

- » BOOST PERFORMANCE
- » REDUCE COST
- » INCREASE AGILITY
- » ENHANCE CRM
- » SHORTEN TIME TO MARKET
- » DRIVE INNOVATION
- » IMPROVE EFFICIENCY
- » INCREASE ADAPTIVITY
- » ENABLE BUSINESS TRANSFORMATIONS
- » ENSURE REGULATORY COMPLIANCE



CONSULTING > SOLUTIONS > OUTSOURCING

Amazon Web Services: prêt pour l'entreprise?

Une analyse de la sécurité des services web d'Amazon

Aurélien Pelletier

Mars 2010

Agenda

1 – Cloud Computing

- *Qu'est que le Cloud Computing*
- Les 3 différents modèles de services du Cloud
- Les 4 modes de déploiement

2 – Amazon Web Services

- Amazon Simple Storage Service (S3)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Block Store (EBS)
- Amazon Virtual Private Cloud (VPC)

3 – La sécurité d'AWS

- La sécurité et le cloud
- La sécurité d'AWS
- Conformité aux normes ISO 27002

4 – Conclusions



Cloud Computing

Le Cloud computing est un modèle d'accès en réseau et à la demande à des ressources informatiques partagées et configurables (des réseaux, serveurs, du stockage, applications et services) qui peuvent rapidement être provisionnés et mises à disposition avec un effort minime de gestion ou d'interaction avec le fournisseur.

Définition du NIST

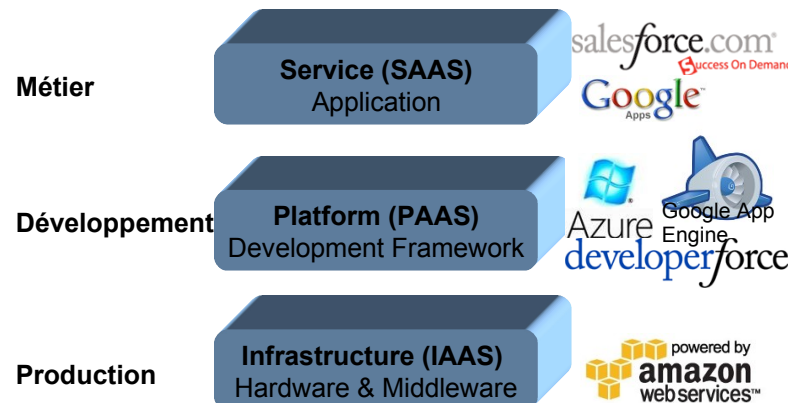
Cinq caractéristiques essentielles

- » (de)Provisionnement rapide
- » Service mesuré
- » Self-Service à la demande
- » Accès en réseau
- » Partage de ressources

Quatre modèles de déploiement

- » Publique
- » Privé
- » Communautaire
- » Hybride

Trois modèles de services



Amazon Web Service Prêt pour l'entreprise ?

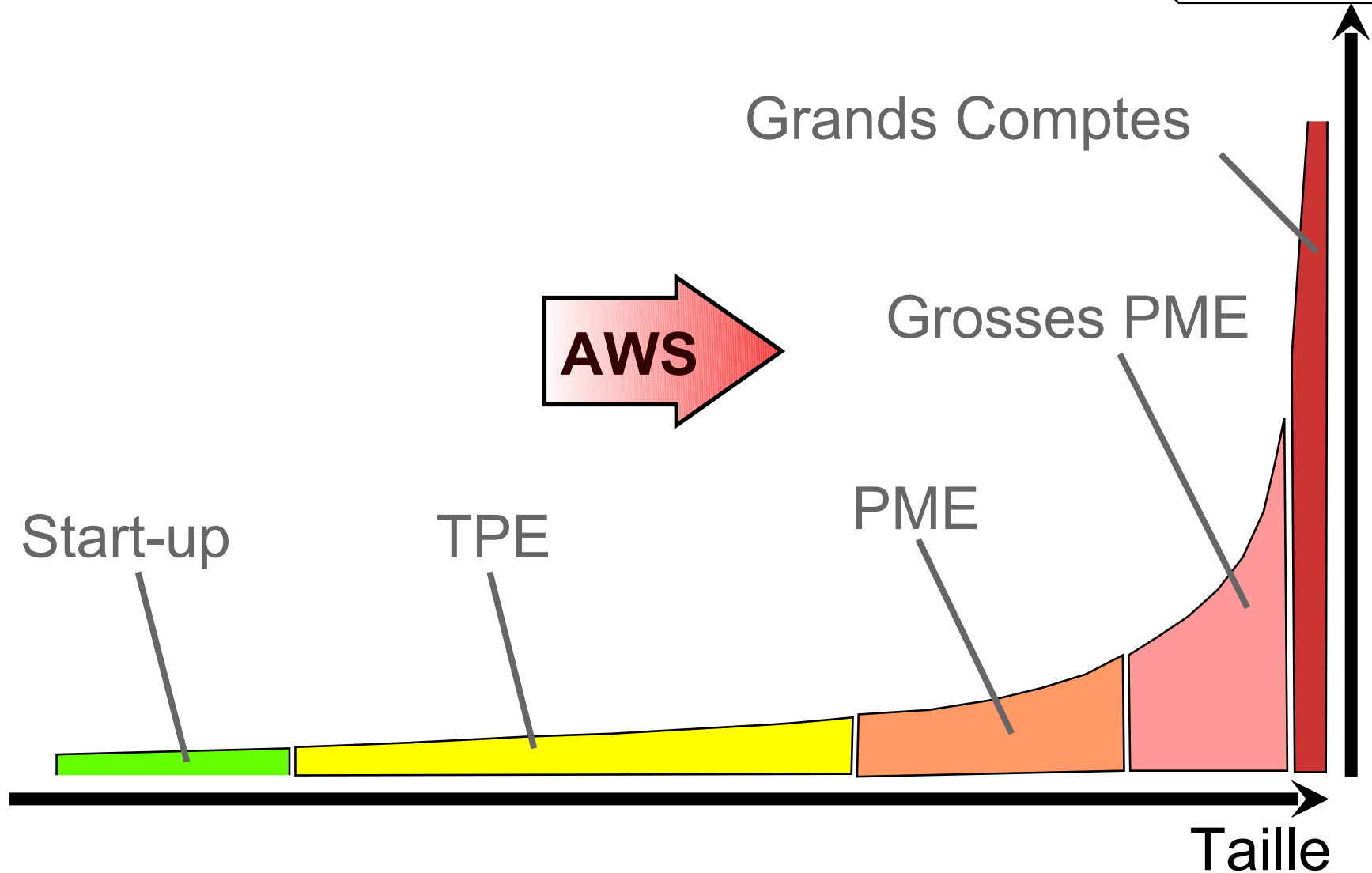
“running a number of servers on the departmental secretary's credit card; after all, computing resources are just office supplies

Michael Nygard



La Long Tail

Appliquée aux budgets IT



Agenda

1 – Cloud Computing

- *Qu'est que le Cloud Computing*
- Les 3 différents modèles de services du Cloud
- Les 4 modes de déploiement

2 – Amazon Web Services

- Amazon Simple Storage Service (S3)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Block Store (EBS)
- Amazon Virtual Private Cloud (VPC)

3 – La sécurité d'AWS

- La sécurité et le cloud
- La sécurité d'AWS
- Conformité aux normes ISO 27002

4 – Conclusions



Amazon Web Services

» Services d'infrastructure et de middleware

- » Partagés
- » Disponibles à la demande (en moins de 5 min)
- » Mesurés
- » Accessible par Internet

- » Stokage S3/EBS
- » Serveurs EC2
- » Réseau VPC
- » D'autres services

» Basé sur

- » Les technologies de virtualization (Xen)
- » Des développements propriétaire et secret

Service (SAAS)
Application

Platform (PAAS)
Development Framework

Infrastructure (IAAS)
Hardware & Middleware



Le rythme de l'innovation d'Amazon AWS

- | | |
|-------------------------------------|------------------|
| » Simple Storage Service (S3) | 13 mars 2006 |
| » Simple Queuing Service (SQS) | 11 juillet 2006 |
| » Elastic Cloud Computing (EC2) | 23 août 2006 |
| » Flexible Payment Service (FPS) | 2 août 2007 |
| » Simple DB | 13 décembre 2007 |
| » DevPay | 13 décembre 2007 |
| » Elastic Block Store (EBS) | 20 août 2008 |
| » Cloudfront | 18 novembre 2008 |
| » Elastic MapReduce | 2 avril 2009 |
| » Virtual Private Cloud | 26 août 2009 |
| » Relational Database Service (RDS) | 27 octobre 2009 |
| » Versionning for S3 | 8 février 2010 |

**3 innovations
majeures
par an**

Amazon Simple Storage Service (S3)

- » Service de stockage
 - » Fiable
 - » Hautement disponible
 - » Capable de monter en charge
 - » Rapide
- » Interface HTTP(s) ou SOAP
- » Gestion des droits d'accès (ACL)
- » Replication synchrone des données dans plusieurs centre de données physiquement éloignés
- » Fichier de 1 octet à 5 Go
- » Support du protocole Bittorrent
- » Conçu pour une disponibilité de 99,99% (99,9% garantie par SLA)

Amazon Simple Storage Service (S3)



http://www.allthingsdistributed.com/2009/11/82_billion_objects_in_amazon_s.html

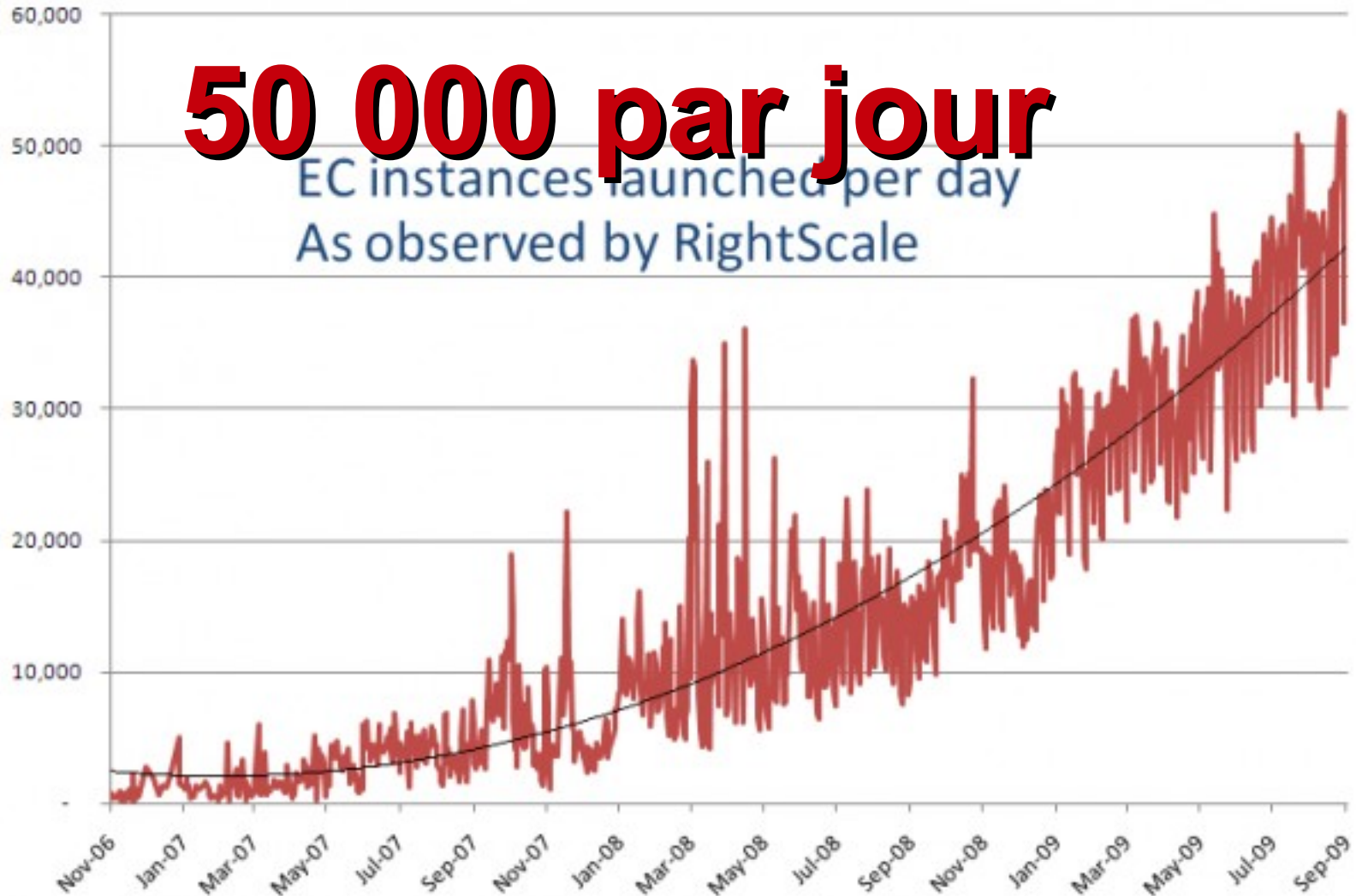
Amazon Elastic Compute Cloud (EC2)

- » Puissance de calcul à la demande
- » Basé sur l'hyperviseur open source Xen
- » Disponibilité de 99,95% garantie par SLA
- » Toutes les instances sont protégé par un firewall
- » Pas de multicast ou de broadcast
- » Possibilité de démarrer des instances dans différentes zones ou régions physiques
- » Services additionnel:
 - Elastic IP: adresse IP publique fixe relié dynamique à des instances
 - Elastic block store (EBS) stockage persistant pour EC2
 - Cloud Watch (monitoring)
 - Auto Scaling
 - Load balancing
 - Hadoop cluster
 - Mysql As A Service (RDS)

Amazon Elastic Compute Cloud (EC2)

50 000 par jour

EC instances launched per day
As observed by RightScale



<http://blog.rightscale.com/2009/10/05/amazon-usage-estimates/>

Elastic Block Store (EBS)

- » Le disque dur des instances EC2 est transient (perdu à chaque arrêt)
- » EBS fournit des espaces de stockage persistents pour EC2
- » EBS est une sorte de NAS (technologie propriétaire Amazon)
- » Un volume EBS est un disque dur non formaté
 - » accessible au niveau block
 - » on peut y installer n'importe quel système de fichiers
 - » ou monter du RAID 5
- » Il est possible de prendre des snapshots et de les sauvegarder vers S3
- » De 1Gb à 1Tb

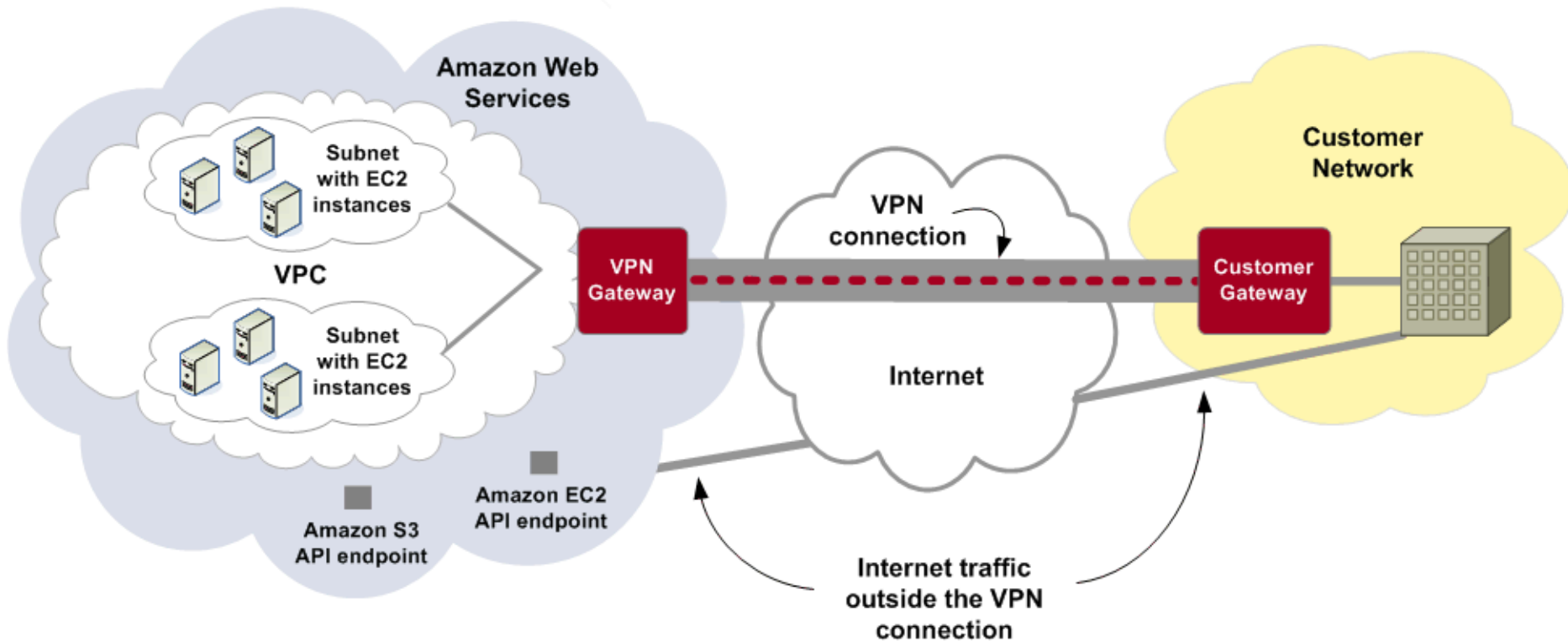
Cloud

Private Cloud

Virtual Private Cloud

Amazon Virtual Private Cloud (VPC)

Un Virtual Private Network (IPSec) pour relier votre datacenter à celui d'Amazon
Les machines virtuelles restent partagé dans un cloud public.



Agenda

1 – Cloud Computing

- Qu'est que le Cloud Computing
- Les 3 différents modèles de services du Cloud
- Les 4 modes de déploiement

2 – Amazon Web Services

- Amazon Simple Storage Service (S3)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Block Store (EBS)
- Amazon Virtual Private Cloud (VPC)

3 – *La sécurité d'AWS*

- La sécurité et le cloud
- La sécurité d'AWS
- Conformité aux normes ISO 27002

4 – Conclusions



Problèmes de sécurité

- » Les caractéristiques essentielles du cloud sont à l'opposé des bonnes pratiques de sécurité:
 - Partage de ressources
 - Accès réseau
 - Provisionning à la demande

- » Le business model pose des problèmes légaux

- » Sans parler de la **confiance**

Amazon Web Services SECURITY

TODAY
9:30



Amazon Web Service Security



Security.

We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet. Accordingly, [...], you acknowledge that

you bear sole responsibility for adequate security,
protection and backup of Your Content and Applications.

We strongly encourage you, where available and appropriate, to

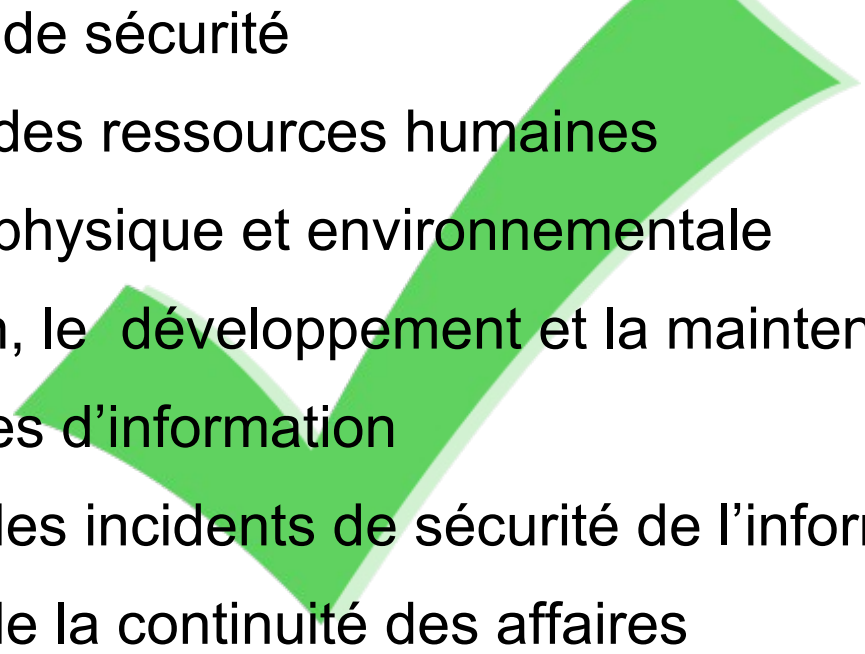
- (a) use encryption technology to protect Your Content from unauthorized access
- (b) routinely archive Your Content
- (c) keep your Applications or any software that you use or run with our Services current with the latest security patches or updates.

We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications.

<http://aws.amazon.com/agreement/>

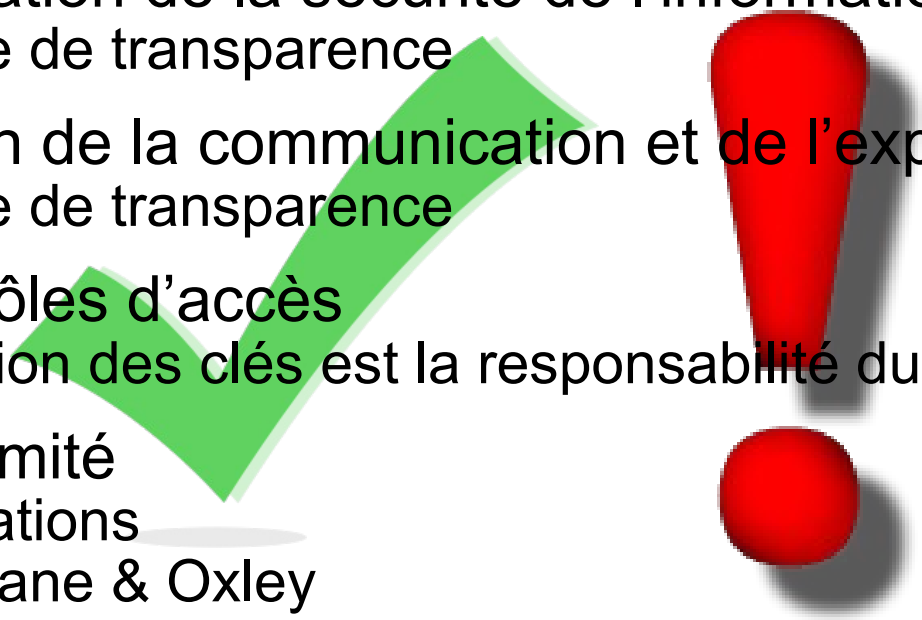
11 thèmes de sécurité de l'information :

- » La politique de sécurité
- » L'organisation de la sécurité de l'information
- » La gestion des actifs
- » La sécurité des ressources humaines
- » La sécurité physique et environnementale
- » La gestion de la communication et de l'exploitation
- » Les contrôles d'accès
- » L'acquisition, le développement et la maintenance des systèmes d'information
- » La gestion des incidents de sécurité de l'information
- » La gestion de la continuité des affaires
- » La conformité

- 
- » La politique de sécurité
 - » La sécurité des ressources humaines
 - » La sécurité physique et environnementale
 - » L'acquisition, le développement et la maintenance des systèmes d'information
 - » La gestion des incidents de sécurité de l'information
 - » La gestion de la continuité des affaires

Le moins bon

- » L'organisation de la sécurité de l'information
 - » Manque de transparence
- » La gestion de la communication et de l'exploitation
 - » Manque de transparence
- » Les contrôles d'accès
 - » La gestion des clés est la responsabilité du client
- » La conformité
 - » Certifications
 - Sarbane & Oxley
 - SAS-70 type II
 - HIPAA standards (sécurité des données relatives à la santé)
 - Résultats d'audits consultable sous NDA
 - Audit réalisé à minima tous les 6 mois
 - » Impossible d'auditer soit même AWS



» La gestion des actifs



- Essentiellement de la responsabilité du client
- Le client ne connaît pas le nombre de copies et la localisation exacte de ses données
- Les données stockées ne sont pas chiffré
 - Vous pouvez les chiffrer vous-même

Agenda

1 – Cloud Computing

- *Qu'est que le Cloud Computing*
- Les 3 différents modèles de services du Cloud
- Les 4 modes de déploiement
- Zoom sur les problèmes de Sécurité

2 – Amazon Web Services

- Amazon Simple Storage Service (S3)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Block Store (EBS)
- Amazon Virtual Private Cloud (VPC)

3 – La sécurité d'AWS

- La sécurité et le cloud
- La sécurité d'AWS
- Conformité aux normes ISO 27002

4 – **Conclusions**



» **Amazon AWS prêt pour l'entreprise ?**



» **Votre entreprise prête pour amazon AWS ?**

» Paiement par carte de crédit

» Séparation des ressources de manière logique et non physique

» Ce n'est pas de l'infogérance

- Pas de transfert de risque

- Nécessite des compétences avancées d'administration de système pour garantir la sécurité



Ressources

AWS security center

<http://aws.amazon.com/security/>

Amazon AWS's CTO blog

<http://www.allthingsdistributed.com>

Amazon AWS's Developer blog

<http://aws.typepad.com>

Third party analysis

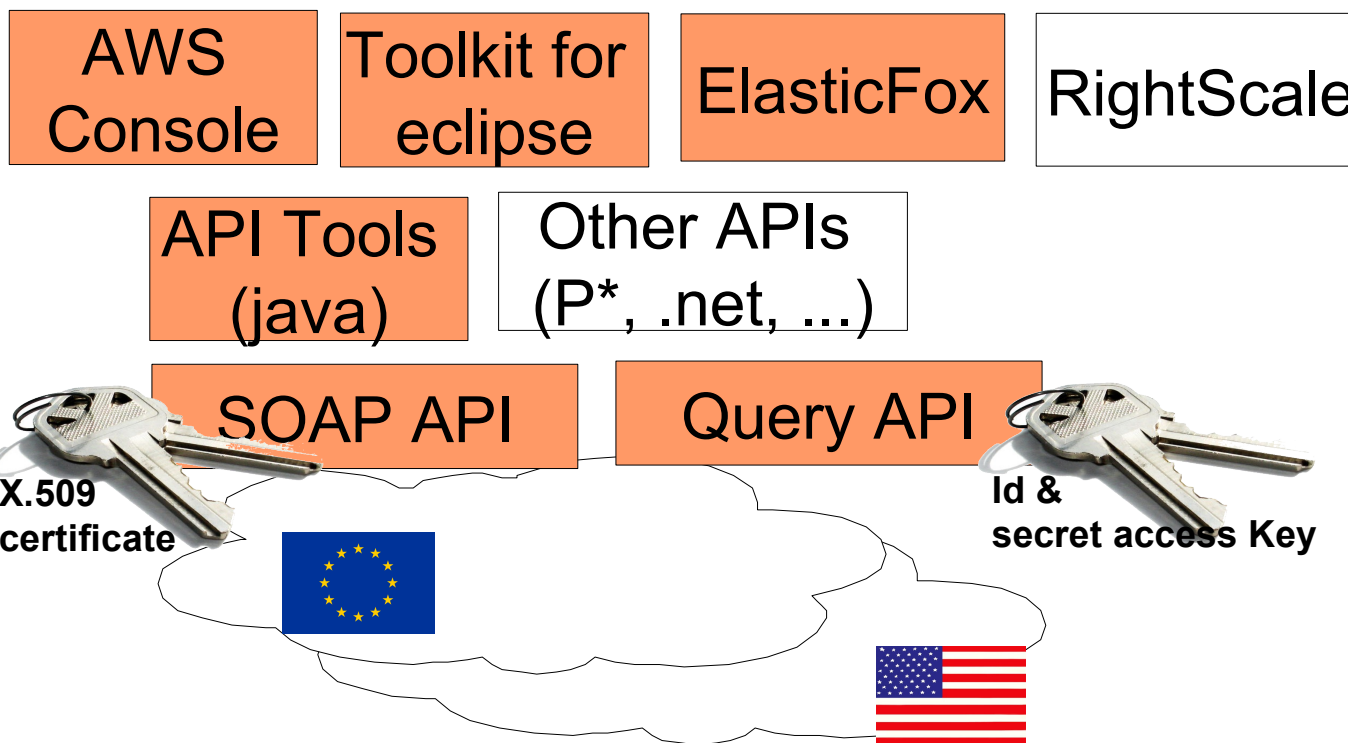
<http://blog.rightscale.com>



Annexes



Amazon AWS tools



AWS console: web management console

RightScale : Third party web management console

ElasticFox: Firefox plugin

Amazon secret keys

Amazon credentials
Multiple factor Authentication
Credentials rotation

X.509 certificate
to access SOAP Web Services (WS-Security)

Proprietary private/public key signing
to access HTTP query API

ssh v2 private keys
To log in EC2 instances



Cloud
management

Access
to instances

Network & Physical security

- » **Data center:** Non-descript locations, human and electronic surveillance, two-factor authentication entry, access on as-needed basis, access is logged/reviewed, employee background checks
- » **Physical host:** two factor authentication required to access Dom0 (Xen's Linux partition), host OS security is up to the customer, AWS employees do not have host OS access (brick AMI), IdM integration is up to customer, calls to instantiate/terminate AMIs require customer's private key generated when you create an account
- » **Network security:** pre-configured FW with all ports off, packet sniffing is blocked by the hypervisor, vigilantly monitor port scanning, etc.
- » Security claims have not been verified by an accredited 3rd party

Source: [Amazon Web Services: Overview of Security Processes](http://developer.amazonwebservices.com/connect/entry.jspa?externalID=1697&categoryID=55)

<http://developer.amazonwebservices.com/connect/entry.jspa?externalID=1697&categoryID=55>

- **La politique de sécurité**

- » Document de politique de sécurité de l'information
 - Process de développement prenant en compte les problématiques de sécurité de la conception à la mise en production
 - Modélisation des menaces
 - Analyse de code
 - Tests d'intrusion régulier
- » Révision régulière de la politique de sécurité
 - Au moins tous les 6 mois



- **L'organisation de la sécurité de l'information**

- » Contrôle interne
 - » Certifications
- » Contrôle des tiers
 - » ??



La gestion des actifs

Essentiellement de la responsabilité du client

Le client ne connaît le nombre de copies et la localisation exacte de ses données

Les données stockées ne sont pas chiffré



La sécurité des ressources humaines

Enquête poussée sur les employés d'Amazon AWS ayant accès aux serveurs

Révision régulière des droits

Révocation immédiate des droits d'accès en cas de départ



La sécurité physique et environnementale



Zones sécurisées

Data center dans un périmètre de sécurité de type militaire

Plusieurs authentification à plusieurs facteurs avant d'accéder aux salles serveurs

Sécurité des équipements

Data center de type tiers 4 (aucun SPOF, disponibilité de 99,995%)



• La gestion de la communication et de l'exploitation

Procédures d'exploitation

- » Bonne gestion des patchs et de la maintenance

Planification du système capacity planning

Prévention des codes mobiles et malveillants

gestion de la sécurité du réseau

- » Gestion des attaques de deny of services
- » Scan de port, packet sniffing, ip spoofing imposs.
- » End-point en SSL



Sauvegardes

- » Données stockées de manière redondante dans de plusieurs lieux physiquement distinct (S3)

Prestations de services en provenance de tiers ??

- » Lack of transparency on technical architectures (NAS or DAS, xen rchitecture)



- **Les contrôles d'accès**

Authentification à plusieurs facteurs

Certificats X509

clef ssh publique privé

rotation automatique des clés



Les employés d'amazon ne peuvent pas se logger sur les serveurs des clients



La gestion des clés est la responsabilité du client

- **L'acquisition, le développement et la maintenance des systèmes d'information**

- » Bonne gestion des patches et de la maintenance
- » Solide procédures de test et de validation avant mise en production
- » Contrôles cryptographiques
- » Gestion des vulnérabilités techniques



- **La gestion des incidents de sécurité de l'information**

Rapports des événements et faiblesses de la sécurité de l'information.
Tableau de bord



Gestion des incidents et des améliorations de la sécurité de l'information

» Tous les actions et incidents sont enregistré pour chaque services

- **La gestion de la continuité des affaires**

Conçu pour

Plusieurs centre de données dans différentes zones géographique sur différents continents



Data center de type tiers 4

SLAs de 99.95% pour EC2 et 99.9% pour S3

- **La conformité**

Légale

Application des lois locales

» Certifications

- » Sarbane & Oxley
- » SAS-70 type II
- » HIPAA standards (sécurité des données relatives à la santé)
- » Résultats d'audits consultable sous NDA
- » Audit réalisé à minima tous les 6 mois
- »



- »Lack of transparency on audits (volume of business)
- »Ability to audit AWS