

# Formation Cloud Security

---

JAOUHER KHARRAT



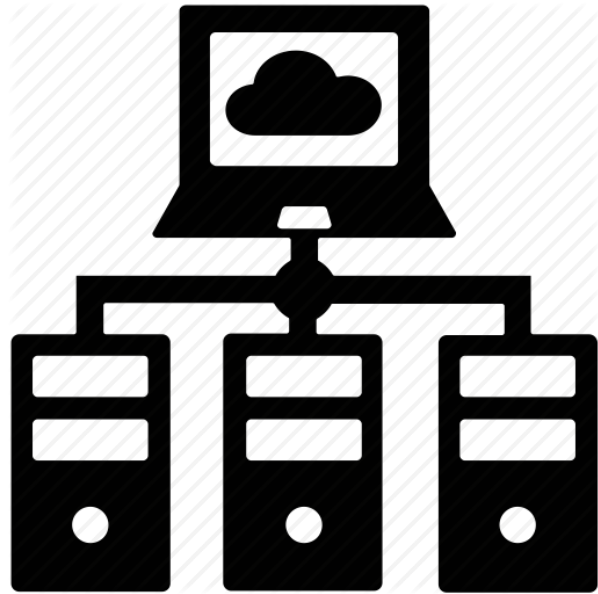
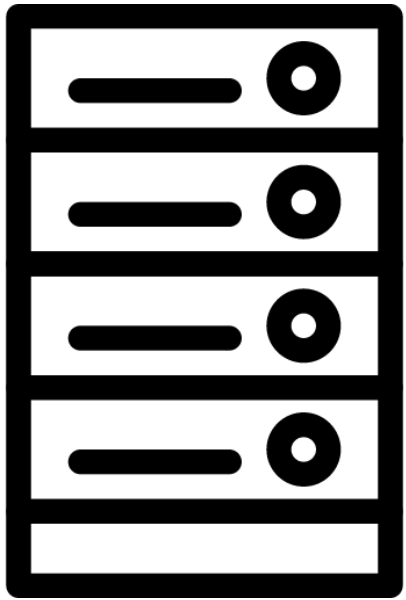
# C'est quoi le Cloud?

---

LE CLOUD EST UN MODEL POUR ASSURER UN ACCÈS PRATIQUE ET SUR DEMANDE DE PARTOUT VERS UN ENSEMBLE PARTAGÉ DE RESSOURCES.

# Quels sont ces resources?

---



Provisionnement  
rapide

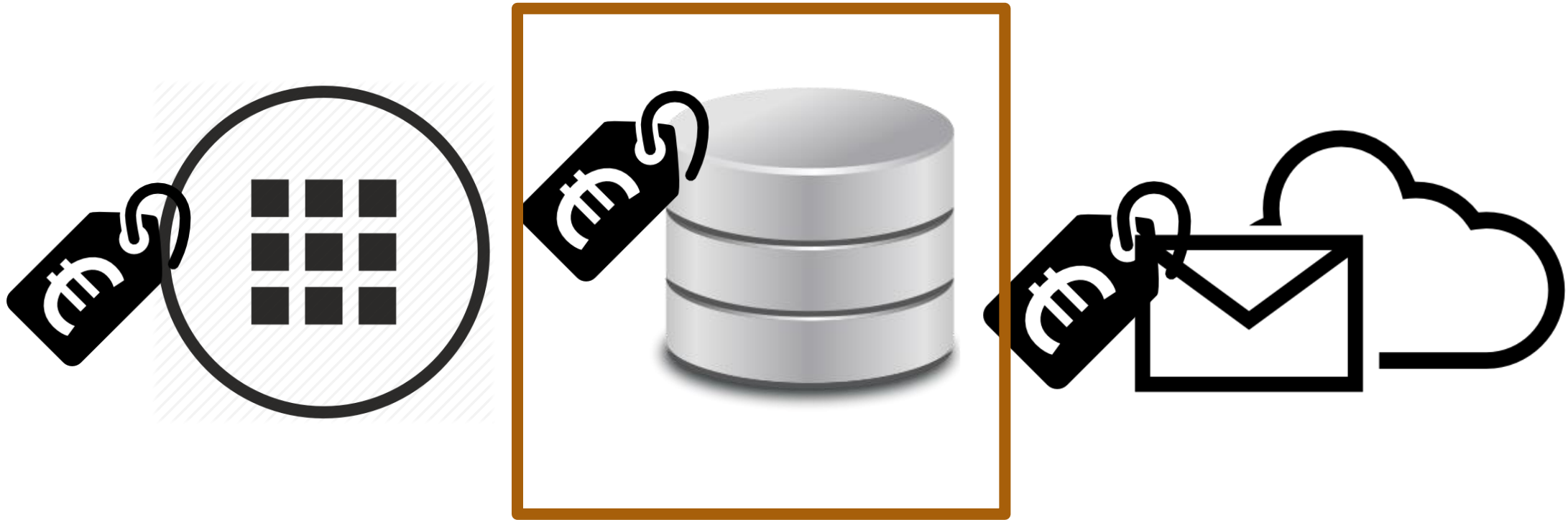




Règles  
essentielles  
pour le Cloud  
computing

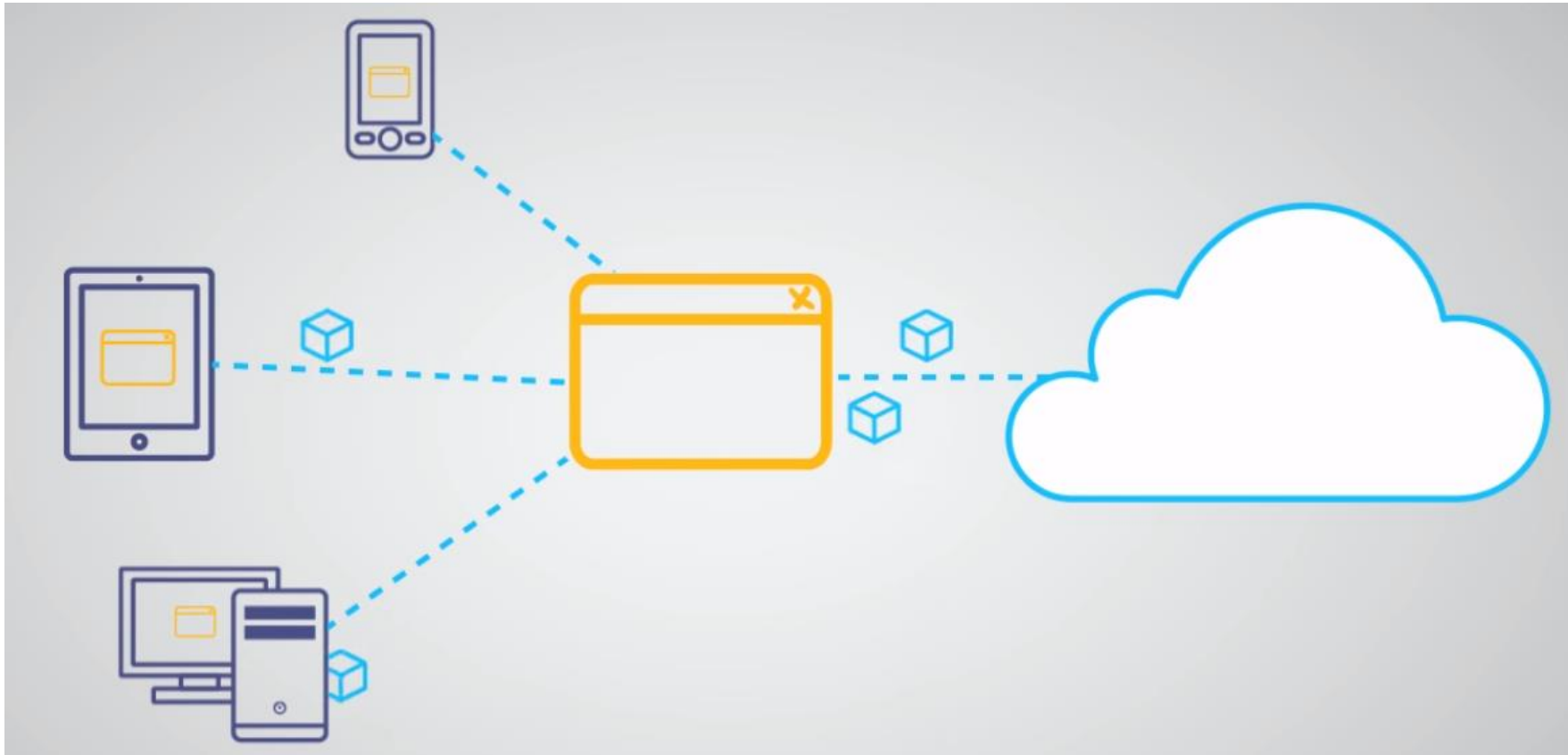
# 1- Self-service à la demande / On-demand self-service

---



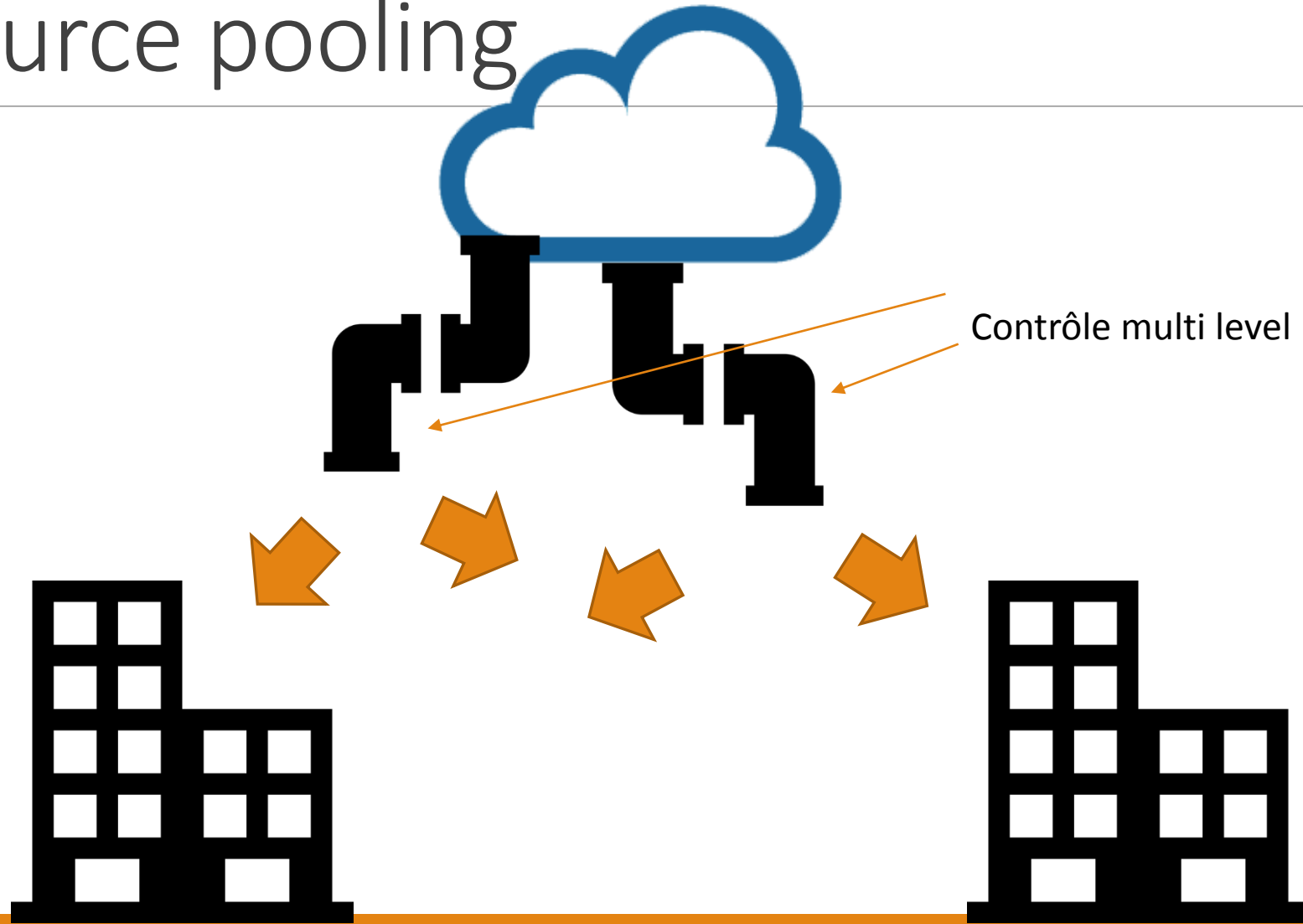
## 2- l'accès au réseau à large bande / Broad network access

---



### 3- Mise en commun des ressources / Resource pooling

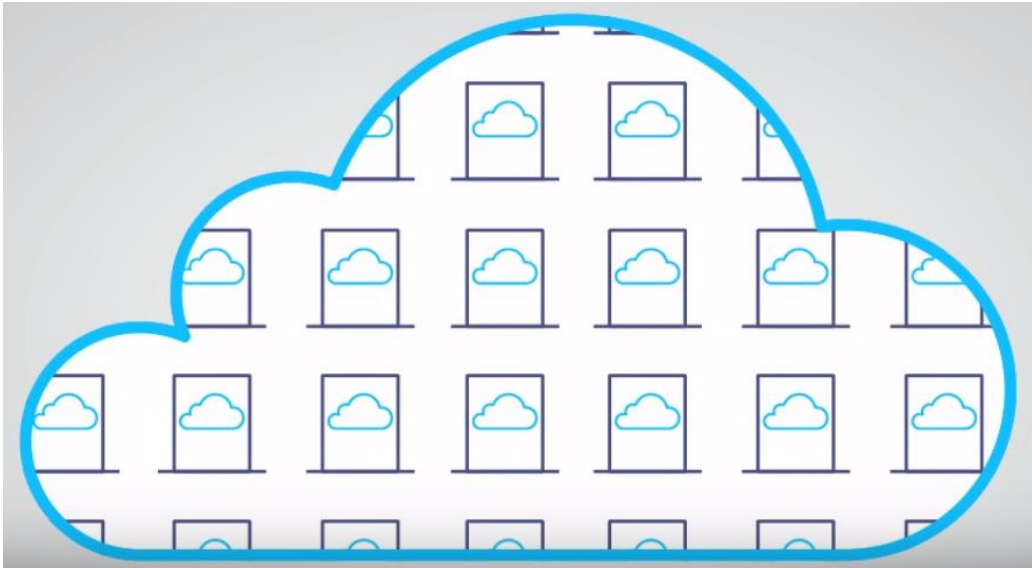
---





## 4- élasticité rapide/ Rapid elasticity

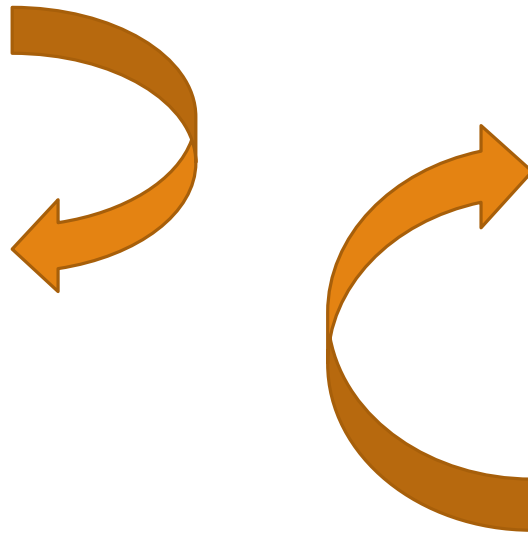
---



# 5- Mesure / Metering

---

Niveau  
d'utilisation

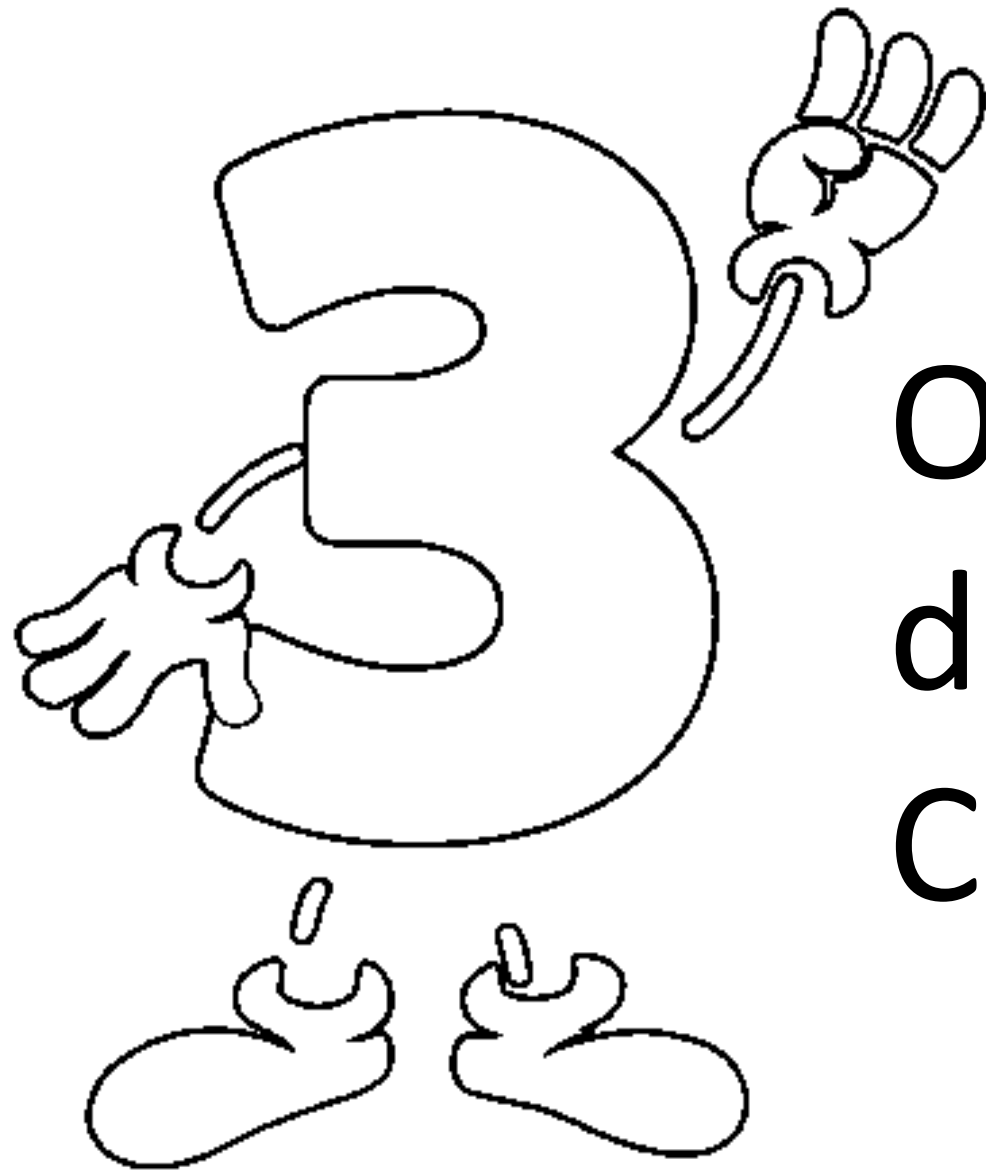


\$1,359



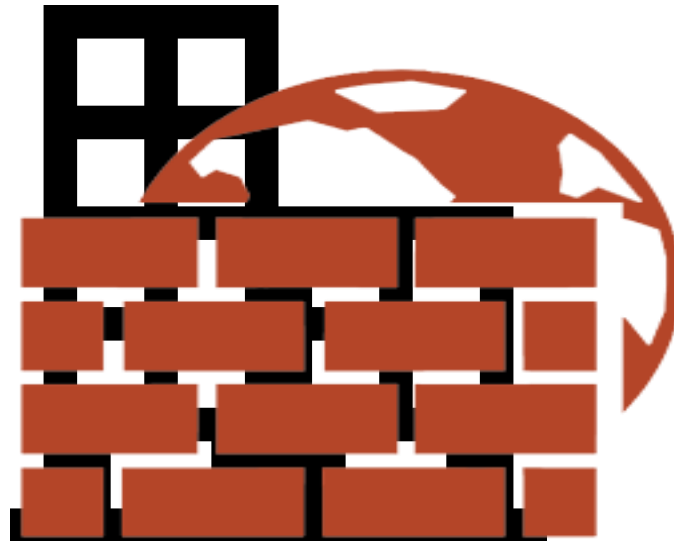
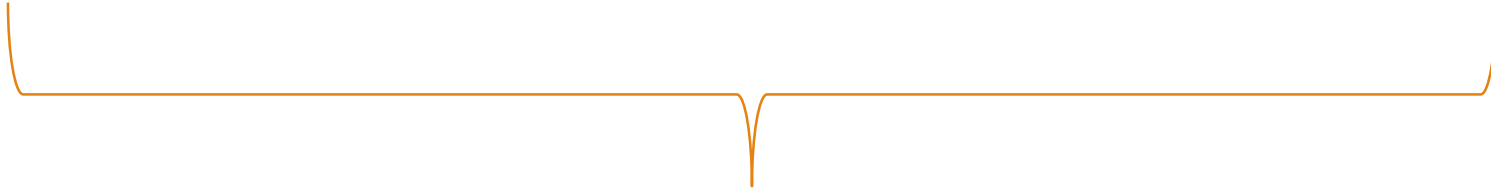
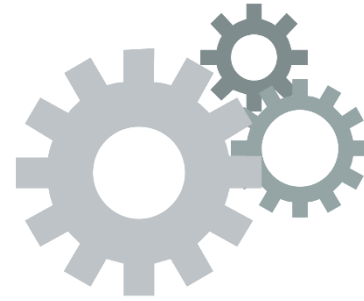
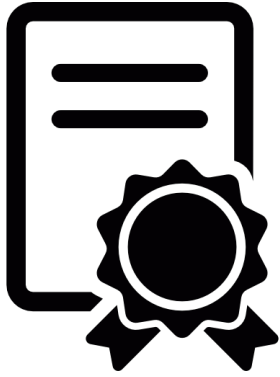
\$175

Coût d'utilisation

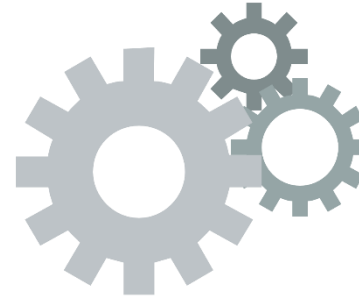


Options pour le  
déploiement  
Cloud





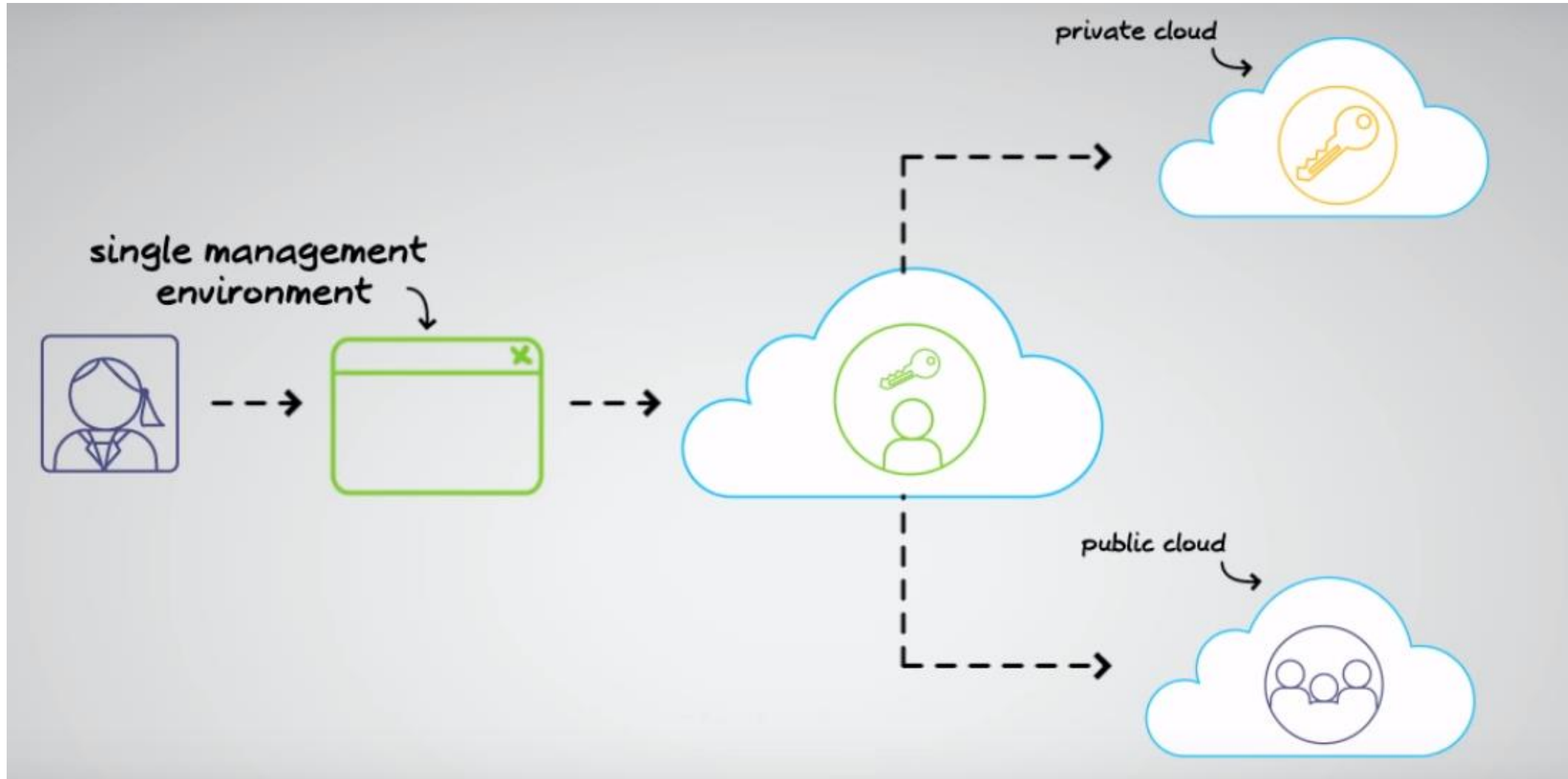
Cloud privé

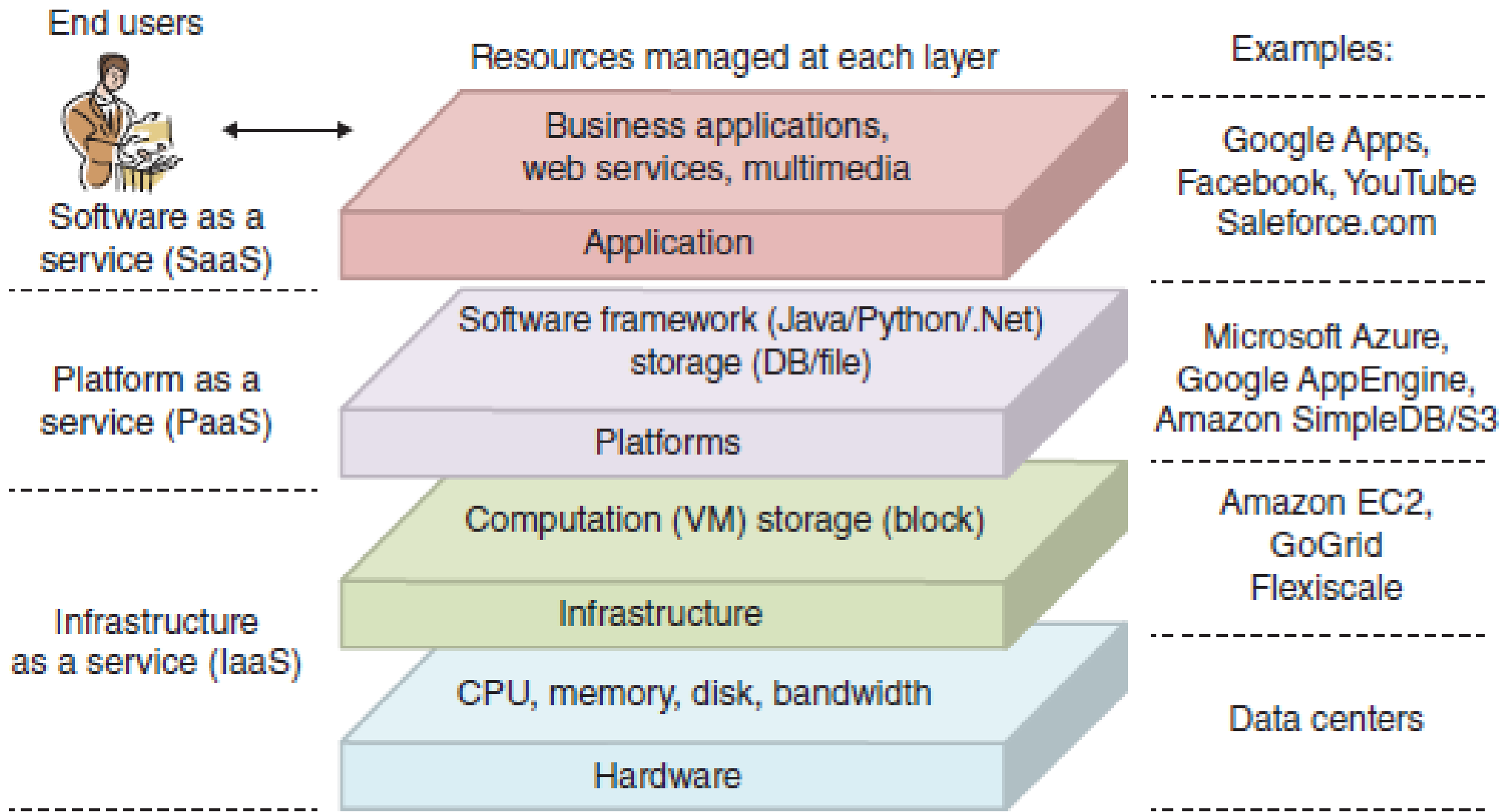


Cloud service  
provider



Cloud Public









Types des services  
IT utilisés à travers  
les nuages privés,  
hybrides et  
publiques

# SaaS Software as a Service

---

utilisée pour désigner une application, mise à disposition à distance par un fournisseur, et accessible par le biais d'un navigateur Internet. Elle est aussi louée, au mois ou à l'usage. Les mises jour sont automatiques.

Elle permet aux utilisateurs :

- Access aux applications
- Sans avoir à gérer ou contrôler le nuage sous-jacent pour le delivery

Exemples

□ Gmail

□ Salesforce.com



# SaaS

---

Le terme SaaS (*logiciel en tant que service*) remplace les termes ASP (*application service provider*) ou encore « *on demand* », précédemment employés. Il est apparu le 28 février 2001, dans un article « *Strategic Backgrounder: Software As A Service* » publié par *The Software & Information Industry's (SIIA) eBusiness Division*, édition de Washington DC

Les principales applications actuelles de ce modèle sont :

- le gestionnaire de relation client (CRM) ;
- la visioconférence ;
- la gestion des ressources humaines<sup>1</sup>;
- les communications unifiées<sup>2</sup> ;
- la messagerie et les logiciels collaboratifs.

# PaaS Platform as a Service

---

- Donne accès aux utilisateurs à un environnement de développement pour leur permettre de créer leur propre applications Cloud en utilisant leurs propres langages de programmation, librairies , services et outils
- L'utilisateur a le contrôle total sur ces applications
- Il a un contrôle sur partiel sur les paramètres de l'espace hébergement
- Il n'a pas de contrôle sur l'infrastructure



# PaaS

---

Ce type de cloud computing permet de mettre à disposition des entreprises un environnement d'exécution rapidement disponible, en leur laissant la maîtrise des applications qu'elles peuvent installer, configurer et utiliser elles-mêmes. Il permet donc d'héberger des applications qui ne sont pas adaptées au modèle du SaaS (par exemple des applications spécifiques, des applications en cours de développement...).

Exemples de fournisseurs:

SAP HANA Cloud Platform<sup>3</sup> by SAP, OVH, AWS Elastic Beanstalk, [Heroku](#), [Gandi](#), exoscale<sup>4</sup>, Force.com, [Google App Engine](#), OpenShift by Red Hat, [Bluemix](#) by [IBM](#), Jelastic or Clever Cloud.

# IaaS: Infrastructure as a Service

---

- Il est le plus utilisé et le plus souvent considéré en tant que LE CLOUD
- Il permet à l'utilisateur de une disposition complète des ressources rapidement et facilement incluant traitement, stockage et les réseaux sans que l'utilisateur n'ait à se soucier de gérer ou contrôler l'infrastructure

Exemple:

OVH

Amazon

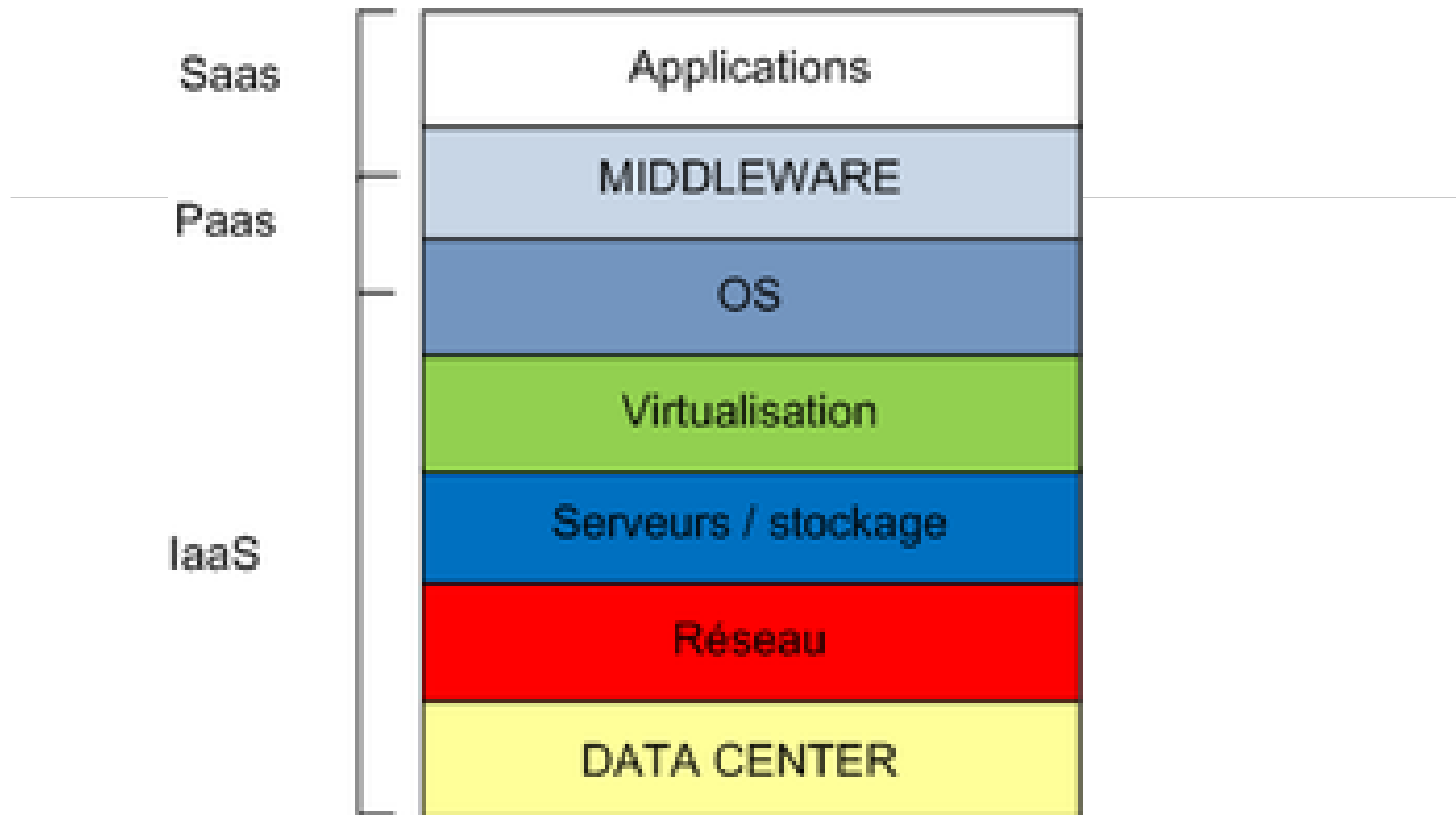
Azure



# IaaS

---

C'est un modèle où l'entreprise dispose sur abonnement payant d'une infrastructure informatique (serveurs, stockage, sauvegarde, réseau) qui se trouve physiquement chez le fournisseur. Cela peut représenter pour certaines directions des systèmes d'information (DSI) un moyen de réaliser des économies, principalement en transformant des investissements en contrats de location.





# Comparatif

---



**SaaS**

Software  
as a Service



**CONSUME**



**PaaS**

Platform  
as a Service



**BUILD ON IT**



**IaaS**

Infrastructure  
as a Service



**MIGRATE TO IT**

# Autres membres de la famille « .AAS »

---

- ❑ **Desktop as a service** (*DaaS* ; aussi appelé en français **bureau en tant que service**, **bureau virtuel** ou **bureau virtuel hébergé**) est l'externalisation d'une virtual desktop infrastructure auprès d'un fournisseur de services.
- ❑ **Data as a service**, ou DaaS, est une technique consistant à faire payer un abonnement pour l'accès à un dépôt de données via une interface fournie par le fournisseur<sup>1</sup>. Comme tous les membres de la famille des "*as a Service*" (AAS), DaaS est basée sur le concept où le produit, les données dans ce cas, peut être fourni à l'utilisateur sur demande<sup>2</sup> quelle que soit la distance entre l'utilisateur et le fournisseur des données.
- ❑ **Communications en tant que Services** (CaaS)
- ❑ **Réseau en tant que Service** (NaaS)

# DATA centers – Cloud providers

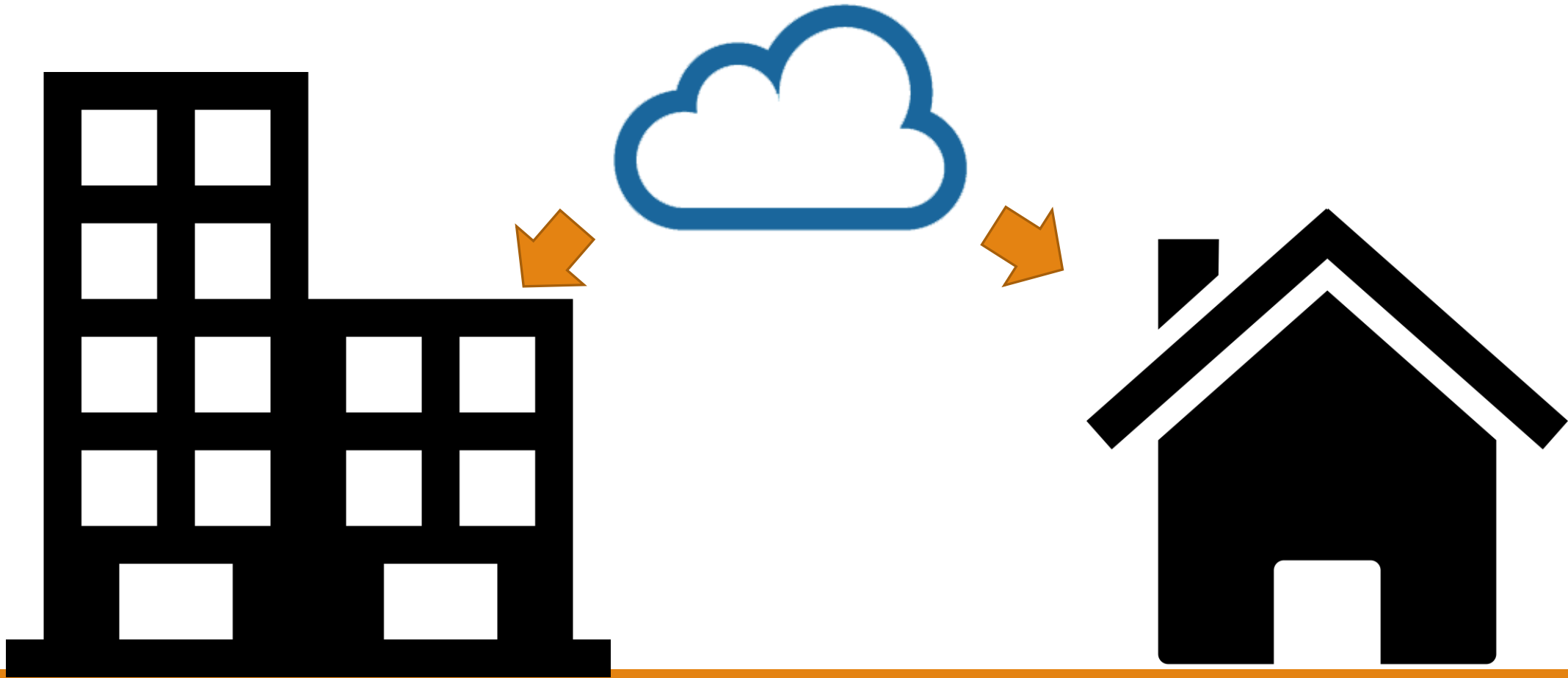
---



- ❑ LA plus part sont très hautement virtualités
- ❑ Il peut prendre 1 ou 2 jours → semaine pour fournir une machine virtuelle
- ❑ Voir plus pour avoir les autorisation nécessaires
- ❑ IaaS comme Amazon sont en expansion rapide a cause de ce besoin de on-demand computing resources en hausse continue
- ❑ Les services IT d'une entreprise ne sont pas capables de fournir aussi rapidement ou quantitativement que ces IaaS providers

# DATA centers – Cloud providers

---



Le fournisseur est payé que pour les coûts opérationnels en cours uniquement pour les ressources informatiques qu'ils utilisent. : « Pay as you use »

«

Le Cloud public est souvent considéré comme le bonne solution pour l'utilisation de ces ressources pour une courte durée



# Avantages Cloud privé

---



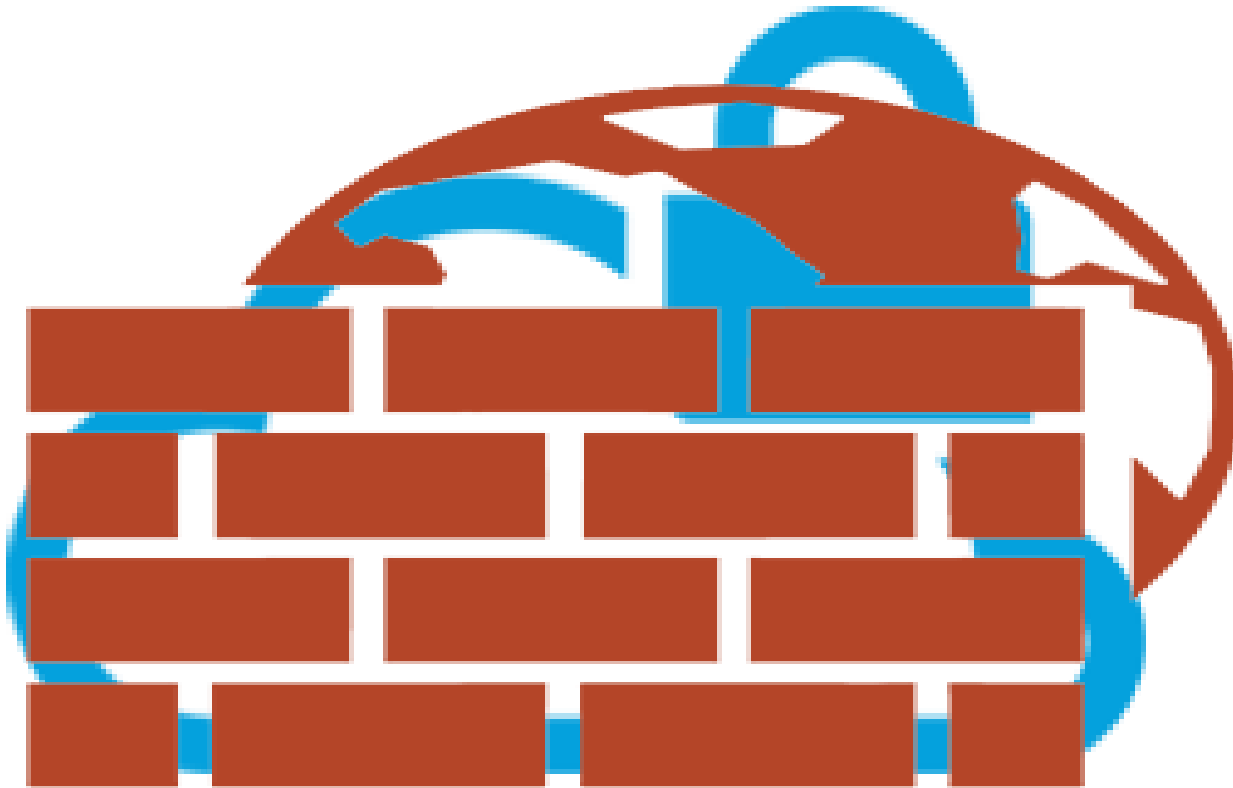
J'ai besoin de 3  
machines  
virtuelles

Cet avantage est étendu dans ces propres data centers, Il aide à répondre plus rapidement à l'évolution des affaires et exigences des clients et réduire le cout en introduisant une plus grande automatisation

Ceci permet de minimiser le cout en introduisant une plus grande automatisation et en améliorant l'efficacité de l'environnement informatique

# Avantages Cloud privé

---



Puisque un cloud privé est à l'intérieur du parefeu:

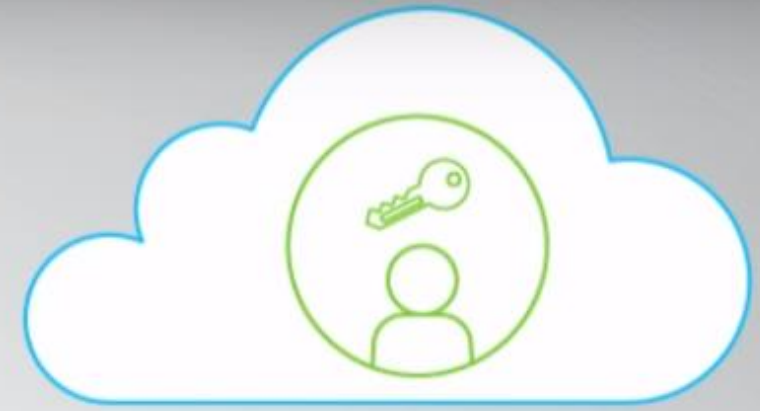
- Il donne également un meilleur contrôle sur la sécurité et informations
- Contribue à assurer la conformité aux règlements



Publique



Privé



Hybride

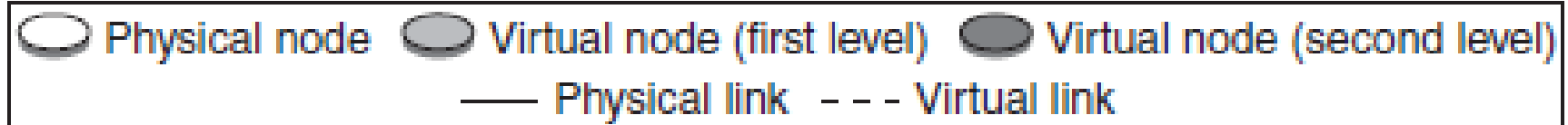
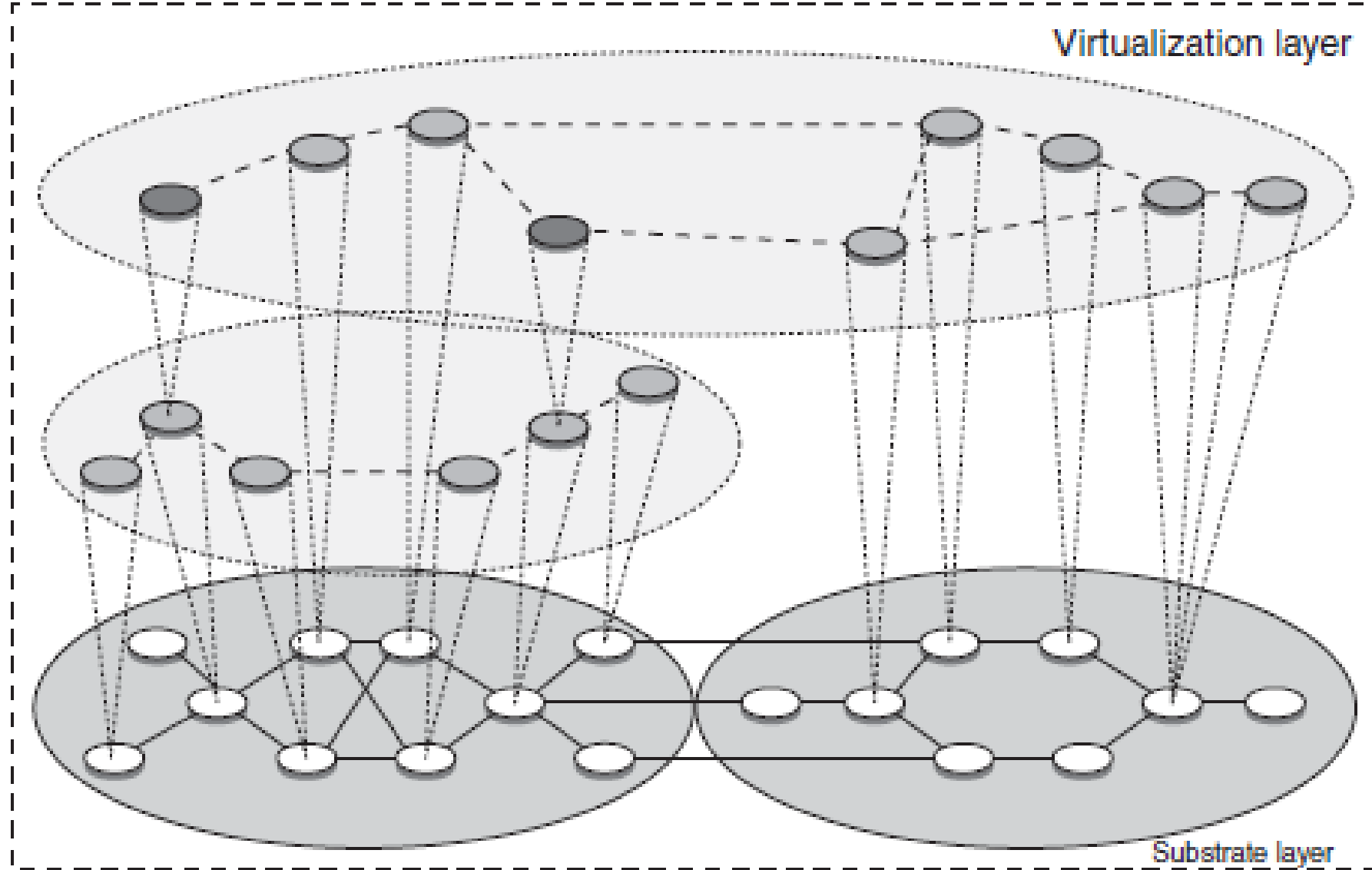
Pour IaaS et pour tous types de cloud, Les entreprises sont capables de développer une infrastructure flexible et agile pour mieux harmoniser les besoins du business tout en réduisant les coûts



# Virtualisation dans le cloud

---

- La virtualisation est l'une des principales technologies habilitantes qui ont fait le modèle de cloud computing une réalité. Dans un premier temps, les technologies de virtualisation ont permis de partitionner un serveur physique en plusieurs environnements isolés appelés VMs qui peuvent éventuellement accueillir différents systèmes d'exploitation et être utilisés par différents utilisateurs ou applications.
- L'une des fonctionnalités puissantes apportées par la virtualisation est la possibilité de facilement migrer les VMs dans le même centre de données ou même entre les centres de données répartis géographiquement. Cette fonction fournit une flexibilité sans précédent pour les opérateurs de réseaux et centres de données leur permettant d'effectuer plusieurs tâches de gestion comme l'optimisation dynamique des allocations de ressources, l'amélioration de la tolérance aux pannes, la consolidation de la charge de travail, ce qui évite la surcharge du serveur, et les activités de maintenance d'ordonnancement.



# Virtualisation dans le cloud

---

Les opérations de virtualisation sont structurées en fonction des composants: calcul, le stockage, le réseau et la gestion.

# Sécurité dans le cloud

---

La sécurité a toujours été une question clé pour les services basés sur le cloud et plusieurs solutions ont été proposées pour protéger le nuage contre les attaques malveillantes. En particulier, les systèmes de détection d'intrusion (IDS) et les systèmes de prévention des intrusions (IPS) ont été largement déployés pour améliorer la sécurité des nuages et ont récemment été habilités avec les nouvelles pour améliorer encore leur efficacité.

FlowIPS, une solution basée sur OpenFlow-IPS pour la prévention d'intrusion dans les environnements de cloud computing.

# Problématiques dans la sécurité

---

## SUR LES DONNÉES

- ❑ *Dépendent du choix des données mises dans le Cloud (Données « coeur de métier » ou non)*
- ❑ *La localisation des données (Duplication, dispersion)*
- ❑ *Des contraintes légales ( notification des violations de données personnelles, Réquisitions judiciaires)*
- ❑ *Protection des données (Qui peut y accéder?)*

## SUR LES APPLICATIONS

- ❑ *Qui a accès à quoi ? ( Profils d'utilisateurs)*
- ❑ *Traçabilité des accès et des actions*

# Les solutions de sécurité

---

## ❖ Localisation des données

- Savoir localiser géographiquement les données (Recommandations du pays et/ou préférences / exigences du client)
- Assurer la purge (destruction sécurisée des données) dans tous les emplacements
- Planifier une récupération d'informations en cas de saisie judiciaire
- Prévoir une réversibilité

# Les solutions de sécurité

---

## ❖ Protection des données

- Chiffrement données (BD et fichiers)
- Chiffrement transparent:
  - À la volée par l'application ou DB (en mode SaaS)
  - Clés stockés dans le Cloud
  - Difficile d'interdire accès des admins au Cloud
- Chiffrement bout en bout (PTP)
  - Clés détenus par clients finaux

# Les solutions de sécurité

---

## ❖ Authentification des utilisateurs

- Nominative → solutions:
  - 2 annuaires cloud/entreprise avec synchronisation
  - Délégation d'authentification
  - Fédération d'identités (SAML,...)

## ❖ Habilitation et contrôle d'accès:

- Permissions d'accès sur ressources et données
- Interdire comptes génériques et partage des comptes



# Les solutions de sécurité

---

## ❖ Traçabilité

- Surveillance des accès aux ressources dans le Cloud / Enquête / Forensics en cas d'accident
- Recueillir des traces complets (centraliser/croiser les logs)
- Protéger l'accès aux traces
- Organiser consultation/transmission des logs aux clients
- Prévoir une purge des logs

# 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/>

# TP:

---

- Essayer <https://jsonplaceholder.typicode.com/> + <https://goo.gl/n9npl6> extension chrome --> tester les services Saas
  - Télécharger et Installer EasyPHP
  - Télécharger et installer owncloud
  - Tester un Cloud public pour un PaaS:  
<https://www.heroku.com/pricing>
- + git account and add / push a repo to yours: <https://github.com/ShinigamiGod/testerKakarot>

# ownCloud

---



**ownCloud** est un logiciel libre offrant une plateforme de services de stockage et partage de fichiers et d'applications diverses en ligne. Il est présenté comme une alternative à Dropbox, lequel est basé sur un Cloud public. Dans ownCloud, le stockage des données se fait au sein de l'infrastructure de l'entreprise et les accès sont soumis à la politique de sécurité informatique de celle-ci.