

Conférence IDC
Cloud Computing 2012

La sécurité des données hébergées dans le Cloud

25/01/2012

Patrick CHAMBET

Responsable du Centre de Sécurité
C2S, Groupe Bouygues

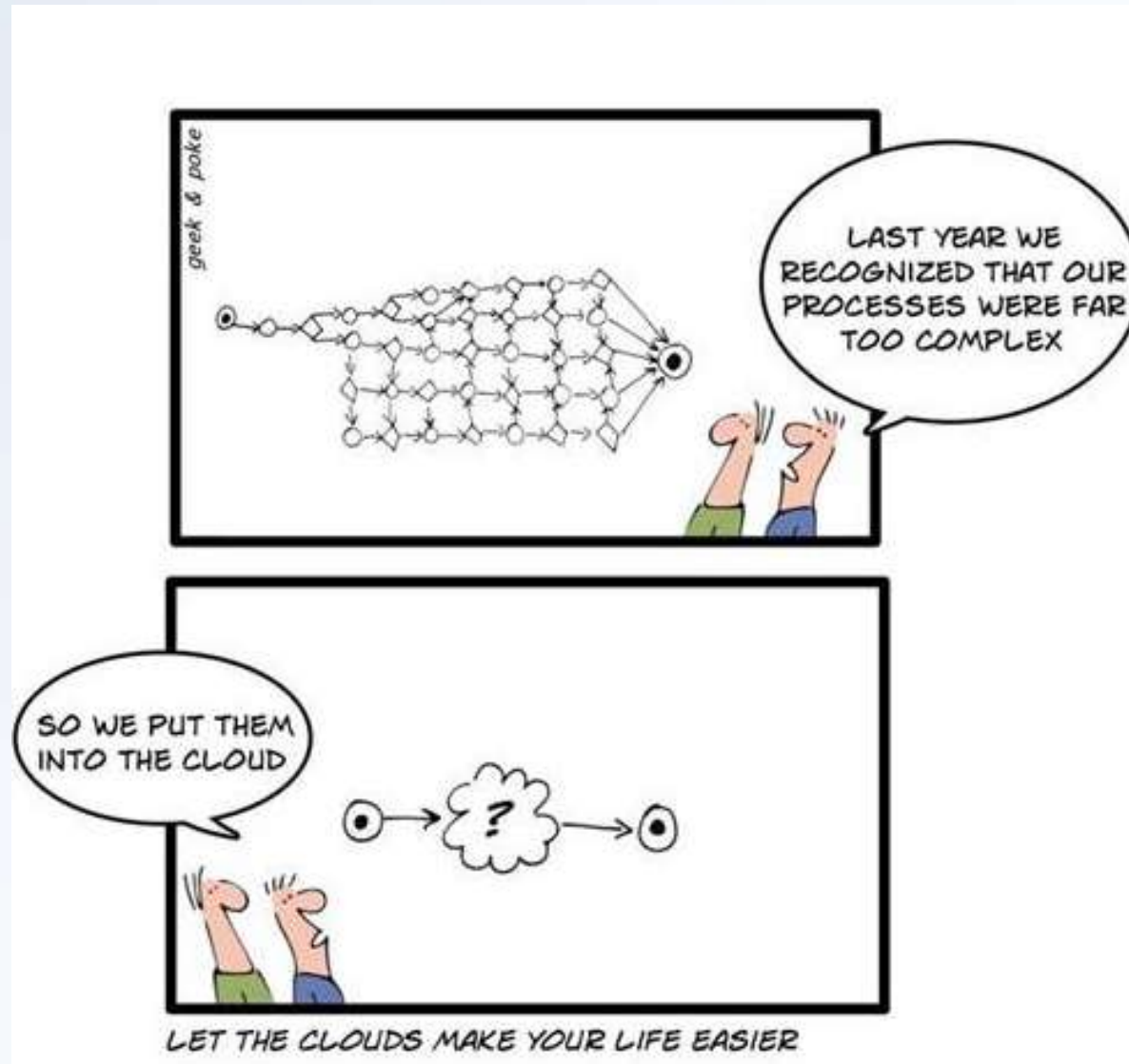




Planning

- **Quelques rappels**
- **Vue simplifiée du Cloud Computing**
- **Les problématiques de sécurité des données**
- **Les moyens de protection des données**

La solution à tous les problèmes ?





Quelques rappels

- **Définition**

- *Capacités informatiques (logiciel, plate-forme, CPU, stockage, ...) délivrées comme des services à la demande*

- **Particularités**

- *Accès distant (réseau)*
- *Pas de visibilité sur l'infrastructure sous-jacente (d'où le terme « nuage »)*
 - Forte mutualisation des ressources
- *Standardisation*
- *Facturation à l'usage, avec de gros écarts possibles*



Quelques rappels

- **3 types de services**

- *SaaS (Software as a Service)*

- Ex: CRM (SalesForce), Google Apps, Office 365

- *PaaS (Platform as a Service)*

- Ex: site Web packagé Apache + PHP + MySQL

- *IaaS (Infrastructure as a Service)*

- Ex: machines virtuelles « nues » créées à la demande



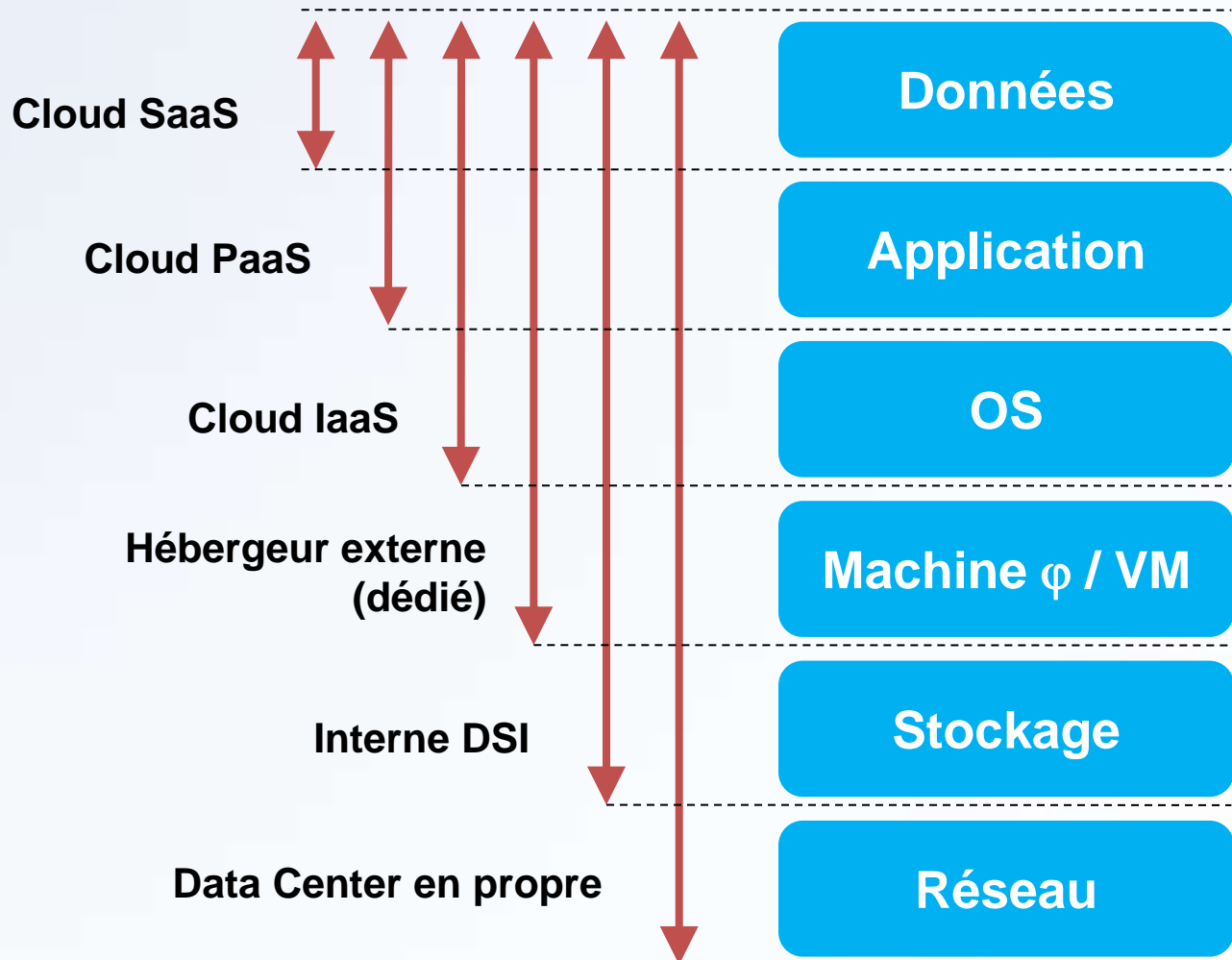
Quelques rappels

- **2 grandes catégories**
 - *Cloud public (on partage l'infra avec d'autres)*
 - *Cloud privé (on partage « peu » de choses)*
- **2 localisations**
 - *Cloud externe (chez un fournisseur de Cloud)*
 - *Cloud interne (dans sa propre DSI)*

➔ *4 possibilités*

Vue simplifiée du Cloud Computing

- Degré de contrôle de l'entreprise



Les problématiques de sécurité

- **Sur les données**

- *Dépendent du choix des données mises dans le Cloud*
 - Données « cœur de métier » ou non
- *De la localisation des données*
 - Duplication, dispersion, lieux géographiques hors UE, ...
- *Des contraintes légales*
 - « Paquet télécom » : notification des violations de données personnelles
 - Réquisitions judiciaires : comment y répondre ?
- *Protection des données*
 - Qui peut y accéder (personnel du fournisseur, étanchéité entre clients) ?



- **Sur les applications**

- *Qui a accès à quoi ?*
 - Profils d'utilisateurs
- *Traçabilité des accès et des actions*
 - Qui a fait quoi, quand, sur quelle donnée, depuis où ?



Les solutions de sécurité

- **Localisation des données**

- *Savoir localiser géographiquement ses données*
 - Pouvoir assurer à ses clients que leurs données sont stockées dans l'UE ou le groupe de l'article 29
- *Savoir s'assurer de la purge (destruction sécurisée) des données clients, à tous leurs emplacements*
- *Planifier la récupération d'informations en cas de saisie judiciaire (ex: messagerie hébergée dans le Cloud)*
- *Prévoir la réversibilité*

Les solutions de sécurité

• Protection des données

• *Chiffrement des données*

- Dans les bases de données
- Dans les fichiers

• *Chiffrement transparent*

- Chiffrement « à la volée » par l'application ou la base de données: facile en mode SaaS
- Les clés de chiffrement sont forcément stockées dans le Cloud
- Difficile d'interdire l'accès des administrateurs du Cloud aux clés

• *Chiffrement de bout en bout*

- Les clés sont détenues par les clients finaux
- Le fournisseur de Cloud ne peut pas déchiffrer les données
- Mais nécessite un client lourd ou un proxy de chiffrement (difficile en mode SaaS)





Les solutions de sécurité

- **Authentification des utilisateurs**

- *Authentification nominative*

- *3 solutions*

- 2 annuaires distincts (entreprise + Cloud) avec synchronisation

- Délégation d'authentification

- Fédération d'identités (SAML, WS-Fédération, ...)

} **Action nécessaire
de la DSI**

- **Habilitation et contrôle d'accès**

- *Mise en place de permissions d'accès fines sur les ressources et les données*

- *Interdire les comptes génériques et le partage de comptes*



Les solutions de sécurité

- **Traçabilité**

- *Deux types de besoins*

1. Surveillance des accès aux ressources dans le Cloud
2. Enquête / forensics en cas d'incident

- *Recueillir des traces suffisamment complètes (centraliser ou croiser les journaux de logs)*
- *Protéger l'accès aux traces par le fournisseur de Cloud*
- *Organiser la consultation ou la transmission des logs au client du Cloud*
- *Prévoir la purge des logs au-delà d'une certaine période*



Les solutions de sécurité

- **Ressources utiles**

- *Cloud Security Alliance*

- <http://cloudsecurityalliance.org/>

- <http://www.cloudsecurityalliance.fr/> (chapitre français)

- *Notamment la Cloud Control Matrix (CCM)*

- <https://cloudsecurityalliance.org/research/ccm/>



Questions ?