



Module Cloud – aspects techniques

Version française

Mise à jour – Février 2017

AGENDA

/ 01	Introduction	Page 3
/ 02	Sécurité	Page 8
/ 03	Performance	Page 30
/ 04	Intégration	Page 33
/ 05	Conclusion	Page 46



/ **01**

Introduction

Rappels (1/3)

3 types de services



SaaS

Fournir des **logiciels** à destination des **utilisateurs finaux**



PaaS

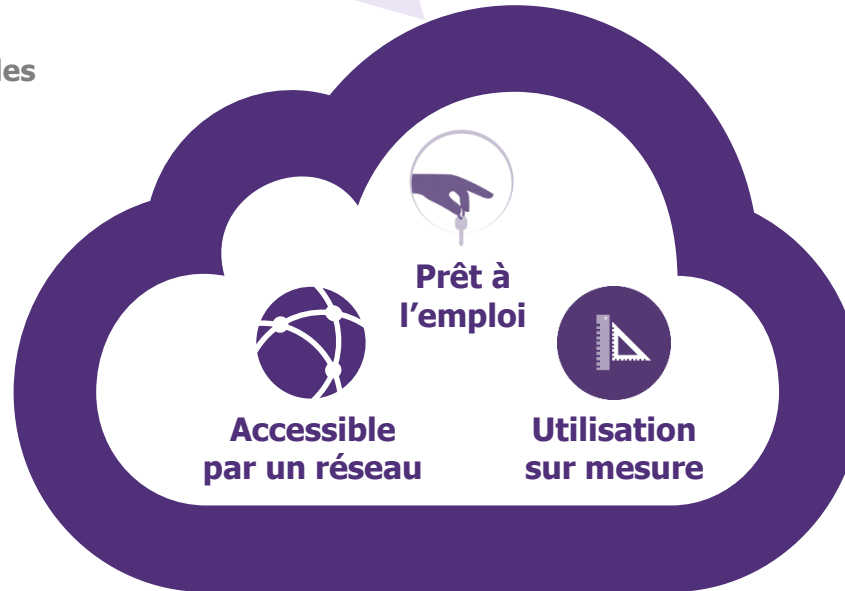
Fournir des **plateformes d'exécution** pour les **développeurs**



IaaS

Fournir des **ressources informatiques** pour les **équipes IT**

Cloud = consommation banalisée d'une ressource de commodité



4 modèles d'hébergement

Public

Une **infrastructure partagée** dont l'usage est ouvert à tous



Privé

Une **infrastructure** dont l'**usage est exclusif** à une organisation



Hybride

Une **composition** dynamique de **plusieurs modèles**



Communautaire

Une **infrastructure partagée** dont l'**usage est réservé à une communauté** d'organisations partageant des intérêts ou des contraintes communs



4 caractéristiques résultantes :



Consommateurs

Self-service

Plus grande agilité

Élasticité

Capacité virtuellement infinie

Mesurable

Facturation à l'utilisation

Mutualisation

Diminution des coûts



Producteurs

Catalogue de services standardisés

Ajustement automatique

Facilite la gouvernance et le management SI

Favorise l'économie d'échelle



Rappels : les cas d'usages (2/3)

3 types de services



SaaS

- Élasticité transparente
- « Pay per user »
- Services historiques mais pas de standards pour l'intégration au SI
- Besoins courants **non cœur de métier**



PaaS

- Élasticité impacte les développements
- « Pay per usage request »
- Pas de standard établi
- Besoins **courts termes**, à **forte variations d'usage**



IaaS

- Élasticité complexe
- « Pay per allocated ressource »
- S'appuie sur une virtualisation déjà maîtrisée
- Introduire de l'**agilité** dans l'infrastructure déjà industrialisée



4 modèles d'hébergement

Public



- Orienté grand public ou entreprises
- Ressources virtuellement infinies
- Contraintes de régulation ou de sécurité

Privé



- Hébergé en On ou Off Premise
- Gestion d'un capacity planning
- Maîtrise de la localisation des données

Hybride



- Potentiellement multi-technologies
- Capacité de débordement
- Approche broker d'infrastructure

Communautaire



- Une réponse spécifique aux contraintes sectorielles d'un métier

Rappels (3/3)



Gouvernance et organisation

Pilotage de la performance et de la qualité de service

- Modalités de **mise en œuvre, pilotage, fin de vie** des **offres de services** orientés Cloud
- Exigences et contraintes de **QoS**
- Politique de **refacturation** des services
- Le **rôle de la DSI** passe du pilotage d'infrastructure au pilotage de fournisseurs. Mise en concurrence de la DSI
- Adapter les **processus internes** (support utilisateurs centralisé, gestion des incidents...)
- ...



Sécurité et Architecture

Garantie de la pérennisation du SI

- **Sécurité** : L'utilisation de cloud public nécessite l'exposition du SI de façon sécurisée à l'opérateur du cloud
- Assurer **l'intégration et l'interopérabilité** des différents services souscrits
- Forte **dépendance** au réseau d'accès
- ...



Aspects légaux et contractuels

Contractualisation et confidentialité des données

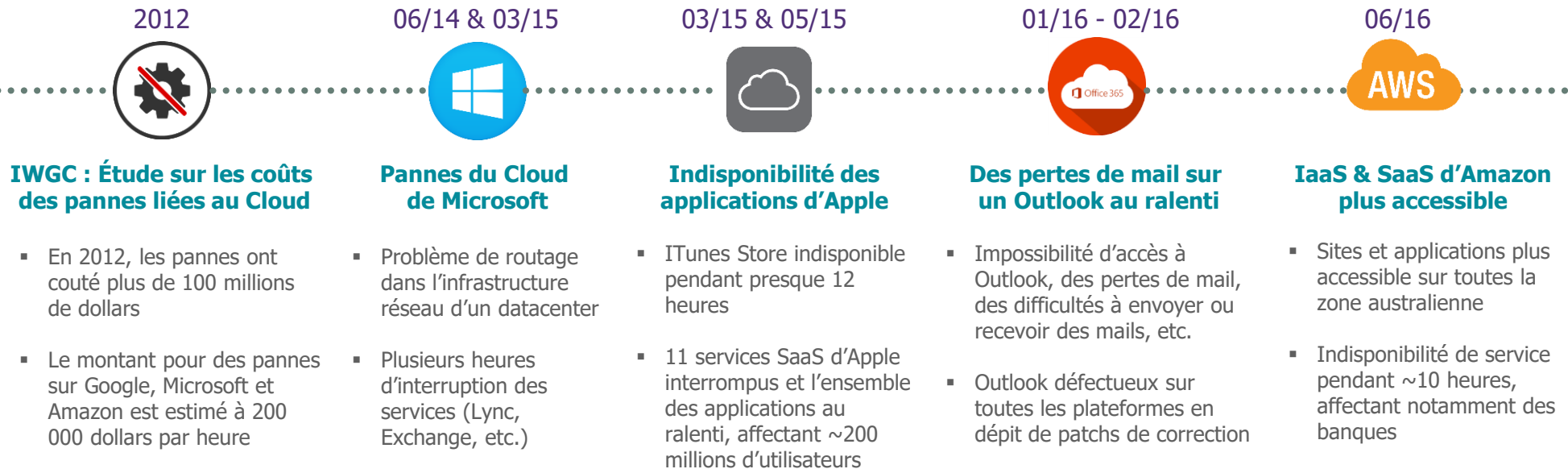
- Contractualisation et modalités de **réversibilité**
- **Confidentialité** : le fournisseur peut avoir accès aux données.
- Prendre en compte les **régulations** spécifiques à l'entreprise ou à l'offreur (Patriot act, CNIL, contraintes sectorielles, ...)
- ...

Les défis pour les architectes du SI



Sécurité : comment garantir la sécurité / fiabilité du cloud ?

Quelques incidents majeurs de ces dernières années :



Performance : comment tirer un bénéfice concret de l'élasticité du Cloud pour gérer la montée en charge ?



Intégration : comment intégrer les services Cloud entre eux et avec le SI traditionnel ?



/ **02**

Sécurité



/ **02.1**

Vue d'ensemble des risques

Quels risques ?



Les risques du cloud computing

Disponibilité

- Le cloud introduit une forte **dépendance au réseau** d'accès
- Comment gérer **l'indisponibilité** des fournisseurs de services ?
- Quels mécanismes pour assurer la **résilience** d'une infrastructure cloud ?



Confidentialité

- Le **fournisseur peut accéder** aux données
- Niveau de **contrôle** plus **faible** sur les infrastructures
- Comment gérer **identités** et les **autorisations d'accès** au cloud ?
- Comment assurer le **cloisonnement des données** sur une infrastructure mutualisée ?



Intégrité

- Comment gérer la **cohérence des données** sur une infrastructure répartie ?



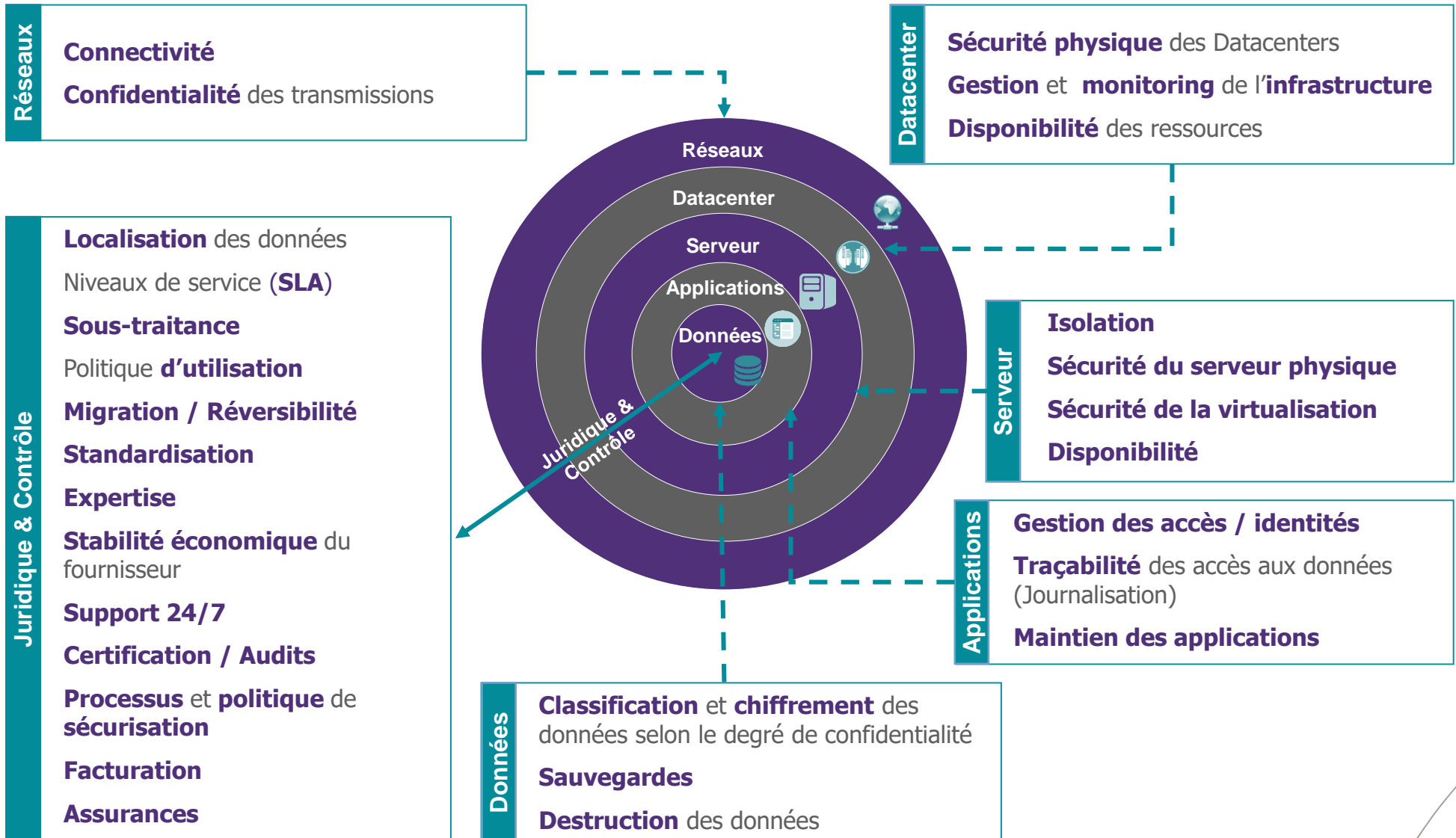
Traçabilité & Organisation

- **Auditabilité** des **fournisseurs** (données, applications, accès, ..)
- Perte de **contrôle** sur les composants (logiciels, infrastructure,..) employés
- Dépendance au fournisseurs et problématiques de **réversibilité**
- Risques juridiques liés à la **localisation** des données



Ces risques dépendent fortement des offres de services (SaaS, PaaS, IaaS public, privé, hybride...)

La cible pour évaluer les risques du point de vue de l'utilisateur





/ **02.2**

Focus sur la disponibilité

De la virtualisation serveur au cloud

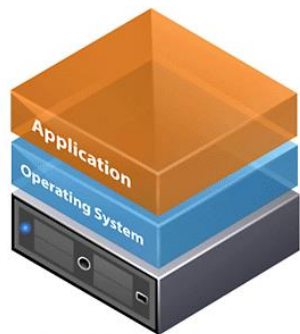


Au début des années 2000, la virtualisation serveur était en haut du hype cycle de Gartner, elle est aujourd'hui devenue un principe de base d'autres technologies et notamment du Cloud.

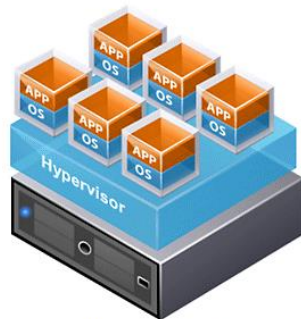
Quelques éléments clés sur la virtualisation :



- Marché établi dominé par VMware et Microsoft
- Technologie mature
- Permet de dé-corréler les ressources physiques des ressources logiques



Traditional Architecture



Virtual Architecture



Couche logicielle

- API cloud
- Orchestrateur
- Elastic load balancing...



Cloud

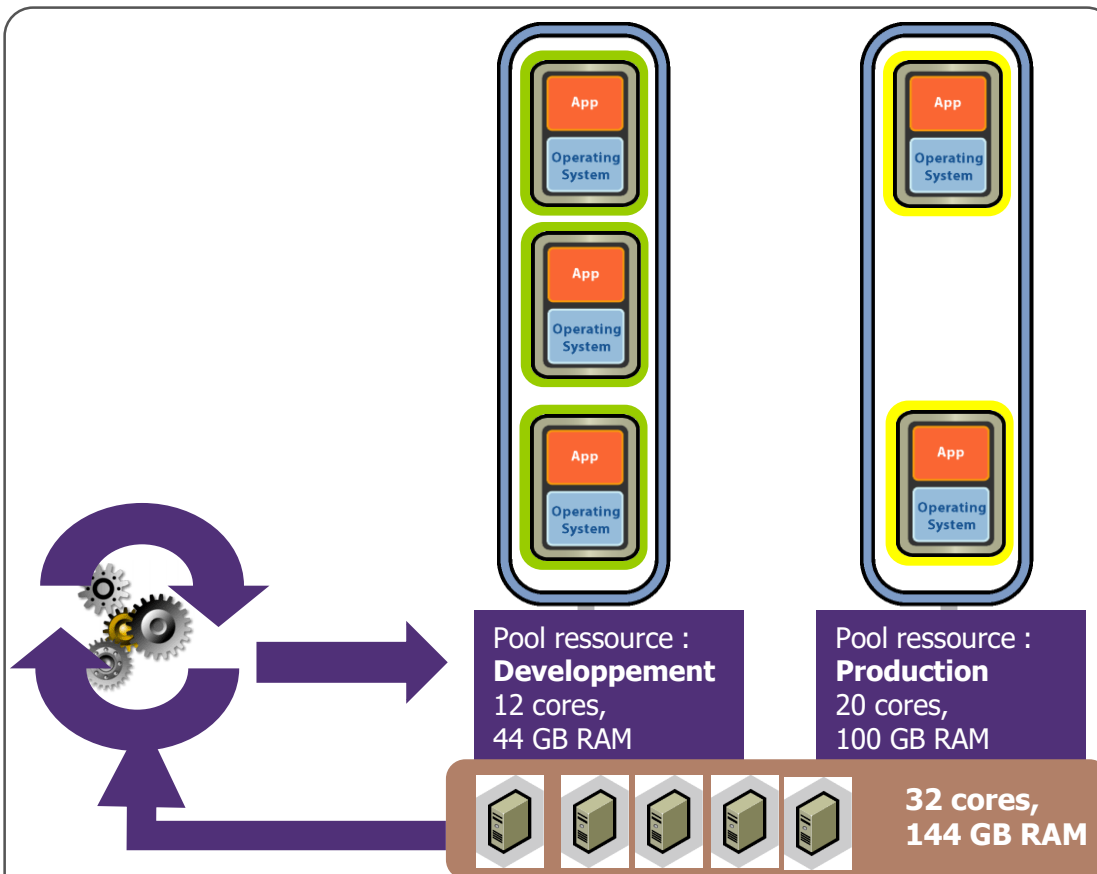


Comprendre la virtualisation c'est se donner les clés pour comprendre les bases technologiques du Cloud. C'est pourquoi, les slides suivants exposent les fonctionnalités de la virtualisation (via l'exemple VMware) puis celles inhérentes au Cloud (via l'exemple d'AWS)



Focus sur la disponibilité – les outils à disposition (1/9)

Principe : Les **pools de ressource** permettent de diviser un cluster d'hôtes ESX en plusieurs groupes de ressources (CPU et mémoires) indépendants. Elles permettent ainsi de garantir à un groupe de VM (resource Pool) une quantité de ressources (CPU et RAM) selon des règles de priorités établies.

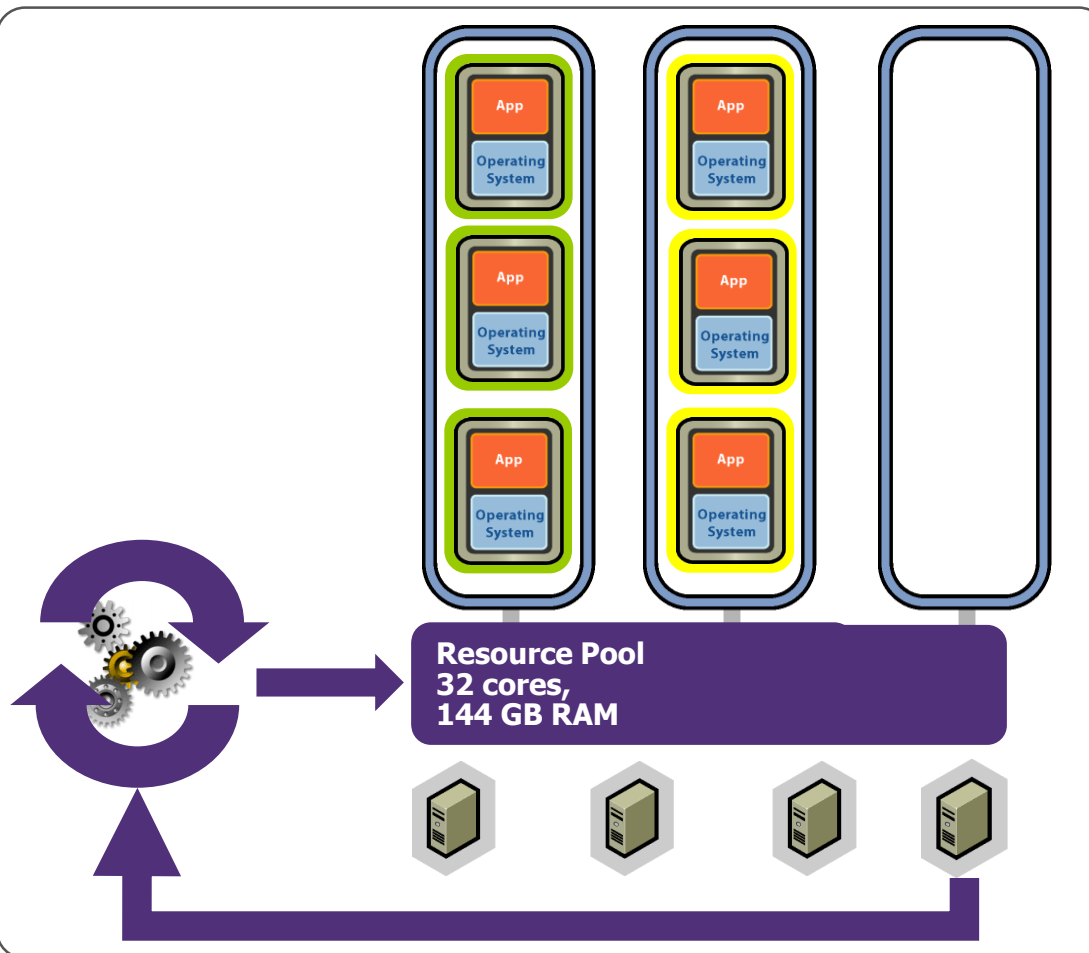


Fonctionnement :

- Création de deux pools:
 - Pool **Développement criticité faible** et option [Partages CPU] sur [normal]
 - Pool **Production criticité élevée** et option [Partages CPU] sur [Élevée]
- Le Pool Production n'utilise pas la totalité de ses ressources, le Pool Développement peut alors les utiliser si besoin.
- Les besoins du Pool Production augmentent, il récupère ses ressources car celles-ci lui sont garanties par l'option [Élevée]

Focus sur la disponibilité – les outils à disposition (2/9)

Principe : Distributed Resource Scheduler (DRS) permet **l'allocation dynamique des ressources** aux machines virtuelles en fonction des ressources disponibles sur les hôtes physiques. Il déplace les VM en fonction des ressources de l'hôte physique.

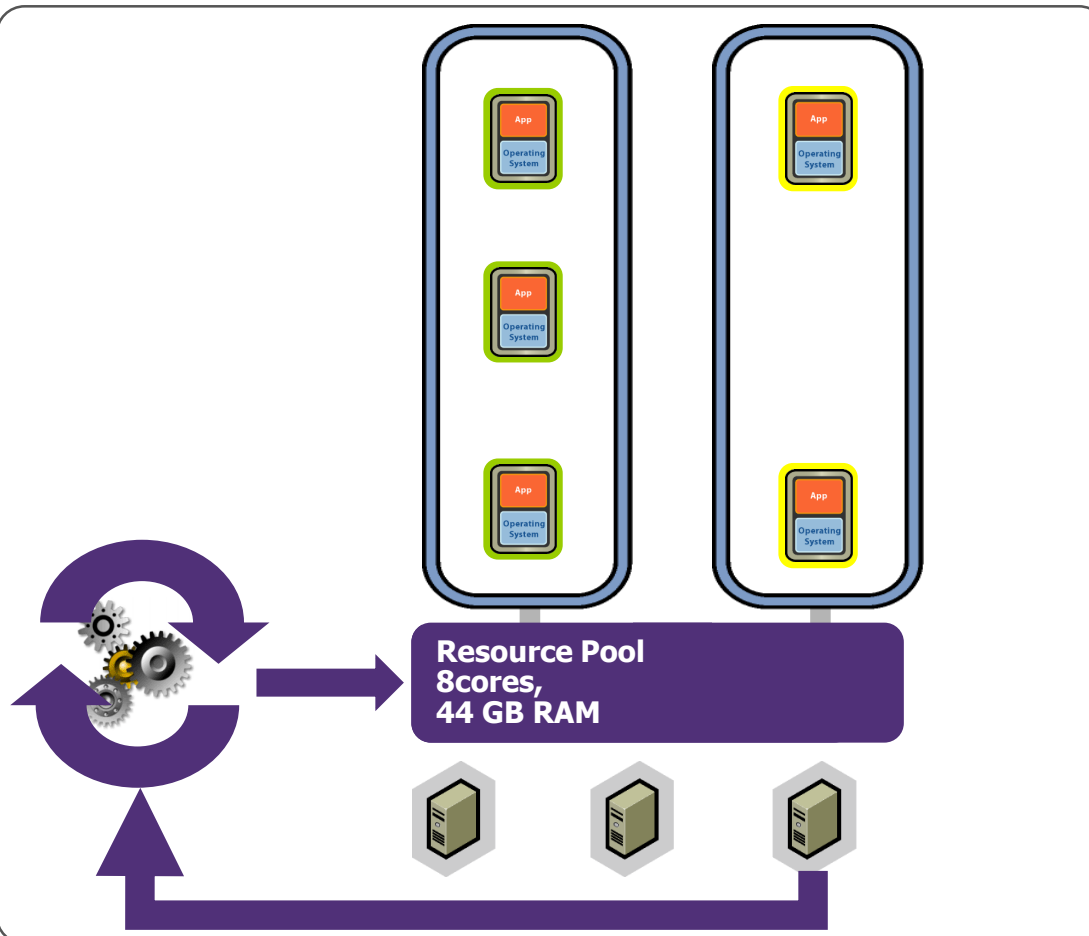


Cas 1 : Augmentation des ressources physiques

- Ajout d'un nouveau serveur physique dans le pool d'ESX existant
- Les ressources CPU/RAM disponibles dans le pool se voient ainsi augmentées
- Déplacement **automatique** des machines virtuelles vers le nouveau ESX pour **répartir la charge** sur chaque ESX du groupe

Focus sur la disponibilité – les outils à disposition (3/9)

Principe : DRS permet **l'allocation dynamique des ressources** aux machines virtuelles en fonction des ressources disponibles sur les hôtes physiques. Il déplace les VM en fonction des ressources de l'hôte physique.



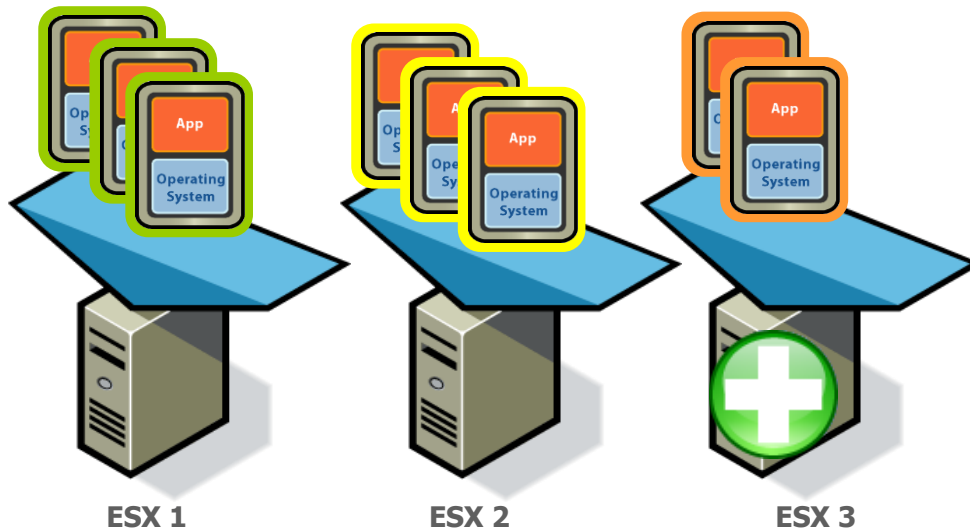
Cas 2 : Augmentation des ressources virtuelles

- Les ressources CPU/RAM consommées par une machine virtuelle augmentent considérablement
- **DRS** effectue des **déplacements de machines virtuelles** de façon à **garantir** à toutes les machines de chaque ESX **les ressources nécessaires**
- Les déplacements de machines virtuelles sont effectués en fonction des règles préalablement définies

Focus sur la disponibilité – les outils à disposition (4/9)

Principe : vMotion permet la **migration à chaud** de machines virtuelles en cours d'exécution d'un ESX à l'autre **sans interruption de service**.

Migration automatique sans interruption



Cas : Effectuer une maintenance sur un ESX

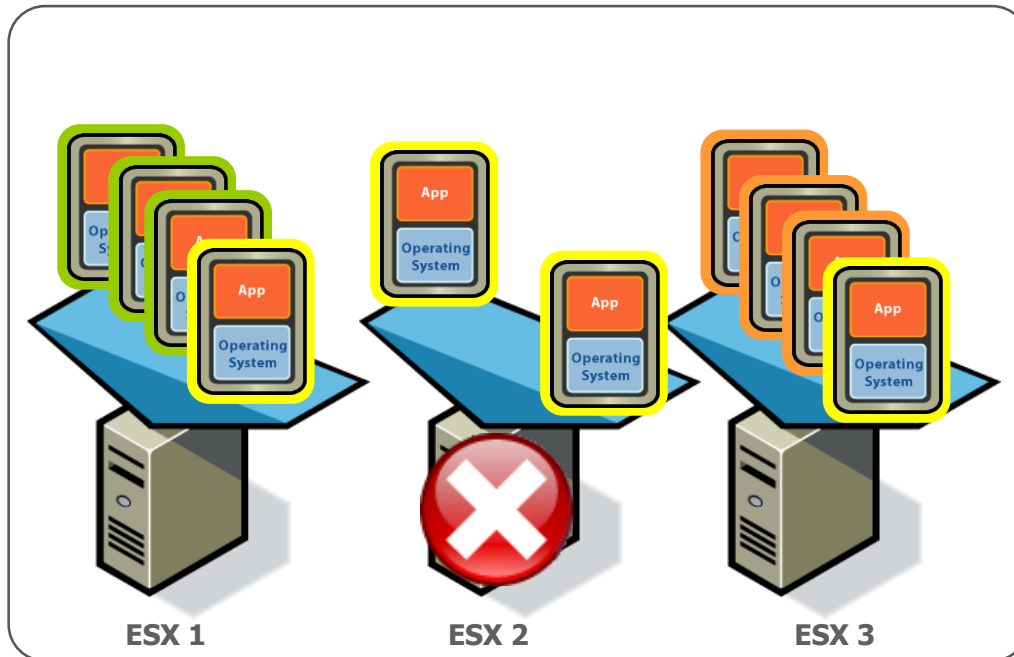
- vMotion migre les machines virtuelles de ESX 2 sur ESX 1 et ESX 3 sans interruption
- L'ESX 3 est mis en mode maintenance
- DRS combiné à vMotion migre **automatiquement et sans interruption** les machines virtuelles de l'ESX en mode maintenance (ESX3) vers les ESX 1 et ESX 2



La migration à chaud n'est pas disponible chez Amazon Web Services

Focus sur la disponibilité – les outils à disposition (5/9)

Principe : En **cas de panne matérielle** sur un hôte physique, VMware **High Availability (HA)** assure le **redémarrage** des machines virtuelles sur un autre hôte selon certaines conditions.



Cas : Perte du processeur d'un hôte physique

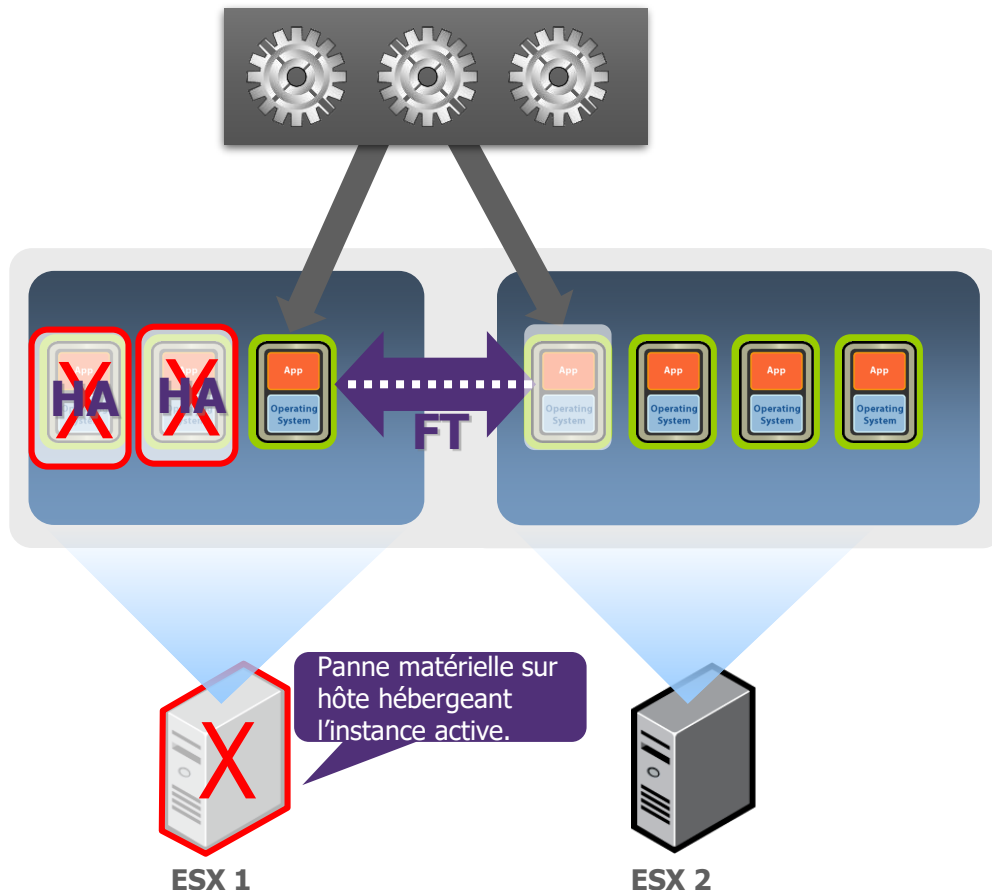
- Panne matérielle sur l'ESX 2 (Ex : perte du processeur)
- VMware **redémarre** les machines virtuelles de l'hôte défaillant **sur les autres hôtes du cluster ESX**
- Les machines virtuelles sont redémarrées en fonction des règles de redémarrage préalablement définies (Ex: redémarrage automatique avec une priorisation des machines virtuelles par criticité)



La gestion de la haute disponibilité n'est pas disponible chez Amazon Web Services

Focus sur la disponibilité – les outils à disposition (6/9)

Principe : Fault Tolerance (FT) assure la **basculer automatique et sans interruption** des applications en cas de panne matérielle sur le serveur hôte. Il maintient l'exécution simultanée de deux instances d'une même machine virtuelle.

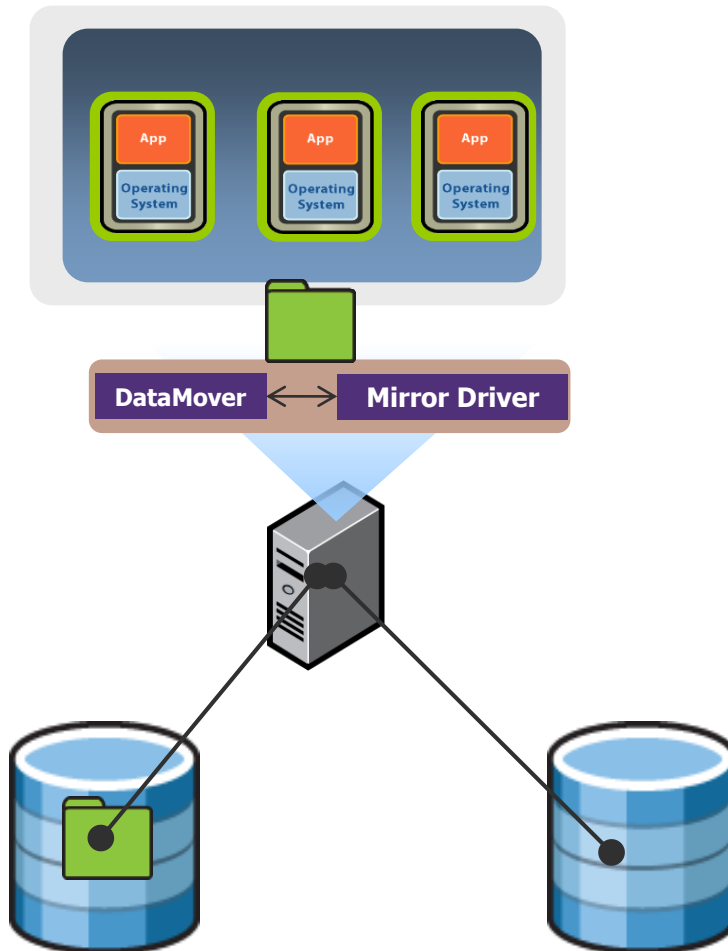


Cas : Panne matérielle sur un hôte physique

- VMware FT est activé sur la 3ème machine virtuelle de l'ESX 1. Une deuxième instance de cette même machine est démarrée sur l'ESX 2
- Une seule instance est active et accessible pour les utilisateurs
- Les **données** et état de l'instance active **sont copiés** (synchrone ou asynchrone) **vers l'instance non active**
- VMware FT n'est pas activé pour les autres machines virtuelles de l'ESX
- **L'instance passive devient active sans interruption** des services démarrés
- VMware HA permet par exemple de redémarrer les autres machines virtuelles

Focus sur la disponibilité – les outils à disposition (7/9)

Principe : Storage vMotion permet la **migration des fichiers** de disque des machines virtuelles d'une baie de stockage à une autre **sans interruption** de la machine virtuelle.



Fonctionnement :

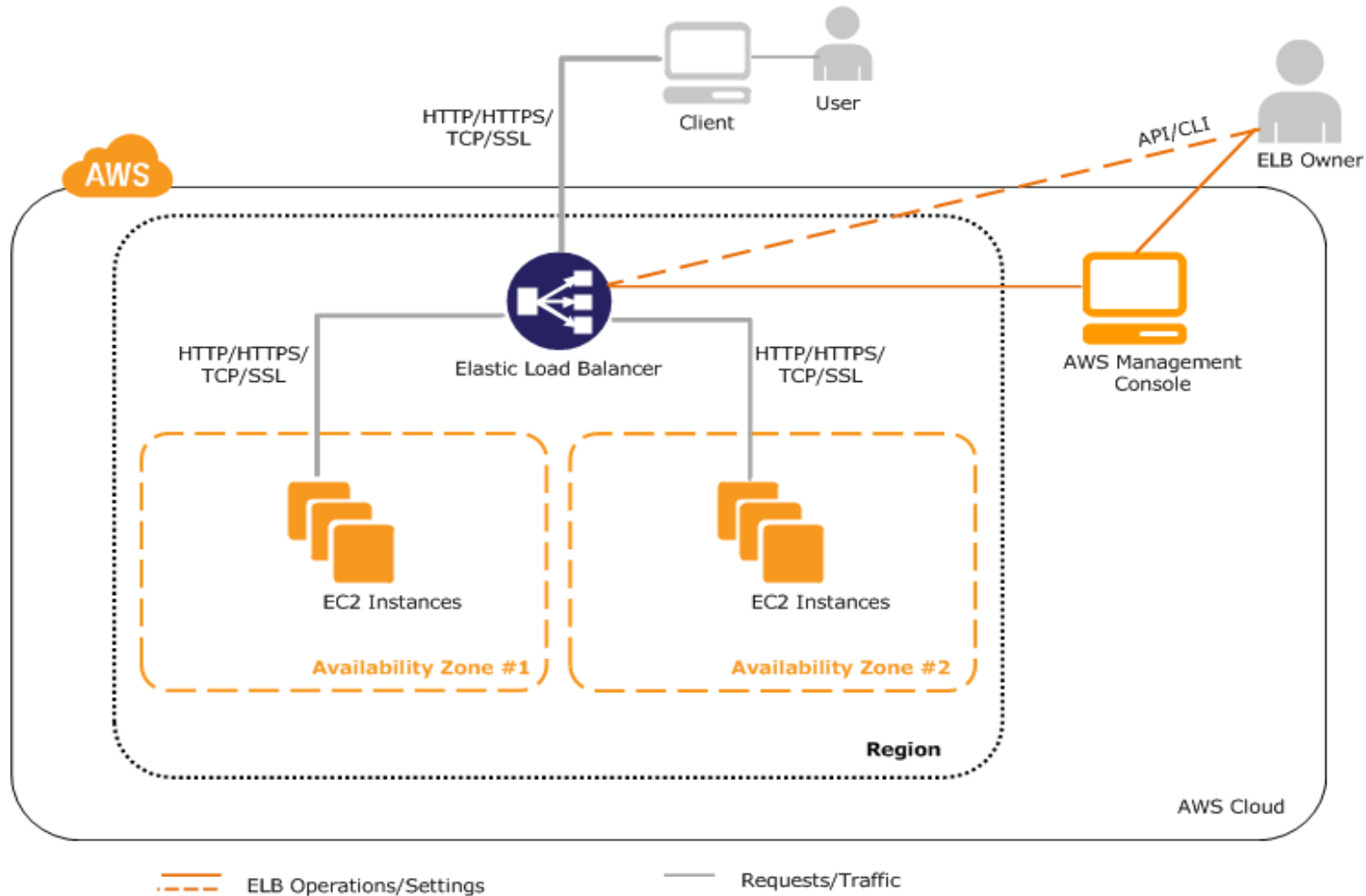
- Situation nominale: la machine virtuelle accède à son stockage sur le datastore présent dans la baie de stockage principale
- Migration du stockage sur une deuxième baie : déclenchement de Storage vMotion
- Les mécanismes DataMover et Mirror sont activés grâce à un driver sur la machine virtuelle
- **DataMover** permet la **copie des fichiers** du datastore vers le stockage de destination
- Une VM fantôme est démarrée sur le datastore copié par DataMover
- **Mirror** permet la **mise en miroir** des nouveaux fichiers/modifications sur le datastore de destination
- Dès la copie avec DataMover terminée, seul le datastore de la baie de destination est actif
- Le datastore (fichier de la VM) est supprimé de la source

Focus sur la disponibilité – les outils à disposition (8/9)

Exemple du cloud public Amazon (1/2)

▪ Elastic Load Balancing

- Utilisé avec AutoScaling: permet l'ajout automatique de ressources à un ensemble de ressources réparties sur plusieurs zones distantes accessibles via une unique Virtual IP

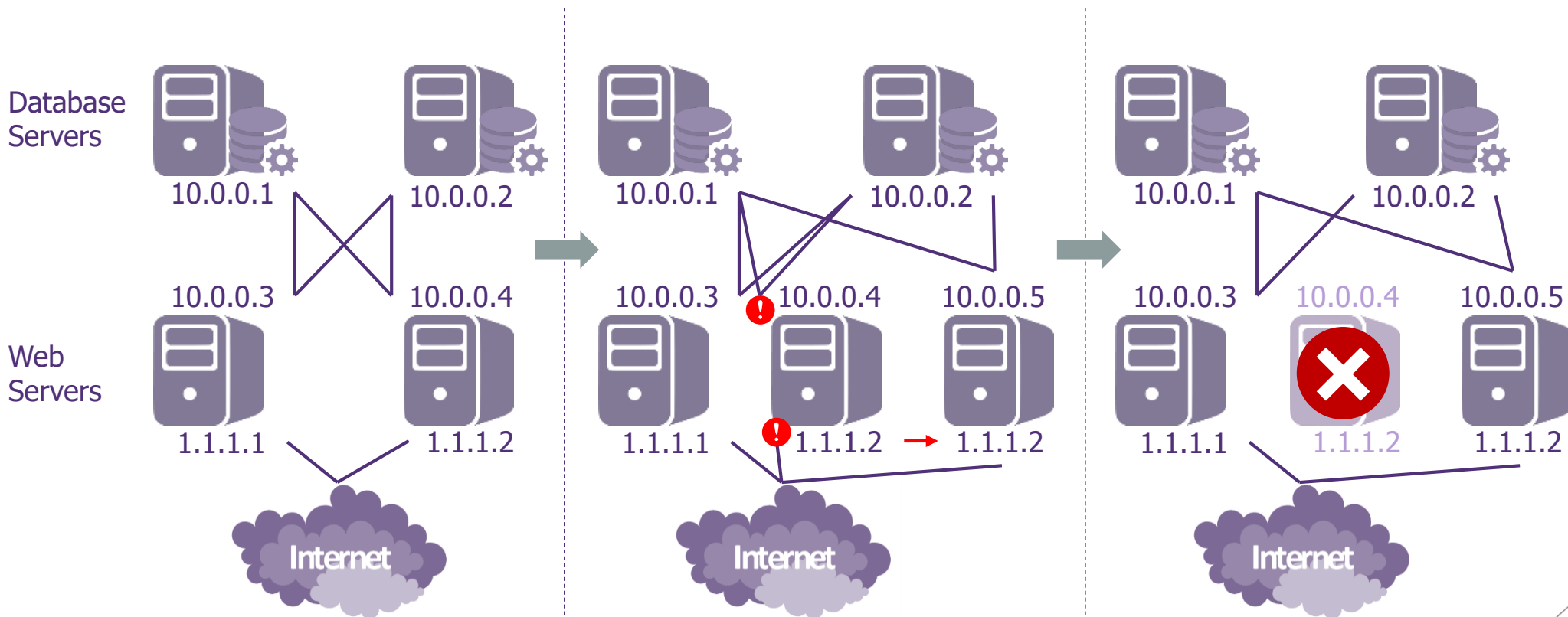


Focus sur la disponibilité – les outils à disposition (9/9)

Exemple du cloud public Amazon (2/2)

▪ Elastic IP adress

- ▶ Permet la réattribution **manuelle** d'une adresse IP existante à une nouvelle ressource
- ▶ Moins coûteux en temps que d'associer un DNS à une nouvelle IP



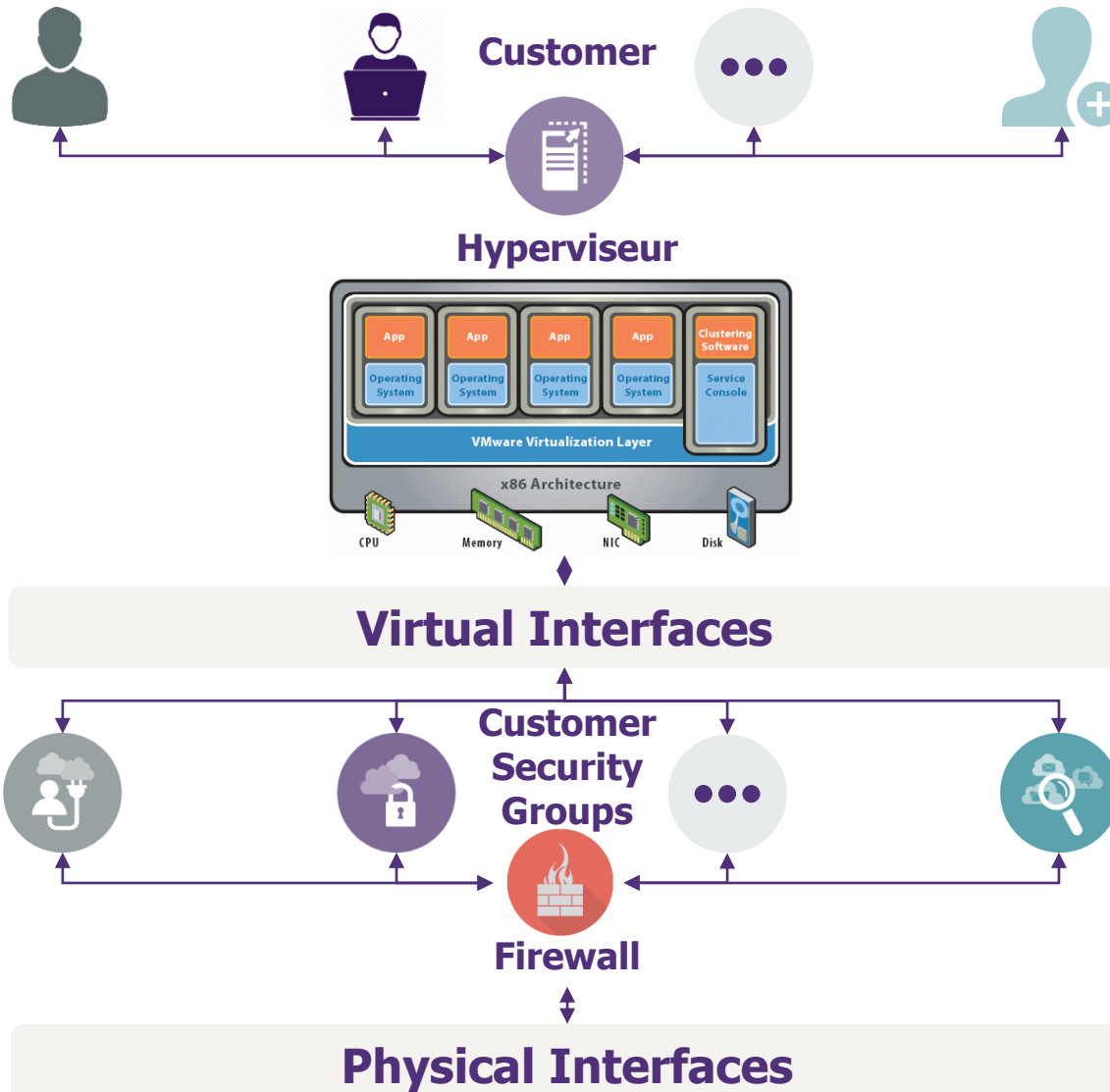


/ **02.3**

Focus sur la confidentialité

Focus sur la confidentialité – les outils à disposition (1/2)

Exemple d'Amazon IaaS : cloisonnement des instances



Un firewall est intégré à l'hyperviseur. Ce firewall isole les accès entre les interfaces réseau virtuelles et la couche physique

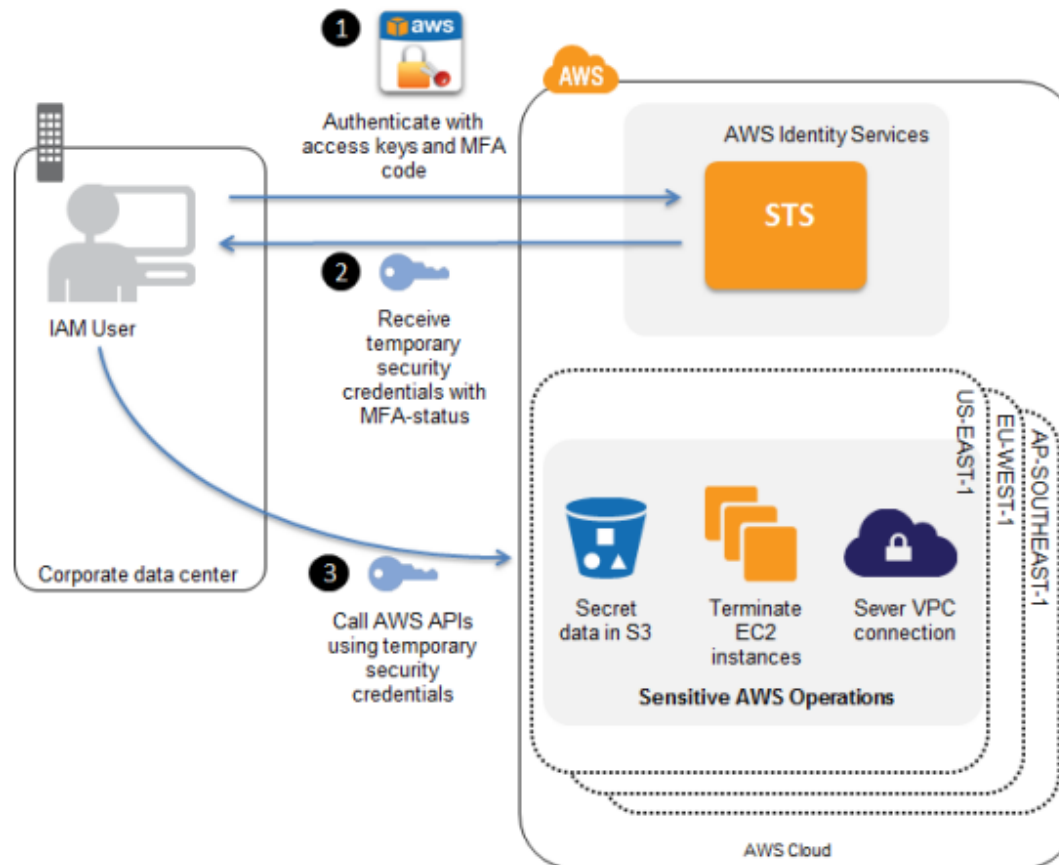


Le stockage se fait uniquement sur des disques virtuels et il n'est pas possible d'accéder directement aux contenus des disques physiques

Focus sur la confidentialité – les outils à disposition (2/2)

Exemple d'Amazon : gestion des identités et des accès aux ressources

- Amazon fournit un ensemble de fonctionnalités (clefs d'accès, mots de passe, ...) permettant de gérer les comptes et habilitations vers les différents services offerts
- Notamment, **Multi-Factor Authentication** permet une authentification forte basée sur des clefs temporaires :



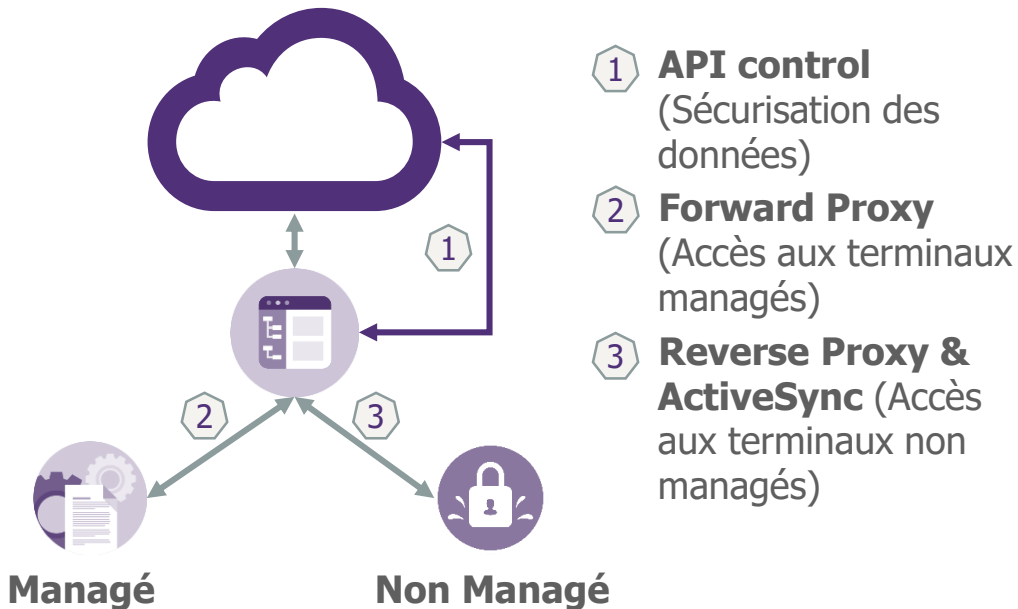
CASB : Cloud Access Security Brokers



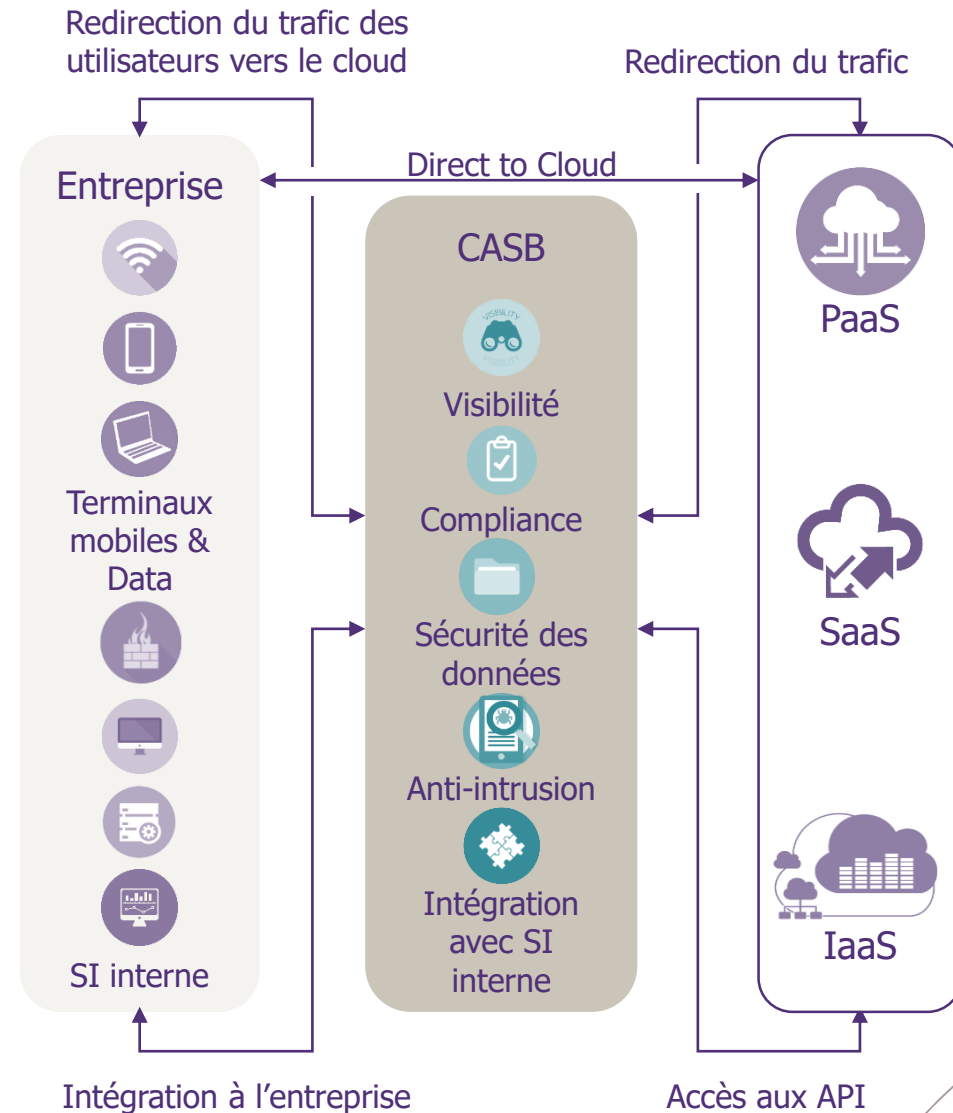
Les CASB sont des fournisseurs de services situés entre les utilisateurs du SI et les divers services Cloud.

Spécialistes en matière de sécurité, ils apportent une expertise permettant de prévenir les risques inhérents au Cloud.

- 3 principales architectures :



- Principaux acteurs :





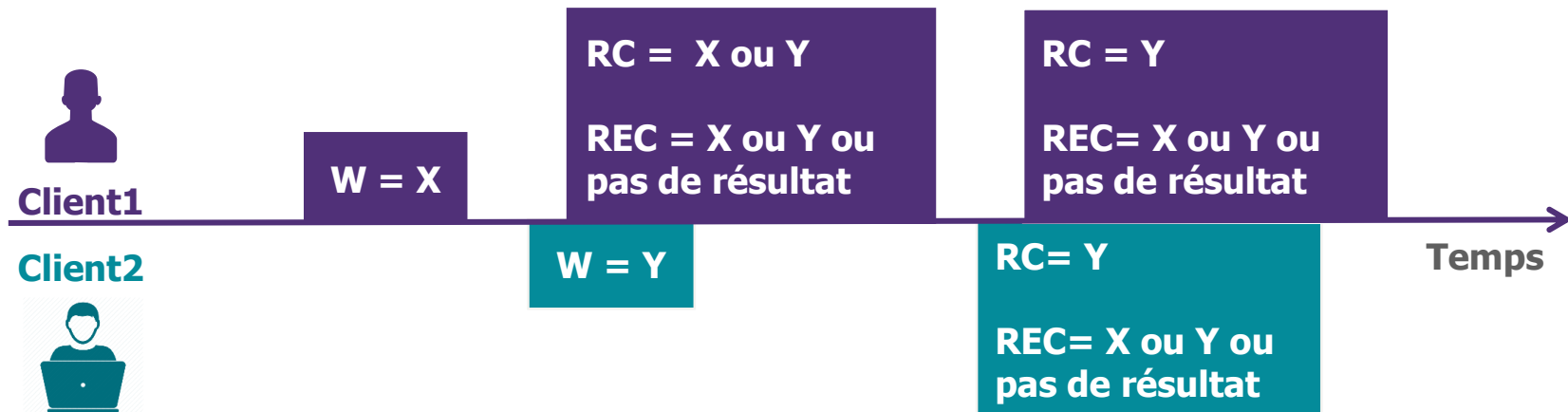
/ **02.4**

Focus sur l'intégrité

Focus sur l'intégrité – les outils mis à disposition

Exemple PaaS : Amazon Simple DB

- Amazon Simple DB conserve des données géographiquement distribuées ou situées localement en fonction des besoins clients (contraintes juridiques, contraintes techniques, etc)
- 2 modes de lecture pour gérer la consistance souhaitée :
 - Éventuellement consistante (REC) avec les données fournies plus rapidement mais moins fiables
 - Consistante (RC) avec les données fournies plus lentement mais bénéficiant d'une bonne fiabilité

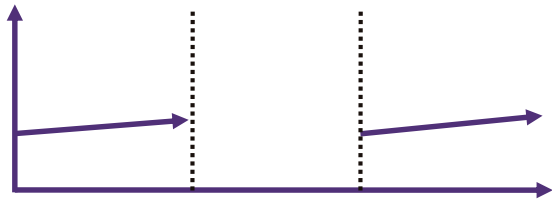




/ **03**

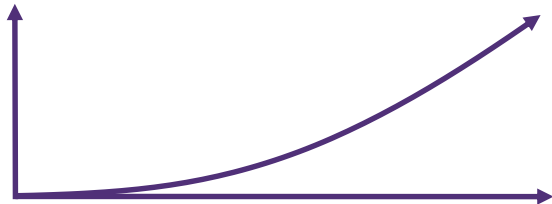
Performance

Les patterns de charges



On et Off

Ex: Streaming des JOs



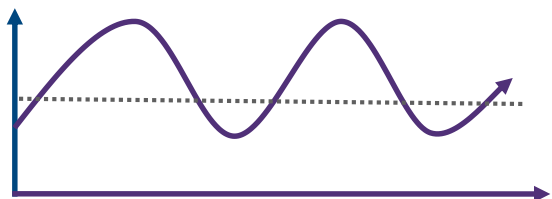
Croissance Rapide

Ex: Site de jeu en ligne connaissant un fort succès



Surcharge Imprévisible

Ex: Site de prévision de trafic en cas de fortes intempéries



Surcharge Prévisible

Ex: Accès jour vs. nuit sur un site Internet

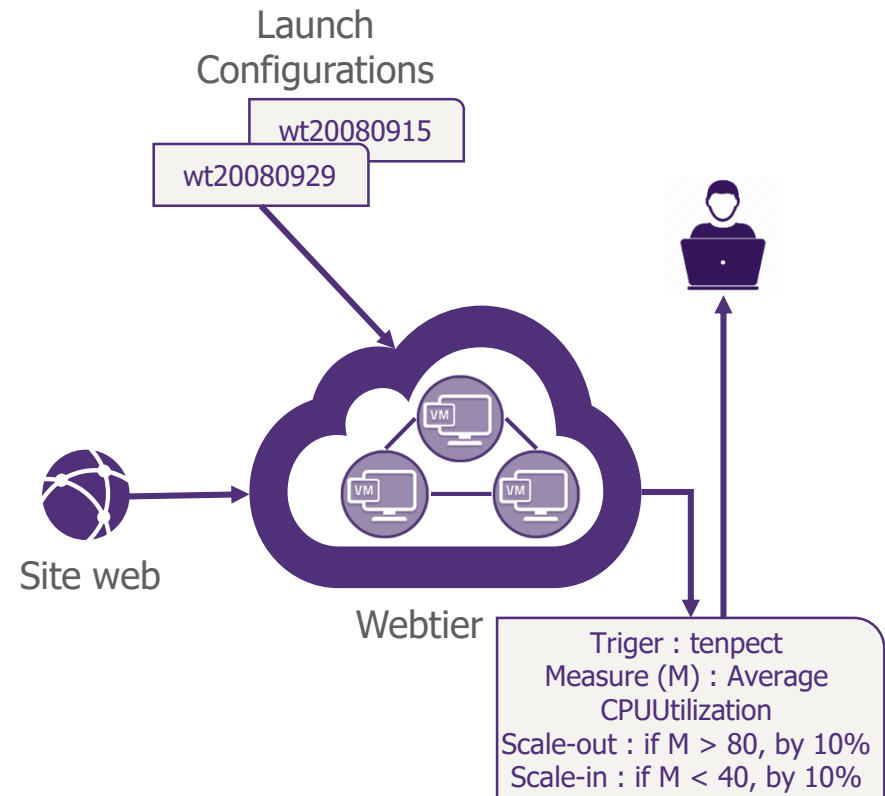




L'Auto Scaling d'Amazon permet de réguler le nombre d'instances en fonction de la charge

Pour cela, il faut créer un **Auto Scaling Group** :

- 1 Définition du nombre mini/maxi d'instances (**Facturé par instances !**)
- 2 Afin de limiter les changements, définition d'un **intervalle entre les changements systèmes**
- 3 Définition du **template d'instanciation** des nouvelles instances
- 4 Définition des **conditions de scale up /scale down** (manuel, programmé, charge CPU, ...)
- 5 Définition des **politiques de scale up/scale down** (doubler les instances, en ajouter qu'une,...)
- 6 Définition des modalités de **notifications par mail**





/ **04**

Intégration

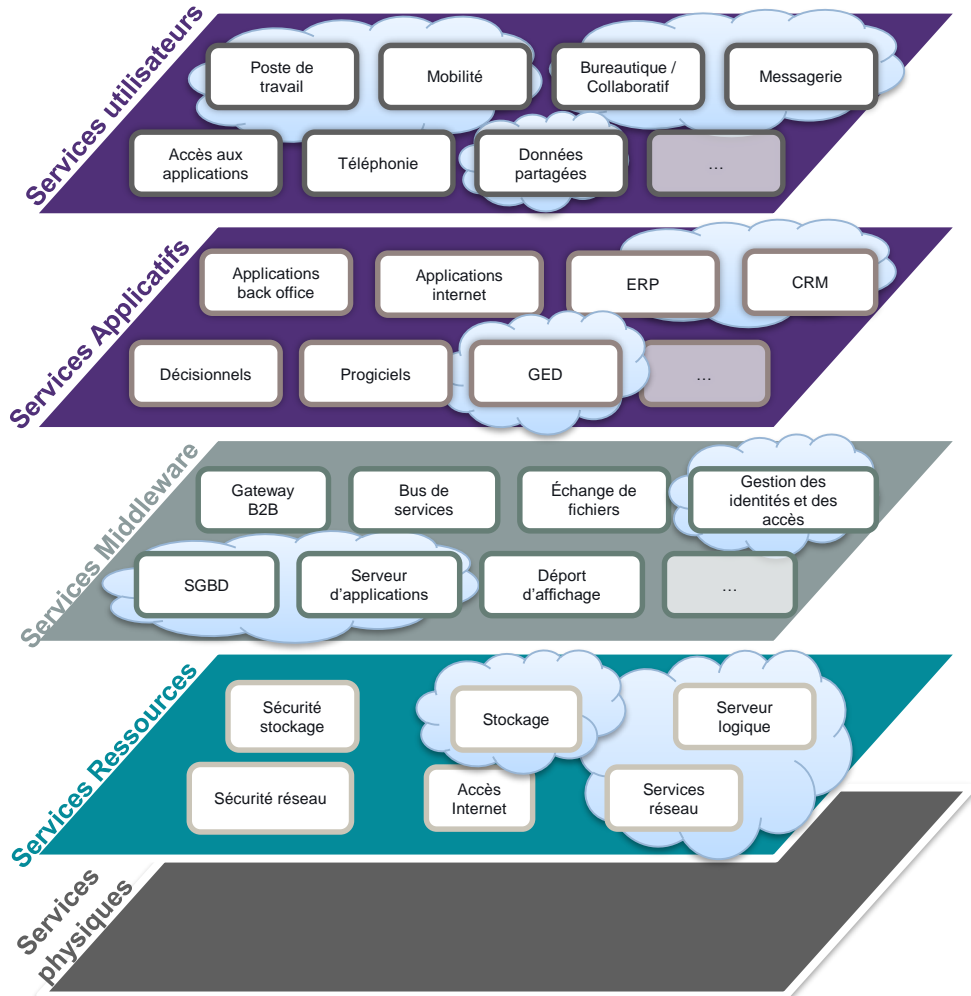


/ **04.1**

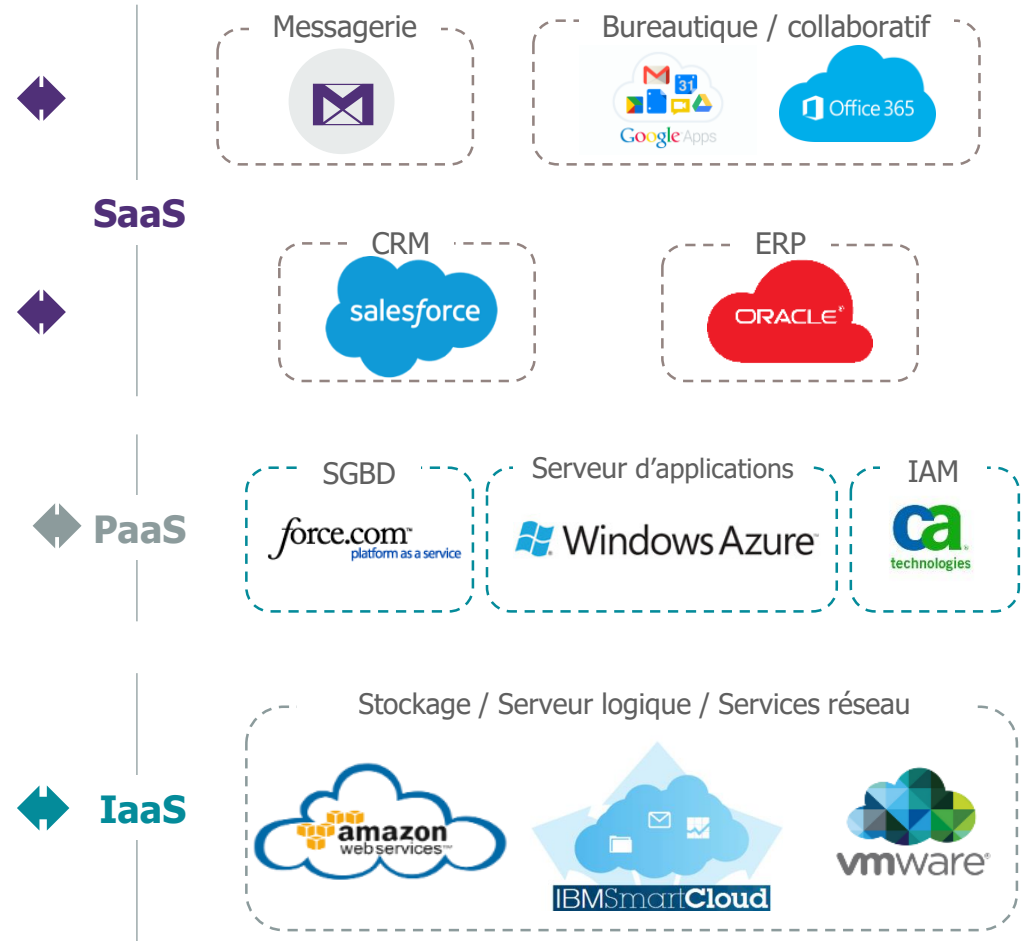
Vue d'ensemble des problématiques d'intégration

Des services à intégrer sur toutes les couches du SI

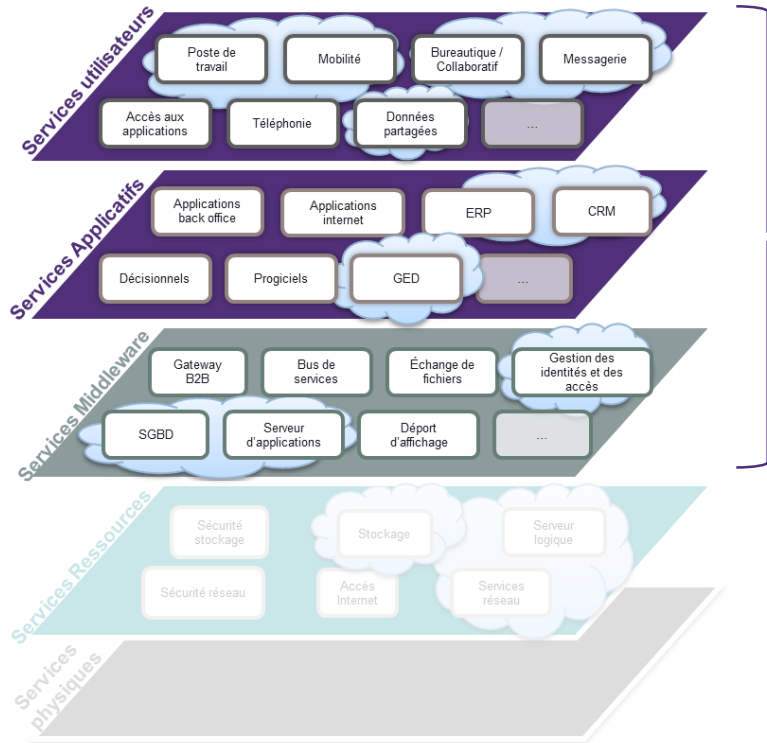
Le SI modélisé par couches :
Modèle SOI de Wavestone



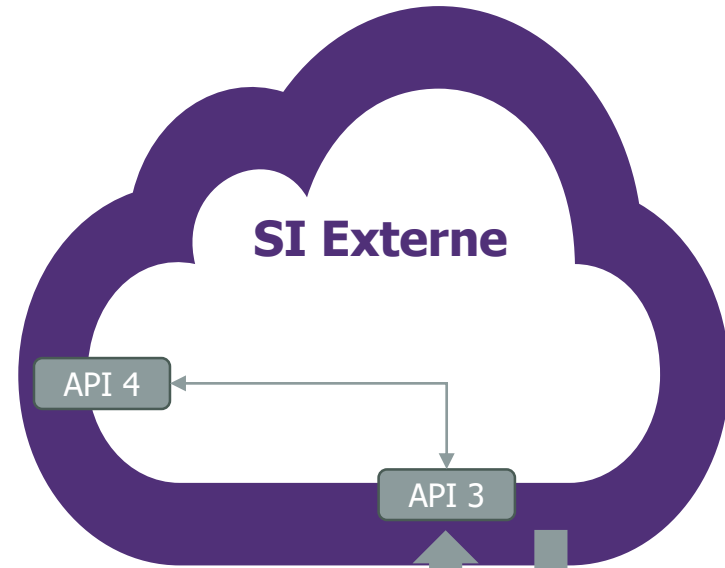
Les services cloud à intégrer:



Les problématiques sur les couches applicatives



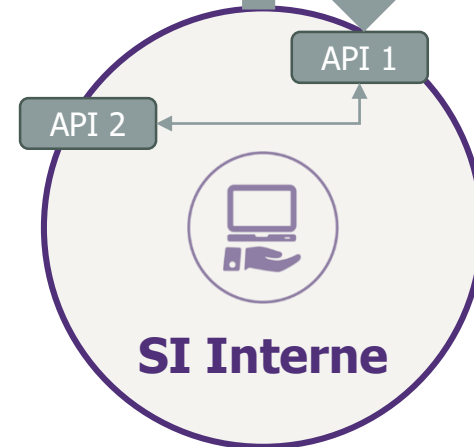
Gestion des **identités et accès** aux applications cloud ?



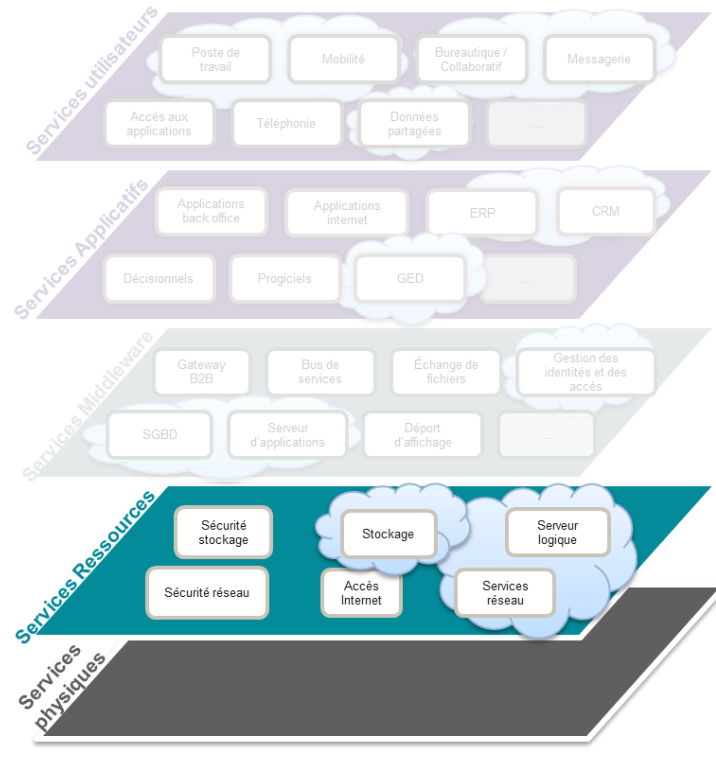
Échange de données
Cloud2Cloud ou
Cloud2SI ?



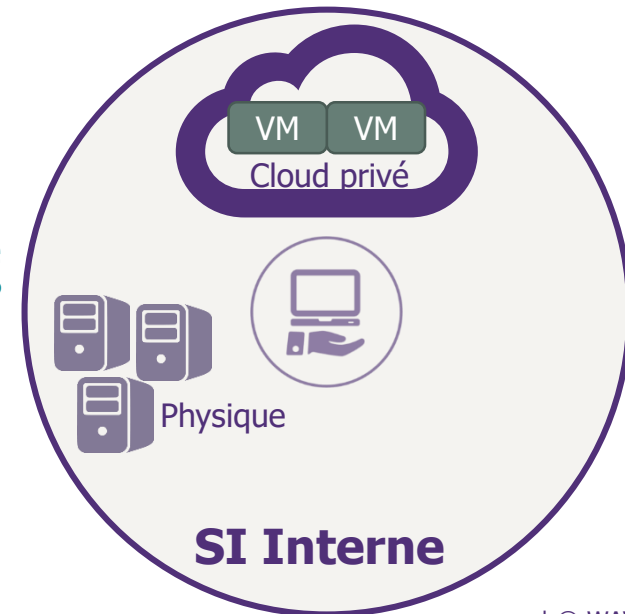
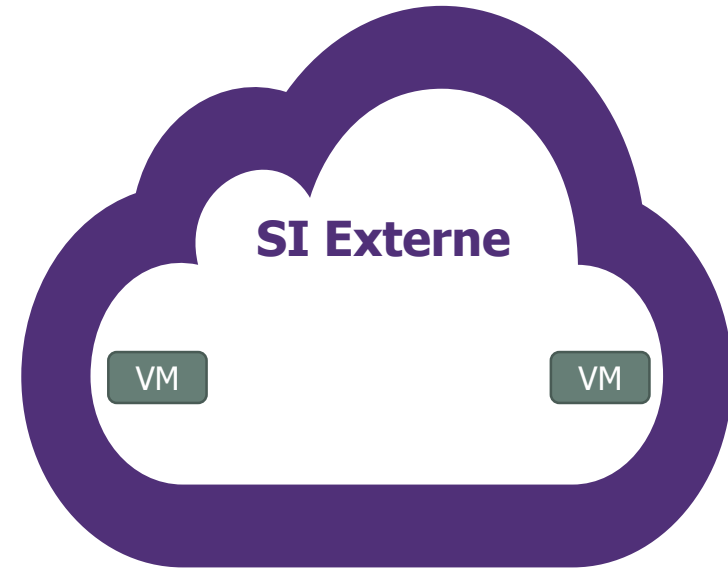
Gestion du **cycle de vie** des applications cloud ?



Les problématiques sur les couches d'infrastructure



Accéder aux services du SI de manière unifiée ?



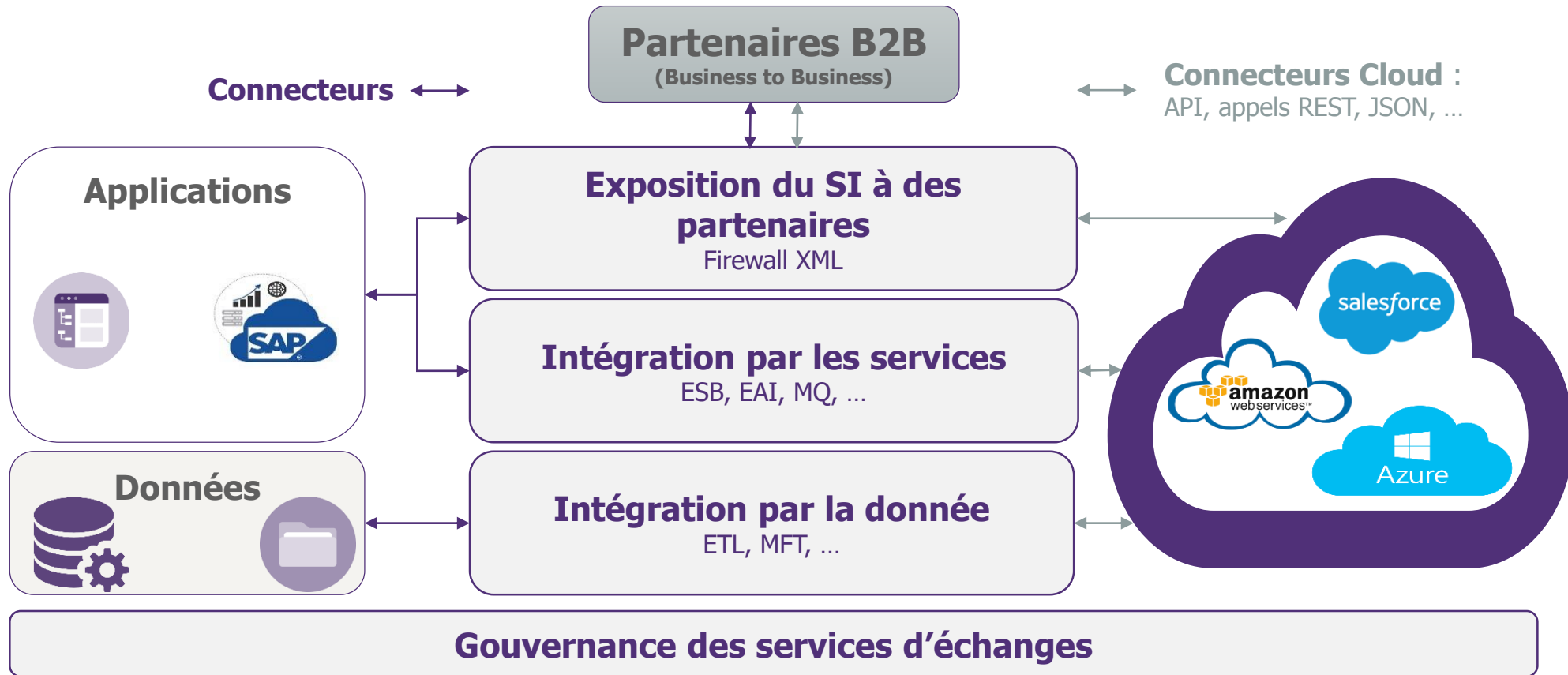
Piloter le cloud hybride



/ **04.2**

Intégrer les couches applicatives

Mettre en place des connecteurs spécifiques pour les services d'échanges



De nouveaux termes apparaissent : ESB, iPaaS, ...

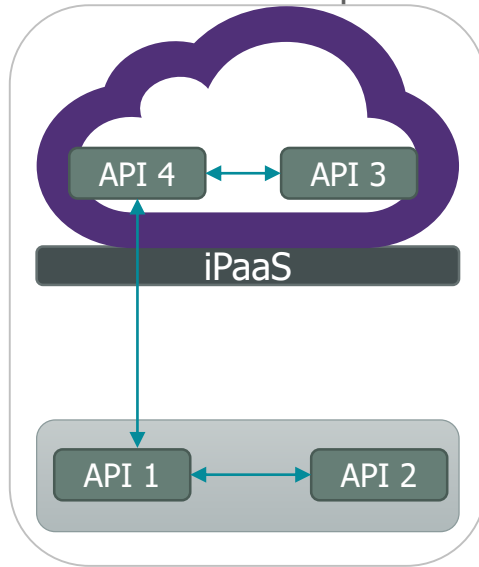
En **2016**, au moins **35%** des grandes et moyennes entreprises dans le monde utiliseront une ou plusieurs offres d'IPaaS sous différentes formes . (Gartner, Mars 2011)



Adapter les topologies de déploiement aux cas d'usage

Public

- Intégration Cloud2Cloud et SI2Cloud
- Mise en œuvre simple

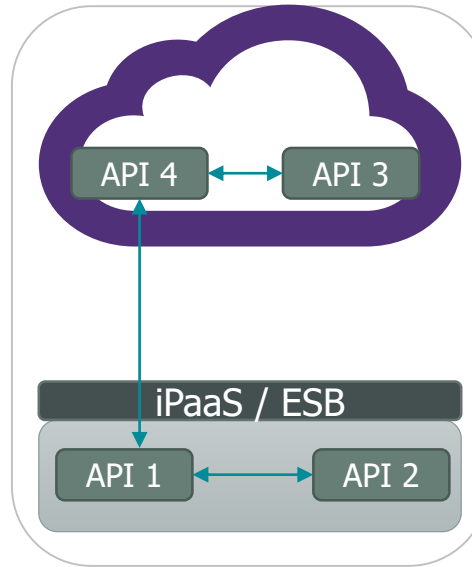


cloudhub



Interne

- Intégration SI2SI et SI2Cloud
- Mise en œuvre complexe

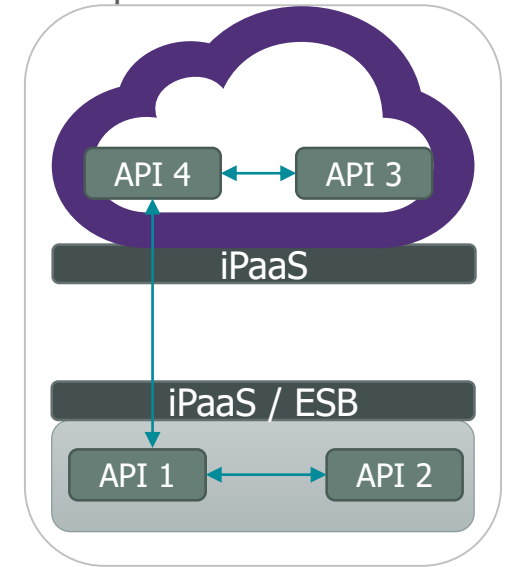


Mule ESB



Distribuée

- Tout type d'intégration
- Mise en œuvre et gestion complexe



INFORMATICA | CLOUD



Ces solutions sont pour la plupart relativement jeunes
(les leaders de l'intégration ne sont pas encore tous positionnés)



Adapter la consommation d'API Cloud suivant la stratégie DSI

Une API Cloud est une façon de consommer les services et les ressources proposés par les fournisseurs Cloud.



Cloud Provider : plus d'innovation au prix d'une adhérence avec le fournisseur

- **Stratégie** : les développeurs font directement appel aux API fournisseurs dans leur code

► **Acteurs** :



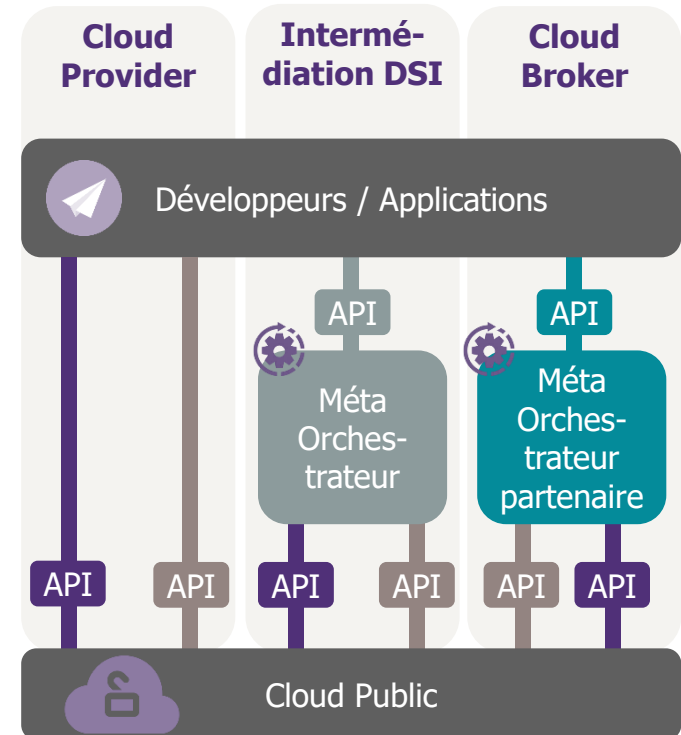
Intermédiation DSI : une décorrélation prudente entre les applications et le fournisseur mais coûteuse

- **Stratégie** : la DSI ajoute une couche d'abstraction en interne. Les développeurs n'utilisent que les API et le framework présentés par la DSI
- **Acteurs** : DSI Interne



Cloud Broker : transition plus aisée vers le Cloud sans disruption de la relation fournisseur

- **Cloud Broker** : API pour une plateforme Cloud qui permet de consommer des services « packagés » par la DSI
- **Pure Player** : Framework et API développés par un tiers pour rendre transparent les services cloud des fournisseurs aux applications
- **Stratégie** : les développeurs utilisent les API & les framework présentés par l'infogérant



► **Acteurs Pure Player** :



► **Acteur Cloud Broker** :





/ **04.3**

Intégrer les couches d'infrastructures

Pilotage unifié de l'infrastructure



Pilotage unifié :
Portail self-service, Catalogue de services, Provisioning, Reporting, Facturation, Mobilité des ressources

- 10/2014 :** EMC rachète Maginatics, Spanning et Cloudscaling
- 09/2014 :** HP se renforce dans le cloud avec le rachat d'Eucalyptus
- 09/2013 :** Cloud et Big Data : Bull s'offre fastConnect
- 05/2013 :** VMware lance son cloud public



Librairies:



Clouds hybrides :



Aucun standard pour la gestion de clouds (malgré des tentatives comme OCCI)

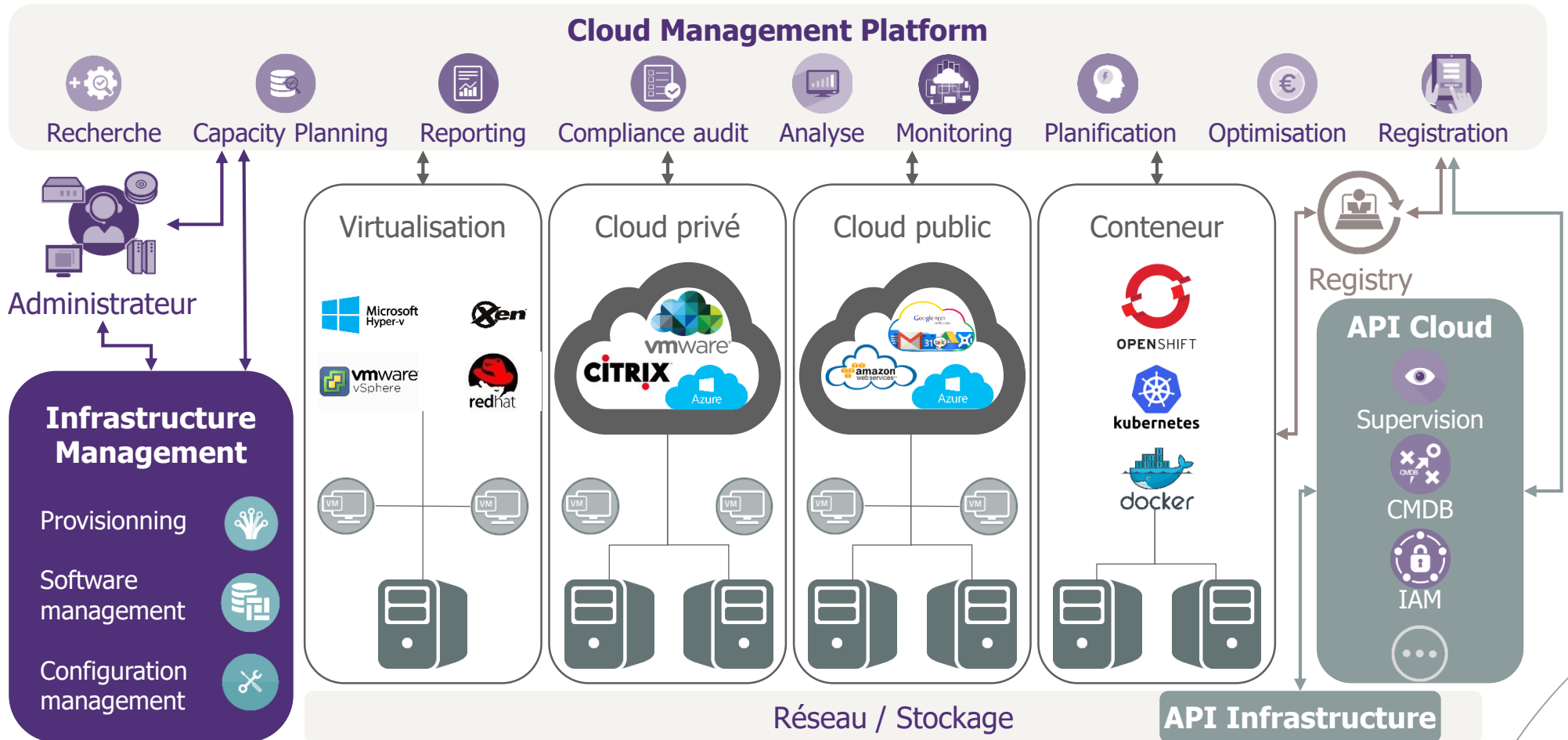


CMP : Cloud Management Platform














Les CMP sont des solutions logicielles permettant de gérer de manière unifiée et centralisée diverses plateformes de Cloud : publiques, privées ou hybrides, voire même pour certains, les plateformes traditionnelles.

Utilisateurs



Les solutions du pilotage du cloud

	Librairies	Clouds hybrides	Managers
Description	Fournissent une API qui permet de gérer les clouds de plusieurs fournisseurs (public ou privé). Elles traduisent l'API des fournisseurs en la leur.	Permet la construction d'un cloud privé ainsi que le pilotage d'autres clouds : <ul style="list-style-type: none"> - Mono-acteurs : étend le cloud privé sur d'autres clouds publics / privés avec la même technologie - Multi-acteurs : unifie la gestion du cloud privé avec diverses solutions - Cloud privé + AWS : étend le Cloud privé avec la gestion d' Amazon WS 	Permet de centraliser la gestion de clouds publics et privés via un unique tableau de bord
Acteurs	 	<div>Cloud privé + AWS</div> <div>    </div> <div> <div>Multi-acteurs</div> <div>   </div> </div> <div> <div>Mono-acteurs</div> <div>   </div> </div>	 
Maturité	Ces librairies ne couvrent pas toutes les fonctionnalités des fournisseurs mais offrent une base pour créer son propre outil de gestion	Solutions variées offrant une interopérabilité des clouds encore relativement faible	Le nombre de clouds gérés est important, cependant les solutions de clouds privés gérées sont principalement open-sources



Synthèse

- **Aucun standard** pour la gestion de clouds (malgré des tentatives comme OCCI de OpenStack)
- Solutions relativement jeunes → **peu de retours d'expérience**



/ **05**

Conclusion

Synthèse sur la sécurité



Une sécurité souvent accrue par rapport aux offres de services internes



Les offreurs de cloud investissent davantage dans ces domaines que la plupart des organisations : souvent grâce à des techniques de virtualisation ou des mécanismes de sécurité techniques avancés.



Ils contrôlent régulièrement leur sécurité, disposent **d'équipes dédiées** au maintien et à l'amélioration du niveau de sécurité et se font **régulièrement auditer**.

Beaucoup de documents en ligne pour les curieux

Les offreurs communiquent beaucoup autour de la sécurité pour rassurer

■ Azure

- ▶ Trust center: <https://www.windowsazure.com/en-us/support/trust-center/security/>

■ Amazon

- ▶ Livre blanc sécurité Amazon: http://awsmedia.s3.amazonaws.com/pdf/AWS_Security_Whitepaper.pdf
- ▶ Best practices de conception: http://media.amazonwebservices.com/AWS_Cloud_Best_Practices.pdf
- ▶ Résumé incident Amazon: <http://aws.amazon.com/fr/message/65648/>
- ▶ AutoScaling : http://docs.amazonwebservices.com/AutoScaling/latest/DeveloperGuide/AS_Concepts.html
- ▶ SimpleDB : <http://docs.amazonwebservices.com/AmazonSimpleDB/latest/DeveloperGuide/ConsistencySummary.html>
- ▶ ...

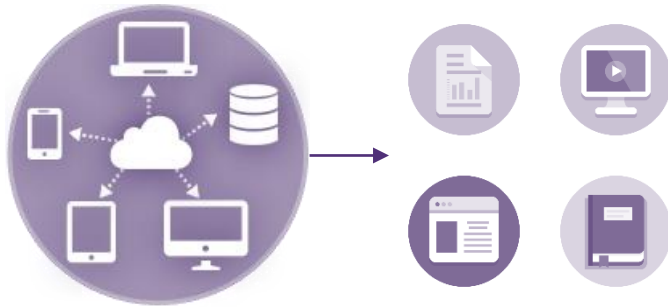


Synthèse sur l'intégration



Des standards d'intégration pour le cloud outillés mais encore en émergence

Rupture des usages ...



Consommation banalisée de l'IT comme une ressource de commodité

... et pourtant

Interfaces encore très hétérogènes et difficulté à faire adopter les standards en émergence



En attendant

Pas de rupture dans la façon de concevoir et d'opérer l'architecture d'intégration du SI !!