateurs et serveurs

La quasi-totalité des ordinateurs du Trésor public proviennent essentiellement des constructeurs HP et DELL. On peut citer entre autres :

- HP L1908w
- HP Pro 3520
- HP 52031a
- HP LE1901w
- Et autres DELL

Concernant les serveurs, il y en a pas mal au rang desquels :

Matériel	Caractéristiques
5 serveurs HP Proliant DL 380 G7 (2 servant de serveurs Citrix, 1 pour MacAfee antivirus, 1 pour UAP et le dernier pour Orion)	• Un processeur **Intel Xeon E5606** (2.13 GHz - L3 8 Mo - Quatre coeurs - 80 W) • **6 Go** de mémoire vive**ECC** de type **DDR3-SDRAM** • **18 slots mémoires DIMM disponibles** supportant jusqu'à 384 Go de mémoire • Lecteur DVD-ROM • Châssis avec **8 emplacements disques durs hot-plug 2.5" SAS/SATA (SFF)** • Contrôleur de stockage **HP Smart Array P410i/512Mo** avec prise en charge **RAID 0,1, 5, 10 et 50** • Gestion à distance : Gestion **iLO3** (Integrated Lights-Out 3) • **Alimentation 460W** (non redondante)

1 serveur DELL PowerEdge R410	• Fréquence du processeur: 2,4 GHz, Intel® Xeon® séquence 5000, • Modèle de processeur: E5620. Capacité totale de stockage: 600 Go, • Vitesse de rotation du disque dur: 10000 tr/min, • Capacité disque dur: 300 Go. Mémoire interne: 8 Go, • Type de mémoire interne: DDR3-SDRAM, • Mémoire interne maximale: 128 Go. • Taille de la mémoire vidéo: 8 Mo, • Adaptateur graphique: G200eW, Matrox. • Caractéristiques réseau: Gigabit Ethernet, • Contrôleur de réseau local (LAN): Broadcom BCM5716
1 serveur DELL PowerEdge R510	• Fréquence du processeur: 2,13 GHz, • Famille de processeur: Intel® Xeon® séquence 5000, • Modèle de processeur: E5606. • Capacité totale de stockage: 0 Go. • Mémoire interne: 2 Go, • Type de mémoire interne: DDR3-SDRAM, • Fréquence de la mémoire: 1333 MHz. • Type de châssis: Support
1 serveur HP Proliant DL 380P Gen8 servant de serveur web	• Fréquence du processeur: 2 GHz, • Famille de processeur: Famille Intel® Xeon® E5, • Modèle de processeur: E5-2620. • Disque dur, taille: 2.5", • Interface du disque dur: Série ATA III, Série Attachée SCSI (SAS), Niveaux RAID: 0, 1, 1+0, 5, 5+0. • Mémoire interne: 8 Go, • Type de mémoire interne: DDR3-SDRAM, • Mémoire interne maximale: 768 Go. • Adaptateur graphique: G200, • Famille d'adaptateur graphique: Matrox. • Technologie de câblage: 10/100/1000Base-T(X)

7 serveurs IBM System X3550 M4 servant de serveurs de Base de données.	• Fréquence du processeur: 2,2 GHz, • Famille de processeur: Famille Intel® Xeon® E5 • Modèle de processeur: E5-2660. • Capacité totale de stockage: 0 Go • Disque dur, taille: 2.5" • Interface du disque dur: SATA, Série Attachée SCSI (SAS). • Mémoire interne: 8 Go, Type de mémoire interne: DDR3-SDRAM • Mémoire interne maximale: 768 Go. • Taille de la mémoire vidéo: 16 Mo • Adaptateur graphique: G200eR2, Famille d'adaptateur graphique: Matrox. • Caractéristiques réseau: Gigabit Ethernet • Contrôleur de réseau local (LAN): Intel I350AM4 • Technologie de cablâge: 10/100/1000Base-T(X)
1 serveur IBM Blade Center H	• Interface: USB 2.0. Couleur: Noir. • Poids: 41 kg. • Dimensions (LxPxH): 400 x 736 x 482 mm, Type de châssis: 9U • Exigences d'alimentation: 200-240V
2 serveurs IBM System P5	
2 serveurs IBM System X3650 M2 servant de serveurs système.	• Fréquence du processeur: 2 GHz • Famille de processeur: Intel® Xeon® séquence 5000 • Modèle de processeur: E5504. • Capacité totale de stockage: 0 Go • Disque dur, taille: 2.5" • Interface du disque dur: Série Attachée SCSI (SAS).

	• Mémoire interne: 3 Go • Type de mémoire interne: DDR3-SDRAM • Mémoire interne maximale: 128 Go. • Caractéristiques réseau: Gigabit Ethernet. • Systèmes d'exploitation compatibles: Microsoft Windows Server 2003
1 serveur Oracle SUN Sparc enterprise M4000	• Mémoire interne: 4 Go • Type de mémoire interne: DDR2 • Fréquence de la mémoire: 667 MHz
1 serveur enterprise storage GTK	•

2.1.2 Inventaire des logiciels et systèmes d'exploitation

Concernant les logiciels et systèmes d'exploitation, la Direction Générale du Trésor et de la Comptabilité Publique en dispose de plusieurs types :

- Les logiciels de production au rang desquels PEC MER, SYGACUT, RED CONS, STAT, ALJASTER etc. tournant sur ORACLE 6i.
- Les logiciels de sécurité au rang desquels MacAfee version 8.1 (sur la quasi-totalité des machines) et Kaspersky (sur les laptops de travail).
- Les systèmes d'exploitation quant à eux s'articulent autour de Windows 8.1 Professionnel, Windows Vista et Windows 7 Professionnel pour l'ensemble des PC (Tous les systèmes étant de 32 bits) d'une part et Ubuntu, Debian 4.0, Unix (AIX 5 et Sun Solaris), Windows server 2003, Windows server 2008 pour les serveurs d'autre part.
- Et d'autres utilitaires tels que VNC etc.

2.1.3 Inventaire des équipements réseaux

Les équipements réseaux utilisés par le Trésor Public sont essentiellement de la marque Cisco et diffèrent suivant les différentes séries. Le tableau suivant inventorie lesdits équipements réseau :

Routeurs	Switches et autres équipements
Cisco 1700 servant pour la fonctionnalité NAT	7 Switches Fibre optique
Cisco 1900 Series servant pour l'internet	Modem ETX-203A
2 Cisco ASA 5510	Modem ASMI-52L
Cisco 2800 Fibre Optique	3 Modems EtherAccess ETX-202
4 Cisco 1800	2 transceivers TP-link
Cisco 1900	Switch 2950
Cisco 2900	Switch 2960
4 Cisco 1900	Switch 2960 G
Cisco 3600	Switch 3550
Cisco 800	Switch 3550 G
LiveBox Business 140 Orange Côte d'Ivoire	Switch 2960 S

2.2 Architecture et topologie du réseau central et des succursales

2.2.1 Plan d'adressage

Le plan d'adressage du Trésor public dans son entièreté est

2.2.2 Description de l'architecture du réseau

2.3 Les aspects de la sécurité existante

2.3.1 Sécurité réseau

2.3.2 Sécurité des systèmes

CHAPITRE 3 : CARTOGRAPHIE DES INSUFFISANCES TECHNIQUES

3.1 Analyse de l’architecture réseau et système

3.1.1 Reconnaissance du réseau et du plan d'adressage

3.1.2 Sondage système et des services réseaux

3.2 Analyse des insuffisances

3.2.1 Serveurs de messagerie

3.2.2 Serveurs de données

3.2.3 Serveurs proxy

Conclusion

DEUXIEME PARTIE

ETUDE TECHNIQUE DE LA SOLUTION

INTRODUCTION

Le terme «**Cloud**» se retrouve progressivement vulgarisé au niveau aussi bien de l'entreprise que du grand public, ne serait-ce que par cette publicité nous vantant le «Cloud maîtrisé».

Le terme «*Cloud*» en langue anglaise signifie «nuage». Ce terme nous renvoie à deux significations. La première évoque une notion d'éther, de légèreté, d'élévation (vapeur), et la seconde, qui est son antonyme, une notion de brume, de nébuleux voire fumeux.

Beaucoup d'entre nous sont dans la confusion, « écartelés » entre les deux significations.Nous sommes attirés par une forme d'objectif qui nous semble inéluctable et qui « ne peut que nous élever », tout en étant dans une forme de confusion, de nébulosité, concernant le concept.

Le**Cloud**ou plus précisément le**Cloud Computing**peut se traduire en français par**informatique dans les nuages**.

Mais qu'entendons-nous par la notion de Cloud dans le monde de l'informatique?

Aujourd'hui, est-ce devenu un terme marketing mis à toutes les sauces ? Certainement,mais est-ce uniquement cela ?

Sont-ce des services informatiques gratuits, ou presque, tels que:

• Une messagerie (Free, Hotmail, Gmail...)?
• Un espace de stockage (DropBox, Google Drive, SkyDrive...)?
• Une suite bureautique (Office 365, Google Docs)?
• Du partage de vidéo (YouTube, Dailymotion)?
• Des réseaux sociaux (Facebook, LinkedIn, Viadeo...) ?

Est-ce la fin de la Direction des Systèmes d'Information (DSI) au sein des entreprises avec une reprise en main de l'informatique par les directions métier? Est-ce une informatique qui n'appartient plus à la DSI et qu'elle ne gère plus ?

Est-ce une conspiration de certains lobbies, des États-Unis et de la NSA (*National Security Agency*) pour prendre la main sur nos données personnelles mais aussi sur celles de nos entreprises ?

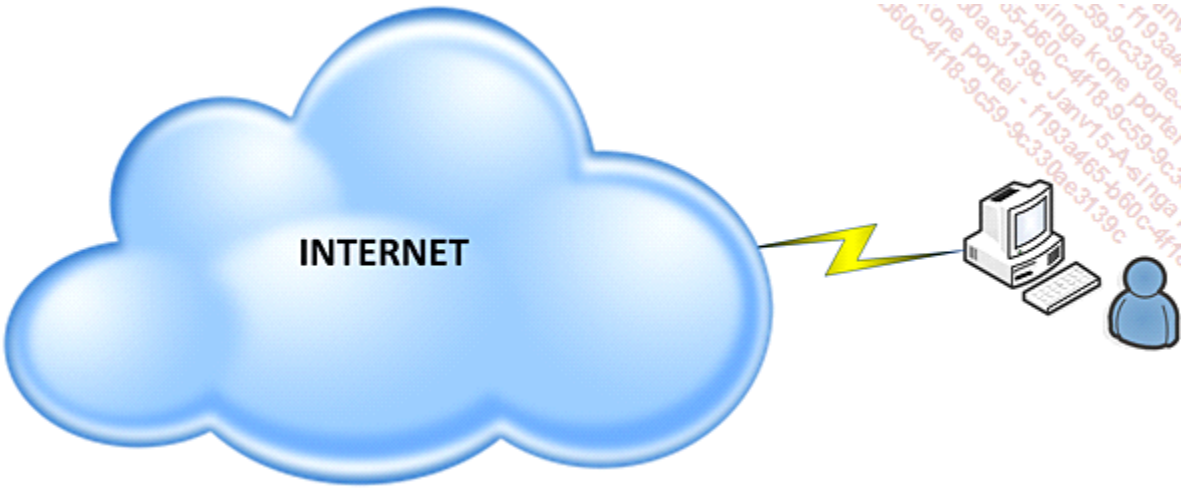
Ces interrogations sont légitimes et peuvent contenir une part de vérité. Notre but dans cet ouvrage est d'éclaircir le concept et d'expliquer les enjeux et la démarche sous-jacente de sa mise en œuvre dans une entreprise ou une organisation.

CHAPITRE 1 : Qu'est-ce que le Cloud Computing ?

1.1 Une informatique distribuée et ses éléments constitutifs

Le Cloud Computing est un terme à la mode, abondamment utilisé de nos jours, pour décrire un éventail de technologies. Il est donc important d'en définir la notion, les limites et d'identifier ce qu'il peut avoir d'innovant par rapport aux pratiques déjà anciennes d'infogérance.

L'origine du concept du Cloud provient du fait que les informaticiens symbolisent Internet sous la forme d'un nuage dans leurs schémas.

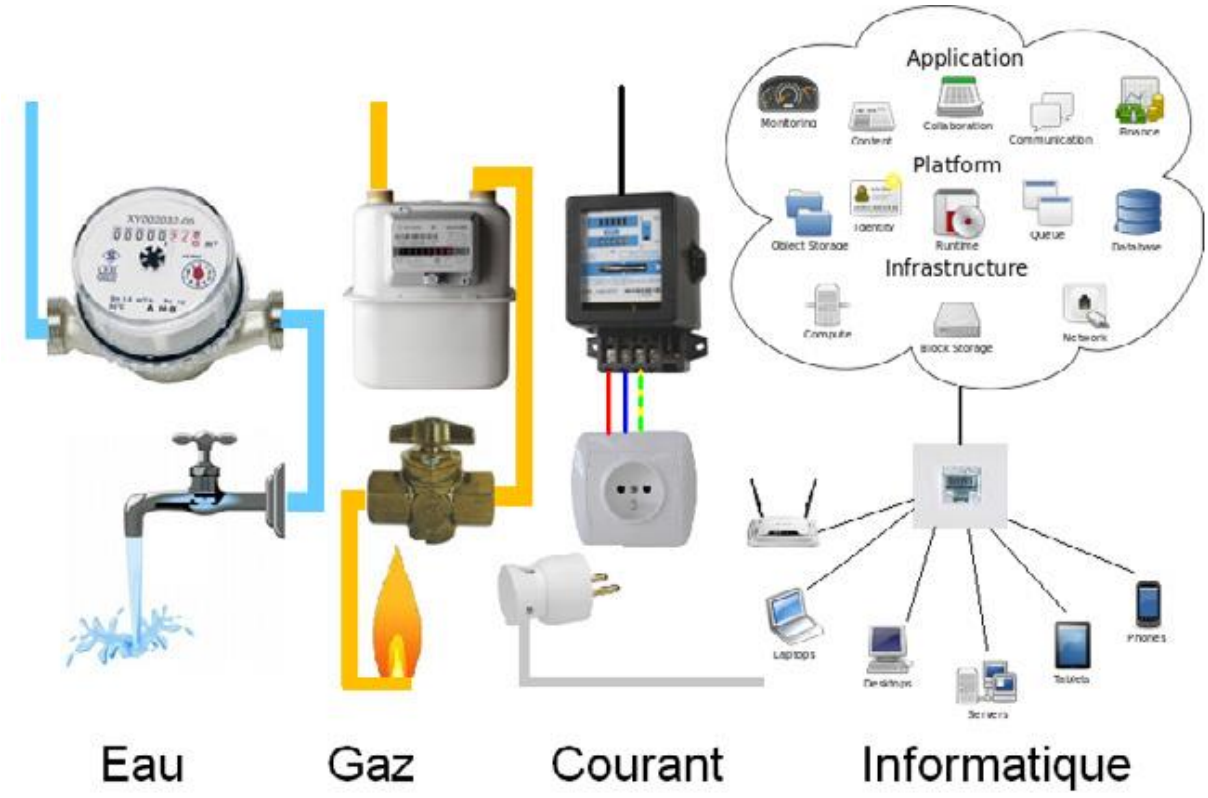


Symbolisation par les informaticiens de l'accès à Internet

La définition suivante du Cloud Computing est un extrait simplifié de la définition du National Institute of Standards and Technology (NIST, Etats-Unis) et du Groupe spécialisé de l'UIT.

«*Le Cloud Computing est un modèle qui offre aux utilisateurs du réseau un accès à la demande, à un ensemble de ressources informatiques partagées et configurables, et qui peuvent être rapidement mises à la disposition du client sans interaction direct avec le prestataire de service*.»

En d'autres termes, dans une entreprise « abonnée au Cloud », l'informatique serait distribuée exactement comme l'eau, le gaz ou l'électricité : il suffit de se brancher pour en bénéficier, la facture se fait selon la consommation et durant les périodes de non-utilisation (les congés, les vacances), on peut simplement fermer le compteur.



De plus la définition du NIST pour le Cloud Computing s'appuie sur les critères suivants :

- cinq caractéristiques essentielles,

- trois modèles de services,
- quatre modèles de déploiement.

Selon le NIST, le Cloud Computing ou informatique en nuage doit posséder cinq caractéristiques essentielles :

- Le service doit être en libre-service à la demande.
- Il doit être accessible sur l'ensemble d'un réseau.
- Il doit y avoir une mutualisation des ressources.
- Il doit être rapidement élastique (adaptation rapide à une variation du besoin).
- Le service doit être mesurable (mesure et affichage de paramètres de consommation).

Selon le NIST, le Cloud Computing ou informatique en nuage doit posséder cinq caractéristiques essentielles :

- Le service doit être en libre-service à la demande.
- Il doit être accessible sur l'ensemble d'un réseau.
- Il doit y avoir une mutualisation des ressources.
- Il doit être rapidement élastique (adaptation rapide à une variation du besoin).
- Le service doit être mesurable (mesure et affichage de paramètres de consommation).

En plus des caractéristiques évoquées par le NIST, les services Cloud Computing possèdent des caractéristiques supplémentaires qui les distinguent des autres technologies :

- En général, les utilisateurs du *Cloud Computing* ne sont pas propriétaires des ressourcesinformatiques qu'ils utilisent. Les serveurs qu'ils exploitent sont hébergés dans des data centresexternes.
- Les services sont fournis selon le modèle pay-per-use ou le modèle d'abonnement.
- Les ressources et les services fournis au client sont souvent virtuels et partagés par plusieurs utilisateurs.

- Les services sont fournis via l'Internet.

En clair, Le « Cloud Computing » est un néologisme utilisé pour décrire l'association d'Internet (« Cloud », lenuage) et l'utilisation de l'informatique(« Computing »). C'est une manière d'utiliserl'informatique dans laquelle tout est dynamiquement couple et évolutif et danslaquelle les ressources sont fournies sous laforme de services au travers d'Internet. Lesutilisateurs n'ont ainsi besoin d'aucune connaissance ni expérience en rapport avec la technologie derrière les services proposés.

Comme décrit précédemment, le Cloud Computing correspond au développement et à l'utilisation d'applications accessibles uniquement via Internet.

Les utilisateurs dépendent ainsi uniquement d'Internet pour utiliser leurs logiciels, ils ont la possibilité d'accéder à des services sans installer quoi que ce soit d'autre qu'un simple navigateur Internet. Avec le Cloud Computing, les informations sont stockées de façon permanente sur Internet, au sein de puissants et/ou nombreux serveurs dédies.

Actuellement, la frénésie autour du Cloud Computing a atteint son paroxysme en raison de la démocratisation des connexions Internet dites « haut débit » ainsi que de l'accroissementde la capacité et de la puissance des disques durs, des puces et des centres de traitement de données (« datacenters »), en même temps que le décroissement de leur prix. Les utilisateurs ne font que louer ce matériel auprès de fournisseursde service quipeuvent alors servir des millions de clients avec quelques centaines ou milliers de machines.

Aujourd'hui, le Cloud Computing est exploité par la quasi-totalité des grandes entreprises car il fournit une analyse sophistiquée des données de la manière la plus rapide possible.

Le Cloud Computing est perçu aujourd'hui comme quelque chose d'extrêmement puissant, capable de résoudre plusieurs milliards de milliards (10^{18}) de traitements informatiques a la seconde, ce qui est largement supérieur à n'importe lequel des ordinateurs de bureau modernes seulement capables de milliers de milliards (10^{12}) d'opérations a la seconde.

Cette puissance phénoménale est fournie par des architectures distribuées constituées d'ordinateurs « low-cost » (peu couteux) qui s'échangent et se distribuent le travail en permanence. Elle est désormais à disposition de n'importe qui au travers d'Internet, que ce soit pour des utilisations financières (analyses), scientifiques (climat, statistiques) ou même médicales.

1.1.1 La virtualisation

La virtualisation consiste à faire fonctionner un ou plusieurs systèmes d'exploitation sur un ou plusieurs ordinateurs. Cela peut sembler étrange d'installer deux systèmes d'exploitation sur une machine conçue pour en accueillir qu'un, mais comme nous le verrons par la suite, cette technique a de nombreux avantages.

Il est courant pour des entreprises de posséder de nombreux serveurs, tels que les serveurs de mail, de nom de domaine, de stockage pour ne citer que ceux-ci. Dans un contexte économique où il est important de rentabiliser tous les investissements, acheter plusieurs machines physiques pour héberger plusieurs serveurs n'est pas judicieux. De plus, une machine fonctionnant à 15 pour cent ne consomme pas plus d'énergie qu'une machine fonctionnant à 90 pour cent. Ainsi, regrouperces serveurs sur une même machine peut donc s'avérer rentable si leurs pointes de charge ne coïncident pas systématiquement.

Enfin, la virtualisation des serveurs permet une bien plus grande modularité dans la répartition des charges et la reconfiguration des serveurs en cas d'évolution ou de défaillance momentanée.

Les intérêts de la virtualisation sont multiples. On peut citer :

- L'utilisation optimale des ressources d'un parc de machines (répartition des machines virtuelles sur les machines physiques en fonction des charges respectives).
- L'économie sur le matériel (consommation électrique, entretien physique, surveillance).
- L'installation, tests, développements sans endommager le système hôte.

1.1.2 Le Datacenter

Un centre de traitement de données (datacentre en anglais) est un site physique sur lequel se trouvent regroupés des équipements constituantsdu système d'information de l'entreprise (mainframes, serveurs, baies de stockage, équipements réseaux et de télécommunications, etc.). Il peut être interne et/ou externe à l'entreprise, exploité ou non avec le soutien de prestataires. Il comprend en général un contrôle sur l'environnement (climatisation, système de prévention contre l'incendie, etc.), une alimentation d'urgence et redondante, ainsi qu'une sécurité physique élevée.

Cette infrastructure peut être propre à une entreprise et utilisé par elle seule ou à des fins commerciales. Ainsi, des particuliers ou des entreprises peuvent venir y stocker leurs données suivant des modalités bien définies.

Exemple d'un Datacenter

1.1.3 La plateforme collaborative

Une plate-forme de travail collaboratif est un espace de travail virtuel. C'est un site qui centralise tous les outils liés à la conduite d'un projet et les met à disposition des acteurs.

L'objectif du travail collaboratif est de faciliter et d'optimiser la communication entre les individus dans le cadre du travail ou d'une tâche. Les plates-formes collaboratives intègrent généralement les éléments suivant :

- Des outils informatiques

- Des guides ou méthodes de travail en groupe, pour améliorer la communication, la production, la coordination.
- Un service de messagerie.
- Un système de partage de ressources et de fichiers.
- Des outils de type forum, pages de discussions
- Un trombinoscope, ou annuaire des profils des utilisateurs.
- Des groupes, par projet ou par thématique.
- Un calendrier ;

Représentation d'une plateforme collaborative

1.2 Les différents modèles de déploiement

On distingue le Cloud privé (réservé à un client) du Cloud public (proposé à tous). Entre les deux, on trouve des modèles dits « communautaires », « hybrides » ou même « souverains ».

1.2.1 Le Cloud privé

Ce modèle est très proche de l'infogérance (ou « outsourcing ») classique : le client est le seul utilisateur du service qui lui est dédié. Le matériel (hardware : les serveurs, dispositifs de copie, pare-feu etc.) peut être opéré et maintenu par un fournisseur de Cloud aux termes d'un contrat d'outsourcing. L'accès aux ressources peut être limité au personnel du client, par un réseau local physique ou virtuel (wide area network). Dans ce modèle, le contrat peut souvent être négocié (adapté aux besoins spécifiques du client).

De nos jours, une organisation peut être en possession de son propre système d'information (réseaux, serveurs et logiciels). Elle peut proposer, de la même manière que pour des services publics, d'accéder à des services cette fois-ci dits «maison» avec

un stockage des données en interne et des niveaux de service définis. Nous parlons alors de Cloud privé.

En première approximation, nous pouvons considérer que Cloud privé = réseau interne.

En guise d'exemple, on peut citer le logiciel de gestion de l'organisation.

Nous voyons là aussi que ce n'est pas le périphérique d'accès qui fait la différence car, dans certaines entreprises, nous pouvons nous connecter à notre logicielde gestion depuis notre ordinateur personnel. Dans ce cas, l'accès au Système d'Information (SI)de l'entreprise et au Cloud privé est réalisé au traversd'une connexion à un réseau virtuel sécurisé (VPN ouVirtual Private Network).

1.2.2 Le Cloud Communautaire

Un groupe de clients accèdent aux ressources d'un même fournisseur. En général, il s'agit de répondre à des besoins particuliers comme le respect de dispositions légales ou un niveau de sécurité déterminé. Ce groupe peut être ouvert à des nouveaux venus partageant les mêmes besoins. L'accès aux ressources ainsi mises en commun est généralement restreint aux utilisateurs du réseau (wide area network).

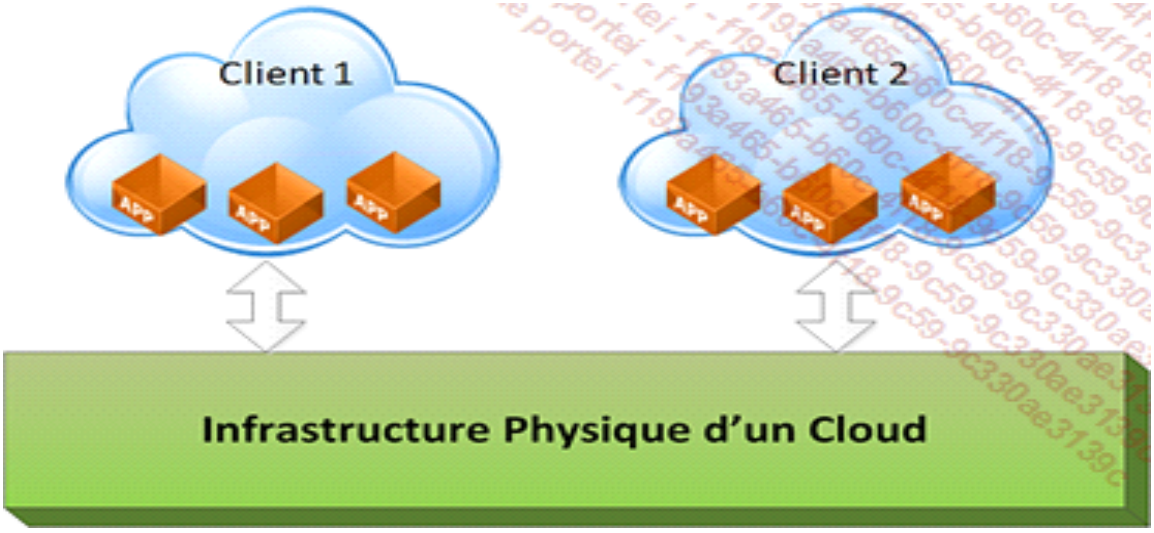
En d'autres termes imaginons des organisations avec des Clouds privés interconnectés sans ouverture vers l'extérieur.

Exemple : Des hôpitaux partageant des dossiers de patients, un logiciel de gestion mutualisé.

1.2.3 Le Cloud Public

Une infrastructure, une plateforme et des logiciels sont mis en place et gérés par le fournisseur de Cloud, qui invite le grand public (des entreprises, des clients ou des

utilisateurs finaux) à utiliser ce service. Ce peut être gratuit dans une certaine mesure, ou payant. L'accès au service se fait généralement par internet.
En tant qu'utilisateurs personnels, nous accédons via des services à des données stockées chez des fournisseurs/hébergeurs avec qui nous avons contractualisé le service et les niveaux de service associés. Ces fournisseurs/hébergeurs ayant une accessibilité directe sur l'Internet, nous parlons alors deCloud public.
En première approximation, nous pouvons considérer queCloud public = Internet!
Exemples : les réseaux sociaux, notre messagerie privée, l'extranet de notre société.
En général, l'utilisateur peut se connecter au Cloud public depuis sonpériphérique d'accès (PC, tablette tactile, smartphone, télévision...) à l'intérieur ou à l'extérieur de son entreprise. Par contre, les données ne sont pas stockées au sein de celle-ci.
Il n'est pas toujours facile en tant qu'utilisateur de savoir si l'on se connecte réellement à un Cloud public.
L'intérêt pour le fournisseur/hébergeur provient d'une mutualisation de son infrastructure vis-à-vis de plusieurs clients. Nous parlons alors de la notion de multi tenants (ou multi-locataires pour tenir compte de l'acceptation anglaise de **"tenant"**).



Multitenants -plusieurs clients hébergés sur une même architecture physique

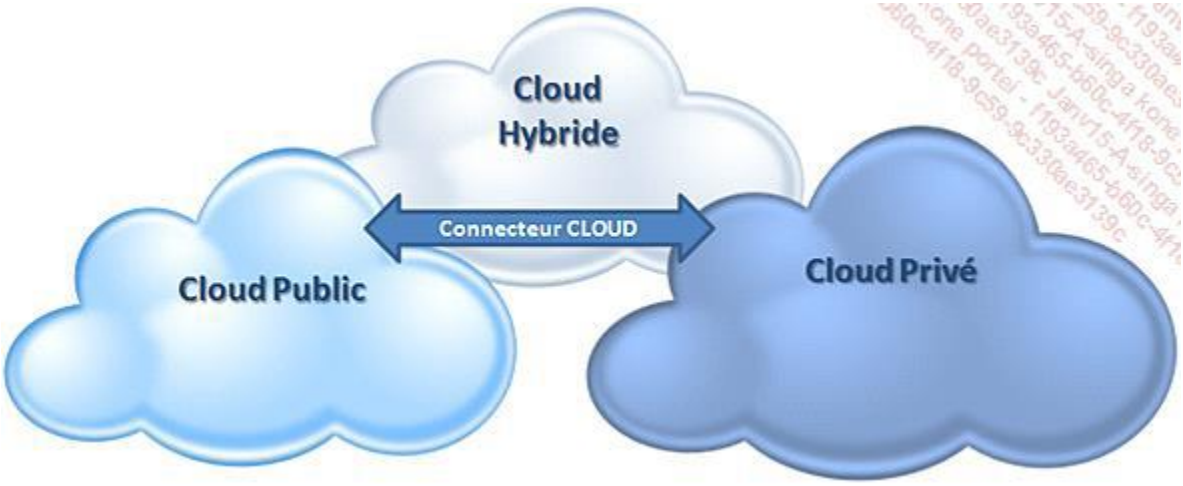
1.2.4 Le Cloud Hybride

Le Cloud hybride désigne une combinaison de Clouds privé, communautaire et public. Un client peut alors répartir données et accès aux applications de traitement entre les différents types de Cloud, cet accès pouvant être plus ou moins restrictif selon les cas. Il est également possible et souvent inévitable de combiner les divers services Cloud

externes (publics et/ou privés) et une infrastructure interne. Il est évident qu'un modèle totalement externe est irréaliste pour la majorité des entreprises dont le fonctionnement repose sur une informatique de production lourde qui n'a pas été conçue à l'origine pour tirer profit des possibilités du Cloud. Le modèle hybride s'impose donc souvent et les entreprises doivent s'attendre à des investissements conséquents afin d'intégrer les services internes et externes, privés et publics. La capacité de gérer un environnement hybride fera la différence entre réussite et échec.

De plus, de nos jours, l'informatique est communicante et les systèmes d'informations sont connectés. Prenons l'exemple de la messagerie qui permet d'envoyer des messages au sein de notre organisation mais aussi vers des utilisateurs du Cloud public; nous parlons alors de Cloud hybride.

Le fait que des échanges s'effectuent de manière automatisée entre un Cloud public et un Cloud privé au travers de ce que l'on appelle communément un connecteur définit la notion de Cloud hybride.



Cloud hybride

1.2.5 Le Cloud Souverain

Il combine les *Clouds* public et communautaire à l'échelle d'un pays afin notamment de se rattacher à un cadre juridique et économique déterminé.

1.3 Les différents modèles de services

On distingue principalement trois types de services au niveau du Cloud Computing, auxquels viennent s'ajouter deux autres types de plus en plus fréquents de nos jours. On peut donc citer :

- L'infrastructure en tant que service (IaaS: Infrastructure as a Service): serveur virtualisé et à la demande, data centre virtualisé, espace de stockage flexible et à la demande, réseaux locaux flexibles (LAN), pare-feux, services de sécurité, etc.

  L'offre donne un accès partagé à une grande puissance de calcul, ou de stockage, ou de communication. Plutôt que de devoir acquérir toute cette puissance (dont il n'a sans doute besoin que de manière épisodique, périodique ou pour des tests momentanés), le client achète un accès qui lui fournira toute la puissance, l'espace ou la rapidité de communication nécessaire au moment voulu.

- La plate-forme en tant que service (PaaS: Platform as a Service): plate-forme de fourniture de service Cloud Computing (gestions des services clients, facturations, etc.). C'est aussi une plate-forme qui propose une solution logicielle de développement : un environnement spécifique qui permet à l'utilisateur d'écrire et de tester des applications qui tourneront sur cette plateforme ou sur une installation similaire. C'est le cas par exemple d'un réseau social ou d'un constructeur qui offre une plateforme qui permet à des développeurs de créer des applications spécialement destinées à interagir avec ce réseau, avec l'écosystème ou l'univers fonctionnel de ce constructeur. La plateforme (middleware) définit les standards qui permettront de s'adresser de manière large et interopérable à de nombreux clients et d'élargir leur choix en matière de logiciel. Il est clair que ce service PaaS peut être hébergé sur une infrastructure IaaS.

- L'application en tant que service (SaaS: Software as a Service): applications métiers relation client, support (CRM), RH, Finance (ERP), payement en ligne, place de marché électronique (pour le TPE/PME), etc. En d'autres termes il s'agit de logiciels loués, à la demande, chez un fournisseur externe. En effet l'offre donne accès à une application complète et opérationnelle à laquelle l'utilisateur accède au moyen de son navigateur Web ou d'un autre logiciel client. Cette manière d'utiliser du logiciel élimine ou réduit fortement le besoin d'installer des programmes sur chaque poste client. De plus, le service est généralement accessible à une gamme la plus étendue possible de matériels : PC, tablettes, téléphones etc. Cela permet par exemple à une jeune start-up d'utiliser un puissant logiciel de gestion de clientèle, qu'elle n'aurait pas pu acquérir pour son usage exclusif. Bien sûr, ce service SaaS peut être aussi hébergé sur une plateforme PaaS et une infrastructure IaaS, ce qui fait aussi que l'on peut avoir différents contrats et différents fournisseurs « en cascade » pour chaque couche : une compagnie A peut offrir l'accès à un logiciel qu'elle a acheté à une compagnie B, qui utilise les standards de la plateforme C et qu'elle fait tourner sur une infrastructure opérée par une compagnie D.

A ces types viennent s'ajouter :

- La communication en tant que service (CaaS: Communication as a Service): service de communication audio/vidéo, services collaboratifs, communications unifiées, messagerie électronique, messagerie instantanée partage de donnée (web conférence).

- Le réseau en tant que service (NaaS: Network as a Service): Internet managé (garantie du débit, disponibilité, etc.), réseaux virtualisés VPN couplée aux services Cloud Computing, bande passante flexible et à la demande.

1.4 Les modes de financement

Une caractéristique du Cloud Computing est le paiement des fournitures selon la consommation. Cependant il existe une série de services qui sont, jusqu'à présent, soit toujours gratuits (comme la consultation de l'internet via un moteur de recherche), généralement gratuits (comme l'accès de base à un réseau social) soit proposés gratuitement dans certaines limites de volume ou de pages (comme le courrier ou l'agenda électronique). Les services « gratuits » ne peuvent se financer que par la publicité ou par l'utilisation du profil même de leurs utilisateurs comme « capital commercialisable ». Il en résulte que le service gratuit n'est viable à long terme que s'il sert d'attraction ou de support pour d'autres activités et s'il parvient à concentrer ou réunir une masse énorme d'utilisateurs : le Cloud Computing gratuit, destiné au grand public, est par excellence un domaine où le potentiel de concentration aux mains de quelques acteurs dominants est extrême.

1.5 Les caractéristiques spécifiques du Cloud

1.5.1 Les caractéristiques de base

- Le client du Cloud accède avec son périphérique (ordinateur de bureau, portable, tablette, téléphone, serveur en ligne) à trois couches de services (infrastructure, plateforme, applications) ;
- A l'exception des périphériques, l'infrastructure, les plateformes, les applications sont propriété du fournisseur de Cloud, non de l'utilisateur ;
- L'utilisateur interagit avec les services par un réseau, le plus souvent par internet. Les données sont donc distantes : leur support de stockage ne se trouve plus sous le contrôle direct de l'utilisateur ;
- L'accès se fait de n'importe où (la localisation du périphérique n'a pas d'importance) ;
- L'accès se fait à n'importe quel moment. Il n'y a pas d'heures « de bureau » ou « de travail » par rapport à des périodes de repos ou d'indisponibilité. Comme c'est le cas pour l'eau ou l'électricité, la disponibilité de l'infrastructure est normalement constante ;

- L’infrastructure distante stocke les données tandis que des applications logicielles en permettent l’accès ou le traitement ;
- L’utilisation des logiciels fournis pour l’accès et le traitement des données se fait à la demande ;
- Le paiement des services se fait normalement selon l’usage (sur base des volumes transférés, de l’espace disque, du nombre d’utilisateurs), ce qui évite aux nouveaux clients de devoir supporter l’ensemble des coûts qui résulteraient d’une exclusivité. Certaines entreprises donnent au grand public des accès totalement gratuits (mais limités en volume) qu’elles financent par la publicité.

1.5.2 Les éléments nouveaux

Il y a cependant d’autres caractéristiques, spécialement importantes, qui marquent une différence par rapport à l’infogérance (ou outsourcing) classique :

- **La mouvance géographique :** L’usage des services, et particulièrement de l’infrastructure, est optimisé dynamiquement dans un réseau de serveurs, ce qui fait que la localisation des données et de la machine qui en assure le traitement à un temps donné est souvent fluctuante (et inconnue de l’utilisateur, qui en général n’a pas à s’en soucier). Cette répartition dynamique correspond à une certaine nécessité. Une distribution vraiment « mondiale » de l’infrastructure en réseau sera la plus efficace pour la simple raison que – du fait de la rotation de la terre et de différentes cultures ou besoins – les uns travaillent à l’heure de pointe tandis que d’autres dorment, dînent, ne font rien ou fort peu de choses. La conséquence est que les opérateurs sont amenés à migrer constamment les charges de travail d’un centre de traitement à un autre pour une utilisation optimale du matériel. Cela ne sera pas sans influence sur le régime juridique applicable au traitement.
- **La flexibilité :** C’est la capacité d’adapter constamment le service (infrastructure, plateforme et applications) à des besoins fluctuants, comme par exemple la quantité de données à traiter par une application, le nombre

d’utilisateurs simultanés qui peuvent interagir, etc… On peut sur ce point distinguer la faculté d’adaptation dite « horizontale » (qui se réfère au nombre des transactions ou requêtes à traiter) et « verticale » (qui se réfère à la taille de ces transactions). Le partage A la différence de l’infogérance classique, les ressources sont mises en commun pour servir à un nombre fluctuant et indéterminé de « consommateurs ». Le comportement de certains a évidemment une influence sur les performances que les autres peuvent obtenir, étant donné que les ressources physiques et virtuelles sont constamment assignées et réassignées selon la demande.

- **Des pratiques contractuelles spécifiques :**Sur le plan des contrats qui peuvent être établis entre le fournisseur de Cloud et l’utilisateur, on retrouve les caractéristiques de l’infogérance ou outsourcing : un contrat de service récurrent, qui consiste à confier à un tiers tout ou partie de la gestion de son système d’information.

Toutefois, plus on progresse du « Cloud privé » vers le « Cloud public », plus le contrat est un contrat d’adhésion, c'est-à-dire une liste de conditions à prendre ou à laisser. A la limite, l’adhésion se borne à marquer son accord, par un clic de souris dans une check box « J’accepte vos conditions ». Bien plus, il arrive que le fournisseur de Cloud se réserve alors le droit de modifier unilatéralement les conditions du contrat, l’utilisateur étant alors plus ou moins informé, renouvelant tacitement son adhésion selon le principe « qui ne dit mot consent ».

Ces caractéristiques écartent le Cloud du contrat d’infogérance classique qui comporte généralement des clauses permettant :

- La mesure du niveau de service, régulièrement rapportée à l’utilisateur ;
- L’audit indépendant des performances, sur demande ;
- Des pénalités en cas de performance insuffisantes ;
- Des garanties de réversibilité.

Il est bon de noter que le fournisseur de Cloud est souvent dans l'incapacité technique d'agir autrement. On se retrouve ici dans un cas similaire à la distribution d'eau, de gaz ou d'électricité : quand une infrastructure est partagée par des milliers, voire des millions d'utilisateurs, il est difficile de vouloir négocier des avantages particuliers, le fournisseur ne pouvant pas avantager individuellement tel ou tel utilisateur. Il y a cependant des cas où le fournisseur définit plusieurs classes d'utilisateurs, plus ou moins avantagés selon leur abonnement.

1.5.3 Les aspects écologiques

Il est rassurant d'espérer que l'utilisation du Cloud permettra de diminuer l'éparpillement de machines individuelles, qui souvent, dans le cas de petits serveurs, tournent « à vide » la plupart du temps. Certains rapports mettent en avant le fait que les machines de dernière génération utilisées dans les centres de Cloud bénéficient aussi d'un meilleur rendement énergétique6. Le gain écologique et énergétique constitue un argument de vente des acteurs du Cloud, certains mettant en évidence des économies allant jusqu'à 90 %.Cependant, pour constater une réelle différence globale, il faudrait pouvoir compter sur un net progrès du côté des périphériques (par exemple une généralisationdes tablettes dépourvues de disque dur interne) car un PC ou un serveur utilisé comme périphérique en réseau ne consomme pas moins que la même installation indépendante. Or, on l'a vu, la plupart des entreprises qui ont recours au Cloud sont contraintes d'adopter une solution hybride (le « tout Cloud » n'est pas d'actualité). Les périphériques nouveaux ne remplacent pas, mais viennent en supplément des périphériques classiques.
Certains mettent donc en avant un revers de médaille écologique, sur la base des arguments suivants :

- Le Cloud se compose de gros centres de traitement distants et interconnectés par des réseaux à grande bande passante, dont chaque composant est consommateur d'énergie ;

- Ces gros « datacenters » sont très énergivores et leur fonctionnement est soumis à des contraintes complémentaires (espace au sol, climatisation, refroidissement, ventilation, protection, éclairage de nuit, surveillance) ;
- Une grande part de l'énergie est quand même gaspillée et ne sert qu'à répondre aux pics de charge ;
- En plus de la consommation d'électricité, il est indispensable de doubler l'installation par des batteries et des groupes électrogènes qui permettent de garantir un fonctionnement en continu tout en comprenant (et émettant quand ils fonctionnent) une quantité importante de polluants ;

1.5.4 Les aspects économiques

- Du point de vue du client
    - La réduction des coûts d'entrée

La réduction des coûts liés à l'acquisition et à la maintenance d'une infrastructure informatique est présentée comme le principal incitant pour les clients potentiels du Cloud. Cette réduction (ou élimination) du ticket d'entrée est particulièrement intéressante pour les PME et entreprises naissantes, qui peuvent concentrer leurs capacités de financement sur le développement de leur cœur de métier et bénéficier directement des solutions informatiques les plus performantes sans devoir y investir leur capital.

- Réduction du délai « pour être opérationnel »

Pour les mêmes raisons, spécialement pour les entreprises naissantes (startups et PME) l'effort pour être opérationnel et le délai (time to market) pour y parvenir est considérablement réduit. Cela permet d'être directement compétitif avec les entreprises établies de longue date. Pour les entreprises existantes, le Cloud permet d'évoluer et de rester compétitif sans devoir consacrer trop de temps et de ressources à la gestion du changement.

- Facturation selon l'usage

L'utilisation du Cloud est un cas de passage de l'investissement en capital à une dépense opérationnelle.

- Du point de vue des acteurs du Cloud
    - Un investissement important

La mise en place d'un Cloud public par un « vendeur de ressources » exigera un investissement de départ plus important que s'il s'agissait d'une infrastructure privée : en effet, il faut être d'une part flexible pour s'adapter aux besoins très divers des clients et leur offrir une large interopérabilité, et d'autre part être extensible (« scalable ») afin de répondre à une charge d'utilisation variable en volume, sans limites prédéfinies. L'exigence de disponibilité permanente et la mise en place de mesures de sécurité et de redémarrage correspondantes augmentent l'investissement.

- Un système de facturation selon l'usage

L'adaptation des coûts à l'utilisation réelle des ressources nécessite la mise en place d'un support aux utilisateurs de qualité et d'un nouveau système de facturation lié aux indicateurs d'utilisation.

1.5.5 Les rôles ou métiers du Cloud

Le Cloud permet aux acteurs (et personnes) d'exercer plusieurs métiers ou rôles qui s'attachent à une activité économique ou technique précise et sont générateurs d'emploi. Une part de ses emplois (principalement ceux qui sont nécessaires pour le fonctionnement du fournisseur, sa sécurité, son audit) peuvent se substituer à des emplois traditionnels de l'informatique d'entreprise ou de département, tout en étant facilement délocalisables (vu la mobilité des infrastructures Cloud).

Le **fournisseur** de Cloud (Cloud provider) est celui qui propose un service Cloud aux clients, soit par des interfaces applicatifs dédiés (APIs ou plateformes PaaS), par l'offre de machines virtuelles (partagées) ou par l'offre d'accès direct, plus ou moins privé, à des ressources d'infrastructure (IaaS : puissance, stockage etc.) de plateforme ou d'applications. Les métiers sont en nombre et variés selon l'importance du centre, durant son érection (métiers spécialisés de la construction) et durant son fonctionnement (ingénieurs, administrateurs, opérateurs, agents de sécurité). L'intégrateur de Cloud (ou « revendeur ») est un acteur de service qui se charge d'implémenter de manière opérationnelle unservice Cloud auprès d'un client. Il peut se charger de créer pour le client une interface unique qui donne accès à divers types de Cloud (par exemple au cas où un même client utilise des services différents pour la gestion de ses relations avec sa clientèle (le CRM), son courrier électronique, son archivage des données). Il assistera le client dans les choix qui correspondent le mieux à ses besoins. Il peut se charger de tâches de formation, gestion du changement etc.

L'**intégrateur** peut également être un conseiller, quoi que cette mission de consultance doive se faire de manière indépendante de toute revente. Ici aussi, il s'agira, spécialement lors d'études préalables ou d'audits, d'évaluer les services qui répondent le mieux aux besoins, sans négliger les perspectives économiques (à qui confier ses données, pour quel bénéfice), techniques (sous quels standards, niveau d'interopérabilité) et juridiques (sous quel régime contractuel et légal, dans quel écosystème, et sous quelles garanties).

Cette analyse doit être poussée en fonction de la nature des activités de l'entreprise : le niveau de sécurité attendu pour les données, le degré de transparence du système, la performance et la disponibilité des services, l'adéquation des applications de l'entreprise au modèle de Cloud computing et la gestion du risque de se voir « prisonnier de son fournisseur (vendor lock-in) ». Utiliser un service Cloud pour donner accès à des applications standards et conserver ses documents (les applications bureautique de Google par exemple) est simple, mais intégrer des services Cloud à une informatique de production critique pour l'entreprise et en tirer de réels avantages l'est beaucoup moins. Les entreprises qui migreront certaines de leurs applications vers le Cloud auront besoin d'un conseiller compétent pour évaluer les contrats de niveau de service (SLAs) proposés par les fournisseurs. Alors qu'aujourd'hui les contrats protègent essentiellement le fournisseur, cette situation se modifiera rapidement sous la pression de la clientèle qui demandera des termes et conditions basés sur ses besoins et une gouvernance transparente du fournisseur.

L'expertise en matière de **sécurité et l'audit** constituent un métier en soi. Les clients les plus importants seront intransigeants sur la capacité de leur(s) fournisseur(s) à fournir la capacité et la performance nécessaire afin d'obtenir un haut niveau de satisfaction des utilisateurs tout en assurant la sécurité des données. Ils demanderont très certainement d'avoir la possibilité de surveiller et mesurer certains paramètres caractéristiques du fonctionnement du système global.

L'éditeur de logiciels applicatifs peut créer des produits pouvant fonctionner sur le Cloud (ou adapter des produits existants) et placer ces produits auprès d'un fournisseur de Cloud, pour que ce dernier les propose à ses clients et lui restitue une partie des redevances payées par les clients qui adopteront le service SaaS. C'est ainsi qu'un logiciel de gestion de clientèle ou de gestion de projets peut être installé par l'éditeur chez divers fournisseurs de Cloud. Ce nouveau marché constitue pour les éditeurs une alternative à la vente pure et simple de licences au client final. Dans ce cadre, il ne faut pas négliger l'activité d'adaptation ou de réécriture des applications. Un des intérêts du Cloud est de permettre l'ajustement dynamique des ressources en fonction de la charge imposée aux applications ; cette possibilité est d'autant plus appréciable que la charge est variable. Les entreprises ont donc intérêt (tant du point de vue financier que de celui de la qualité des services offerts à ses employés, ses clients et ses fournisseurs) à migrer ce type d'applications de leur infrastructure interne, nécessairement surdimensionnée pour supporter les variations de charge, vers un service Cloud. Cette stratégie ne sera cependant efficace que si les applications (en particulier leur architecture) sont adaptées aux caractéristiques de fonctionnement spécifiques du Cloud. Il est donc également judicieux de concevoir les nouvelles applications dans cet esprit.

Il y a **d'autres fournisseurs d'outils** ou **composants** Cloud (matériel ou logiciel) pour lesquels ce nouveau marché représente une opportunité économique : serveurs, dispositifs de stockage, infrastructure de réseaux de télécommunication, sécurisation,

environnements de développements, programme de gestion de parc de machines virtuelles par répartition de charge, etc.
Ce qui est vrai pour les applications l'est également pour les infrastructures, dans la mesure où le modèle hybride est celui qui sera le plus adopté et où les entreprises continueront à concevoir et gérer leurs propres centres de calcul. En d'autres termes, les concepts et techniques sous-tendant le fonctionnement du Cloud (la virtualisation et la réallocation dynamique des ressources par exemple) vont aussi se voir appliqués dans les centres de calculs privés. Il y a donc là aussi une expérience métier précieuse à valoriser.

Enfin au sein des **utilisateurs directs** ou « finaux », une série de compétences sont requises pour contracter (décider), contrôler, gérer les droits, former, évaluer l'impact économique de l'utilisation du Cloud.

CHAPITRE 2 : Les opportunités et risques du Cloud Computing

2.1 Les opportunités du Cloud Computing

Le *Cloud* présente de nombreuses opportunités ou bénéfices, qui découlent des caractéristiques que nous venons d'évoquer :

- Il y a réduction du besoin de dépenses en capital liées à la création d'une infrastructure et/ou à l'acquisition de licences applicatives ;
- L'entreprise peut se concentrer, non sur son informatique, mais sur ses clients, sur l'efficacité de son personnel (utilisateur du *Cloud*) et leurs besoins, c'est-à-dire son activité essentielle ;
- Les coûts deviennent opérationnels, et sont liés à la performance et à l'activité réelle de l'entreprise (pas d'activité = pas de coût ; grande activité génératrice de profits = coûts proportionnels) ;
- L'entreprise bénéficie de l'économie d'échelle liée au partage des ressources avec de nombreux autres utilisateurs (réduction des coûts unitaires) ;
- L'entreprise bénéficie de performances plus stables ou « lissées » réparties entre un grand nombre d'utilisateurs qui ne travaillent pas tous en même temps;
- Les utilisateurs comprennent mieux le coût directement lié à leur activité (les charges peuvent être réparties dans l'entreprise en fonction de critères objectifs);
- La refacturation de coût réel des services rendus aux clients de l'entreprise utilisatrice est facilitée et peut être justifiée ;
- Au meilleur contrôle des coûts (qui deviennent plus opérationnels) correspond une réduction des frais généraux et un meilleur contrôle des profits opérationnels (revenus – coûts opérationnels et FG) ;
- La gestion prévisionnelle des besoins est grandement facilitée : on ne doit plus se soucier de savoir comment prévoir, anticiper et absorber d'éventuels pics de charge ;

- L’entreprise est plus agile, plus flexible quant à l’essai, à la décision d’utiliser ou non, voire d’abandonner telle ou telle application. En conséquence, un nouveau service aux clients peut être lancé plus rapidement et à moindre risque;
- L’entreprise est libérée de l’impératif de mettre périodiquement « à niveau » (upgrading) les infrastructures, les plateformes et les applications. Il n’est plus nécessaire de supporter ces coûts considérables et « à sens unique » : on paie à la demande et on peut revenir à la situation antérieure si la demande n’existe plus ;
- Le sentiment de sécurité n’est pas diminué. Il est plutôt augmenté, surtout dans le cas des PME et des utilisateurs individuels qui ne font pas de backup journalier de leurs données : quiconque a déjà vu son PC se faire voler ou son disque dur devenir illisible n’a pas besoin d’un long discours pour comprendre les avantages du *Cloud* : e-mails, contacts, les documents et photos ne sont plus perdus. On les retrouve immédiatement sur le *Cloud* avec un PC neuf.

2.2 Les risques du Cloud Computing

2.2.1 Classification des risques

Il est avantageux de classifier les risques du Cloud computing en fonction du modèle de service (IaaS, PaaS ou SaaS) et du modèle de déploiement (public, privé, hybride). En effet, cette classification permet de se concentrer sur les risques qui sont vraiment pertinents pour chaque situation.

2.2.1.1 Classification en fonction du modèle de service

L’entité qui fait appel à un fournisseur de services Cloud, tout en restant propriétaire des actifs informatiques hébergés par le Cloud, abandonne une partie du contrôle et de la visibilité sur les personnes, les processus et les techniques utilisées pour gérer ces actifs. Le niveau de visibilité est à considérer quand on identifie les risques et qu’on les évalue. En effet, chaque modèle de service Cloud a sa propre visibilité qui varie en fonction du nombre de couches du modèle de services qui sont prises en charge par le Cloud. Le modèle IaaS offre un fort niveau de visibilité à l’entité utilisatriceparce qu’il remplace uniquement l’infrastructure, alors que le modèle SaaS offre une plus faible visibilité parce qu’il remplace non seulement l’infrastructure, mais aussi les logiciels système, les données et les applications. Dans le modèle IaaS, l’entité utilisatrice de services Cloud gère elle-même les risques liés à la gestion des logiciels système, des données et des applications, alors que dans le modèle SaaS, elle externalise cette gestion sur base de contrats de niveau de services (SLA – Service Level Agreements) avec son fournisseur. Les risques liés à l’utilisation du Cloud sont cumulatifs en fonction du modèle de service auquel ils se rattachent : le modèle IaaS présente une série de risques qui lui sont spécifiques et qui sont liés à la gestion de l’infrastructure ; le modèle PaaS présente les mêmes risques avec, en plus, ceux qui sont spécifiques à ce modèle et qui sont liés à la gestion des logiciels système ; enfin, le modèle SaaS présente, en plus, les risques spécifiques qui sont liés à la gestion des données et des applications.

2.2.1.2 Classification en fonction du modèle de déploiement

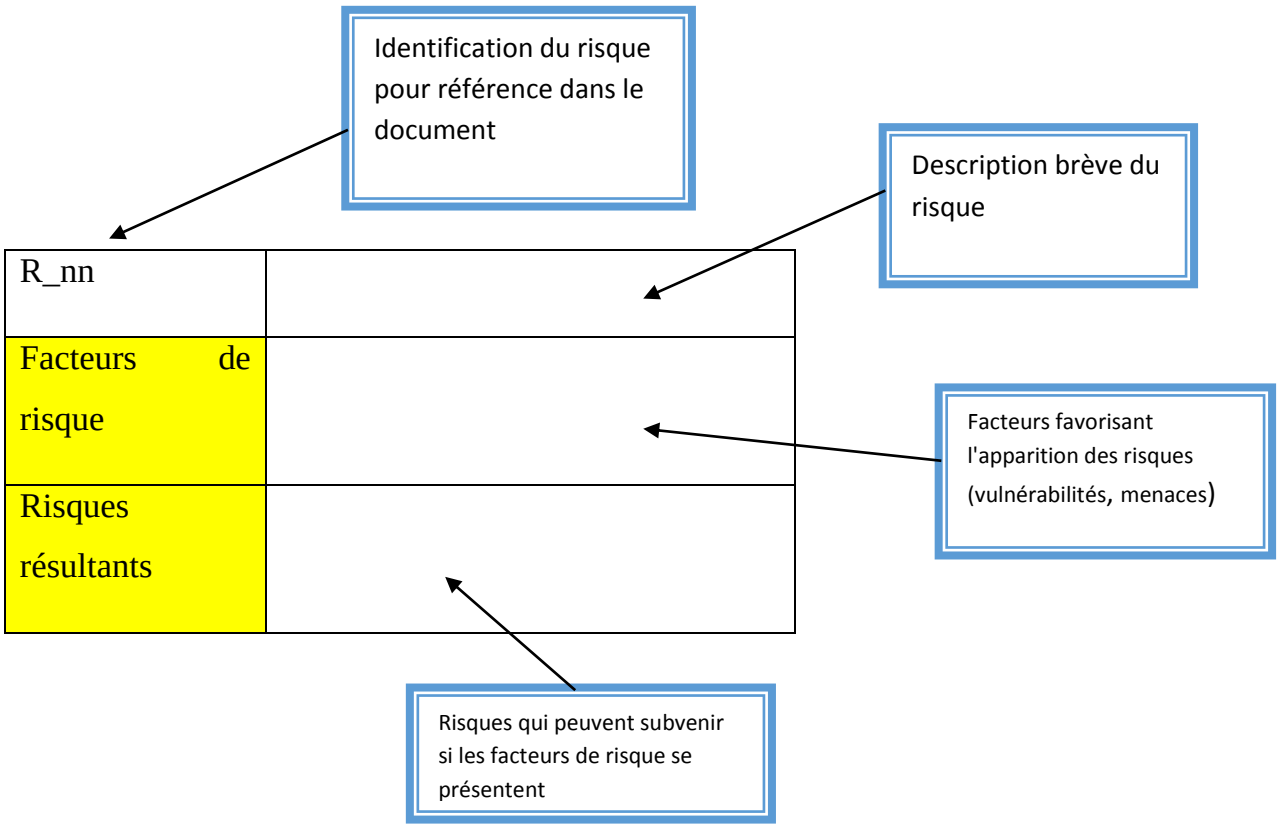
Certains risques sont spécifiques au modèle de déploiement du Cloud : privé, public, ou hybride. Le facteur déterminant est le degré de confiance qui lie les participants (le fournisseur de services Cloud et les entités utilisatrices du Cloud ; les entités utilisatrices entre elles). En particulier, un Cloud public est utilisé par des entités qui n'ont rien en commun et qui ne sont liées par aucun lien de confiance, alors que les entités utilisatrices d'un Cloud privé peuvent en avoir. Les risques associés à l'utilisation du Cloud sont différents dans ces deux cas.

2.2.1.3 Les risques génériques

Il y a des risques liés à l'utilisation du Cloud qui sont génériques, c'est-à-dire qu'ils ne dépendent ni du modèle de service, ni du modèle de déploiement.

2.2.2 Fiches de description des risques

Les risques sont présentés sous forme de fiches. Une fiche se présente comme suit :



Fiche de description des risques

2.2.2.1 Risques classifiés par modèle de service

a- Pour le IaaS

Risques spécifiques au modèle IaaS:

R_01	Transfert hors des frontières
Facteurs de risque	Les fournisseurs de service *Cloud* sont souvent des multinationales, et l'information peut être localisée dans des pays dont la législation diffère de celle à laquelle l'entreprise est soumise, en particulier ce qui concerne la protection des données à caractère personnel. Les autorités du pays où l'information aboutit peuvent exiger l'accès à l'information, parfois sans garantie que l'accès est justifié.
Risques résultants	• Divulgation de données non autorisée • Non-conformité aux lois

R_02	Multi-tenancy
Facteurs de risque	Pour profiter des avantages du *Cloud*, une entité utilisatrice partage les ressources (espace de stockage, hardware, réseau…) avec les autres entités. Les ressources doivent être isolées pour éviter la divulgation d'une entité à l'autre. Des défauts d'isolation peuvent se produire, par exemple quand un espace de stockage est libéré par une entité, puis récupéré par une autre sans que le contenu soit effacé.
Risques résultants	• Divulgation de données non autorisée

R_03	Contrôle des mesures de sécurité
Facteurs de risque	Le fournisseur de services *Cloud* doit s'équiper de protections et installer les politiques et processus associés afin d'atteindre au minimum le niveau de sécurité exigé par l'entité utilisatrice du *Cloud*. L'entité utilisatrice n'a pas toujours la possibilité de vérifier que le fournisseur de services remplit ses obligations. .
Risques résultants	• Blocage dû à l'indisponibilité du *Cloud* • Perte d'information • Divulgation de données non autorisée

R_04	Infrastructure délocalisée
Facteurs de risque	La délocalisation (*offshoring*) de l'infrastructure augmente les sources possibles d'attaques. Le contrôle de la sécurité par le fournisseur de services *Cloud* et la vérification par l'entité utilisatrice du *Cloud* peuvent être difficiles dans des pays éloignés.
Risques résultants	• Blocage dû à l'indisponibilité du *Cloud* • Perte d'information • Divulgation de données non autorisée

R_05	Maintenance des machines virtuelles
Facteurs de risque	Les fournisseurs de service IaaS permettent aux entités utilisatrices de créer des machines virtuelles suivant leurs besoins. Ces machines virtuelles doivent recevoir des correctifs (patches). Dans le cadre d'un service IaaS, c'est généralement la responsabilité de l'entité utilisatrice du Cloud. Des machines virtuelles non utilisées peuvent être oubliées et laissées en l'état, ce qui laisse la porte ouverte aux attaques.
Risques	• Blocage dû à l'indisponibilité du *Cloud* • Perte d'information

résultants	• Divulgation de données non autorisée

R_06	Authentification
Facteurs de risque	L'authentification doit être mutuelle entre le fournisseur de services *Cloud* et l'entité utilisatrice du *Cloud*. Alors que l'accent est souvent mis sur l'authentification de l'entité utilisatrice vis-à-vis du fournisseur de service, l'authentification dans l'autre sens peut être négligée, ce qui ouvre la voie à des usurpations d'identité ou à des attaques par intermédiaire (*man-in-the-middle attack*).
Risques résultants	• Divulgation de données non autorisée

b-Pour le PaaS

Les risques spécifiques au modèle PaaS, qui s'ajoutent aux risques spécifiques au modèle Iaas:

R_07	Utilisation du SOA
Facteurs de risque	L'architecture SOA (Service Oriented Architecture), souvent présente dans l'offre PaaS, peut présenter des vulnérabilités, soit au sein des services eux-mêmes, soit au travers de leurs interactions. Les librairies SOA sont gérées par le fournisseur de services Cloud, et l'entité utilisatrice n'a pas le contrôle direct sur la gestion de ces éléments, ce qui peut laisser la place à des vulnérabilités publiées mais non corrigées.
Risques résultants	• Blocage dû à l'indisponibilité du Cloud • Perte d'information • Divulgation de données non autorisée

R_08	Fin de contrat
Facteurs de risque	En fin de contrat entre le fournisseur de services Cloud et l'entité utilisatrice, les applications qui ont été développées dans l'environnement PaaS doivent être effacées du Cloud par le fournisseur de service. Si des détails échappent à la procédure d'effacement et subsistent sur le Cloud, ils peuvent être récupérés par un tiers et révéler des vulnérabilités de l'application.
Risques résultants	• Perte d'information • Divulgation de données non autorisée

c- Pour le SaaS

Les risques spécifiques au modèle SaaS, qui s'ajoutent aux risques spécifiques aux modèles Iaas et PaaS:

R_09	Propriété des données
Facteurs de risque	Le fournisseur de services *Cloud* fournit les applications, et l'entité utilisatrice apporte les données. Si la propriété des données n'est pas clairement définie, le fournisseur de services peut refuser l'accès aux données, voire exiger des frais supplémentaires en fin de contrat pour les restituer.
Risques résultants	• Perte d'information • Risque financier

R_10	Fin de contrat
Facteurs de risque	En fin de contrat entre le fournisseur de services Cloud et l'entité utilisatrice, les données qui ont été stockées dans l'environnement SaaS doivent être effacées du Cloud par le fournisseur de service. Si des données échappent à la procédure d'effacement et subsistent sur le Cloud, elles peuvent être révélées à un tiers non autorisé.
Risques résultants	• Divulgation des données non autorisée

R_11	Cycle de développement des applications
Facteurs de risque	Le cycle de développement des applications (*SDLC – System Development Life Cycle*) est sous le contrôle du fournisseur de services Cloud. L'entité utilisatrice a peu de contrôle, en particulier sur les exigences de sécurité qui ont été prises en compte au long du cycle de développement. Ce manque de contrôle peut aboutir à un niveau de sécurité qui ne remplit pas les besoins des utilisateurs de l'application.
Risques résultants	• Divulgation des données non autorisée • Perte d'information • Blocage dû à l'indisponibilité des applications sur le Cloud

R_12	Gestion des identités et des accès
Facteurs de risque	Les fournisseurs de services Cloud offrent leurs services et leurs applications à plusieurs entités en même temps, ce qui exige une gestion des identités et des accès (IAM – Identity and Access Management). Si le fournisseur de services Cloud ne gère pas l'IAM correctement, les applications et – au travers des applications – les données qu'elles traitent peuvent être lues ou modifiées par d'autres entités utilisatrices du Cloud.

Risques résultants	• Divulgation des données non autorisée • Perte d'information

R_13	Changement de fournisseur
Facteurs de risque	Rien n'est généralement prévu pour faciliter la portabilité du service et des données d'un fournisseur de services Cloud à un autre, en particulier quand le fournisseur ne rend pas un service satisfaisant ou qu'il tombe en faillite, ou que (pour éviter la faillite) il révise ses conditions contractuelles. De même, la décision d'une entité utilisatrice du Cloud de renoncer à ce service et de rapatrier les services et les données en interne se heurte à des difficultés.
Risques résultants	• Blocage dû à l'indisponibilité des applications sur le Cloud • Perte d'information • Blocage dû à l'indisponibilité des applications sur le Cloud

R_14	Conformité aux politiques d'achat
Facteurs de risque	Les politiques d'achat de matériel et de logiciel des entreprises peuvent être négligées quand l'entreprise opte pour un service Cloud, ce qui peut mener à des incompatibilités entre les applications du Cloud et les applications qui sont exploitées en interne.
Risques résultants	• Blocage dû à des dysfonctionnements des applications sur le Cloud

R_15	Vulnérabilité des navigateurs Internet
Facteurs de risque	Les applications offertes par les fournisseurs SaaS sont généralement accessibles au travers d'un navigateur (*browser*) et d'une connexion sécurisée. Les navigateurs sont une cible courante d'attaques. Si le navigateur est compromis, l'application l'est aussi ; la connexion sécurisée ne résout pas le problème.

Risques résultants	• Blocage dû à l'indisponibilité des applications sur le Cloud • Perte d'information • Divulgation de données non autorisée

2.2.2.2 Risques classifiés par modèle de déploiement

a- Cloud Public

R_16	Partage avec de nombreuses entités
Facteurs de risque	Le Cloud public est partagé entre de nombreuses entités utilisatrices qui n'ont pas d'intérêt commun ni d'exigence identique en matière de sécurité. Les opportunités de violation de la sécurité sont plus nombreuses.
Risques résultants	• Blocage dû à l'indisponibilité des applications sur le Cloud • Perte d'information • Divulgation de données non autorisée

R_17	Dommages collatéraux
Facteurs de risque	Une attaque vers une entité utilisatrice d'un Cloud public peut avoir un impact sur les autres entités utilisatrices du même Cloud. C'est particulièrement le cas des attaques distribuées par déni de service (DDoS – Distributed Denial of Service), ainsi que de l'exploitation des vulnérabilités du logiciel géré par le fournisseur de services Cloud, que le fournisseur tarde parfois à corriger.
Risques résultants	• Blocage dû à l'indisponibilité des applications sur le Cloud • Perte d'information • Divulgation de données non autorisée

b- Cloud Privé

R_18	Investissements nécessaires
Facteurs de risque	Un Cloud privé peut être perçu par une entreprise comme un moyen de supprimer les coûts liés à l'acquisition, à la maintenance et aux opérations des systèmes informatiques. Il est parfois difficile de faire accepter par les gestionnaires de l'entreprise qu'il y a un coût lié à l'adoption d'un Cloud privé ; les budgets sont parfois rognés, ce qui mène à des capacités insuffisantes.
Risques résultants	• Risques financiers; coûts imprévus • Blocage dû à l'indisponibilité des applications sur le Cloud

c- Cloud Hybride

Les risques sur le Cloud hybride sont la combinaison des risques sur les Clouds privé et public. De plus, le risque suivant est spécifique au Cloud hybride :

R_19	Interdépendance
Facteurs de risque	Dans le cas où différents types de Cloud sont mélangés, un Cloud d'un type peut avoir besoin d'accéder à un Cloud d'un autre type. Si les niveaux de sécurité sont différents, cela peut mener à la nécessité d'accéder à des systèmes dont la sécurité est critique à partir de systèmes moins critiques. Les mesures spéciales de sécurité qui sont nécessaires ne sont pas toujours mises en place.
Risques résultants	• Perte d'information • Divulgation de données non autorisée

2.2.2.3 Risques génériques

Le risque suivant ne dépend ni du modèle de service ni du modèle de déploiement:

R_20	Coût
Facteurs de risque	Une entité utilisatrice de services *Cloud* peut voir ses systèmes hébergés sur le *Cloud* bloqués par le fournisseur de services s'il ne paye pas les redevances à temps à son fournisseur.
Risques résultants	• Risque financier • Blocage dû à l'indisponibilité des applications sur le Cloud.

2.3 La gestion des risques

Une fois les risques identifiés, il convient de les gérer et de déterminer quelles mesures de sécurité réduisent ces risques jusqu'à un niveau acceptable par l'entreprise, et ce, de la manière la plus économique possible. L'approche proposée ici comporte quatre étapes :

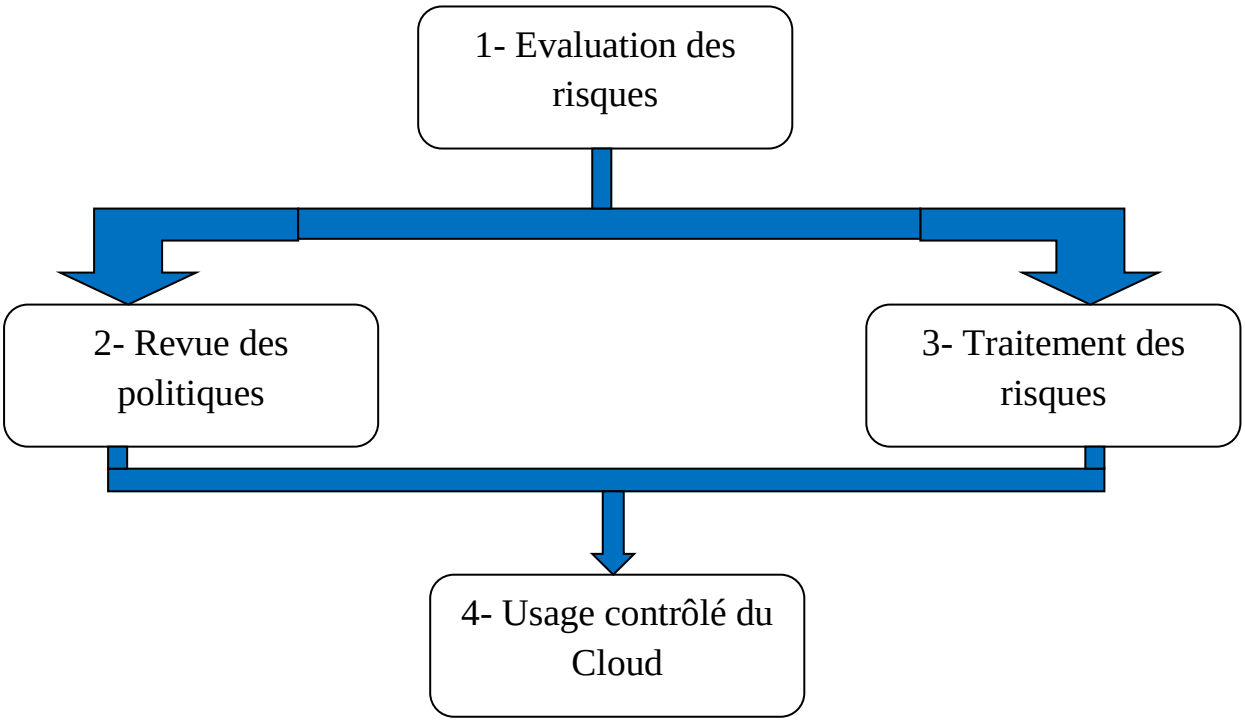
1. Evaluation des risques: Les risques qui ont été identifiés et qui sont liés à l'introduction du *Cloud* doivent être évalués afin de déterminer ceux qui doivent être réduits et qui doivent être couverts en priorité.

2. Revue des politiques: Afin de se préparer à l'introduction du *Cloud* dans l'entreprise, les politiques de sécurité doivent être revues (et, dans certains cas, créées). Cette étape assure que les règles de sécurité sont bien établies.

3. Traitement des risques: Dans cette étape, on détermine les mesures de sécurité qui sont nécessaires pour couvrir de manière appropriée les risques prioritaires ; on sélectionne le fournisseur de services *Cloud* en lui imposant ces mesures.

4. Usage contrôlé du *Cloud:* On utilise les services du fournisseur de service *Cloud* tout en maintenant la surveillance de ses prestations, particulièrement en matière de sécurité.

Les étapes sont illustrées ci-dessous :



Gestion des risques

2.3.1 L'évaluation des risques

Deux méthodes existent pour réduire les risques jusqu'à un niveau qui est acceptable :

- Agir sur la source: On s'efforce de diminuer la probabilité qu'une menace s'exerce sur l'informatique et les informations ;
- Agir sur la cible: On met en place des mesures de sécurité plus strictes qui protègent mieux les informations contre les vulnérabilités du système informatique.

On le voit, le but n'est pas d'éliminer le risque (on ne peut jamais l'éliminer entièrement), le but est de le diminuer jusqu'à un niveau résiduel qui est considéré comme acceptable par l'entreprise. C'est la direction de l'entreprise qui peut décider si un risque résiduel est acceptable ou non, pas le service informatique. Néanmoins, la direction a besoin de l'avis de ses informaticiens pour prendre des décisions en

connaissance de cause. Afin de pouvoir décider si un risque peut être accepté, il faut l'évaluer. Même s'il est impossible d'évaluer un risque de manière tout à fait rigoureuse (un risque est par nature inconnu), des méthodes structurées permettent une évaluation pratique et des comparaisons. Un exemple de méthode très simple à mettre en œuvre consiste à évaluer les risques sur base de deux facteurs : la probabilité d'occurrence de la menace d'une part, et les vulnérabilités que la menace tentera d'exploiter d'autre part. On place les risques sur une échelle bidimensionnelle comme ci-dessous :

Menace / Vulnérabilité	Probabilité d'occurrence faible (exemple: 1 fois par an)	Probabilité d'occurrence moyenne (exemple: 1 fois par mois)	Probabilité d'occurrence forte (exemple: 1 fois par jour)
Vulnérabilité importante (une technique peut élaborée permet de menacer la sécurité)			
Vulnérabilité normale (il faut une expertise particulière pour menacer la sécurité)			
Vulnérabilité faible (il faut des efforts démesurés pour menacer la sécurité)			

Echelle d'évaluation des risques

On place chaque risque identifié sur l'échelle en fonction d'une estimation de la probabilité d'occurrence de la menace (axe horizontal) et de la vulnérabilité des systèmes informatiques que la menace peut exploiter (axe vertical).

2.3.2 Revue des politiques

Les politiques de sécurité de l'entreprise doivent être revues (voire créées si elles n'existent pas encore) avant toute utilisation d'une nouvelle solution informatique. Ce principe s'applique au Cloud comme à toute nouvelle solution. Les domaines suivants peuvent faire l'objet de la revue :

- Classification de l'information: Afin de garantir un niveau de protection approprié aux informations, il convient de les classifier pour indiquer le degré souhaité de protection lors de leur manipulation. Certaines informations peuvent nécessiter un niveau de protection spécial parce que leur perte ou leur divulgation met l'entreprise en danger ;
- Conformité aux exigences légales: L'entreprise est soumise aux lois de protection des informations à caractère personnel, et la politique de sécurité de l'entreprise doit refléter les obligations en cette matière. Certains secteurs, comme la santé ou les institutions financières, sont soumis à des exigences légales spécifiques qui se reflètent aussi dans leurs politiques de sécurité ;
- Continuité des opérations: Si l'entreprise a une politique en matière de reprise après désastre, celle-ci se matérialise par un plan de continuité (*Business Continuity Plan*) ;
- Politique d'achat de matériel et de logiciel: Le cas échéant, l'entreprise doit s'assurer qu'il n'y a pas d'incompatibilité entre les applications offertes sur le *Cloud* et celles qu'elle continue à exploiter en interne.

La revue de ces domaines avant l'introduction du *Cloud* peut mener à des modifications :

- Classification de l'information: L'entreprise peut décider de créer une classe d'informations particulièrement sensibles qui ne seront jamais transférées sur un *Cloud* si le risque de perte ou de divulgation est évalué comme trop élevé dès lors qu'on les migre sur un *Cloud*. Ceci pourrait s'appliquer à des descriptions de procédés industriels ou de stratégie commerciale, dont la divulgation à des tiers pourrait mettre la pérennité de l'entreprise en péril ;

- Conformité aux exigences légales: L'entreprise peut décider de créer une classe d'informations à caractère personnel qui ne seront jamais transférées sur un *Cloud* si le risque d'utilisation non contrôlée est évalué comme trop élevé dès lors qu'on les migre sur un *Cloud*. Par exemple, dans un hôpital, les données médicales des patients peuvent faire l'objet d'une telle classification ;

- Continuité des opérations: Quoique l'introduction du *Cloud* n'ait un impact que sur le plan de continuité et, généralement, aucun impact sur la politique de continuité, il est prudent de revoir cette politique à la lumière des nouveaux risques liés à l'utilisation du *Cloud*. Si l'entreprise n'a pas encore de politique de continuité, l'introduction du *Cloud* est l'occasion d'en établir une ;

- Politique d'achat: Elle doit éventuellement être revue si des applications sont utilisées en interne après l'introduction du *Cloud*.

2.3.3 Le traitement des risques

Une fois qu'on a évalué les risques sur l'échelle d'évaluation (voir l'exemple au point 4.3.1), on détermine quels sont les risques qui doivent être réduits et par quelles mesures. Dans notre exemple, un risque qui, après évaluation, est placé sur une cellule verte est faible et peut ne pas être réduit ; un risque sur une cellule jaune est significatif et doit être réduit si possible ; un risque sur une cellule rouge est non acceptable et doit impérativement être réduit :

- Soit on diminue la probabilité par des mesures préventives. Par exemple, on fait la distinction entre les informations très sensibles (qu'on ne stocke jamais sur un *Cloud*), et les autres informations (qui peuvent être stockées sur un *Cloud*), et ce, afin de diminuer la probabilité de divulgation d'informations sensibles à l'extérieur de l'entreprise ;

- Soit on réduit les vulnérabilités par des mesures généralement techniques. Par exemple, on impose au fournisseur de services *Cloud* de chiffrer toutes les informations — tant sur les réseaux que sur les unités de stockage, avec de la cryptographie forte.

Une fois qu'on a éliminé les risques « rouges » et qu'on a réduit les risques « jaunes » chaque fois que c'est possible, on obtient un ensemble de mesures de sécurité qui couvrent les risques de manière adaptée et qui réalisent le niveau de sécurité que l'entreprise veut atteindre. La liste ci-dessous donne des exemples de mesures de sécurité à envisager (et à sélectionner suite à l'étape de traitement des risques) :

- Mesures contractuelles – L'entreprise peut imposer des clauses contractuelles au fournisseur de services *Cloud* pour diminuer certains risques :

    - S'assurer que le contrat avec le fournisseur de services *Cloud* garantit que l'entreprise utilisatrice reste l'unique propriétaire des informations et des applications qui ont migré sur le *Cloud* ;
    - Ajouter au SLA du fournisseur de service *Cloud* l'obligation d'avoir un processus de gestion de vulnérabilités des hyperviseurs13 ;
    - Ajouter au SLA du fournisseur de service *Cloud* l'obligation d'avoir un processus de gestion des changements qui inclut au minimum une analyse de risques ;
    - S'assurer que des dispositions existent qui permettent de changer de fournisseur de services *Cloud* sans perdre des informations ou des applications et ce, dans des délais raisonnables ;
    - Si nécessaire, inclure des limitations géographiques pour la localisation de l'information qui réside sur le *Cloud* ;

- Mesures de sécurité mises en œuvre par le fournisseur – L'entreprise peut exiger des informations du fournisseur de service Cloud :

    - Description des règles régissant qui, parmi le personnel du fournisseur de services *Cloud* (ou de ses sous-traitants), a le droit d'accès aux informations de l'entreprise ;

- Description des protections réseaux (pare-feu, antivirus, protection contre les attaques par déni de service…) mises en place par le fournisseur de services *Cloud* ; description du processus de gestion de ces protections ;
- Description du processus de gestion des droits d'accès au sein de l'organisation du fournisseur de services *Cloud* ;
- Description des mesures cryptographiques : algorithmes, longueur de clefs, gestion des clefs ; o Description des mesures techniques d'effacement de données libérées et de destruction de médias informatiques ;
- Description du plan de continuité mis en place par le fournisseur de services *Cloud* ; preuve que des exercices sont effectués régulièrement ;
- Preuve que le fournisseur de services *Cloud* fait l'objet d'audits réalisés régulièrement par des auditeurs certifiés ;

- Choix d'un mode particulier de gestion du Cloud – L'entreprise peut décider de se limiter à un Cloud privé si le caractère « multi-tenant » des Clouds publics présente des risques évalués comme inacceptables ;
- Mesures mises en œuvre au sein de l'entreprise utilisatrice du Cloud :

    - Organiser une campagne de sensibilisation à la sécurité de l'utilisation du *Cloud* ;
    - Accéder au *Cloud* exclusivement au travers de navigateurs sécurisés (utilisation de *sandboxes*) ou de stations virtuelles sécurisées ;
    - Revoir les plans de continuité (*Business Continuity Plan, Disaster Recovery Plan*) afin de parer à une indisponibilité prolongée du *Cloud*.

2.3.4 L'usage contrôlé du Cloud

La sécurité est un processus continu, c'est-à-dire qu'elle ne s'arrête pas à l'établissement d'un service comme le *Cloud* ; elle doit s'exercer aussi pendant l'exploitation du service. L'entreprise utilisatrice de services *Cloud* doit vérifier régulièrement que le fournisseur de services *Cloud* remplit ses obligations contractuelles et, s'il le faut, obtenir des preuves ; il en va de même en ce qui concerne les mesures de sécurité mises en œuvre par le fournisseur de services. D'autre part, l'entreprise doit vérifier que le programme d'audit IT auquel elle est soumise prend en compte l'utilisation du *Cloud* et que ses auditeurs internes sont formés à ces vérifications.

CHAPITRE 3 : Vue d'ensemble sur Windows Azure

3.1 Qu'est-ce que Windows Azure ?

Microsoft Azure (**Windows Azure** jusqu'en 2014) est le nom de la plate-forme applicative en nuage de **Microsoft**. Son nom évoque le concept de « **Cloud computing** » ou informatique en nuage (l'externalisation des ressources informatiques d'une entreprise vers des datacenters distants).
Microsoft Azure est en outre une plateforme ouverte et flexible de Cloud que vous pouvez utiliser pour stocker des données, des applications hôtes et des services pour le streaming multimédia et les applications mobiles.
Les solutions prises en charge sont les suivantes :

- Infrastructure

Microsoft Azure fournit une infrastructure à la demande qui évolue et s'adapte aux nouveaux besoins de votre entreprise. Que vous cherchiez à créer des applications ou à exécuter des applications existantes, nous vous fournissons le meilleur rapport qualité/prix et la meilleure assistance de bout en bout.

- Applications web

Microsoft Azure offre des options de développement, de déploiement et d'évolutivité sécurisées et flexibles pour toutes les applications Web, quelle que soit leur taille. Tirez parti de vos outils existants pour créer et déployer des applications sans vous préoccuper des contraintes de gestion de l'infrastructure.

- Applications mobiles

Connectez votre application dans le cloud.
Microsoft Azure permet de créer rapidement et facilement des applications mobiles susceptibles d'évoluer. En seulement quelques minutes, vous pouvez stocker des données dans le Cloud, authentifier des utilisateurs et envoyer des notifications Push vers des millions d'appareils.

- Développement et test

Développez et testez plus rapidement les applications
Microsoft Azure vous permet de développer et de tester plus rapidement les applications, à un coût avantageux, et offre la flexibilité nécessaire au déploiement local ou dans le Cloud.

- Big data

Améliorez vos prises de décision avec HDInsight de Microsoft Azure, une solution Big Data fournie par Apache Hadoop. Communiquez ces connaissances provenant de tous types de données aux utilisateurs professionnels par l'intermédiaire de Microsoft Excel.

- Données multimédias

Les Services de média Microsoft Azure vous permettent de créer des solutions de distribution multimédia évolutives, rentables et complètes capables de diffuser en continu des données multimédias vers des plateformes et appareils Adobe Flash, Android, iOS, Windows et autres.

- Stockage, sauvegarde et récupération

Microsoft Azure fournit des solutions de stockage, de sauvegarde et de récupération dans le cloud évolutives et durables pour toutes les données. Azure fonctionne avec votre infrastructure existante, ce qui permet d'optimiser votre stratégie de continuité des activités et de fournir le stockage nécessaire pour vos applications de Cloud de façon économique.

- Identité & Gestion de l'accès

Active Directory de Microsoft Azure offre un service d'identité dans le cloud adapté aux entreprises. Il procure une expérience d'authentification unique pour les applications de Cloud et locales. Pour plus de sécurité et de conformité, ce service permet une authentification multi-facteur.

3.2 Infrastructure as a service

3.2.1 Azure Resource Manager

L'infrastructure de votre application est généralement constituée de plusieurs composants (peut-être une machine virtuelle, un compte de stockage et un réseau virtuel ou une application web, une base de données, un serveur de base de données et 3 services de tiers). Vous ne voyez pas ces composants comme des entités distinctes, mais plutôt comme des parties associées et interdépendantes d'une seule et même entité. Vous avez alors besoin de regrouper le déploiement, la gestion et la surveillance de ces différentes parties. Azure Resource Manager vous permet de travailler avec les ressources de solution sous forme de groupe. Vous pouvez déployer, mettre à jour ou supprimer toutes les ressources de votre solution dans le cadre d'une opération unique et coordonnée. Vous utilisez un modèle de déploiement pouvant fonctionner avec différents environnements (environnements de test, intermédiaire et de production). Le gestionnaire de ressources assure la sécurité, les fonctions d'audit et de balisage pour vous aider à gérer vos ressources après le déploiement.

TERMINOLOGIE

- Ressource : Elément gérable disponible dans Azure. Les ressources telles que les machines virtuelles, les comptes de stockage, les applications web, les bases de données et les réseaux virtuels sont courantes, mais il en existe beaucoup d'autres.

- Groupe de ressources : Conteneur réunissant les ressources associées d'une solution Azure. Le groupe de ressources peut inclure toutes les ressources de la solution, ou uniquement celles que vous souhaitez gérer en tant que groupe.

- Fournisseur de ressources : Un service qui fournit les ressources que vous pouvez déployer et gérer via Resource Manager. Chaque fournisseur de ressources propose des opérations pour travailler avec les ressources déployées. Parmi les fournisseurs de ressources courants figurent Microsoft.Compute, qui fournit la ressource de machine virtuelle ; Microsoft.Storage, qui fournit la ressource du compte de stockage ; et Microsoft.Web, qui fournit des ressources liées aux applications web.

- Modèle Resource Manager : Un fichier JSON (JavaScript Objet Notation) qui définit une ou plusieurs ressources à déployer vers un groupe de ressources. Il définit également les dépendances entre les ressources déployées. Le modèle peut être utilisé pour déployer les ressources de manière cohérente et répétée.

- Syntaxe déclarative : La syntaxe qui vous permet de déclarer « Voici ce que je souhaite créer » sans avoir à écrire la séquence de commandes de programmation pour le créer. Le modèle Resource Manager est un exemple de syntaxe déclarative. Dans le fichier, vous définissez les propriétés afin de déployer l'infrastructure vers Azure.

    - Avantages de l'utilisation de Resource Manager

Resource Manager offre plusieurs avantages :

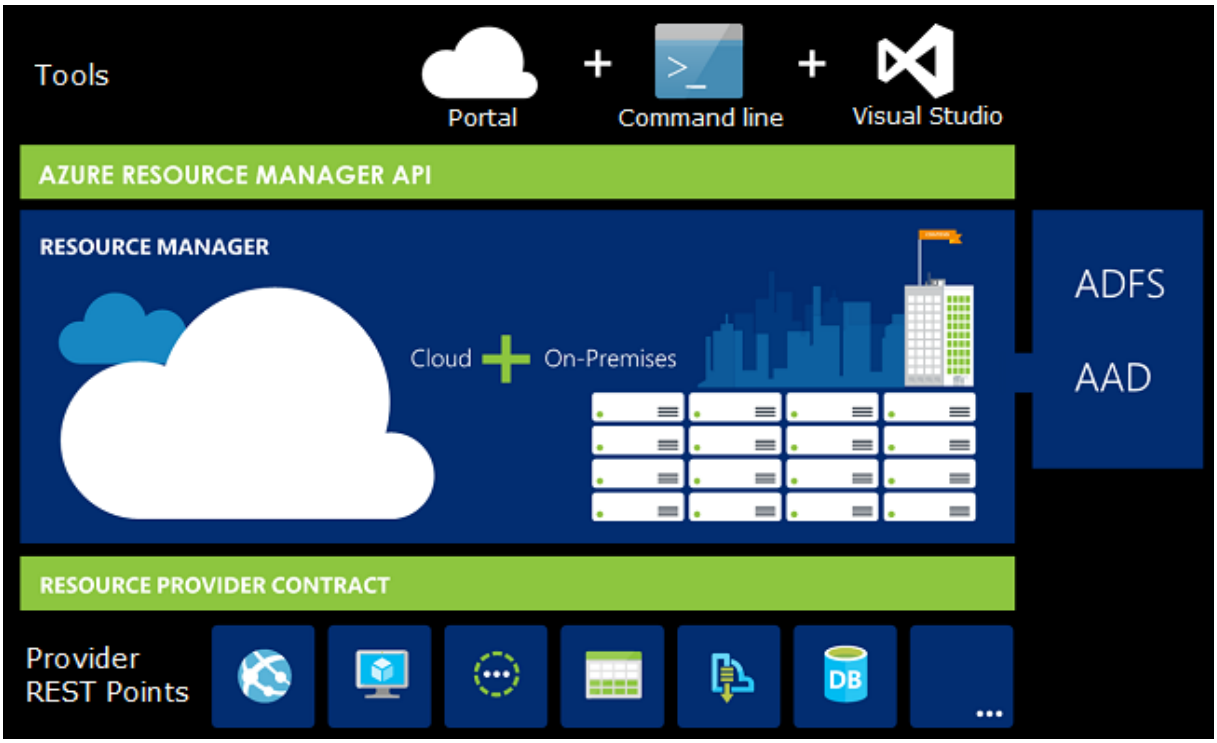
- Vous pouvez déployer, gérer et surveiller toutes les ressources de votre solution comme un groupe, plutôt que de les gérer individuellement.
- Vous pouvez déployer votre solution à plusieurs reprises tout au long du cycle de vie de développement et avoir ainsi l'assurance que vos ressources présentent un état cohérent lors de leur déploiement.
- Vous pouvez gérer votre infrastructure à l'aide de modèles déclaratifs plutôt que de scripts.
- Vous pouvez définir les dépendances entre les ressources afin de les déployer dans le bon ordre.
- Vous pouvez appliquer le contrôle d'accès à tous les services dans votre groupe de ressources, car le contrôle d'accès en fonction du rôle (RBAC) est intégrer en mode natif à la plateforme de gestion.
- Vous pouvez appliquer des balises aux ressources pour organiser logiquement toutes les ressources de votre abonnement.
- Vous pouvez clarifier la facturation de votre organisation en affichant les coûts d'un groupe de ressources partageant la même balise.

Resource Manager propose une nouvelle façon de déployer et de gérer vos solutions.

- Couche de gestion cohérente

Resource Manager fournit une couche de gestion cohérente pour les tâches à effectuer via Azure PowerShell, l'interface de ligne de commande Azure, le portail Azure, l'API REST et les outils de développement. Tous les outils utilisent un ensemble commun d'opérations. Vous utilisez les outils qui vous conviennent le mieux et vous pouvez les utiliser indifféremment sans risque de confusion.

L'illustration suivante montre comment tous les outils interagissent avec la même API Azure Resource Manager. L'API transmet les requêtes au service Resource Manager, qui authentifie et autorise les requêtes. Ensuite, Resource Manager achemine les requêtes vers les fournisseurs de ressources appropriés.



- Assistance

Les suggestions suivantes vous aideront à tirer le meilleur parti de Resource Manager lorsque vous travaillez avec vos solutions.

1. Définissez et déployez votre infrastructure via la syntaxe déclarative dans les modèles du Resource Manager, et non via des commandes impératives.
2. Définissez toutes les étapes de déploiement et de configuration dans le modèle. Aucune étape manuelle ne devrait intervenir dans la configuration de votre solution.
3. Exécutez des commandes impératives pour gérer vos ressources, par exemple démarrer ou arrêter une application ou une machine.

4. Organisez des ressources avec le même cycle de vie dans un groupe de ressources. Utilisez des balises pour toute organisation des ressources.

    - Groupe de ressources

Lorsque vous définissez votre groupe de ressources, vous devez prendre en compte certains facteurs importants :

1. Toutes les ressources de votre groupe doivent partager le même cycle de vie. Les opérations de déploiement, de mise à jour et de suppression porteront sur toutes les ressources du groupe. Si l'une des ressources, comme un serveur de base de données, doit exister dans un autre cycle de déploiement, elle doit appartenir à un autre groupe de ressources.
2. Chaque ressource ne peut exister que dans un seul groupe de ressources.
3. Vous pouvez à tout moment ajouter ou supprimer une ressource au niveau d'un groupe de ressources.
4. Vous pouvez déplacer une ressource d'un groupe de ressources vers un autre groupe.
5. Un groupe de ressources peut être utilisé pour définir l'étendue du contrôle d'accès des actions administratives.
6. Une ressource peut interagir avec celles d'autres groupes de ressources. Cette interaction est courante lorsque les deux ressources sont liées, mais ne partagent pas le même cycle de vie (par exemple, applications Web connectées à une base de données).

Lorsque vous créez un groupe de ressources, vous devez indiquer un emplacement pour ce groupe. Vous vous demandez peut-être « Pourquoi un groupe de ressources a-t-il besoin un emplacement ? Et, si les ressources peuvent avoir des emplacements différents de celui du groupe de ressources, pourquoi l'emplacement du groupe de ressources a-t-il une importance ? ». Le groupe de ressources stocke des métadonnées sur les ressources. Par conséquent, lorsque vous spécifiez un emplacement pour le groupe de ressources, vous indiquez où stocker ces métadonnées. Pour des raisons de conformité, vous devrez peut-être vous assurer que vos données sont stockées dans une région particulière.

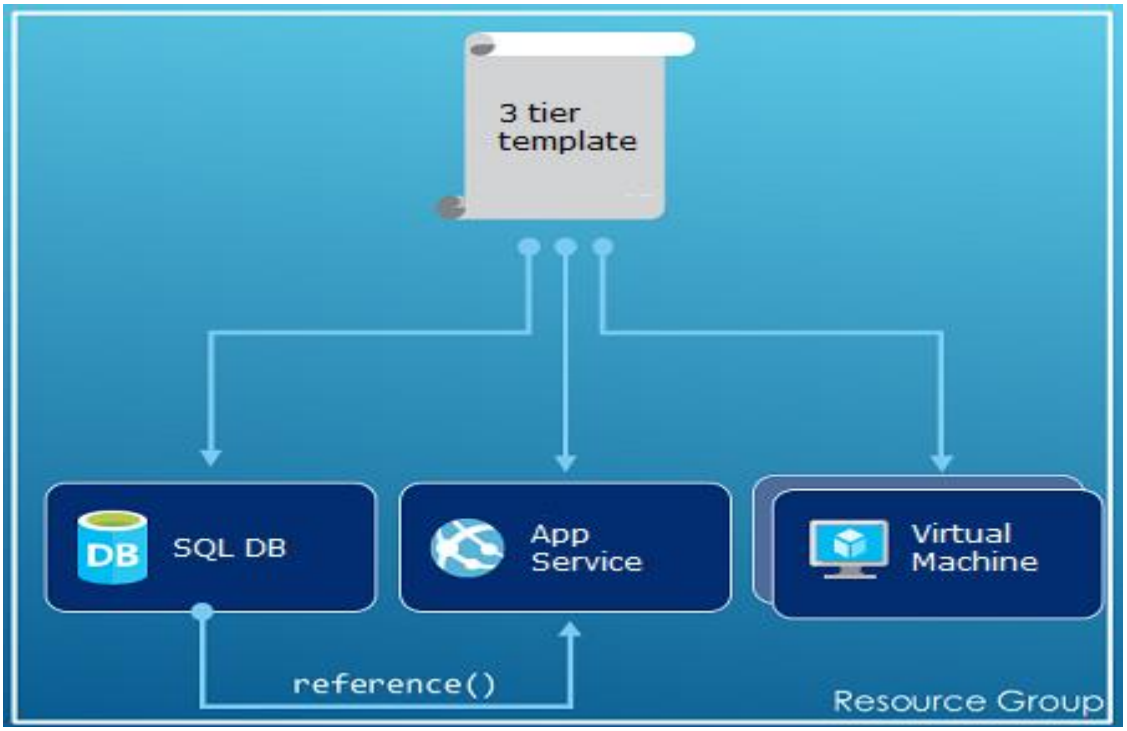
    - Fournisseurs de ressources

Chaque fournisseur de ressources propose un ensemble de ressources et d'opérations permettant de gérer un service Azure. Par exemple, si vous voulez stocker des clés et des secrets, vous travaillez avec le fournisseur de ressources **Microsoft.KeyVault**. Ce fournisseur de ressources fournit un type de ressource appelé **vaults** pour la création du coffre de clés et un type de ressource appelé **vaults/secrets** pour la création d'un secret dans le coffre de clés.

Avant de commencer à déployer vos ressources, vous devez connaître les fournisseurs de ressources disponibles. Connaître les noms des fournisseurs de ressources et des ressources vous permettra de mieux définir les ressources que vous allez déployer dans Azure.

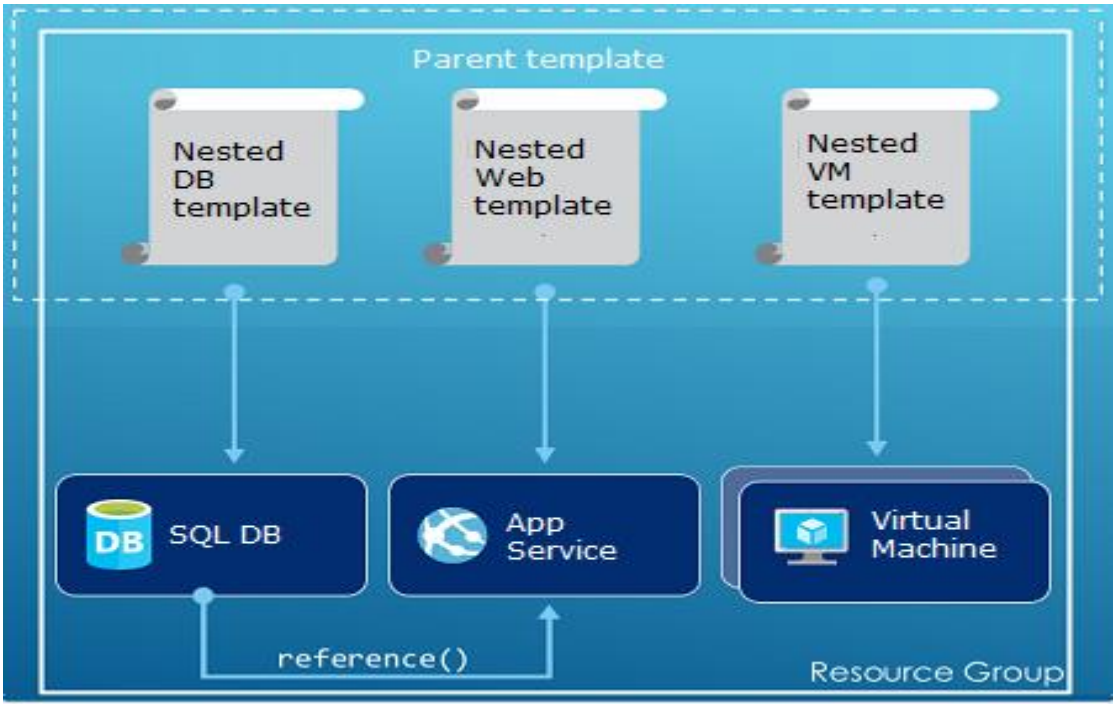
- Déploiement de modèle

Avec Resource Manager, vous pouvez créer un modèle (au format JSON) définissant l'infrastructure et la configuration de votre solution Azure. Un modèle vous permet de déployer votre solution à plusieurs reprises tout au long de son cycle de vie pour avoir la garantie que vos ressources présentent un état cohérent lors de leur déploiement. Lorsque vous créez une solution à partir du portail, cette solution inclut automatiquement un modèle de déploiement. Vous n'êtes pas contraint de créer votre modèle à partir de zéro, car vous pouvez partir du modèle de votre solution et le personnaliser en fonction de vos besoins spécifiques. Vous pouvez récupérer un modèle pour un groupe de ressources existant en exportant l'état actuel du groupe de ressources ou en affichant le modèle utilisé pour un déploiement particulier. L'affichage du modèle exporté est un moyen utile pour en découvrir plus sur sa syntaxe.
La manière dont vous définissez les modèles et les groupes de ressources dépend entièrement de vous et de la façon dont vous voulez gérer votre solution. Par exemple, vous pouvez déployer votre application à trois niveaux via un modèle unique pour un groupe de ressources unique.



Cependant, il est inutile de définir toute votre infrastructure dans un seul modèle. Il peut être judicieux de diviser les exigences de votre déploiement dans un ensemble de modèles ciblés destinés à un usage particulier. Vous pouvez facilement réutiliser ces

modèles pour différentes solutions. Pour déployer une solution particulière, créez un modèle de référence qui relie tous les modèles requis. L'illustration suivante montre comment déployer une solution à trois niveaux via un modèle parent qui inclut trois modèles imbriqués.



Azure Resource Manager analyse les dépendances pour vérifier que les ressources sont créées dans l'ordre approprié. Si une ressource dépend d'une valeur d'une autre ressource (par exemple, une machine virtuelle ayant besoin d'un compte de stockage pour les disques), vous devez définir une dépendance.

Vous pouvez également utiliser le modèle pour les mises à jour de l'infrastructure. Par exemple, vous pouvez ajouter une ressource à votre solution et ajouter des règles de configuration pour les ressources qui sont déjà déployées. Si le modèle spécifie de créer une ressource, mais que cette ressource existe déjà, Azure Resource Manager effectue une mise à jour au lieu de créer une autre ressource. Azure Resource Manager met à jour l'actif existant vers l'état qu'il présenterait s'il s'agissait d'une nouvelle ressource.

Resource Manager fournit des extensions pour les cas qui nécessitent des opérations supplémentaires, comme l'installation d'un logiciel spécifique non inclus dans la configuration. Si vous utilisez déjà un service de gestion de configuration, comme DSC, Chef ou Puppet, vous pouvez continuer à travailler avec ce service en utilisant des extensions.

Pour finir, le modèle devient partie intégrante du code source de votre application. Vous pouvez l'archiver dans votre référentiel de code source et le mettre à jour à mesure que votre application évolue. Le modèle est modifiable par le biais de Visual Studio.

Une fois votre modèle défini, vous êtes prêt à déployer vos ressources dans Azure.

- Tags

Resource Manager fournit une fonctionnalité de balisage vous permettant de catégoriser les ressources en fonction de vos exigences de gestion ou de facturation. Utilisez des balises lorsque vous disposez d'un ensemble complexe de groupes de ressources et de ressources et que vous souhaitez les visualiser de la façon qui vous convient le mieux. Par exemple, vous pouvez baliser des ressources qui jouent un rôle similaire dans votre organisation ou qui appartiennent au même département. Sans balises, les utilisateurs de votre organisation peuvent créer plusieurs ressources qui peuvent s'avérer difficiles à identifier et à gérer ultérieurement. Par exemple, vous pouvez souhaiter supprimer toutes les ressources d'un projet particulier. Si ces ressources ne sont pas balisées pour le projet, vous devez les rechercher manuellement. Le balisage constitue un levier important pour réduire les coûts inutiles dans votre abonnement.

Les ressources ne doivent pas nécessairement appartenir au même groupe de ressources pour partager une balise. Vous pouvez créer votre propre taxonomie de balise pour vous assurer que tous les utilisateurs de votre organisation utiliseront des balises communes plutôt que d'appliquer par inadvertance des balises légèrement différentes (telles que « dept » au lieu de « département »).

Mais vous avez également la possibilité de consulter les ressources balisées via le portail Azure.

- Contrôle d'accès

Resource Manager vous permet de déterminer les utilisateurs qui sont autorisés à exécuter des actions spécifiques pour votre organisation. Il intègre en mode natif le contrôle d'accès en fonction du rôle (RBAC) à la plate-forme de gestion et applique ce contrôle d'accès à tous les services de votre groupe de ressources.

Il existe deux principaux concepts à comprendre lorsque vous travaillez avec le contrôle d'accès en fonction du rôle :

- Définition des rôles : décrivent un jeu d'autorisation et peuvent être utilisées dans plusieurs affectations.
- Attributions des rôles : associer une définition à une entité (utilisateur ou groupe) pour une portée spécifique (abonnement, groupe de ressources ou ressource). Les portées inférieures héritent de la même attribution.

Vous pouvez ajouter des utilisateurs à des rôles prédéfinis spécifiques à la plate-forme et à la ressource. Par exemple, vous pouvez tirer parti du rôle prédéfini appelé Lecteur pour autoriser les utilisateurs à consulter des ressources sans pouvoir les modifier. Vous pouvez attribuer le rôle Lecteur aux utilisateurs de votre organisation qui ont besoin de ce type d'accès, puis appliquer ce rôle à l'abonnement, au groupe de ressources ou à la ressource.