Cloud Computing et Sécurité

Dominique Jouniot
dominique.jouniot@thylenea-si.com

Février 2017
1.0

Table des matières

Écosystème du Cloud Computing

- Les précurseurs : acteurs traditionnels et/ou à l'origine
- Les suiveurs : Il a bien fallu s'y mettre
- L'explosion : Tout le monde veut manger, donc ...
- La rationalisation des outils.

1. L'ecosystème

1.1. Les Origines

Démarré avant 2010, on trouve à ce moment dans l'écosystème :

- Amazon
- Yahoo
- Saleforce
- Gogrid

et Google...

Écosystème Origine

1.2. Les Attentistes

Rentrés par la suite, car le marché semblait bon :

- Microsoft Office 365. uniquement le mail, en réaction à Google
- Apple Icloud
- Ubuntu : Ubuntu One

1.3. L'explosion

Depuis envriron 2010, tout le monde tente d'offrir du "cloud" (l'interprétation de la définition change souvent).

Même les SSI proposent quelque chose. Les sociétés éditrices y voient souvent un nouveau moyen de "pénétration du marché.

- Cependant, tout n'est brillant ! !
- Attention à la sécurité et à l'infrastructure

Quelques acteurs (totalement non exhaustif):

- Dropbox : essentiellement du stockage
- Cloudwatt : IAAS français
- OVH : le fourre-tout du "cloud"
- IBM BPASS : SAAS (offre SmartCloud)
- OwnCloud : Ils porposent une offre complète ou faite votre "cloud" vous-même
- Microsoft Office 365 et Azure : On offre tout (SAAS collaboratif et Office)
- Bitnami, Turnkey : Grâce à Linux et à OpenVZ, on peut faire du "cloud" facilement. Plutôt "Outsider"

1.4. Définition du "Cloud"

Définition et concepts

"Le cloud Computing est un modèle permettant d'offrir un accès simple, en tout lieu et à la demande, avec un ensemble de ressources informatiques configurables et partagées : réseaux, serveurs, stockage, applications et services. cet ensemble de ressources peut être rapidement approvisionné et mise en service avec un minimum d'efforts de gestion et d'interventions du fournisseur" - NIST

Complément : Services partagés / Standard / Packagés

possibilité de servir de nombreuses entreprises utilisatrices de différentes ressources informatiques qui sont virtuelles et non réellement localisées. Affectées en fonction de la demande.

Complément : Scalabilité / Élasticité de la tarification

Les ressources sont rapidement et automatiquement disponibles. Provisionning et déprovisionning rapide et adaptable.

1.4.1. Présentation des modèles

5 caractéristiques essentielles

- Accès partout
- Elasticité rapide : augmentation de la capacité selon les besoins
- Utilisation quantifiable (sur mesure) : Facturation quantifiée selon les ressources utilisées
- Service à la demande (disponibilité) : Tout est automatisé et la disposition en libre-service
- Partage des ressources

3 modèles

- Saas (Software as a service) : Applications et Services. Domaine des utilisateurs finaux
- Paas (Plateform as a service) : Capacité de développement. Domaine des développeurs applicatifs
- Iaas (Infrastructure as a service) : Datacenter, Storage. Domaine des architectes réseaux et systèmes

4 Modèles de déploiement

- Public
- Private
- Hybrid
- Community

Complément : Iaas : Infrastructure as a service

Consommation de services de type Infrastructure (services fournit par le Cloud)

- Réseaux
- Stockage
- Serveur Hardware
- Virtualisation
- Serveur Software (OS)

Complément : Paas : Plateform as a service

Consommation de services de type Plateforme (services fournit pas le cloud)

- A minima la même chose que Iaas
- Bases de données
- Middelware

Complément : Saas : Software as a service

Consommation de services de type logiciels

- Même chose que Iaas
- Même chose que Paas
- Applications

1.4.2. Description des modèles d'usage

Cloud Public

- Utilisation ouverte au grand public
- Hébergé, géré et exploité par une entreprise, une institution académique, une organisation gouvernementale ou par une combinaison d'entre eux
- Ce modèle existe dans les locaux du prestataire de services Cloud

Cloud Privé

- Usage exclusif de l'infrastructure Cloud par une entreprise
- Hébergé, géré et exploité par l'entreprise, le prestataire de service Cloud ou par une combinaison des deux
- Ce modèle peut exister dans ou en dehors des locaux de l'entreprise

Cloud Communautaire

Usage exclusif d'une communauté spécifique de clients d'entreprise ayant les mêmes préoccupations

Hébergé, géré et exploité par une ou plusieurs communautés, un tiers ou une combinaison d'entre eux

Ce modèle peut exister dans ou en dehors des locaux de l'entreprise

Cloud hybride : Combinaison des trois

Combinaison des 2 ou 3 modèles de déploiement du Cloud liés entre eux par des technologies standardisées ou propriétaires permettant la portabilité des données et des applications

1.4.3. Pourquoi le Cloud ?

Techniquement

- Le réseau et internet offre du haut débit
- Capillarité des accès très élevé
- Possibilité de virtualisation, donc de scalabilité de la puissance de calcule
- Simplification des dialogues avec les informaticiens (plus de jargon "incompréhensible" ! ! !)

Financièrement

- Passage d'un modèle CAPEX (basé sur les investissements) à un modèle OPEX (dépenses d'exploitation)

- Diminution des coûts de RH et matériels : Donc diminution de l'OPEX
- Allocation de la ressource à la demande : Améliore l'agilité de l'entreprise, donc sa compétitivité

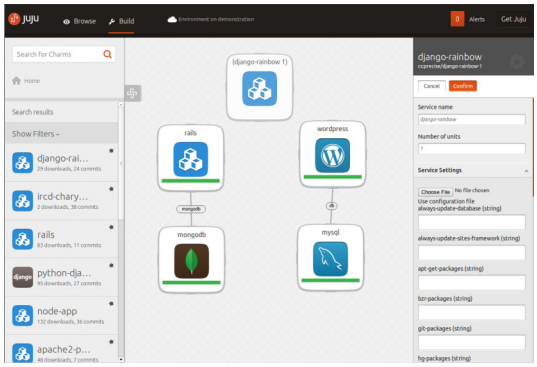
1.5. Les outils d'architecture pour du "Cloud" Privé

L'objectif est de fabriquer facilement des plate-formes de "Cloud" Privé.

Linux et les mécanismes de virtualisation ont beaucoup contribué à ces développements.

Les principaux outils :

- Openstack
  - Possibilité de créer des espaces logiques sur du physique
  - S'appuie sur Linux
- Proxmox
  - Hyperviseur Opensource
  - S'appuie sur Linux LXC, KVM et QEMU
  - Offre de la Virtualisation, de la paravirtualisation et de l'émulation
- Ubuntu Server (depuis 13.04)
  - Développement express des fonctions "Cloud"
  - OS Linux issue de Debian (Couche PAAS)
  - S'appuie sur MAAS (Metal as a Service) pour la gestion IAAS et le provisioning PAAS
  - S'appuie sur OpenStack pour les couches IAAS et SAAS
  - S'appuie sur JUJU pour la couche SAAS
- Et maintenant Docker



JUJU : interface de management d'une architecture "Cloud"

1.6. Le Cas OpenStack

Produire une plate forme Open Source qui permet la mise en place de "Cloud public" ou de "Cloud Privé", massivement configurable

Crée en 2010 par la fusion de RACKSPACE (rendu open source) et de Nebula (produit par la Nasa)

- Licence libre Apache 2.0
- Processus de design ouvert
- Largement accessible en Open Source
- Communauté ouverte et très documentée
- Design modulaire pour le déploiement avec définition d'API
- Développé en Python

De nombreux acteurs commerciaux participent au développent et au déploiement :

Dont : Microsoft, Citrix, Ubuntu, Dell, etc.

S'appuie sur deux grands concepts :

- Le "provisioning" de machines virtuelles
- Le stockage d'objet (Object Storage)

Conseils et Recommandations

II

Pour partir dans le "Cloud", il faut envisager la sécurité de ses données.

Présentation de quelques conseils et recommandations.

1. Conseils, Recommandations et Sécurité

1.1. La Sécurité

Les points principaux

- La virtualisation des services informatiques amène les entreprises à redéfinir les frontières de leurs infrastructures technologiques à l'extérieur des limites physiques de l'entreprise.
- Dans un contexte de menaces externes plus variées et géographiquement disséminées, cet élargissement du périmètre réseau contribue à rehausser la sécurité des infrastructures de l'entreprise.

1.1.1. L'analyse des Risques

On ne part pas dans le "Cloud" sans Politique de sécurité

a) La politique de sécurité

La politique de sécurité, au sens 27001 :

- La réalisation d'une analyse des risques
- La mise en place d'un système de management de la sécurité
    - Equipe et organisation sécurité opérationnelle,
    - Documentations de base (Politiques, normes, standard, procédures)
    - Une méthodologie d'amélioration continue

L'analyse de risque

Le définition du Risque :

- Menace
- Vulnérabilité
- Bien

La couverture des risques :

- STAR

Les documents

- L'engagement de la Direction Générale : (Non conformité majeure)
- La politique de sécurité : Référentiel des règles et couverture des risques
- Les standards techniques et organisationnels
- Les procédures de mise en applications
- Les Enregistrements
- Les K.P.I de sécurité

1.1.2. Les Menaces

Concernant les donnés :

- Disponibilité
- Confidentialité
- Intégrité

Concernant le réseau :

- Tentatives d'intrusion
- Surveiller l'ensemble de la sécurité et activité des réseaux

Concernant les utilisateurs finaux :

- Le contrôle d'accès / authentification
- Gestion des habilitations
- Traçabilité des données
- Renforcement de la sécurité du poste de travail

1.1.3. Les Menaces du cloud

Sept risques ont été définis par les experts

- La confiance dans son prestataire

Sous-traiter ses données les plus sensibles ne peut s'envisager que si l'on a la certitude que les informaticiens du sous-traitant sont dignes de confiance et que leurs faits et gestes sont contrôlés.

- Conformité réglementaire

Les fournisseurs de « cloud computing » doivent se plier à toutes les demandes d'audit externes et disposer de toutes les certifications de sécurité nécessaires pour que leurs clients aient la certitude d'être couverts.

- Localisation des données

L'utilisation de sites de stockage multiples fait partie des points forts du « cloud computing », mais aussi de ses points faibles.

- Isolement des données

Il faut s'assurer de leur chiffrement et de la possibilité de les isoler.

- Récupération des données

Ignorer où se trouvent ses données ne veut pas dire que l'on ne puisse pas avoir l'assurance des moyens mis en place pour leur sauvegarde en cas de problème majeur.

- Coopération avec la justice

Une architecture en « cloud computing » ne doit pas empêcher de répondre aux injonctions de la justice, que ce soit pour des raisons fiscales ou d'ordre juridique.

- Viabilité à long terme

Le fournisseur idéal de « cloud computing » ne défaille jamais et gagne suffisamment bien sa vie pour, d'une part, ne pas déposer le bilan et, d'autre part, ne pas devenir une cible et être absorbé.

1.2. Les Règles de sécurité à suivre et contrôler

- Ces règles sont extraites du référentiel de l'ISF (Information Sécurité Forum, version 2013)
- La 27001 aborde le sujet au travers de normes associées (depuis sa version 2013).
- - L'ISO 27017 :2015 : Contrôles basés sur la 27002 pour les services Cloud
- - L'ISO 27018 :2014 : Code of practice. Pour la protection des données personnelles (PII) dans les clouds publics (agissant en tant que manager de données personnelles)
- Le RGS v2 de l'ANSSI,
- Des tentatives tel que "Secure Cloud" (label de certification supporté par l'ANSSI)
- Le référentiel de qualification des prestataires de services sécurisés d'informatique en nuage (cloud computing) - V1.3 30/07/2014 (Le chapitrage est identique à la 27001)

Attention à la loi dans un contexte internationnal

- Les états sont, en général, souverain sur leur territoire.
- Le "Patriot Act" américain ne garantit pas la divulgation des informations, même si l'éditeur l'affirme
- Le "Safe Harbor", depuis septembre 2016 le "Privacy Shield", devrait garantir la protection des données (Fake ?)

1.2.1. L'outsourcing

Les règles d'outsourcing s'appliquent directement à une migration dans le "Cloud public"

Méthode : CF16.3.1

Etablir un processus afin de suivre les fournisseurs et le transfert d'activité

Méthode : CF16.3.2

Lors de l'établissement des besoins pour l'outsourcing :

- Evaluation des risques et les fonctions métiers à outsourcer
- Evaluer les exigences réglementaires et légales
- Identifier les activités critiques et sensibles
- Prendre en compte la classification de l'information
- Prendre en compte les inter dépendances entre les fonctions outsourcées et les fonctions qui restent en interne
- Préparer les stratégies de sortie dans l'éventualité d'une sortie prématurée du contrat

Méthode : CF16.3.3

Avant de sortir les environnements métiers, s'assurer de l'accord de la sécurité et des propriétaires métier

Méthode : CF16.3.4

Les contrats doivent :

- Etre revu périodiquement
- Approuvés par la direction générale
- Maintenu à jour

Méthode : CF16.3.5

Les contrats doivent :

- S'assurer que le fournisseur se plie à la politique de sécurité
- S'assurer que le fournisseur maintient la confidentialité de l'information
- S'assurer que le fournisseur contrôle l'intégrité de l'information
- S'assurer de la disponibilité des systèmes
- Offrir des mécanismes de suivi et d'exploitation des incidents

Méthode : CF16.3.6

Les fournisseurs doivent :

- Limiter et contrôler les accès aux seul ayant droit
- protéger les informations concernant la vie privée
- Formaliser les relations de sous-traitances qu'ils utilisent

Méthode : CF16.3.7

Les contrats doivent

- S'assurer du suivi des règles de "Change Management"
- S'assurer de la destruction ou retour de l'information à des dates prévues
- S'assurer du BCP (Plan de Continuité d'Activité)

Méthode : CF16.3.8

Les contrats doivent :

- S'assurer des contrôles des licences
- S'assurer de la propriété intellectuelle
- Prévoir la possibilité pour l'organisme d'auditer le fournisseur (détail des modalités d'audit)

1.2.2. La politique de sécurité "Cloud Computing"

Un document de politique de sécurité "Cloud Computing" doit être formalisé

Il doit être fourni à l'ensemble des acteurs de l'entreprise qui peuvent acheter ou utiliser des services "Cloud"

Méthode : CF16.4.1

La politique "Cloud" doit :

- Etre basée sur la stratégie de sécurité de l'organisme
- Approuvée par la Direction Générale
- Distribuée à tous les acteurs concernés de l'organisation
- Appliquée ! !

Méthode : CF16.4.2

L'équipe sécurité doit aider les fonctions métiers à :

- formaliser, contractualiser et acheter les services "Cloud"

Méthode : CF16.4.3

Il convient de s'assurer du niveau de connaissance et de maturité du sujet par les acteurs concernés

Méthode : CF16.4.4 / CF16.4.5

Faire, valider et compléter l'analyse des risques et la classification de l'information

Méthode : CF16.4.6 / CF16.4.10

Définir et mettre en place les standards et les processus de sécurité, en conformité avec la couverture des risques.

On trouve :

- les règles de chiffrement
- les restrictions liées à certaines juridictions (Lois diverses : LCEN, ISF, GDPR, ASIP Santé, RGS v2, etc.)
- La gestion des disques durs, des backups
- La sécurité des communications et des accès (HTTPS, VPN, TLS, etc.)
- La qualité des liens d'accès, les méthodes d'accès (fibre, 3G/4G, sans fils, etc.)

1.3. Quelques questions à se poser

- Les prestataires sont-ils assujettis aux lois de la République Française si les systèmes sont

à l'étranger ?
- Comment faire appliquer les politiques de sécurité internes ? (27001, PGSSI de l'ANSSI, etc.)
- Que faire si le prestataire ferme ?
- Le Cloud est-il auditable ?
- Les données peuvent-elles être tracées dans le nuage ?
- Comment traite-t-on les cas de réversibilité ?
- Qui est responsable de la gestion des vulnérabilités ?
- Qui est responsable en cas d'attaque par rebond ? Qui gère les équipements de sécurité ?
- - Google est souvent utilisé pour faire des DDOS, qui est responsable ? Quels sont les recours possible ?

1.3.1. Aspect réglementaires et contractuels

- Il est recommandé d'élaborer des contrats exhaustifs avec le prestataire qui prennent en compte toutes les contraintes (mais c'est difficile, voir les contrats Google, IBM, etc.)
- Les risques sont identiques (à de l'interne) qu'il s'agisse de la continuité de services, de la capacité à récupérer et consolider les données, du patrimoine de l'entreprise (PRA, PCA, PSI).
- La sécurité des informations constitue également un point fondamental dans un contrat de prestations de services.
- La gestion des vulnérabilités et des tests d'intrusion (les obligations d'accords signés, les limitations liées à la mutualisation, l'intérêt de tels tests ! !)

1.3.2. Contraintes légales

- Le propriétaire des données reste responsable en cas d'infraction à la législation du pays où il est basé.
- Dans une infrastructure mondiale, les données relèvent du régime juridique du pays dans lesquelles elles sont détenues (exemple la Chine).
- Le contrat initial doit contenir toutes les garanties en cas de restitution de l'infrastructure, par exemple lors du rachat de la société informatique.
- Il n'est pas interdit au client du service de Cloud Computing de vérifier que les données sont récupérables, exploitables et de vérifier les possibilités de chiffrement de celles ci.

1.4. Points à faire et contrôler

Les actions

- Demander au fournisseur ses standards de sécurité.
- Demander au fournisseur où vos données seront sauvegardées.
- Demander la législation en vigueur sur la protection des données dans les pays concernés.
- Signer un contrat sur la responsabilité de chacun.
- Mettre en place une authentification forte (si possible en SSO).
- Demander les moyens de vérifier la bande passante et les espaces de stockage.
- Demander au fournisseur de vous garantir la puissance calcul que vous louez.
- Faite des audits pour vous assurer de la conformité du fournisseur de nuage.
- Exiger les résultats des tests d'intrusion, à minima sur les plate-formes mutualisées

Les méthodes de sécurité

- Lutter contre les virus dans les nuages (avec les outils d'anti virus classiques).
- Lutter contre le hacking des nuages (Faire des tests d'intrusion, en accord avec le provider).
- Surveillance des logiciels défectueux (sur les postes locaux).
- Sécurisation des accès aux données.
- Renforcer l'intégrité et la confidentialité des données.
- Garantir la disponibilités des données
- Cohabitation et mutualisation des données dans les Cloud (s'assurer de l'étanchéité).

Ultime conseil

Et ne mettez jamais tous vos œufs dans le même panier !

Conclusion

Peut-on réellement faire des pronostics d'avenir ?

- Une anecdote : X11 et Xerox

PRISM, Snoden et leurs copains ont-ils changer la donne ?

- 30% de CA en moins dans le "Cloud" américain depuis le début des annonces "Snowden"

«

> *Dans un texte de Henri de Gand (1217 – 1293) l'on trouve :*
>
> *Origène sur le chapitre XXVI de la Genèse écrit :*
>
> *« Essayons de faire ce que la sagesse nous enjoint quand elle dit: « Bois l'eau de tes sources et de tes puits et possède en propre ta fontaine » (Pr 5,18 et18).*
>
> *Toi aussi, qui m'écoutes, essaie de posséder ton propre puits et ta propre fontaine » ...*
>
> *C'est pour cela que Zénon dit « Jusqu'à quand dépendras-tu d'autrui? Produis quelque chose de toi-même ».*
>
> *Cité par Gilbert Dahan, Lire la Bible au Moyen Age, Essais d'herméneutique médiévale, Droz, p.29-30, 2009.*

 »

=> C'est beau les nuages, mais ne préfère-t-on pas voir le soleil ?