



Architecture Cloud (AWS)

1^{ère} partie : connaissance générale du Cloud

Didier Meier



- Société de conseil - Accompagnement vers le Cloud
- www.ilki.fr
- dmeier@ilki.fr



Conseil

*De la définition de besoin
au pilotage de projet*



Architecture

*Concevoir des architectures
adaptées à vos besoins*



Formation

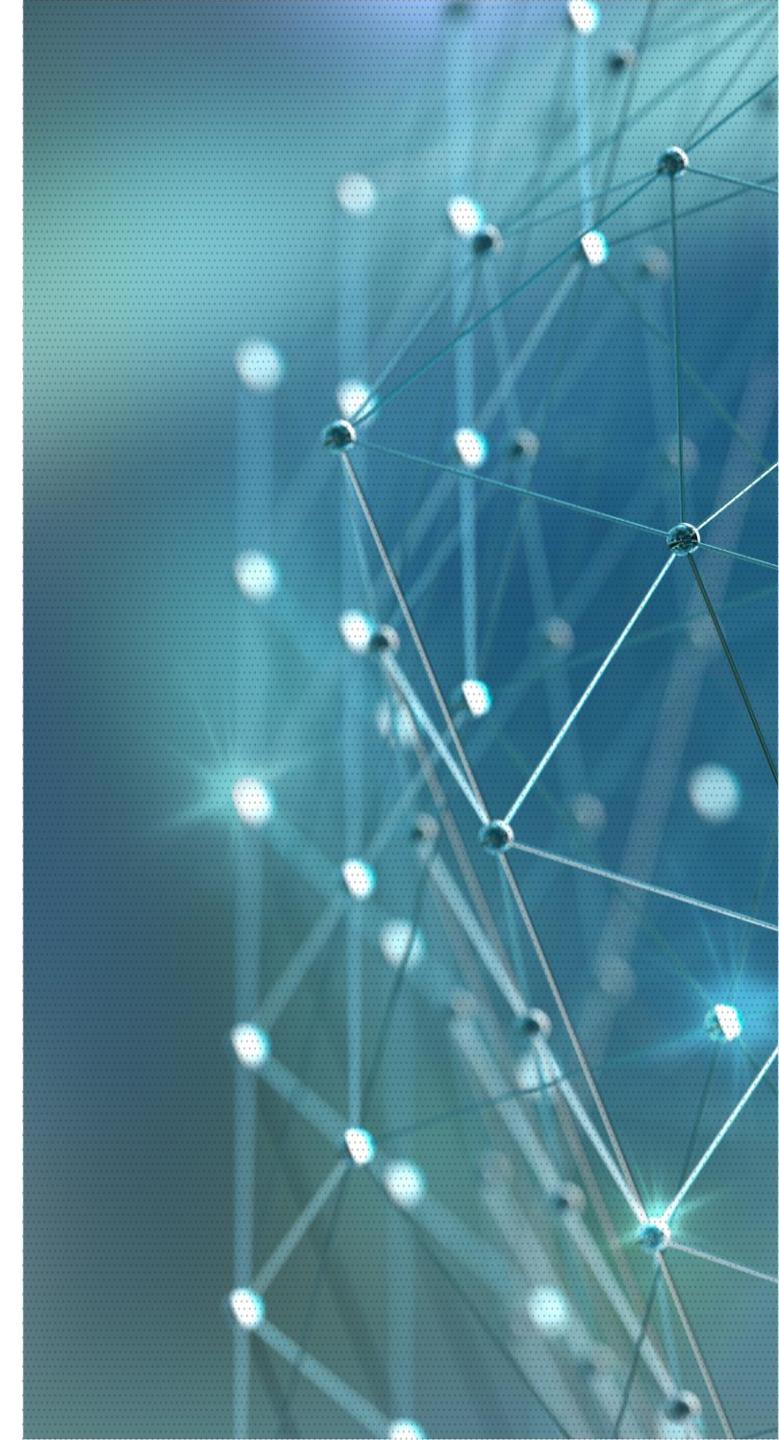
*Séminaires décideurs
Formations techniques
Enseignement supérieur*

Sommaire

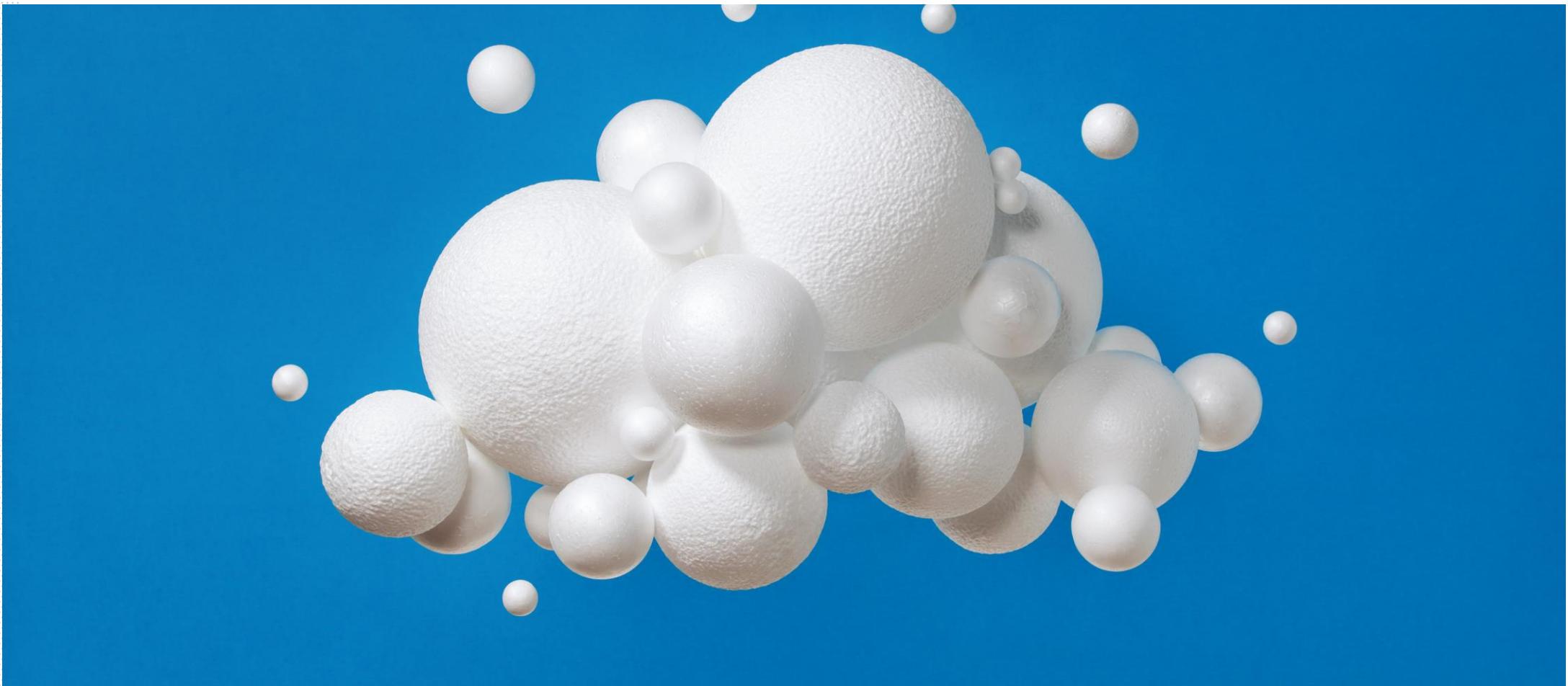
- **Introduction**
- **Cloud Computing**
 - Fondamentaux, bénéfices et enjeux
 - Comprendre les aspects juridiques et la sécurité
- **L'impact du Cloud**
 - L'évolution de la structure des entreprises
 - L'évolution des métiers
- **Un tour d'horizon des solutions des acteurs du marché du Cloud**
 - Software as a Service
 - Platform as a Service
 - Infrastructure as a Service
- **Comment construire son cloud privé**
- **Conclusion**



Introduction



Je travaille dans le cloud...



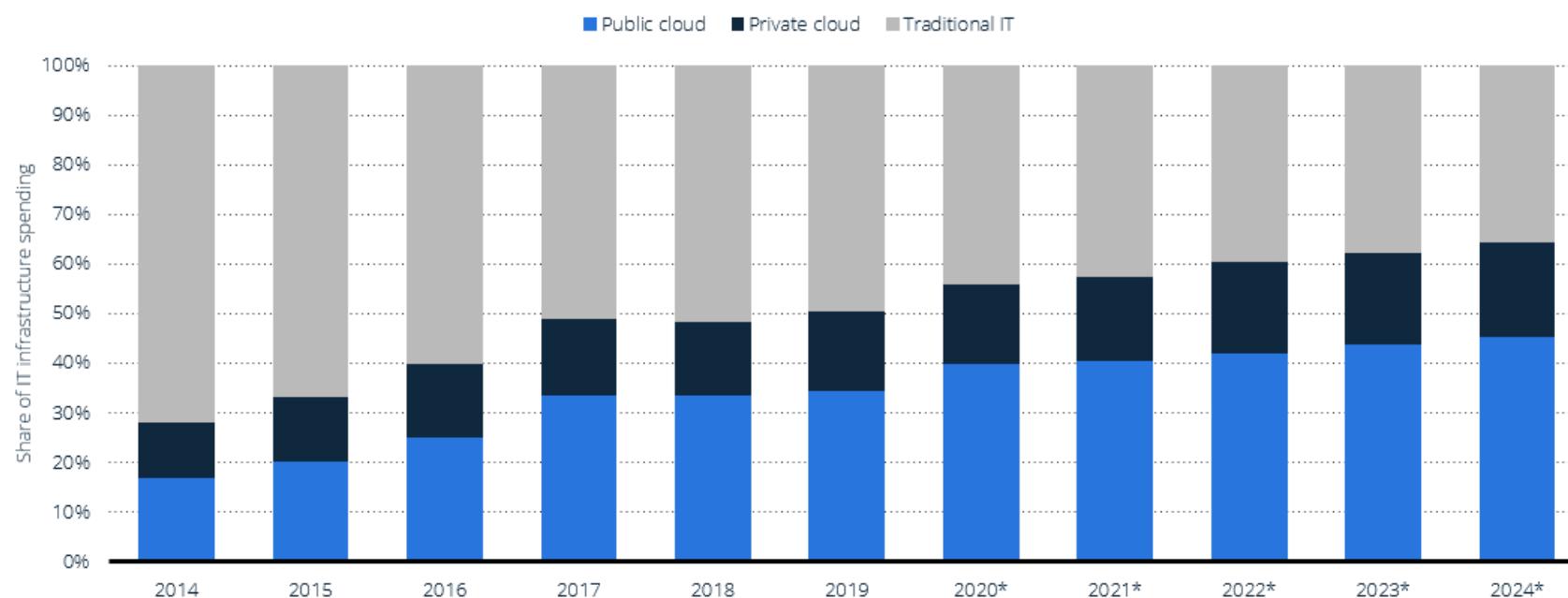
Introduction

- Définition ou définitions...
 - D'où vient le mot Cloud ?
 - ✓ Représentation classique sur tout schéma pour représenter Internet
 - Signifiant « tout ce que l'on ne connaît pas et que l'on ne peut pas représenter »
 - ✓ Par extension, accéder aux applications/données sans savoir où elles sont, qui les gèrent etc.
 - Larousse 2020 :
 - ✓ Informatique en nuage (calqué de l'anglais cloud computing) : modèle d'organisation informatique permettant l'accès à des ressources numériques dont le stockage est externalisé sur plusieurs serveurs.
 - Définition Wikipédia :
 - ✓ Le cloud computing en français l'informatique en nuage, (ou encore l'infonuagique au Canada), correspond à l'accès à des services informatiques (serveurs, stockage, mise en réseau, logiciels) via Internet (le « cloud » ou « nuage ») à partir d'un fournisseur.
 - ✓ Les principaux services proposés en cloud computing sont le SaaS (Software as a Service), le PaaS (Platform as a Service) et le IaaS (Infrastructure as a Service) ou le MBaaS (Mobile Backend as a Service). On distingue généralement trois types de cloud : le cloud public — accessible par Internet —, le cloud d'entreprise ou privé — accessible uniquement sur un réseau privé —, le cloud intermédiaire ou hybride — qui est un mix entre le cloud public et le cloud privé. Le cloud computing permet aux entreprises de minimiser les coûts d'infrastructure informatique [réf. nécessaire] et de bénéficier d'une adaptation des ressources en fonction des fluctuations de l'usage, avec cependant une augmentation notable des coûts d'exploitation du réseau.

Une progression constante

Worldwide information technology (IT) infrastructure spending breakdown (by value) from 2014 to 2024, by deployment type**

Share of IT infrastructure spending worldwide 2014-2024, by deployment type



Source : Statistica

Sommaire

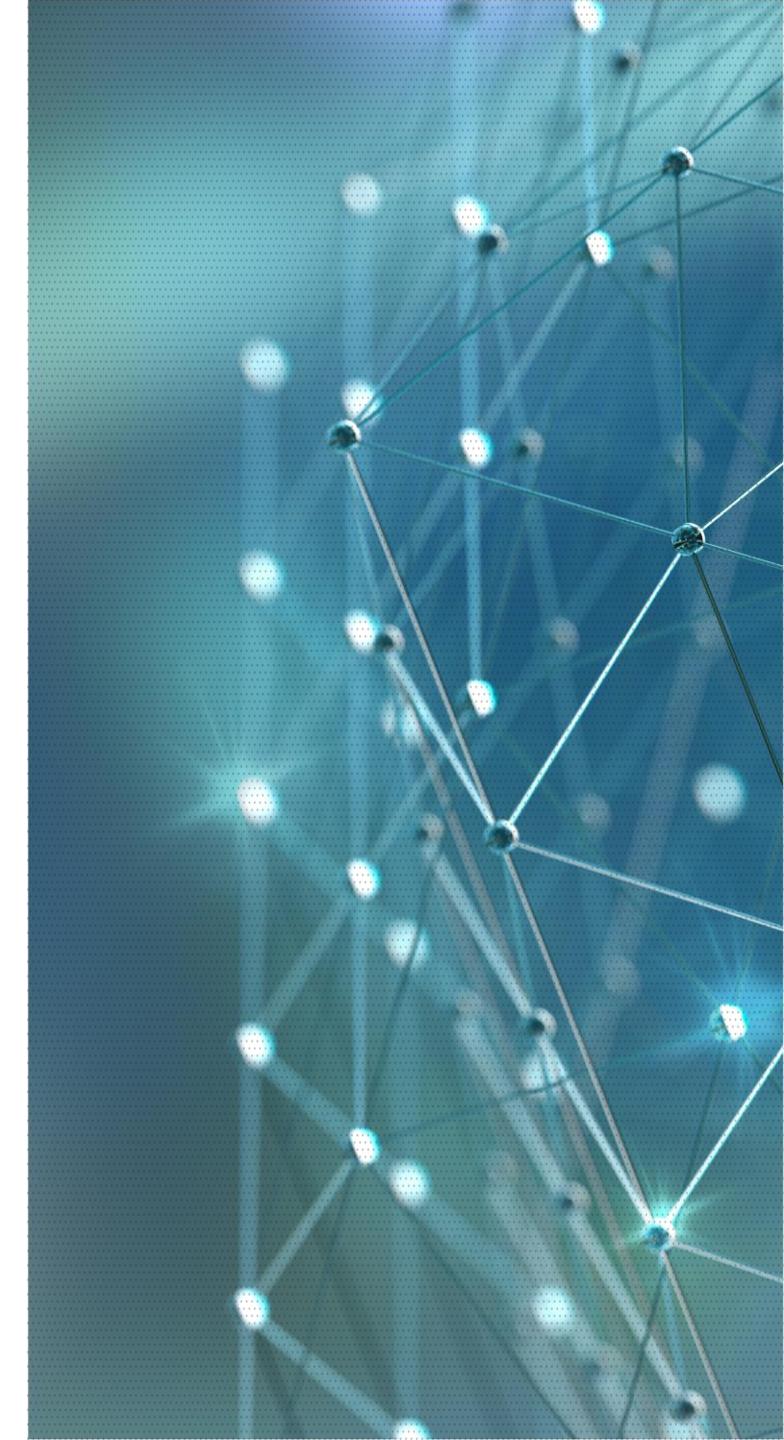
- **Introduction**
- **Cloud Computing**
 - Fondamentaux, bénéfices et enjeux
 - Comprendre les aspects juridiques et la sécurité
- **L'impact du Cloud**
 - L'évolution de la structure des entreprises
 - L'évolution des métiers
- **Un tour d'horizon des solutions des acteurs du marché du Cloud**
 - Software as a Service
 - Platform as a Service
 - Infrastructure as a Service
- **Comment construire son cloud privé**
- **Conclusion**



Cloud Computing

Fondamentaux, bénéfices et enjeux

Comprendre les aspects juridiques et la sécurité



Le cloud selon le NST et l'ISO

National Institute of Standards and Technology – Septembre 2011

Définition reprise par l'ISO : ISO/IEC 17788 – Octobre 2014



5 caractéristiques :

- On demand self service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service



3 modèles de services :

- SaaS
- PaaS
- IaaS



4 modèles de déploiement :

- Cloud privé
- Cloud public
- Cloud communautaire
- Cloud hybride



Qu'est-ce que le Cloud Computing

5 caractéristiques

On Demand Self Service

L'utilisateur peut quand il en a besoin, sans intermédiaire humain et quel que soit le fournisseur de service provisionner ou modifier de la puissance informatique (Réseau, serveurs, stockage...)

Broad Network Access

Toutes ces possibilités sont disponibles à travers un réseau par des mécanismes standards depuis des postes hétérogènes : clients lourds, légers, mobiles...

Resource pooling

Les ressources informatiques (physiques ou virtuelles) sont regroupées (pooled) pour plusieurs utilisateurs de différentes sociétés assignées dynamiquement et réassignées selon la demande

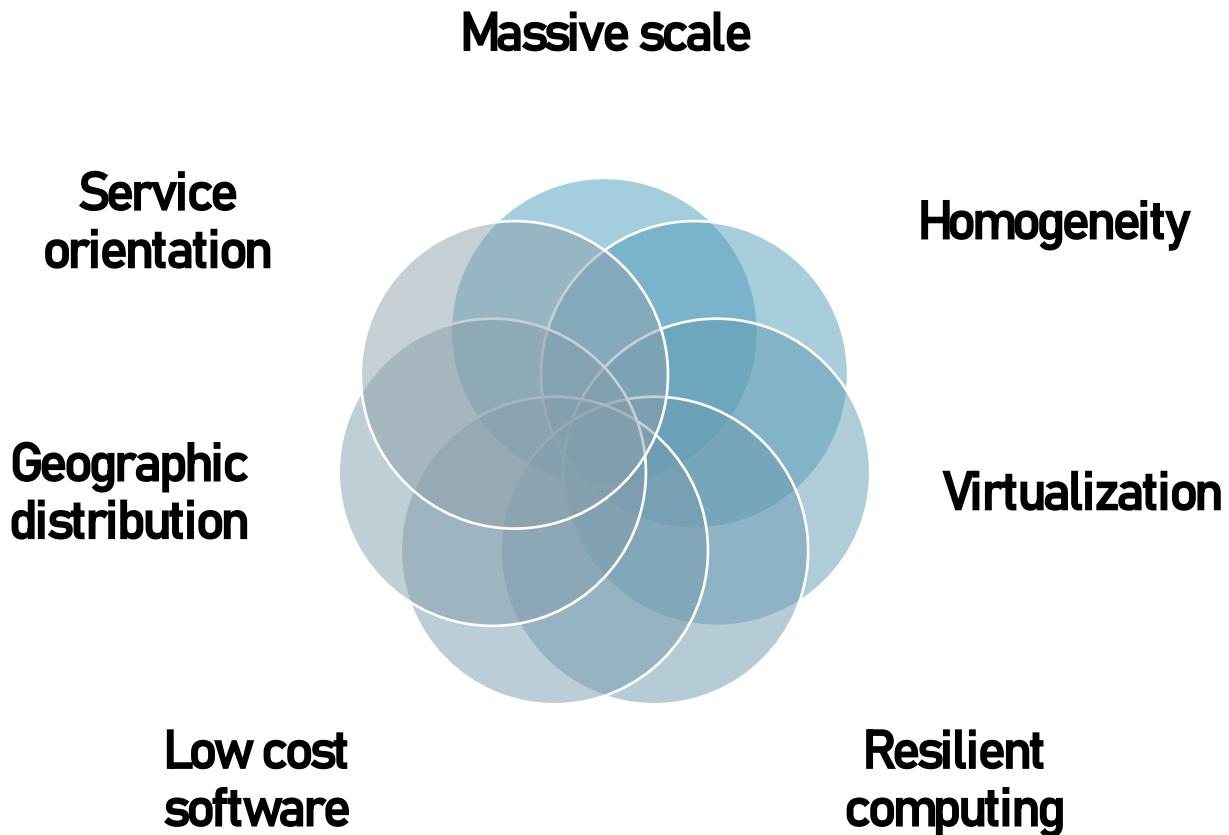
Rapid Elasticity

Les capacités informatiques peuvent être provisionnées ou dé-provisionnées automatiquement le plus souvent

Measured Services

Mesures permanentes selon le service (stockage, nombre d'utilisateurs...) de l'utilisation des ressources, contrôle et optimisation automatique des ressources

Caractéristiques complémentaires



Le cloud selon le NST et l'ISO



5 caractéristiques :

- On demand self service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service



3 modèles de services :

- SaaS
- PaaS
- IaaS



4 modèles de déploiement :

- Cloud privé
- Cloud public
- Cloud communautaire
- Cloud hybride



3 modèles de services : SaaS

- SaaS = Software as a Service
 - Logiciel hébergé chez un fournisseur :
 - ✓ Qui gère tout : mise à jour, support, évolution, qualité de service...
 - Dédié (généralement) à une application ou un groupe d'applications



SaaS

Un petit peu d'histoire

- ASP :
 - Application Service Provider
- En français, FAH :
 - Fournisseur d'applications hébergées
- Très en vogue 1998-2000 :
 - Jusqu'à l'explosion de la bulle Internet
 - Discours sur les applications :
 - ✓ Les applications Web vont tout révolutionner
 - ✓ Mesdames les entreprises, redévelopper tout en Web



Limites des applications Web historiques

- Richesse fonctionnelle inférieure à une application classique
- Le protocole est HTTP :
 - Pas de qualité de service par défaut sur TCP/IP
 - Protocole de transfert de fichiers pas optimisé
- Le client est tout sauf un client léger :
 - Internet Explorer n'est pas un client léger...
 - Gestion des patchs par exemple
- Il existait de nombreux problèmes de conflits:
 - ActiveX uniquement avec I.E
 - Plusieurs JRE nécessaires :
 - ✓ Pas deux JRE sur le même poste
 - Le client riche n'a pas jamais décollé à cause de sa lourdeur (flash, silverlight...)
- Des solutions de contournement :
 - Publication via Citrix d'Internet Explorer
 - Silos applicatifs selon JRE utilisé
 - Virtualisation applicative
 - Accélérateurs et optimiseurs de flux TCP/IP

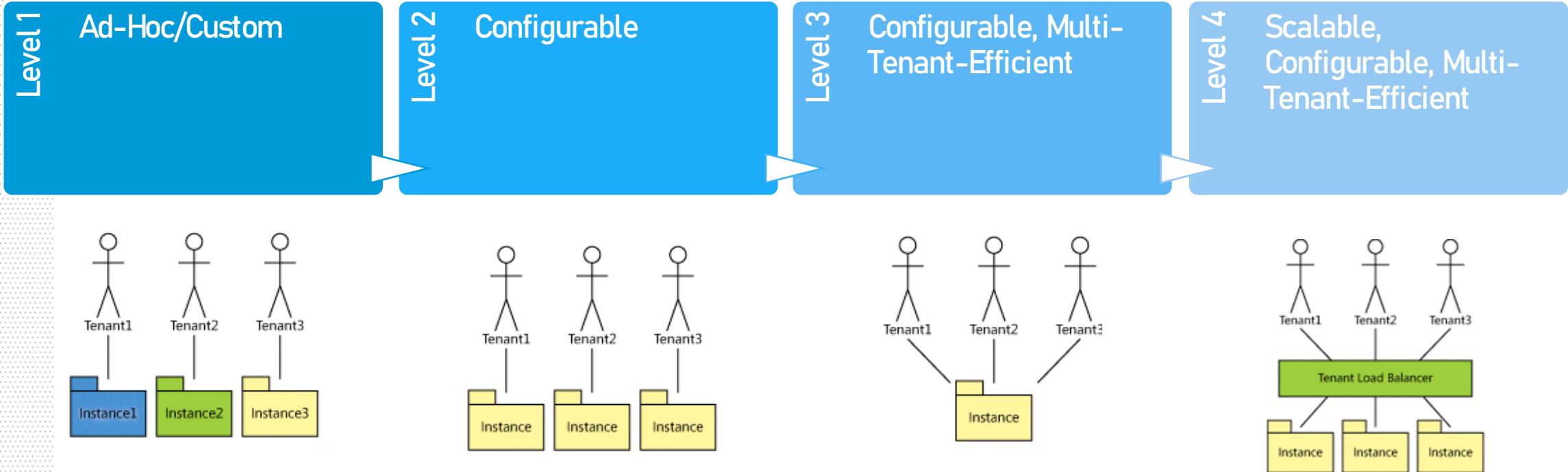


- Une interface différente : DHTML
 - HTML5
 - JavaScript
- Fonctions collaboratives
- API ouvertes
- Service Oriented Architecture
 - Unification des processus en utilisant des modules plus petits appelés « services » pour structurer des grosses applications
- Open Source
 - Pas de déploiement :
 - ✓ Utilisation quel que soit le poste, y compris un mobile
 - Des mises à jour permanentes sans contraintes :
 - ✓ Plus de notions de migration
 - ✓ La « bêta perpétuelle » : release often, release early
 - Accessible depuis partout, même en déconnecté

SaaS versus Software

	Software	SaaS
Licence	« perpétuelle » + maintenance annuelle	Abonnement au nombre d'utilisateurs réels
Maintenance et mise à jour	Coûteuse	Incluse
Maintenance serveurs	Coûteuse	Mutualisée
Postes de travail	PC	PC, Smartphone, tablettes...

SaaS: Maturity Levels



Source : <https://blogs.msdn.microsoft.com/gianpaolo/2006/03/06/saas-simple-maturity-model/>

3 modèles de services : PaaS

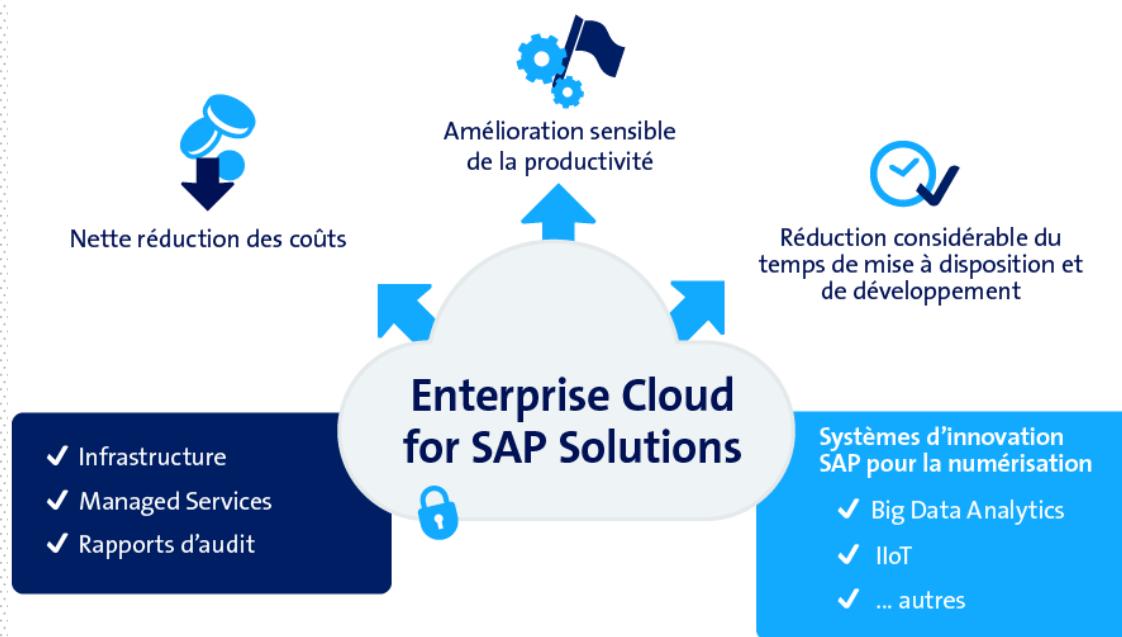
- **PaaS = Platform as a Service**
- **Plate-forme complète de développement et déploiement pour les applications en mode SaaS et services Web :**
 - Conception, intégration de web services, développement, test, travail collaboratif, bug tracking, versioning...
 - Gestions des instances, scalable sur demande, gestion, monitoring et reporting...
- **Socle normalisé pour toutes les étapes de développement d'une application**

Les plates-formes « PaaS » privées

- Plate-forme de type « Lab management » : c'est du IaaS pour les développeurs
- Self-service
 - Délégation de droits : création, nombre de VM, suppression, snapshots...
 - Découpe projets
- Catalogue de machines
 - Templates OS
 - Templates Base de données
 - Templates Outil de développement
- Idéalement relié au « Stage Management »

« PaaS » privées mutualisées

L'exemple de Swisscom avec SAP



L'Enterprise Cloud for SAP Solutions en détail

Prestations standard

- > Services IaaS sur infrastructure SAP certifiée, disponibles en packages avec avoir mensuel pour CPU & RAM
- > Catégories de prix de S à XXL avec différentes durées (de 0 à 3 ans)
- > SAP HANA ready virtual server en t-shirt sizes (de 128 Go à 4 To)
- > Portail Self-Service avec divers profils d'utilisateur, accessible via le web
- > Décompte des prestations pour serveur à l'heure près
- > Stockage dans deux qualités (Standard, Premium Plus)
- > Utilisation dual site dans le stretch cluster via deux centres de calcul Tier IV en Suisse
- > Solutions de sauvegarde automatisées et certifiées SAP sur simple pression de bouton
- > Online ticketing
- > Possibilités de monitoring avec réglages individuels

Prestations en option

- > Server OS management services pour différentes variantes d'OS (Windows & Linux)
- > Licences OS pour les systèmes d'exploitation utilisés
- > Garanties SLA sur les serveurs, droits d'administrateur temporaires possibles
- > Services de sauvegarde (agent based) cohérents avec les applications
- > Rapport d'audit ISAE pour l'infrastructure IaaS employée
- > Service continuity management (garanties RTO/RPO) pour la protection contre les crises informatiques
- > Assistance téléphonique

Services supplémentaires

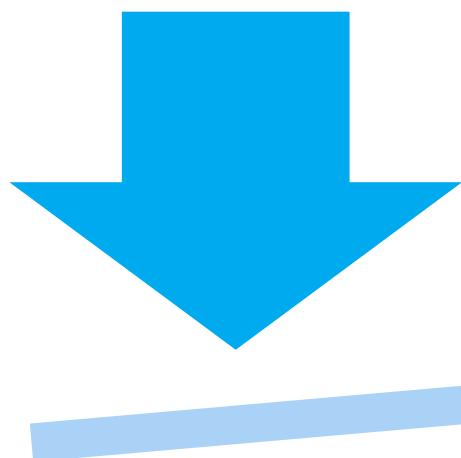
- > Licences et maintenance SAP
- > Assistance de migration et de configuration
- > SAP application management
- > SAP consulting
- > SAP S/4 transition factory
- > WAN connectivity services pour l'intégration à l'Enterprise Cloud for SAP Solutions
- > Autres professional services ou direction de projet

Les vraies plates-formes PaaS pour les applis Cloud

- Managed versus productized platforms
 - Public versus privé
 - La plate-forme est gérée ou vous la gérez
- Portable versus non portable
 - Utilisation des spécifications et des API d'une plate-forme spécifique
 - ou pas de réécriture du code (juste des adaptations)

3 modèles de services : IaaS

- IaaS = Infrastructure as a Service

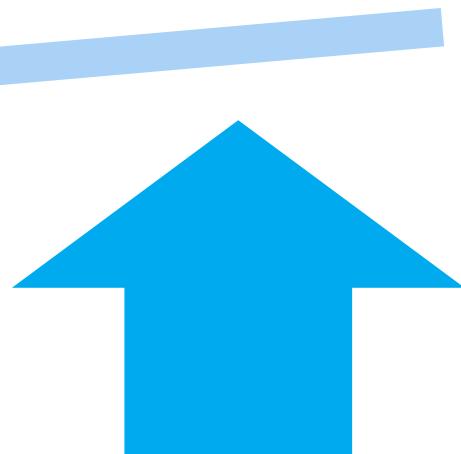


Infrastructure

- Serveurs (et à leurs espaces)
 - CPU
 - mémoire
- Réseau
- Stockage

As a Service

- Facturation à l'utilisation
- Elasticité



Cloud = Virtualisation ?

- Toutes les technologies de virtualisation sont présentes dans le Cloud

Virtualisation de serveurs

Virtualisation de stockage

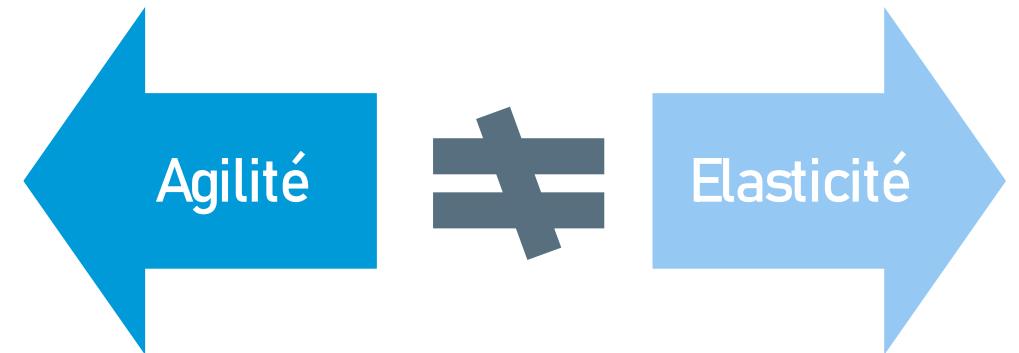
Virtualisation du réseau

Virtualisation de poste de travail

Virtualisation des applications

Les bénéfices de vos architectures de virtualisation

- Virtualisation de serveurs
 - Consolidation de serveurs
 - Disponibilité
 - Facilite les PRA
- Virtualisation de stockage
 - Gestion de l'hétérogénéité du stockage
 - Facilite les PRA
- L'aspect « agilité » a été depuis démontrée
 - Déplacement à chaud de VM, DRS, Storage...
 - Snapshot, templates, clonage...
 - Provisionning des serveurs, des postes de travail...
 - Modifications non perturbatrices des LUN...

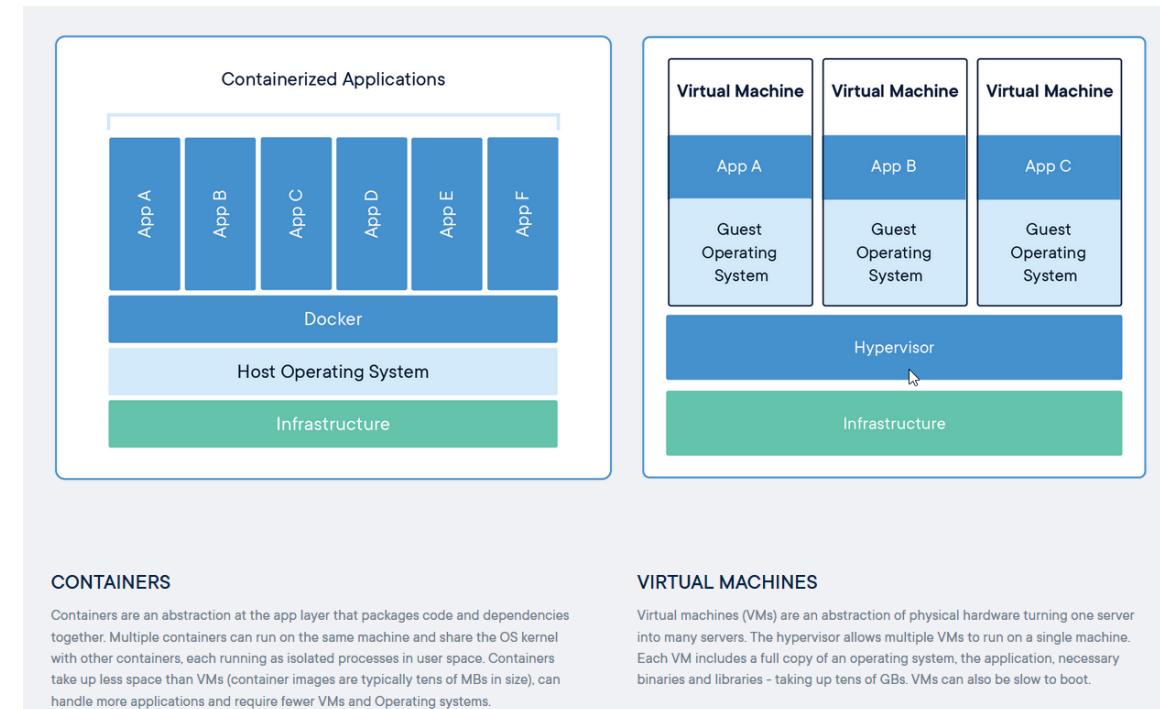


Les dernières évolutions Docker et les containers

- **Histoire**
 - Projet dotCloud (PaaS)
 - Docker 0.1.0 le 25 mars 2013
 - dotCloud devient Docker Inc. le 29 octobre 2013

- **Principes**
 - Plate-forme pour construire, délivrer et exécuter des applications distribuées
 - Fonctionne sous les distributions Linux 64 bits à partir du noyau 3.8+
 - Supportée par Amazon, Google, Rackspace...

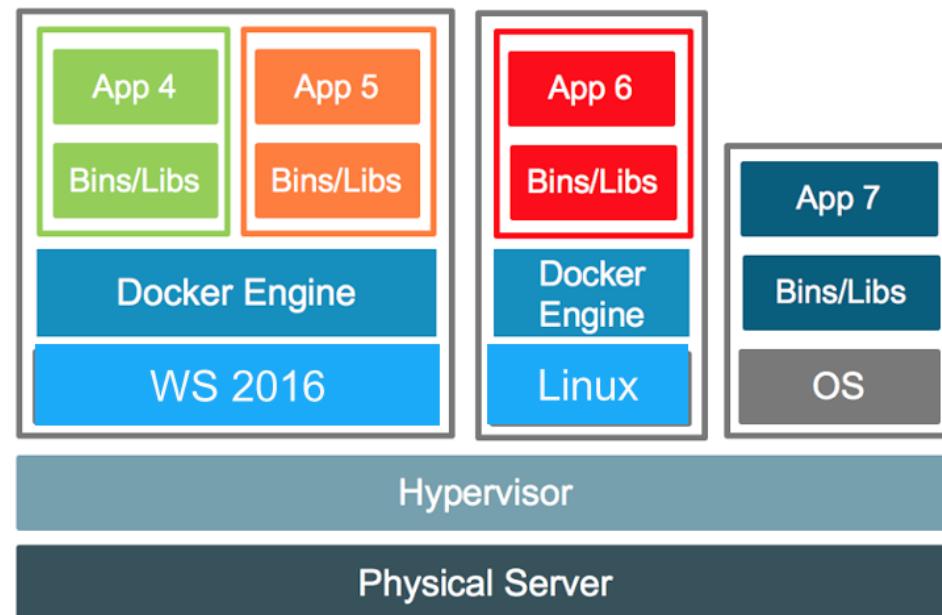
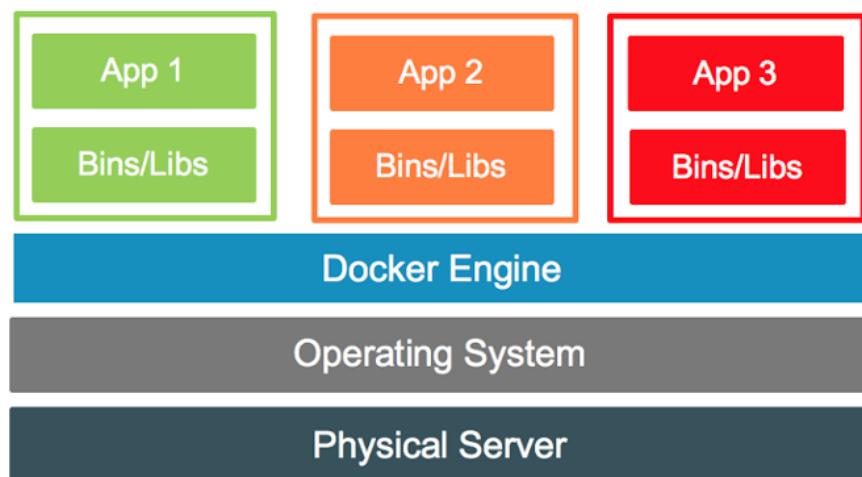
- **Caractéristiques**
 - Léger
 - Portable
 - Autosuffisant



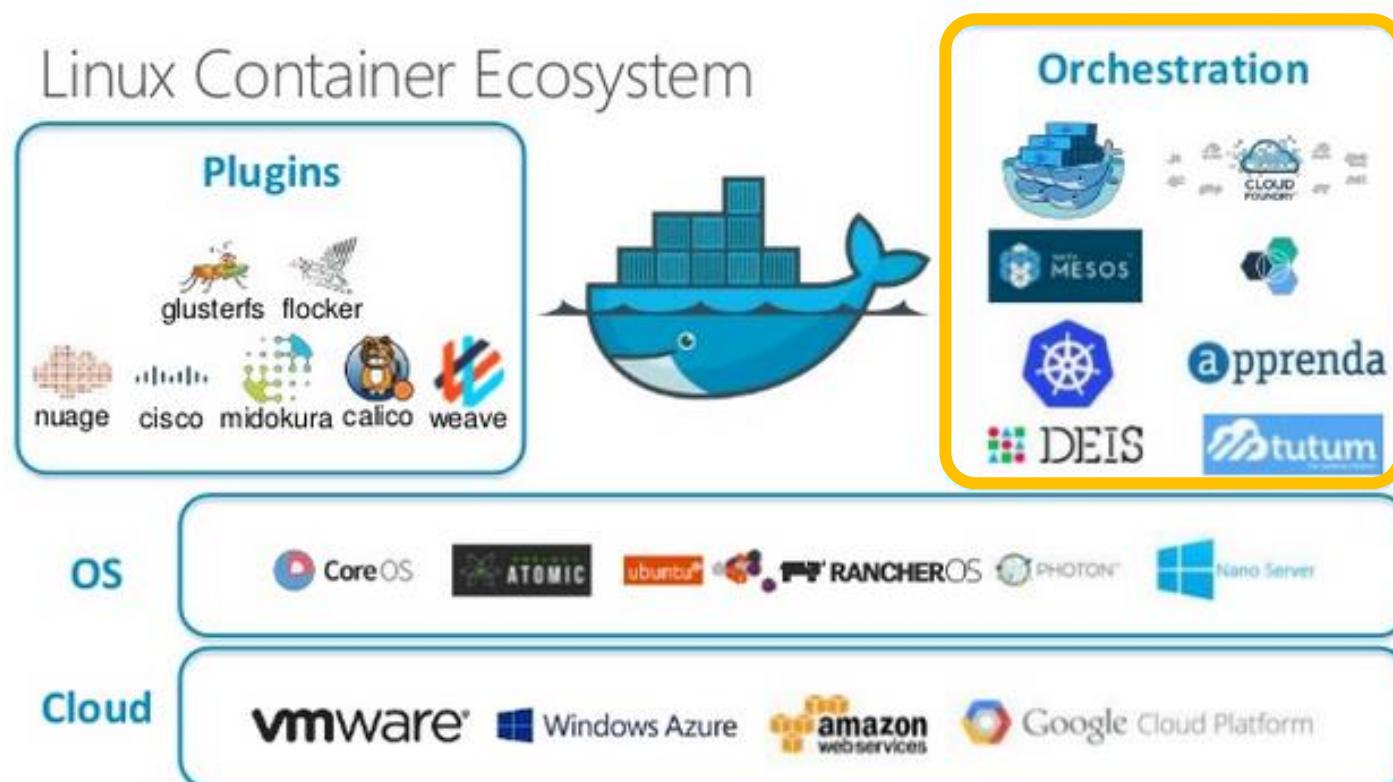
Source : <https://www.docker.com/what-container>

Les dernières évolutions Docker et les containers

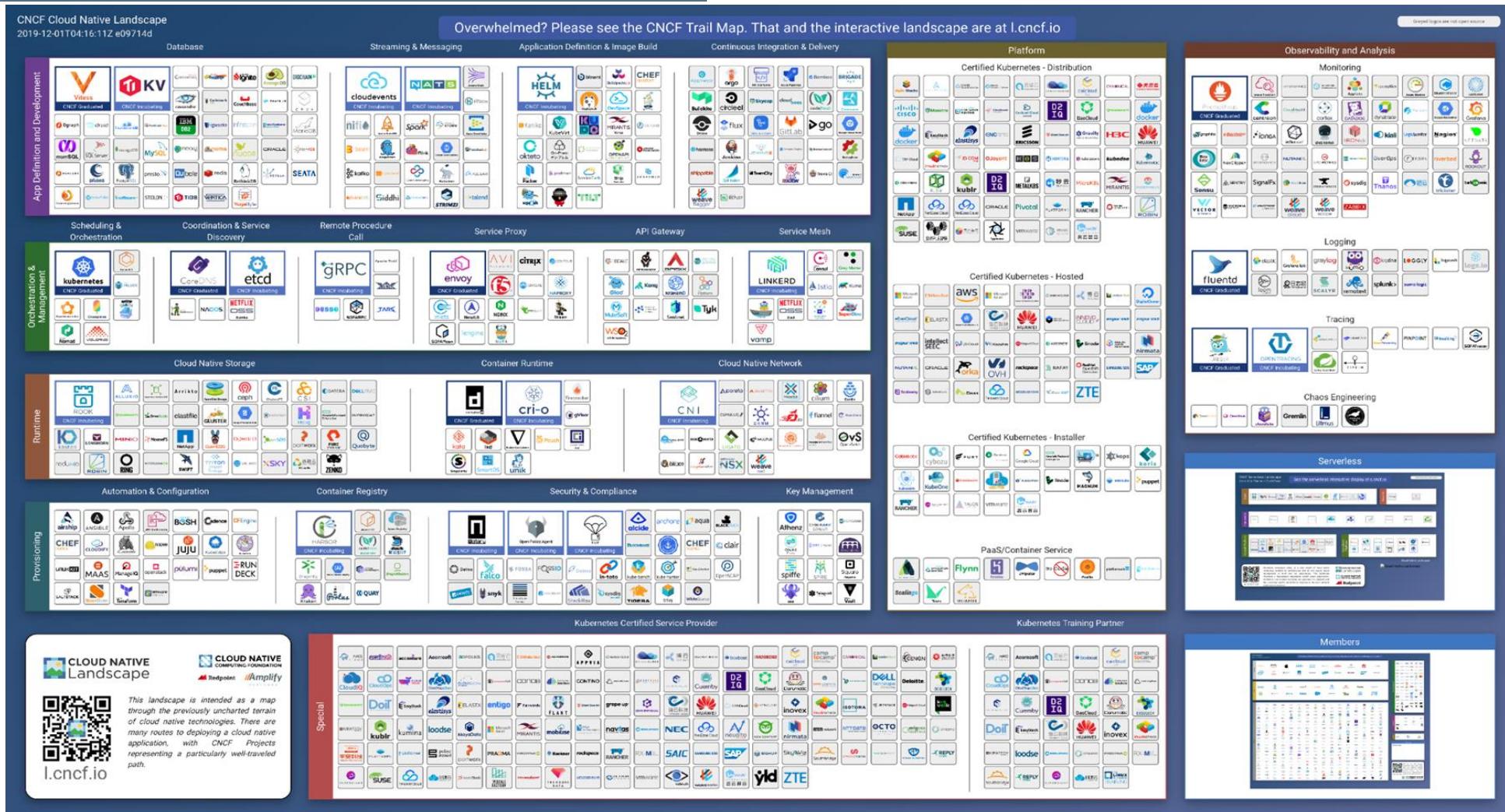
■ Conteneur et machines virtuelles ?



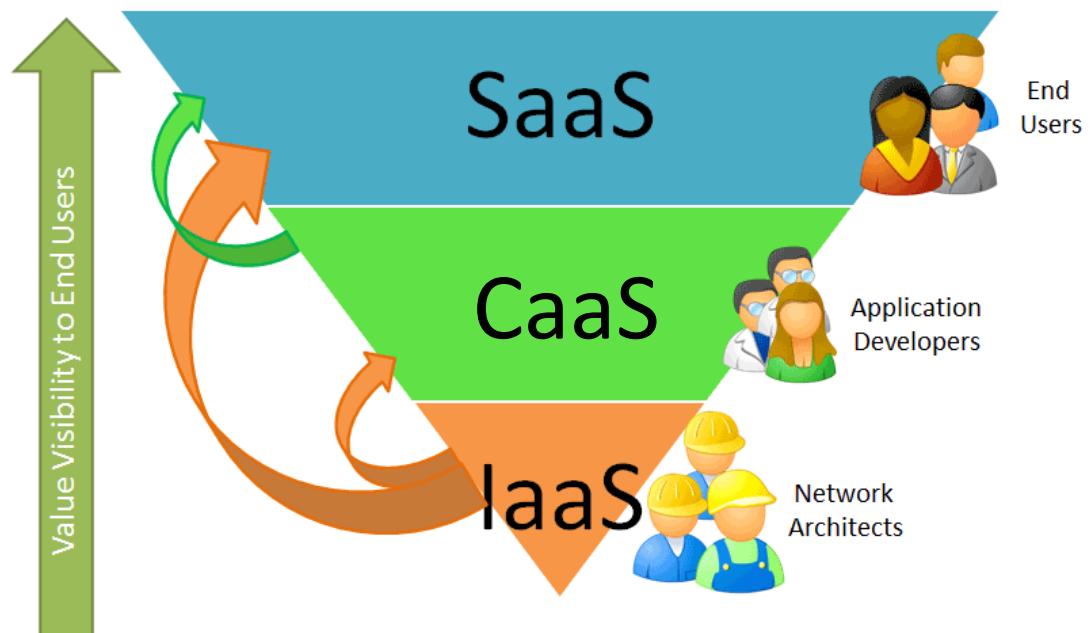
L'étape suivante : Container as a Service



Ecosystème Kubernetes



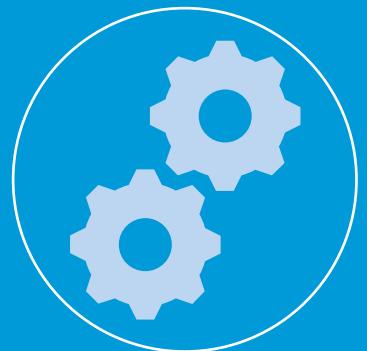
Vers trois nouveaux modèles de services ?



- **Quel rapport avec les containers ?**
 - Le Faas repose sur un format de type container
 - Serverless = Event-Driven Architecture
 - Kubernetes = Long-Running Architecture
- **Principe**
 - Le principe du serverless consiste à déclencher la fonction requise à la demande via un déclencheur logiciel
 - Le principal bénéfice du FaaS consiste à permettre la scalabilité à zéro !
 - Ce mode de fonctionnement est particulièrement intéressant en termes de coût vis à vis des cloud providers et en terme d'optimisation des ressources en cloud privé

- Ne plus avoir à gérer l'infrastructure sous-jacente
 - Economies de temps, de coûts, ...
 - Gestion de la sauvegarde inclue (si activées)
 - Haute disponibilité inclue (si activée)
- Kubernetes
 - AKS, EKS, ...
- AI/ML
 - Datalake, Datawarehouse, SQL, ...
 - ETL/ELT
- Les services s'interconnectent pour former une solution complète et évolutive

Le cloud selon le NST et l'ISO



5 caractéristiques :

- On demand self service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service



3 modèles de services :

- SaaS
- PaaS
- IaaS



4 modèles de déploiement :

- Cloud privé
- Cloud public
- Cloud communautaire
- Cloud hybride

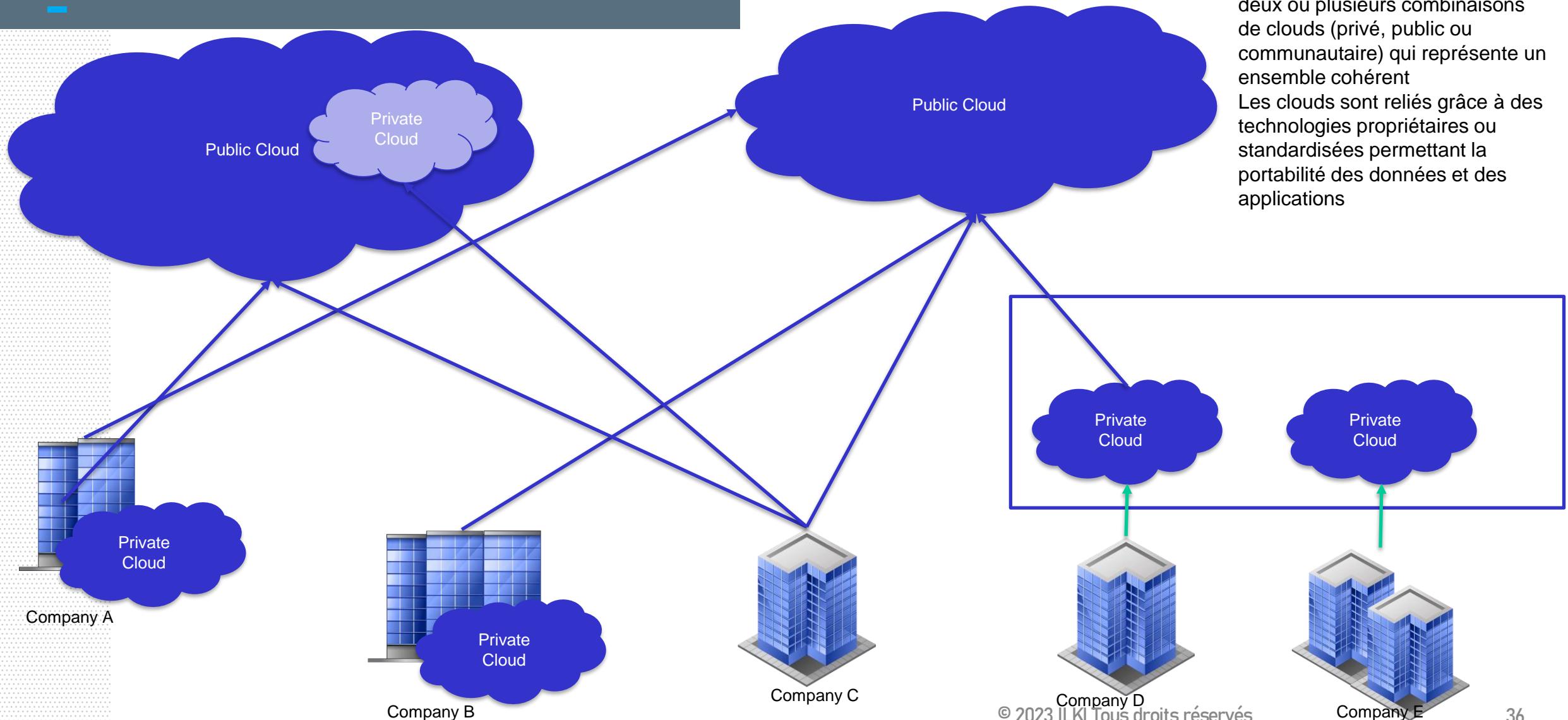


Qu'est-ce que le Cloud Computing

4 modèles de déploiement

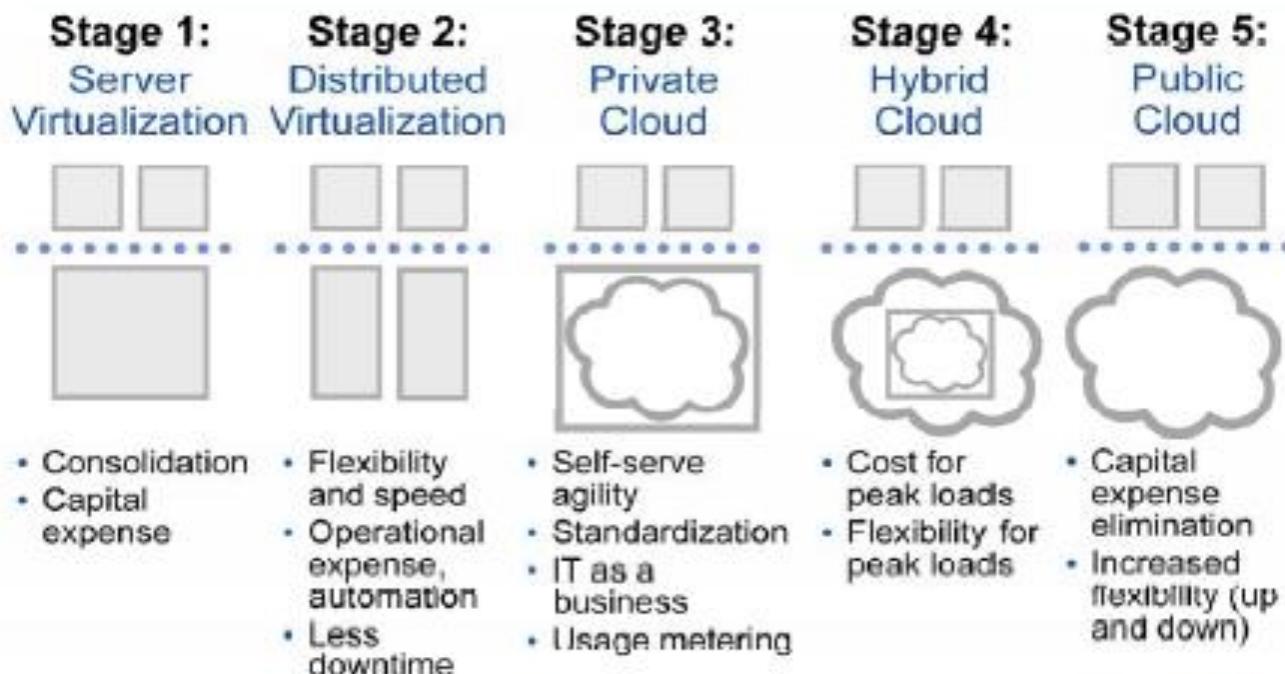
- **Cloud privé**
 - Cloud pour un usage exclusif d'une organisation qui comprend ses propres clients (divisions, filiales...)
 - Le cloud privé peut appartenir et être managé par l'organisation, une société tierce ou une combinaison des deux
 - Le cloud privé peut exister en mode off-premises (hébergé) ou on-premises (sur site)
- **Cloud communautaire**
 - Cloud construit pour une communauté d'utilisateurs de différentes organisations partageant des besoins communs (collectivités, sécurité, conformité...)
 - Le cloud communautaire peut appartenir et être managé par une ou plusieurs des organisations impliquées, une société tierce ou une combinaison
 - Le cloud communautaire peut exister en mode off-premises (hébergé) ou on-premises (sur site)
- **Cloud public**
 - Le cloud est ouvert et peut être utilisé par tout le monde
 - Le cloud public peut appartenir et être managé par une société commerciale, une institution gouvernementale ou universitaire ou une combinaison
 - Le cloud public existe uniquement en mode off-premises (hébergé)
- **Cloud hybride**
 - Un cloud hybride est composé de deux ou plusieurs combinaisons de clouds (privé, public ou communautaire) qui représente un ensemble cohérent
 - Les clouds sont reliés grâce à des technologies propriétaires ou standardisées permettant la portabilité des données et des applications

Modèles de déploiement



Le (vieux) chemin vers le cloud selon le Gartner...

The Road Map Through Private Cloud Computing

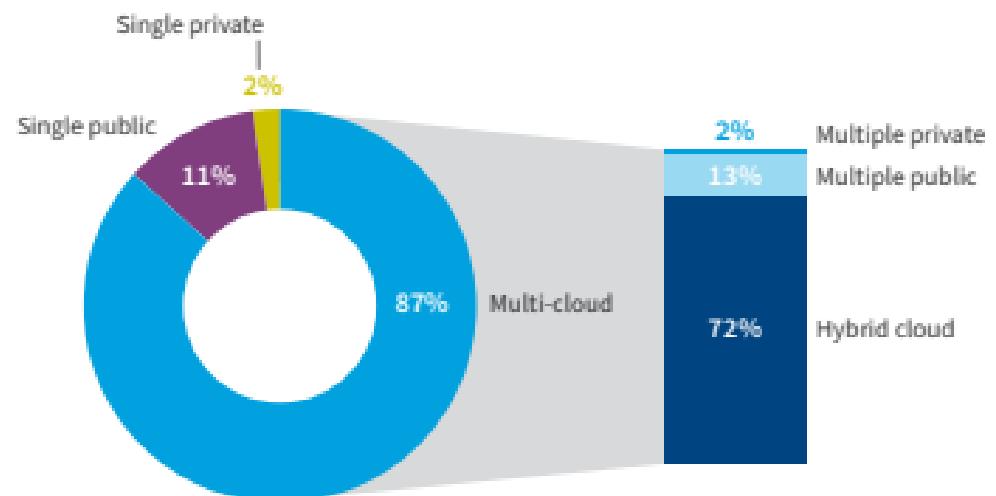


Gartner

Source : Gartner 2013

Quelles stratégies ?

Organizations embrace multi-cloud

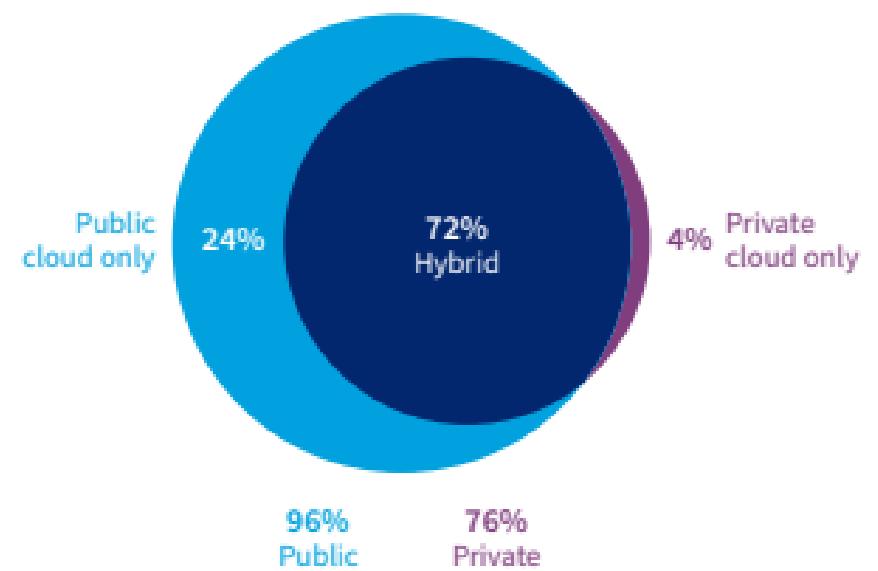


N=750

Source: Flexera 2023 State of the Cloud Report

flexera

Public vs. private cloud usage



N=750

Source: Flexera 2023 State of the Cloud Report

flexera

Cloud Broker

- Société qui gère l'utilisation, les performances et la mise à disposition de services Cloud et qui négocie les relations entre le cloud provider et le cloud consumer
- Exemples : cloud aggregator, cloud integrator, cloud customizer...



Source : NIST

Encore des définitions...

- **Hyperscaler**
 - Nom utilisé pour définir les géants du Cloud Computing : Amazon AWS, Microsoft Azure, Google Cloud, Alibaba
- **Edge computing**
 - Littéralement, traitement (computing) en bordure du réseau
 - Sujet à part entière pour l'IoT ou la 5G (Mobile Edge Computing)
 - Terme également utilisé dans le cloud hybride généralement par abus de langage
- **Fog networking**
 - En référence au Cloud = « tout ce que l'on ne connaît pas et que l'on ne peut pas représenter »
 - Fog = Brouillard
 - ✓ « tout ce que l'on ne connaît pas et que l'on ne peut pas représenter » mais pour le réseau
 - ✓ Sujet à part entière pour l'IoT ou la 5G (Mobile Edge Computing)
 - ✓ Lié également à la virtualisation du réseau, au Software-Defined Network, au SD-WAN...

Multi-cloud

- Selon le NIST, un cloud hybride est composé de deux ou plusieurs combinaisons de clouds (privé, public ou communautaire) qui représente un ensemble cohérent
 - Les clouds sont reliés grâce à des technologies propriétaires ou standardisées permettant la portabilité des données et des applications
- Pour paraphraser la définition du cloud hybride du NIST
 - « Le multi-cloud est composé de deux ou plusieurs clouds publics qui ne représente pas forcément un ensemble cohérent »
 - Une autre acception : une même application peut tourner simultanément sur plusieurs clouds publics
 - ✓ D'où l'arrivée récente du mot omni-cloud pour définir différentes applications sur plusieurs cloud publics
 - Le terme ne s'impose pas
 - Le terme multi-cloud représente les deux concepts

Définition vieillissante

- Cloud privé versus cloud public ?
 - Cloud privé virtuel ?
- Cloud privé versus cloud public versus cloud communautaire ?
 - L'exemple des datacenters dédiés AWS ou Azure pour le gouvernement américain
 - Quid des offres Azure Stack ou AWS Outposts ?
- Comment différencier en SaaS les applications cloud natives des applications web hébergées ?
- PaaS versus IaaS ?
- Quel place pour le PaaS avec les containers et les orchestrateurs de containers ?
 - Le CaaS remplace-t-il le PaaS ?
- Et le multi-cloud dans tout cela ? Et l'omni-cloud ?

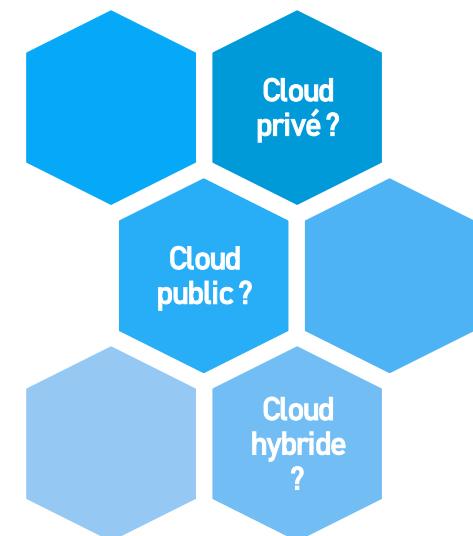
La plus simple des définitions

- **Cloud Computing**
 - L'informatique comme commodités
 - ✓ Eau, gaz, électricité...
 - Commodités = production, gestion de la capacité, transport... le tout facturé à la consommation effective
- **Les maîtres mots**
 - Industrialisation
 - Automatisation et orchestration
 - Gouvernance
 - ✓ Engagements de niveaux de services
 - ✓ Contrat
 - ✓ Coûts
 - ✓ Interopérabilité
 - Sécurité

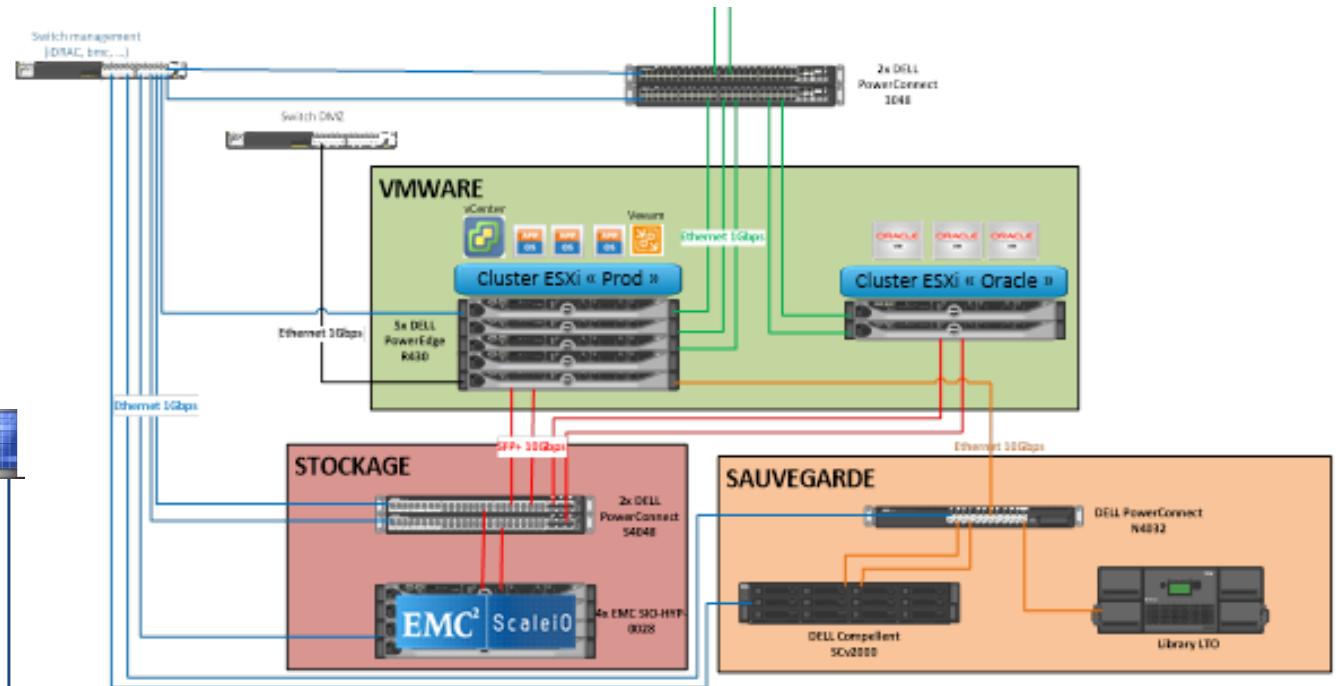
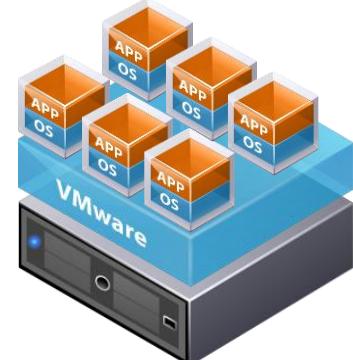
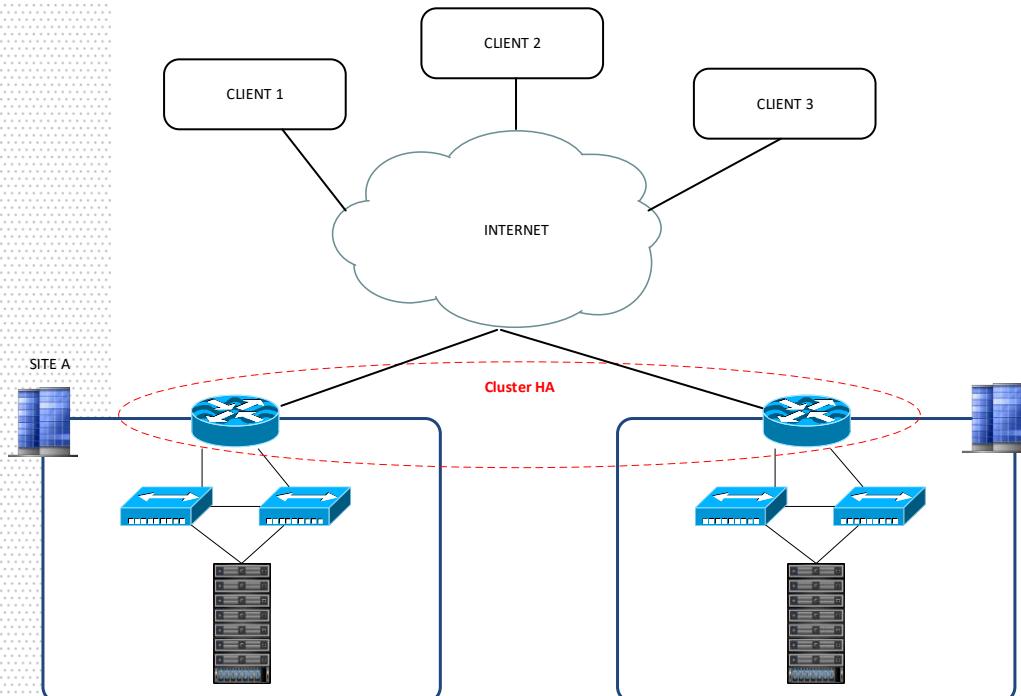


Les bénéfices *a priori* du cloud (tous ?)

- Améliorer le rapport coût- efficacité (*cost-effectiveness*) des services
 - Privilégier les coûts de fonctionnement par rapport aux coûts d'investissements
 - ✓ Diminuer les investissements tout en améliorant la mise à disposition d'un service
 - ✓ Profiter des coûts d'investissement plus bas du provider
 - Profiter de l'élasticité du cloud
 - ✓ Disposer de souplesse dans l'évolution des services à la hausse comme à la baisse dans le principe du XaaS(as a Service)
 - ✓ Pay as you go, pay as you growth...
- Amener de la valeur aux métiers
 - Améliorer l'agilité
 - ✓ Automatiser et orchestrer
 - Améliorer le délai de mise à disposition (*time to market*)
 - Se recentrer sur les tâches à forte valeur ajoutée
- Fiabiliser le datacenter
 - Sécurité de fonctionnement
 - PRA facilité

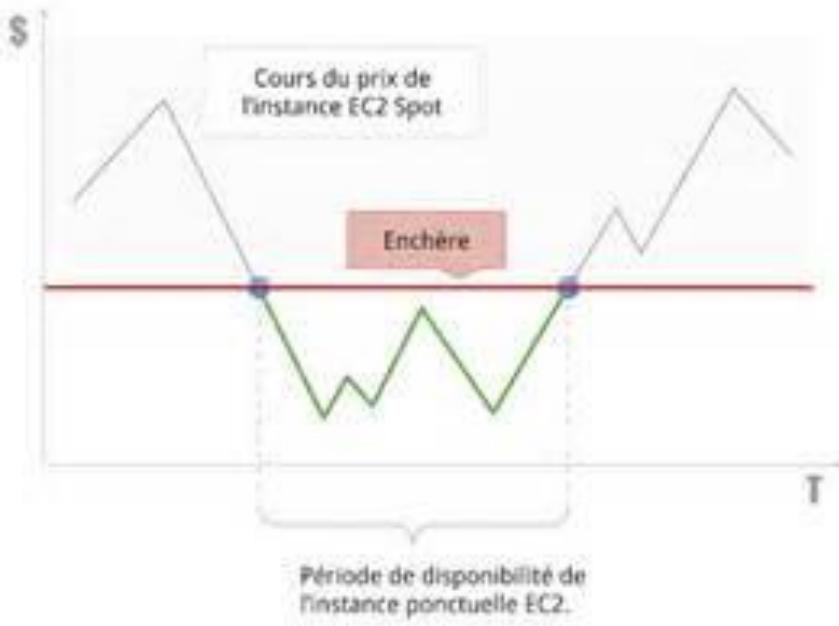


Etude de cas : infrastructure virtuelle ou cloud ?



Serveurs RDS et serveurs Web pour mettre à disposition des applications aux clients

Exemple : calculs financiers

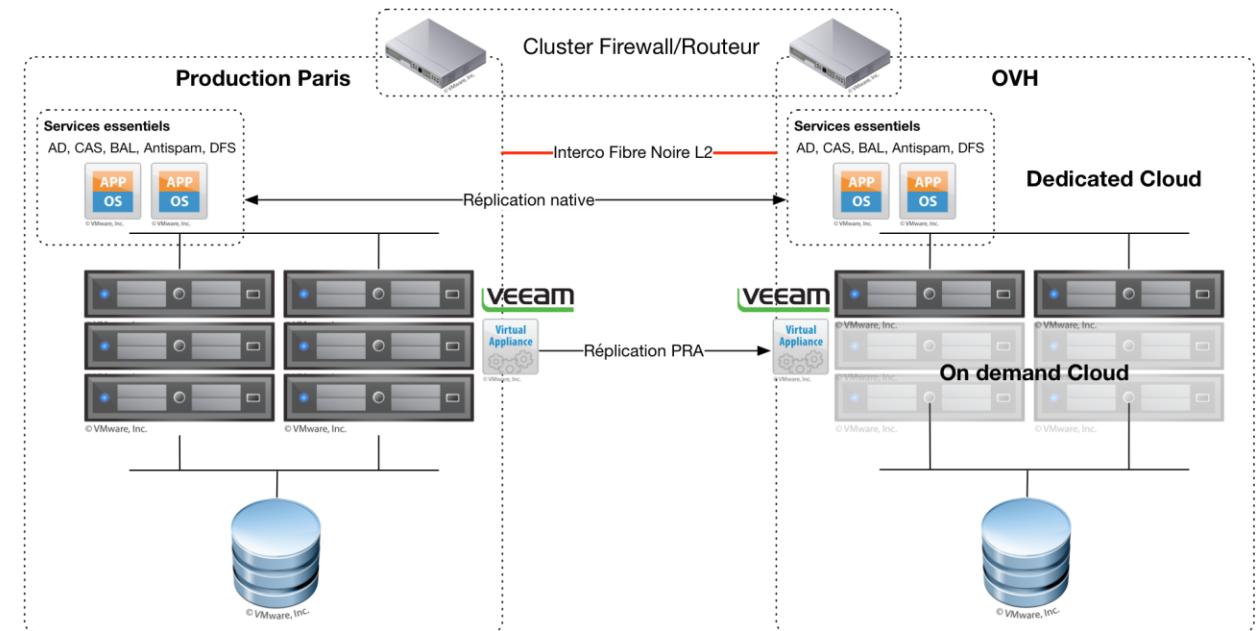


- Application de simulations financières
 - Application indépendante d'autres éléments de l'infrastructure locale
 - Lancée pendant 30 jours sur 30 « énormes » serveurs
 - Utilisés que pour cette période
 - Parallélisable by design
- Projet
 - Généralisation du déploiement quel que soit le nombre de nœuds
 - Puppet
 - Test avec génération de 900 VM sur AWS Irlande
 - 3 heures
 - Anonymisation des données dans un second temps...
 - Industrialisation
 - Serveurs Phénix
 - Spot instances
 - Multi-cloud

Exemple : PSI dans le cloud

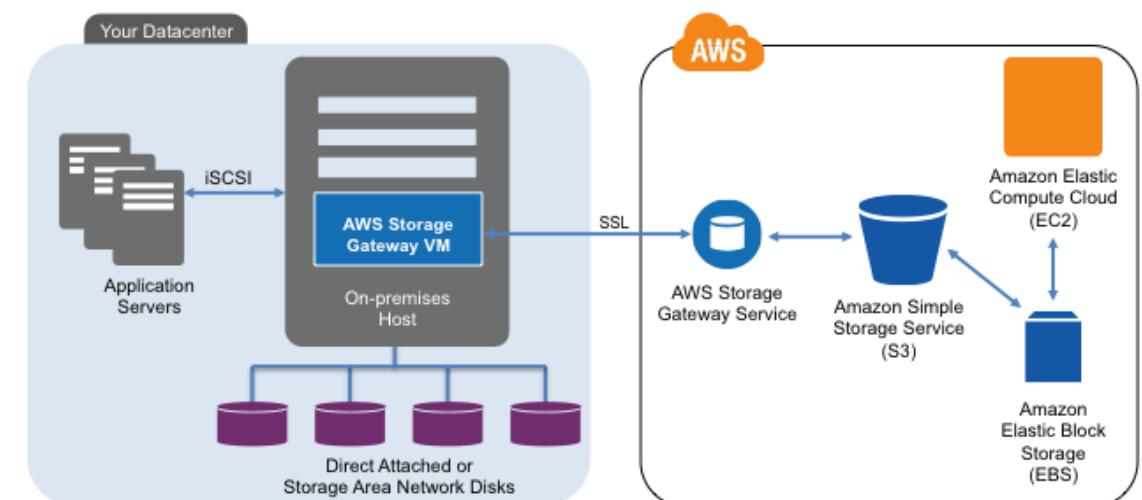
RéPLICATION d'une infrastructure VMWare
dans le Cloud OVH via VEEAM

Interconnexion en fibre noire



Exemple : Hybridation - stockage et archivage dans le cloud

- AWS Storage Gateway
 - Appliance sur vSphere ou Hyper-V
- Trois modes
 - Passerelle de fichiers
 - ✓ Stockage off-premises avec Amazon S3 et cache des données les plus fréquentes sur site
 - Passerelle de volume
 - ✓ Stockage on-premises avec snapshots asynchrones dans Amazon EBS
 - Passerelle de bande
 - ✓ Présentation iSCSI au logiciel de sauvegarde avec stockage off-premises dans Amazon S3 ou Glacier Virtual Tape Shelf
- Azure DataBox Gateway



Les enjeux

Sécurité, fiabilité, SLA et contrats

- Réseau
 - Proverbe : no network, no work
- Quels SLA avec le provider ?
 - SLA réseau + SLA hébergement + SLA infogérance ?
 - Quels contrats ?
 - ✓ Comment sortir du cloud ?
 - ✓ Comment changer de prestataire ?
- Hébergeur
 - 2012 : le bug du 29 février 2012 chez Microsoft Azure
 - 2013 : Amazon entraîne l'arrêt d'Instagram, de Vine...
 - 2014/2015 : Amazon reboota tous ses serveurs sans prévenir pour appliquer un patch Linux
 - 2016 : panne électrique sur la zone AWS australienne pendant 6 heures
 - 2017 :
 - ✓ AWS : panne due à une erreur humaine dans un script...
 - ✓ OVH : SPOF oublié...
 - 2018
 - ✓ Plusieurs sociétés ne peuvent plus s'authentifier sur Microsoft Office 365 toute la journée du 6 mai... juste après que Microsoft ait mis en œuvre des nouvelles fonctionnalités de sécurité...
 - 2019
 - ✓ Problème de 3 heures avec le DNS sur Azure
 - 2020
 - ✓ Impossible pour les européens de créer pendant 3 jours (24-26 mars) des instances sur les datacenters européens
 - 2021
 - ✓ Incendie du datacenter d'OVH
 - ✓ 3 pannes consécutives en décembre chez AWS
 - Et de multiples « plus petites » pannes : <https://downdetector.com/>

- Localisation / transfert
 - Comment garantir que les données sont localisées légalement ?
 - Quel droit au niveau européen ?
- Confidentialité
 - Comment garantir la confidentialité des données ?
 - Quel est l'impact de la GDPR en mai 2018 ?
 - Quel est l'impact du Patriot Act et du Cloud Act ?

- Infrastructures
 - Comment contrôler ses coûts ?
 - ✓ Elasticité
 - Quels coûts pour le réseau ?
- Applications
 - Les redevances logicielles
 - ✓ Tous les éditeurs proposent-ils des modèles de licences adaptés à l'élasticité ?
 - A l'usage
 - Quelle granularité dans le temps : seconde, minute, heure, jour, mois... ?
 - ✓ Si non, comment faire ?
 - Peut-on mélanger deux modèles ?
- Services managés

- **Dépenses d'investissement (CapEx – Capital Expenditure)**
 - Capitalisation d'un bien = actif d'utilisation durable au sein de l'entreprise (immobilisation)
 - Les dépenses d'investissement (CAPEX) concernent l'acquisition d'actifs capables de créer de la valeur pour l'entreprise sur le long terme
 - ✓ Ces dépenses sont amorties et dépréciées tout au long de la durée de vie de l'actif acquis
- **Dépenses d'exploitation (OpEx – Operational Expenditure)**
 - Charges courantes pour exploiter un produit, une entreprise ou un système
 - Les dépenses d'exploitation (OPEX) correspondent aux dépenses courantes :
 - ✓ Pas associées à l'acquisition d'actifs directement créateurs de valeur pour l'entreprise
 - ✓ Charges dans le compte de résultat :
 - Pas d'impacts sur l'endettement
 - Déductibles du résultat fiscal
 - Pas toujours facilement contrôlables

Les enjeux Les applications

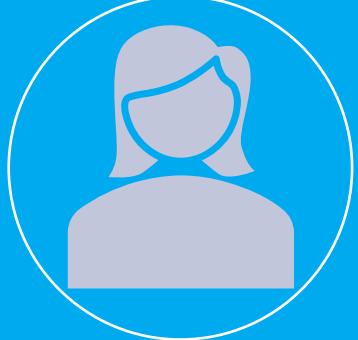
- Traditionnelles :
 - Besoin de fiabilité
 - Matériel redondant :
 - ✓ Agrégation du réseau
 - ✓ Stockage : multipathing
 - ✓ Déplacement de machine, HA ou Fault Tolerance
 - En cas de panne de la zone : réPLICATION + images récupérées sur la zone de secours
- Cloud :
 - Conçu pour la panne : « Design for failure »
 - ✓ Ressources éphémères
 - ✓ Multi-site natif
 - En cas de panne de la zone : recréation de l'image et lancement

→ Besoins d'architectures complètement différentes

Les défis du cloud hybride



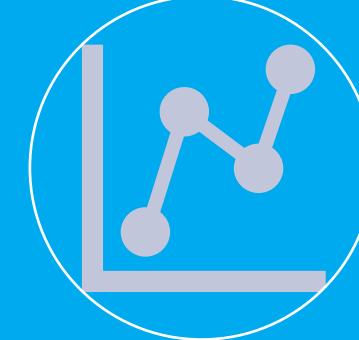
1^{er} défi :
communication
entre les
applications



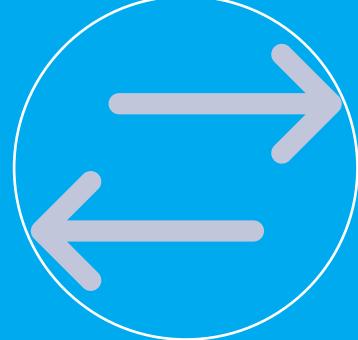
2^{ème} défi :
fédération des
identités



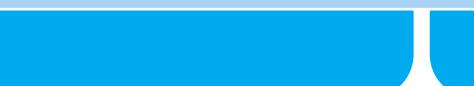
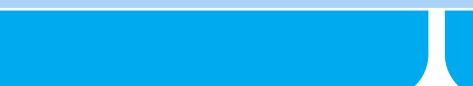
3^{ème} défi :
sécurité entre
les différents
clouds



4^{ème} défi :
performances
du réseau entre
les clouds



5^{ème} défi :
l'interopérabilité
entre les clouds



Principaux organismes de sécurité

- Organisation internationale de normalisation – ISO
- Cloud Security Alliance – CSA
 - <https://cloudsecurityalliance.org/>
 - Cloud Controls Matrix : Principes de sécurité pour guider les fournisseurs de cloud et aider les clients potentiels de cloud à évaluer le risque de sécurité global d'un fournisseur de cloud
 - Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 : Conseils pour gérer et atténuer les risques associés au cloud
- European Union Agency for Network and Information Security – ENISA
 - <https://www.enisa.europa.eu>
 - Cloud Computing Security Risk Assessment : évaluation des risques sur le modèle économique et les technologies du cloud computing.
 - Procure Secure : Guide de surveillance des niveaux de service de sécurité dans les contrats cloud
 - Cloud Security Incident Reporting : Framework de rapport des incidents majeurs de sécurité dans le cloud
- France
 - Agence nationale de la sécurité des systèmes d'information – ANSSI
 - ✓ <https://www.ssi.gouv.fr>
 - ✓ Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage (certnumcloud)
 - ✓ Référentiel général de sécurité (RGS) : Cadre réglementaire spécifique aux systèmes d'information mis en œuvre par les autorités administratives dans leurs relations entre elles et dans leurs relations avec les usagers
 - Commission nationale de l'informatique et des libertés – CNIL
 - ✓ <https://www.cnil.fr>
 - ✓ Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing : Aide aux PME dans la prise de décision lorsqu'elles envisagent d'avoir recours à des prestations de services de Cloud Computing
 - ✓ Les transferts de données à caractère personnel hors Union européenne : Guide destiné à répondre aux interrogations sur les transferts de données personnelles hors de l'Union européenne



Souveraineté

- Deux aspects de la souveraineté numérique
 - Protection des données
 - ✓ Cloud Act
 - ✓ Patriot Act
 - Capacité
 - ✓ Exemple des 48 heures post confinement d'indisponibilité des plaques Azure européennes au profit des sociétés américaines
- Un autre aspect indirect : la conformité légale
 - RGPD et transfert des données en dehors de l'EEE
 - Les obligations de la directive NIS

Le Robert 2023

DÉFINITION	SYNONYMES	COMBINAISONS	EXEMPLES	17 ^e SIÈCLE
DÉFINITION				
Définition de souveraineté nom féminin				
1. Autorité suprême (d'un souverain, d'une nation...). <i>La souveraineté du peuple, fondement de la démocratie.</i>				
2. Caractère d'un État qui n'est soumis à aucun autre État. → indépendance.				

Conformité légale : les « compliance » internationales

- SSAE16 / ISAE3402 (ex. SAS-70 - Statement on Auditing Standards) créée par l'American Institute of Certified Public Accountants (AICPA)
 - Standard qui permet aux utilisateurs de prestations externalisées d'obtenir une assurance quant à la fiabilité du dispositif de contrôle interne de leurs prestations de services
 - ✓ Type I : porte sur la pertinence des contrôles effectués dans une société à une date donnée
 - ✓ Type II : porte sur la pertinence des contrôles effectués dans une société et évalue leur efficacité sur une période de revue d'au moins 6 mois, en particulier pour les entreprises soumises à SOX
- SOC (Service Organisation Control)
 - A ne pas confondre avec le SOC (Security Operation Center)
 - 3 rapports SOC
 - ✓ L'objectif des rapports SOC est d'aider les entreprises à établir la confiance dans leurs processus et contrôles de prestation de services
 - ✓ Le rapport SOC 1 se concentre sur le contrôle interne d'une entreprise lié au reporting financier ; cela permet à l'auditeur d'évaluer les risques associés à l'utilisation de ces services (par exemple : SaaS, data center...)
 - ✓ Le rapport SOC 2 quant à lui se concentre sur des contrôles globaux informatiques basés sur les critères suivants (TSC de l'AICPA) : sécurité, disponibilité, intégrité et confidentialité
 - ✓ Le rapport SOC 3 est similaire au SOC 2 mais il a vocation à être lu et compris par n'importe quelle audience
- PCI-DSS (Payment Card Industry Data Security Standard) Ensemble de 12 règles à respecter afin de protéger les règlements par cartes bancaires, la sécurité des transactions et la confidentialité des données

Understanding SOC reports			
	SOC 1	SOC 2	SOC 3
Purpose	Reports on the controls of the service organization that are relevant to the user organization's financial reporting	Reports on the effectiveness of the controls of the service organization related to compliance or operations, including trust services principles and criteria*	Same purpose as SOC 2
Information required	Details on the system, controls, and tests performed by the service auditor, and results of those tests	Details on the system, controls, and tests performed by the service auditor, and results of those tests	Same information as SOC 2, but with a less detailed description of the controls of the service organization
Audience	User organization's controllers, compliance officers, CFO, CIO, vendor management executives, regulators, other specified parties, and appropriate business partners	User organization's controllers, compliance officers, CFO, CIO, vendor management executives, regulators, other specified parties, and appropriate business partners	Unrestricted and can be viewed by anyone who would like confidence in the controls of the service organization

Spécifiques Américaines

HIPAA (Health Insurance Portability and Accountability Act) porte sur la protection des données médicales du patient

FISMA (Federal Information Security Management Act) propose les règles de sécurité à respecter par les organisations fédérales américaines

Conformité légale

Les données de santé

- L'exception des données de santé à caractère personnel
 - Hébergeurs agréés ou certifiés HDS sur le territoire français
 - ✓ Procédure d'agrément abandonné au profit d'une procédure de certification
 - Le décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel
 - ✓ 2 périmètres de certifications :
 - Hébergeur d'infrastructure physique
 - Hébergeur infogéreur

PRESTATION D'HÉBERGEURS D'INFRASTRUCTURE PHYSIQUE

1. Mise à disposition et maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé
2. Mise à disposition et maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé

PRESTATION D'HÉBERGEUR INFOGÉREUR

3. Mise à disposition et maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information
4. Mise à disposition et maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé
5. Administration et exploitation du système d'information contenant les données de santé
6. Sauvegardes externalisées des données de santé

Source : <https://esante.gouv.fr/labels-certifications/hds/certification-des-hebergeurs-de-donnees-de-sante>

Sociétés internationales : Binding Corporate Rules

- **Code de conduite**
 - définissant la politique d'une entreprise en matière de transferts de données.
 - Permettent d'offrir une protection adéquate aux données transférées depuis l'Union européenne vers des pays tiers à l'Union européenne au sein d'une même entreprise ou d'un même groupe
- **Les entreprises concernées sont les multinationales**
 - exportant des données depuis leurs filiales situées au sein de l'Union européenne vers des pays tiers n'assurant pas un niveau de protection équivalent à celui de l'Union européenne.
- **Alternative aux clauses contractuelles types**
 - puisqu'elles permettent d'assurer un niveau de protection suffisant aux données transférées hors EU au regard des données personnelles et des droits fondamentaux.

Conformité ne signifie pas confidentialité

- « Patriot Act » (Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act)
 - Loi du Congrès des Etats Unis signée par G.Bush en 2001 qui prévoit (entre autres) à son Titre V le « Foreign Intelligence Surveillance ACT » (FISA) donnant accès au FBI aux données personnelles des fournisseurs (d'accès à) Internet, tout en interdisant aux groupes privés d'informer les personnes cibles objet de la transmission de données.
 - Prolongée à plusieurs reprises, la loi a été ré-examinée en juin 2015 sans modification majeure → arrêt de la Cour de Justice Européenne sur le Safe Harbor
- Juin 2018 : Cloud Act (Clarifying Lawful Overseas Use of Data)
 - Clarification du Stored Communications Act
 - Encadre le fait que la justice américaine, dans le cadre d'une procédure judiciaire (enquête pénale), puisse obtenir les données à l'étranger
 - ✓ « within such provider's possession, custody or control »
 - Avis divergents entre les GAFAM et les associations de défense du Net et de la vie privée
 - Contradiction avec les articles 45 à 49 du RGPD
 - ✓ « Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un Etat membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre. »
 - Autorise le gouvernement US à signer des accords internationaux (executive agreements) avec un pays pour permettre la communication de données sans avoir à passer par les procédures classiques
 - ✓ MLAT – accord mutuel d'assistance juridique

Conformité légale : la directive NS

- Depuis mai 2018
 - Directive «NIS » du 6 juillet 2016
 - ✓ <https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/>
 - Mesures destinées à assurer un niveau élevé commun (UE) de sécurité des réseaux et des systèmes d'information
 - ✓ «Opérateur de Services Essentiels»
 - Entités publiques/privées des secteurs de l'énergie, des transports, des banques, santé, eau et infrastructure numérique
 - ✓ « Fournisseur de service numérique »
 - Hébergeur web, Moteurs de recherche en ligne, Service d'informatique en nuage
- NIS 2 adoptée en 2022 et applicable depuis le 17 janvier 2023
 - Définit des mécanismes de coopération entre les Etats
 - Evolution des OSE : administrations publiques, spatial, les fournisseurs de services numériques, réseaux d'eaux usées et de gestion de déchets, services postaux, alimentation, fabricants de produits chimiques et pharmaceutiques

Sécurité et confidentialité : points majeurs

- Pas de régime réglementaire spécifique pour le Cloud
 - Conformité aux règles et lois locales
 - ✓ Le cas de la Chine pour les entreprises françaises
- L'engagement sur la localisation n'est pas négociable
- Si les datacenters ne sont pas dans l'EEE ou dans un pays ayant le même niveau d'exigences
 - Model Clause CE et/ou Binding Corporate Rules
 - ✓ Seule solution pour les Etats-Unis en attendant le nouvel accord...
 - Prise en compte des recommandations de « mesures supplémentaires » du CEPD (Comité européen de la Protection des données = G29)
- Dans l'idéal, chiffrer les données personnelles

La famille ISO/IEC 27000

- Organisation internationale de normalisation
- ISO 27001 : c'est la norme centrale de la famille ISO 2700x, c'est elle qui définit les conditions pour mettre en œuvre et documenter un SMSI.
- ISO 27002 : 114 « best practices » pour la mise en place d'un SMSI*.
- ISO 27003 : processus de la mise en œuvre du SMSI.
- ISO 27004 : mesure du niveau d'efficacité du SMSI et du niveau de sécurité de l'entreprise.
- ISO 27005 : cadre méthodologique pour l'analyse des risques.
- ISO 27006 : exigences pour les audits de certification ISO 27001.
- ISO 27007 : Guide pour l'audit ISO 27001.
- ISO 27008 : Guide pour l'audit ISO 27002.



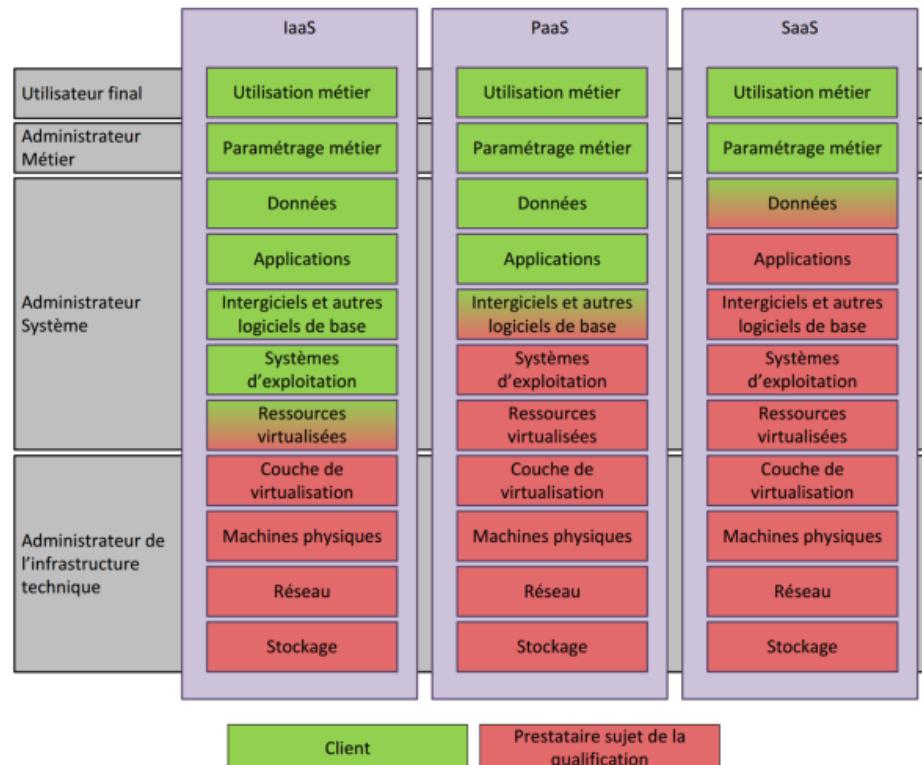
De plus ISO 27301:2011 propose un cadre pour la continuité d'activité

Le contrat Cloud

- **Le contrat cloud**
 - Il existe aujourd'hui une multitude de contrats
 - ✓ Avec une tarification complexe et des engagements multiples
 - Peu de latitudes de négociation à espérer
 - ✓ Industrialisation
 - Idéalement avec une étroite collaboration Informatique / Achats
- **Rappel**
 - Cloud = consommation liée à l'utilisation effective d'un service
 - ✓ Utility / Commodité : eau, électricité...
 - SaaS
 - ✓ Modèle généralement simple
 - ✓ Par unité de temps
 - Généralement le mois
 - ✓ Par utilisateur
 - ✓ Par consommation effective du service
 - Ex : Service de stockage = Go / Mois
 - IaaS
 - ✓ Beaucoup plus compliqué...

Le contrat Cloud

Partage de responsabilité



Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Provider
Identity & access management	Cloud Customer	Cloud Customer	Cloud Provider	Cloud Provider
Application level controls	Cloud Customer	Cloud Customer	Cloud Provider	Cloud Provider
Network controls	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider
Host infrastructure	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider

Legend:

- Cloud Customer** (Blue box)
- Cloud Provider** (Grey box)

Le contrat Cloud

Provider versus Infogéreur

- Un contrat avec le Cloud Provider
 - C'est un marché d'offre (mass customisation)
 - Le périmètre est plus fluctuant
 - Même pour les grands clients le contrat est standard et sera mis en place « online »
 - Paiement à la consommation
 - Le fournisseur peut changer les termes et conditions, c'est au client de tracer les changements
- Un contrat de MSP ou d'infogérance
 - C'est un marché de demande (sur mesure)
 - Se négocie de gré à gré -> le contrat est sur mesure
 - Sur un périmètre plus précis et les règles de son évolution sont décrites
 - Règles de paiement précises
 - Clause d'auditabilité possible
- Question : Comment définir les coûts d'un MCO d'un MSP sur un périmètre fluctuant d'un Cloud Provider ?

Le contrat Cloud

Les clauses clefs

Clauses clefs

- Périmètre des services attendus/fournis
- Définition et niveaux des engagements de services
- Continuité de services
- Sécurité, confidentialité, propriété intellectuelle, localisation
- Réversibilité
- Gouvernance du contrat
- Auditabilité périodique, exceptionnelle, en continu
- Transition
- Conditions tarifaires, pénalités
- Coûts annexes
- Juridiction et cadre légal/règlementaire applicables



Le contrat Cloud

SLA

■ Service Level Agreement

- La qualité des SLA est UNPOINT CRITIQUE du contrat
 - ✓ Les SLA référents sont techniques et opérationnels
 - ✓ Actuellement, les engagements des Cloud Providers sont faibles
- Des pénalités doivent être prévues avec possibilité de résiliation en cas de non tenue chronique et répétée des dysfonctionnements
- La mesure des SLA doit être réalisée de façon non contestable par les parties, et potentiellement par un tiers agréé
- Plus facile avec un Managed Service Provider que avec un Cloud Provider

Le contrat Cloud SLA des providers publics

- Le SLA référent des Cloud Providers publics est la disponibilité du service
- Les engagements des Cloud Providers sont faibles...
 - Les pénalités en cas de sinistre sont faibles
 - Elles ne sont pas négociables



Exemple de SLA sur disponibilité Microsoft

- **SLA : Monthly Uptime Percentage**

$$\frac{\text{Minutes Calendaires} - \text{Minutes D'indisponibilité}}{\text{Minutes Calendaires}} \times 100$$

- Le «crédit de service» est le pourcentage des frais de service mensuels qui vous sont crédités après l'approbation de la demande de règlement de Microsoft.
 - Le crédit doit être demandé par le client
 - Suivi sur console d'administration

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Availability

6. Service Availability.

- The Services, Third-Party Apps and Services, or material or products offered through the Services may be unavailable from time to time, may be offered for a limited time, or may vary depending on your region or device. If you change the location associated with your Microsoft account, you may need to re-acquire the material or applications that were available to you and paid for in your previous region.
- We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.

Exemple de SLAs sur disponibilité : AWS

- Une évolution significative depuis 2018
 - Historiquement limité uniquement à quelques services
 - Tous les SLA : <https://aws.amazon.com/legal/service-level-agreements/>
- Exemple pour EC2

General Service Commitment

AWS will use commercially reasonable efforts to make the Included Services each available for each AWS region with a Monthly Uptime Percentage of at least 99.99%, in each case during any monthly billing cycle (the "Service Commitment"). In the event any of the Included Services do not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.99% but equal to or greater than 99.0%	10%
Less than 99.0% but equal to or greater than 95.0%	30%
Less than 95.0%	100%

- "Unavailable" and "Unavailability" mean:
 - o For Single EC2 Instances, when your Single EC2 Instance has no external connectivity.
 - o For Amazon EC2 (other than Single EC2 Instances), Amazon ECS, or Amazon Fargate, when all of your running instances or running tasks, as applicable, deployed in two or more AZs in the same AWS region (or, if there is only one AZ in the AWS region, that AZ and an AZ in another AWS region) concurrently have no external connectivity.

Exemple de SLA sur disponibilité OVH

Pour pouvoir bénéficier des pénalités en cas de non-respect des SLA, il est indispensable :

d'avoir au moins deux serveurs hosts dans le Private Cloud,
l'option HA activée,
et ouvert un ticket incident.

RESEAU	SERVEUR	STOCKAGE
<ul style="list-style-type: none">OVH garantit que le réseau interne de son datacentre Private Cloud est accessible à 100% du temps, excepté en cas de maintenance planifiée pour laquelle les clients seront avertis.OVH garantit que la connectivité à internet de son Private Cloud est accessible à 99.95% du temps, excepté en cas de maintenance planifiée pour laquelle les clients seront avertis.Pénalité de 5% du montant total de la prochaine facture, par tranche de 10 minutes d'indisponibilité, dans la limite de 100% du montant total de la facture.	<ul style="list-style-type: none">OVH garantit une disponibilité de 99.99% de ses serveurs hosts Private Cloud. Les applications hébergées sur ces serveurs bénéficieront de cette disponibilité grâce à la configuration que les clients apporteront à leur infrastructure. OVH fournit un host de remplacement en moins de 15 minutes en cas de défaillance d'un serveur host.Pénalités : remboursement du serveur host sur la prochaine facture.	<ul style="list-style-type: none">OVH garantit une disponibilité de 100% sur ses stockages. Le système de stockage employé permet d'avoir un stockage maître et un stockage esclave, qui prend le relai en cas de défaillance du premier.Remboursement de 5% du montant du stockage par tranche de 10 minutes d'indisponibilité

- La qualité des SLA est un point critique du contrat
- Des pénalités doivent être prévues avec possibilité de résiliation en cas de non tenue chronique et répétée des dysfonctionnements
- La mesure des SLA doit être réalisée de façon non contestable par les parties, et potentiellement par un tiers agréé

Le contrat Cloud

La réversibilité

- **Point critique de tout contrat d'infogérance**
 - Valable aussi pour les MSP
 - Valable aussi pour les CSP
- **Deux dimensions**

Contractuelle

- Classique chez le MSP
- A priori plus facile chez le CSP car paiement l'usage

Technique

- Cloud lock-in
 - Verrouillage dans un cloud = coût prohibitif pour passer d'un cloud à l'autre
- Comment migrer d'un CSP vers un autre CSP ?

Sommaire

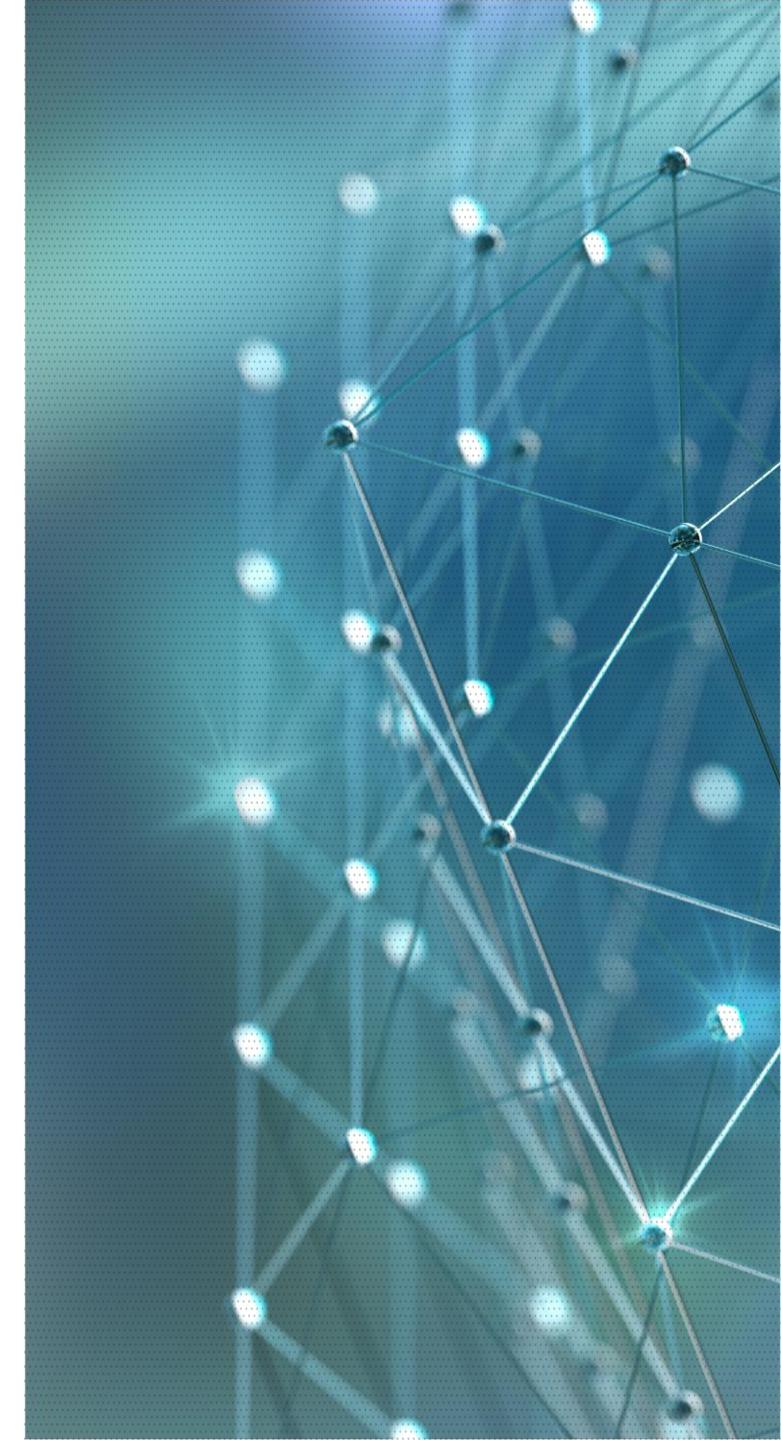
- **Introduction**
- **Cloud Computing**
 - Fondamentaux, bénéfices et enjeux
 - Comprendre les aspects juridiques et la sécurité
- **L'impact du Cloud**
 - L'évolution de la structure des entreprises
 - L'évolution des métiers
- **Un tour d'horizon des solutions des acteurs du marché du Cloud**
 - Software as a Service
 - Platform as a Service
 - Infrastructure as a Service
- **Comment construire son cloud privé**
- **Conclusion**



L'impact du Cloud

L'évolution de la structure des entreprises

L'évolution des métiers



Sommaire

- **Introduction**
- **Cloud Computing**
 - Fondamentaux, bénéfices et enjeux
 - Comprendre les aspects juridiques et la sécurité
- **L'impact du Cloud**
 - L'évolution de la structure des entreprises
 - L'évolution des métiers
- **Un tour d'horizon des solutions des acteurs du marché du Cloud**
 - Software as a Service
 - Platform as a Service
 - Infrastructure as a Service
- **Comment construire son cloud privé**
- **Conclusion**

Evolution de la DSI

- La DSI devient un fournisseur de services Cloud
 - Mais aussi un cloud broker pour les services Cloud
- Objectifs
 - Mieux comprendre les besoins des métiers
 - Mieux leur faire comprendre les besoins de la DSI (interopérabilité, sécurité...)
 - Avoir un véritable « Product Manager »
 - Doit avoir un modèle de vente
 - ✓ Metering / chargeback
 - Définir les SLA
- Des nouvelles tâches
 - La synchronisation des besoins et demandes internes avec les services fournis (Provisionning d'infrastructure) tout en étant caution technique des demandes
 - La relation et la supervision du fournisseur et des prestations fournies en termes de conformité aux SLA, performances, disponibilité
 - La remontée des incidents et leur suivi, des opérations de change,..
 - Le suivi des opérations de maintenance, transition,
 - La gouvernance générale du contrat, dont la tenue des réunions de contrôle et pilotage
 - Le suivi contractuel de la prestation avec les équipes des achats

Une nouvelle organisation

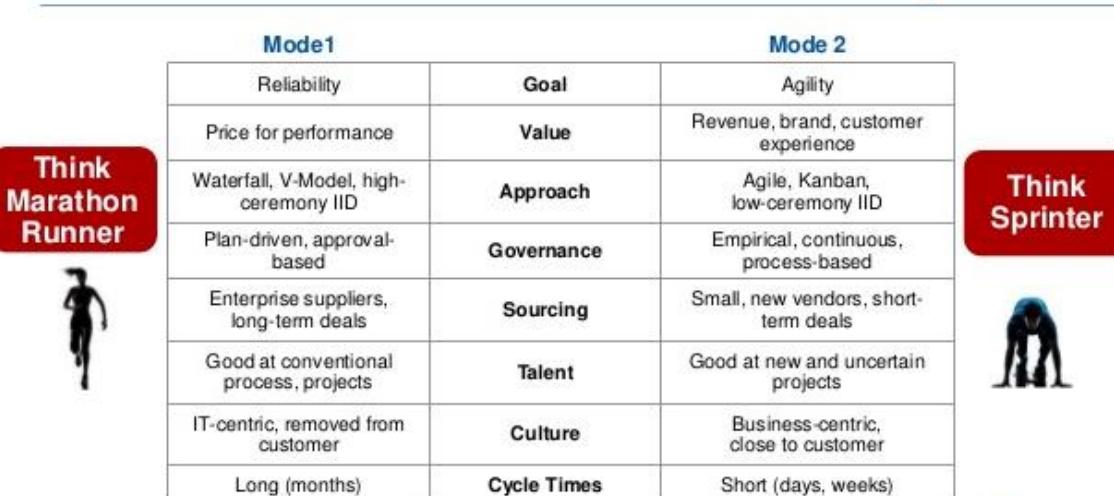
- **Pick one**
 - Cloud Management Center
 - Cloud Command Center
 - Cloud Operations Center
 - Cloud Knowledge Center
 - Cloud Enablement Team
- **Et bien sûr...**
 - Cloud Center of Excellence
- **Idées principales**
 - Equipe transverse chargée
 - ✓ de gérer la stratégie, la gouvernance et les meilleures pratiques en matière de cloud
 - ✓ de jouer le rôle de chef de file du cloud pour l'ensemble de l'organisation



La DSi B-modale

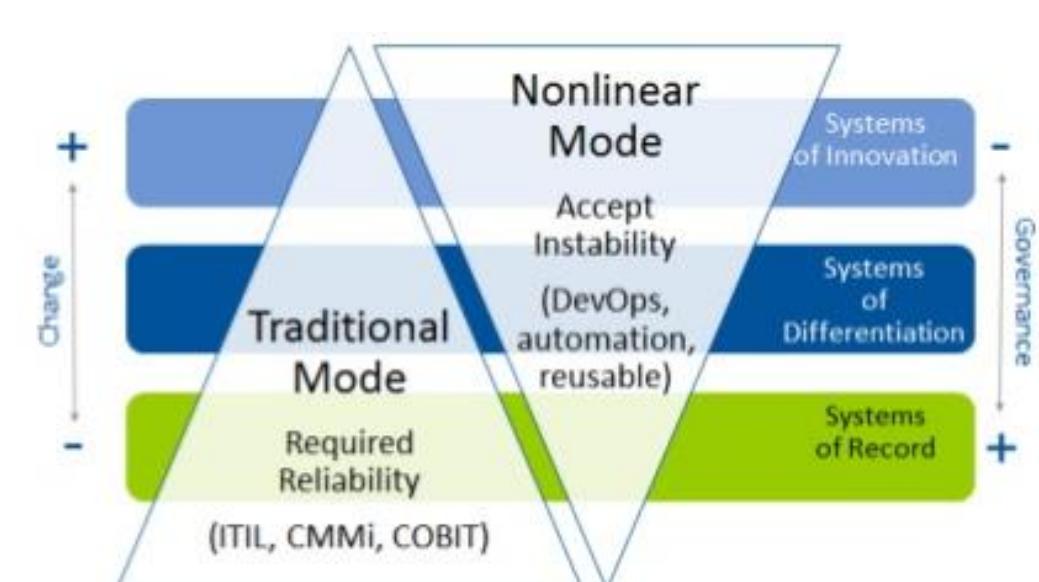
- Mode 1 = IT traditionnelle héritée - dirigée par la DSi
- Mode 2 = IT agile nouvelle - dirigée par les métiers

Bimodal IT = Marathon Runners + Sprinters



@doudpunkt
© 2014 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner





L'impact du Cloud

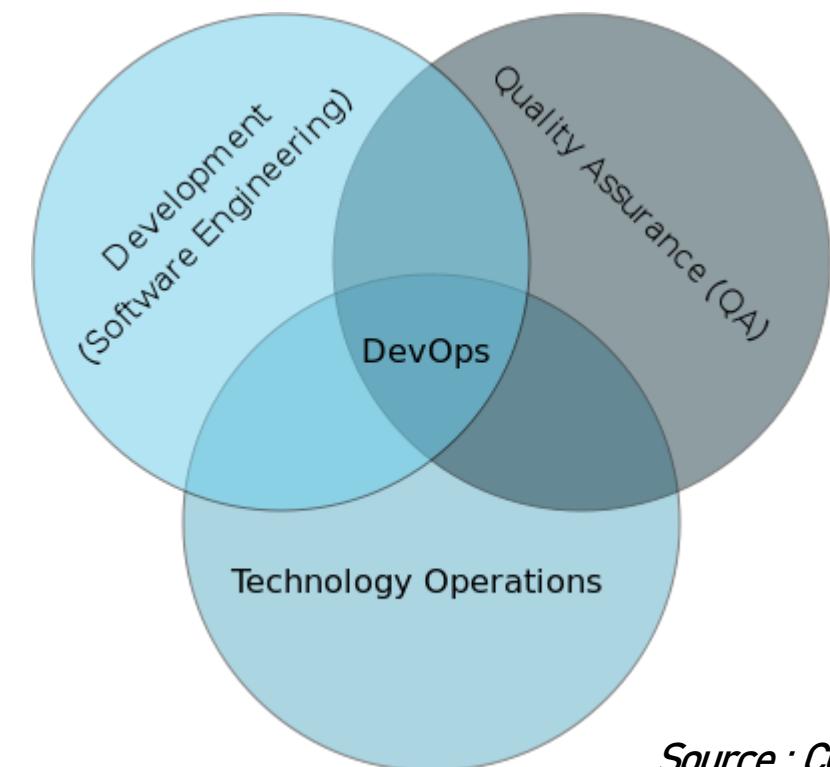
L'évolution de la structure des entreprises

L'évolution des métiers



Nouvelles applications

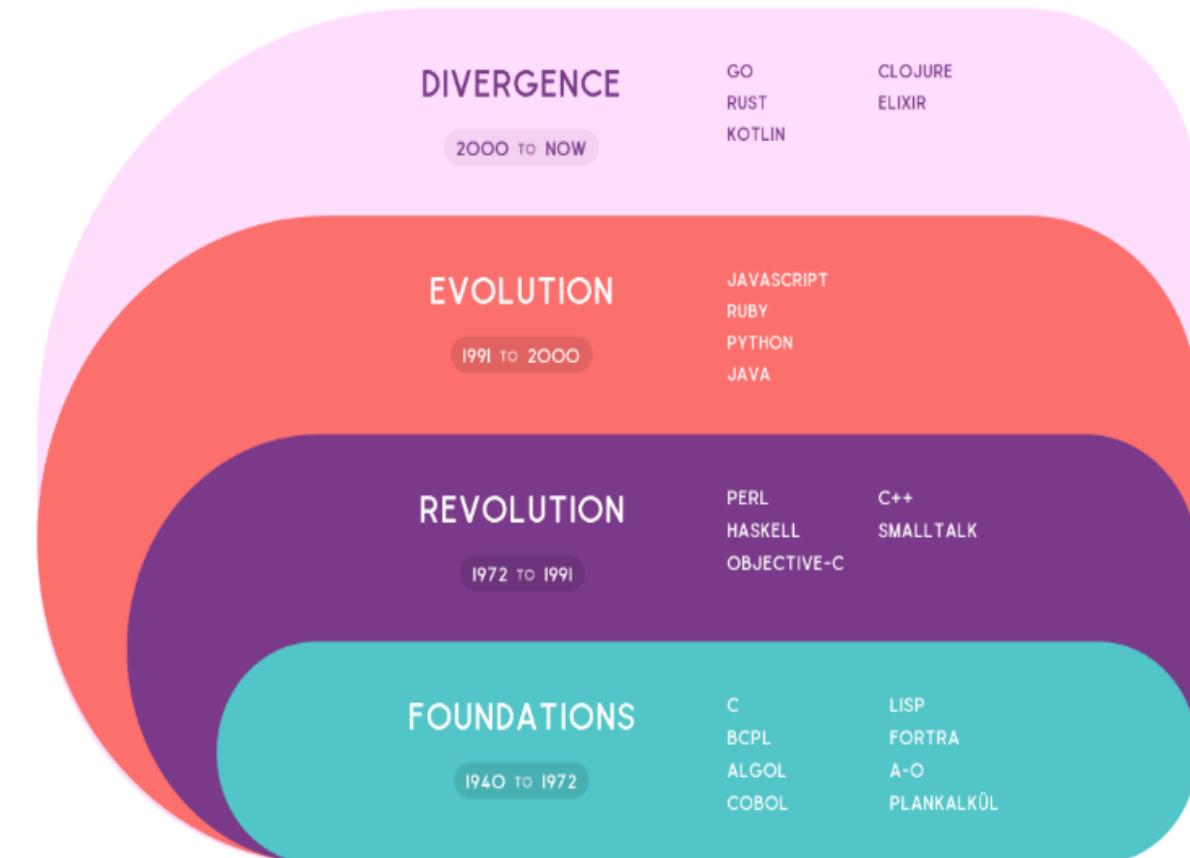
- Self-service et automatisation du provisioning et du cycle de vie
 - Repenser complètement les méthodes actuelles
- Nouvelles applications
 - Penser DevOps
 - Penser Cloud native



Source : CCL - Rajiv Pant

Nouvelles applications

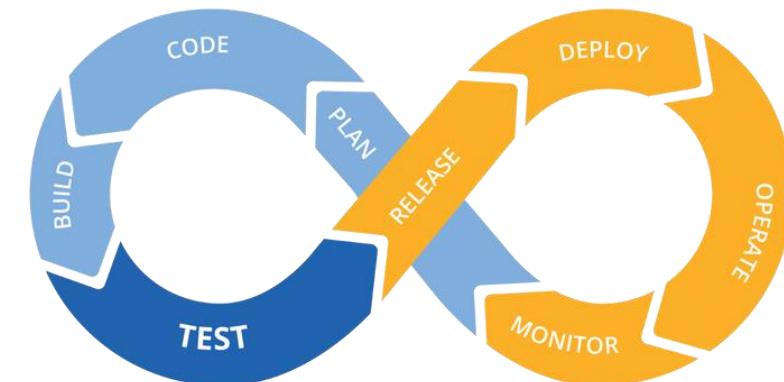
- Quels langages ? Quels Frameworks ?
 - Historiquement, les applications On-Premises se basent sur les langages C/C++, Java...voire Cobol pour les mainframes.
 - Les applications modernes sont orientées vers les langages Web; Java Spring Boot, Javascript, .Net, Go, Node.js, Python, Ruby..
- Vers le Web Assembly ?
 - Développer dans n'importe quel langage, compiler en WASM
 - *One language to rule them all*



Source - *welcomeinthejungle* -

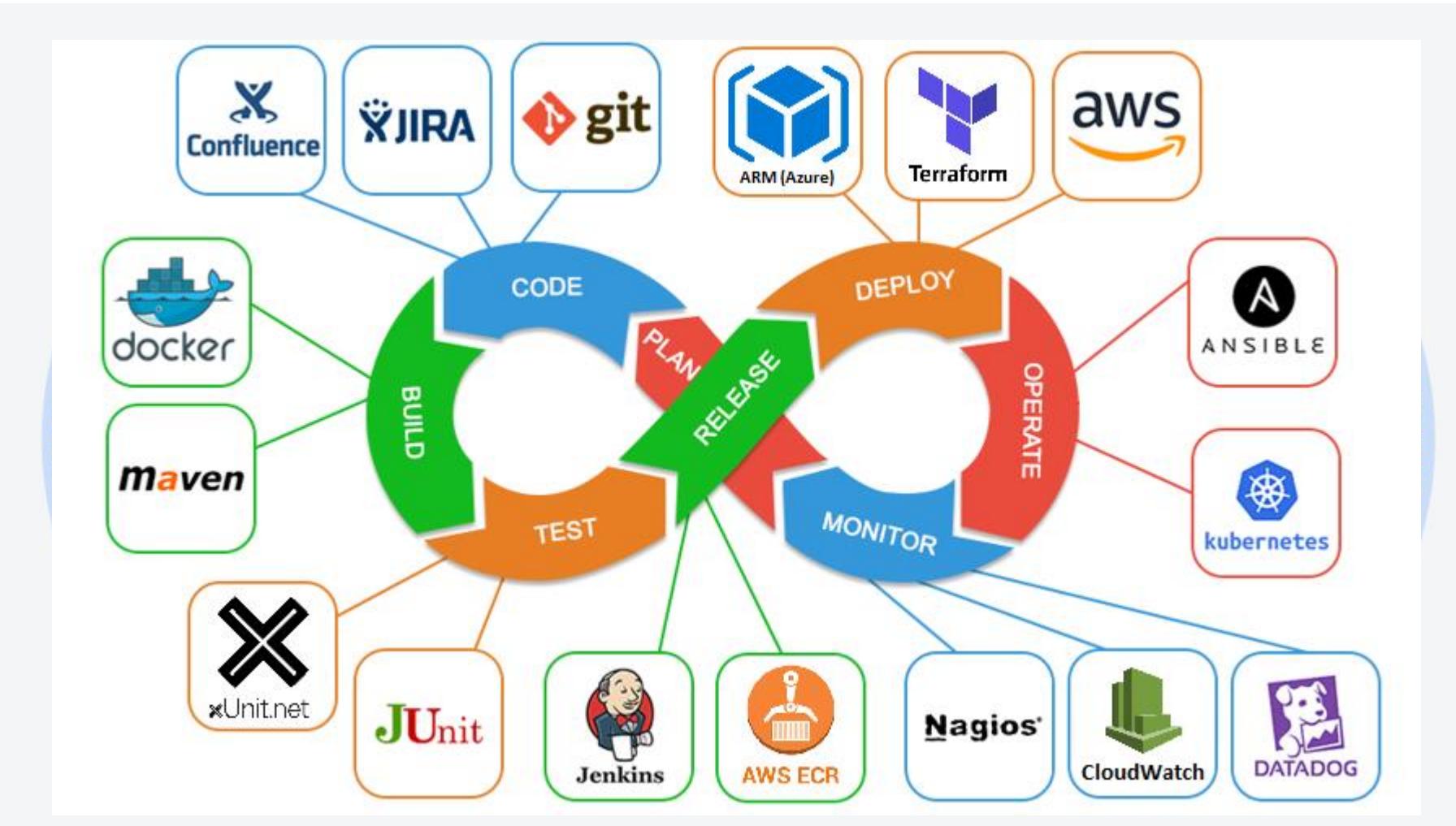
Méthodes de développement agiles

- Adéquation entre développement agile et micro-services
 - Équipe dédiée à une fonctionnalité spécifique
 - Releasing très fréquent - faible adhérence entre équipes
 - Forte automatisation via les technologies de CICD
 - Méthode Scrum, Extreme Programming...
- Adapté à la méthodologie TDD *Test Driven Development*
 - Les tests sont écrits avant le code
- Organisation DevOps
 - Les équipes agiles peuvent travailler de concert avec les Ops sur un modèle DevOps



- Qu'est-ce que la culture Devops ?
 - La notion de Devops doit se voir sous l'angle humain...
 - ✓ ... et pas seulement entre développeurs et administrateurs !
 - Différents principes permettant de faciliter le travail et la relation entre les différentes équipes impliquées dans la gestion d'un Système d'information
 - Adapter et innover dans l'organisation des équipes, la culture d'entreprise, les technologies pour rendre le travail plus efficace
- Les 4 piliers de la culture DevOps
 - Collaboration : favoriser la interactions et la communication entre équipes
 - Affinité : favoriser le partage et la définition d'objectifs communs entre différentes équipes
 - Outils : outiller les équipes afin de mieux piloter, structurer, surveiller, accélérer les changements du SI
 - Scalabilité : organiser et mettre en œuvre des pratiques pour accompagner le développement du SI

Outils



Accompagner les métiers de l'IT

- Cloud = automatisation de nombreuses tâches d'administration et d'exploitation
 - Que vont devenir les administrateurs systèmes ?
- Cloud = les développeurs doivent prendre en compte les dimensions Ops
 - Que vont devenir les développeurs traditionnels ?
- Nouveaux métiers
 - Architecte de service cloud
 - Spécialiste orchestration
 - Gestionnaire de service cloud
 - Administrateur de services cloud
- Evolution d'autres métiers
 - Capacity planning
 - Monitoring
 - ...



Implication des RH

Sommaire

- **Introduction**
- **Cloud Computing**
 - Fondamentaux, bénéfices et enjeux
 - Comprendre les aspects juridiques et la sécurité
- **L'impact du Cloud**
 - L'évolution de la structure des entreprises
 - L'évolution des métiers
- **Un tour d'horizon des solutions des acteurs du marché du Cloud**
 - Software as a Service
 - Platform as a Service
 - Infrastructure as a Service
- **Comment construire son cloud privé**
- **Conclusion**

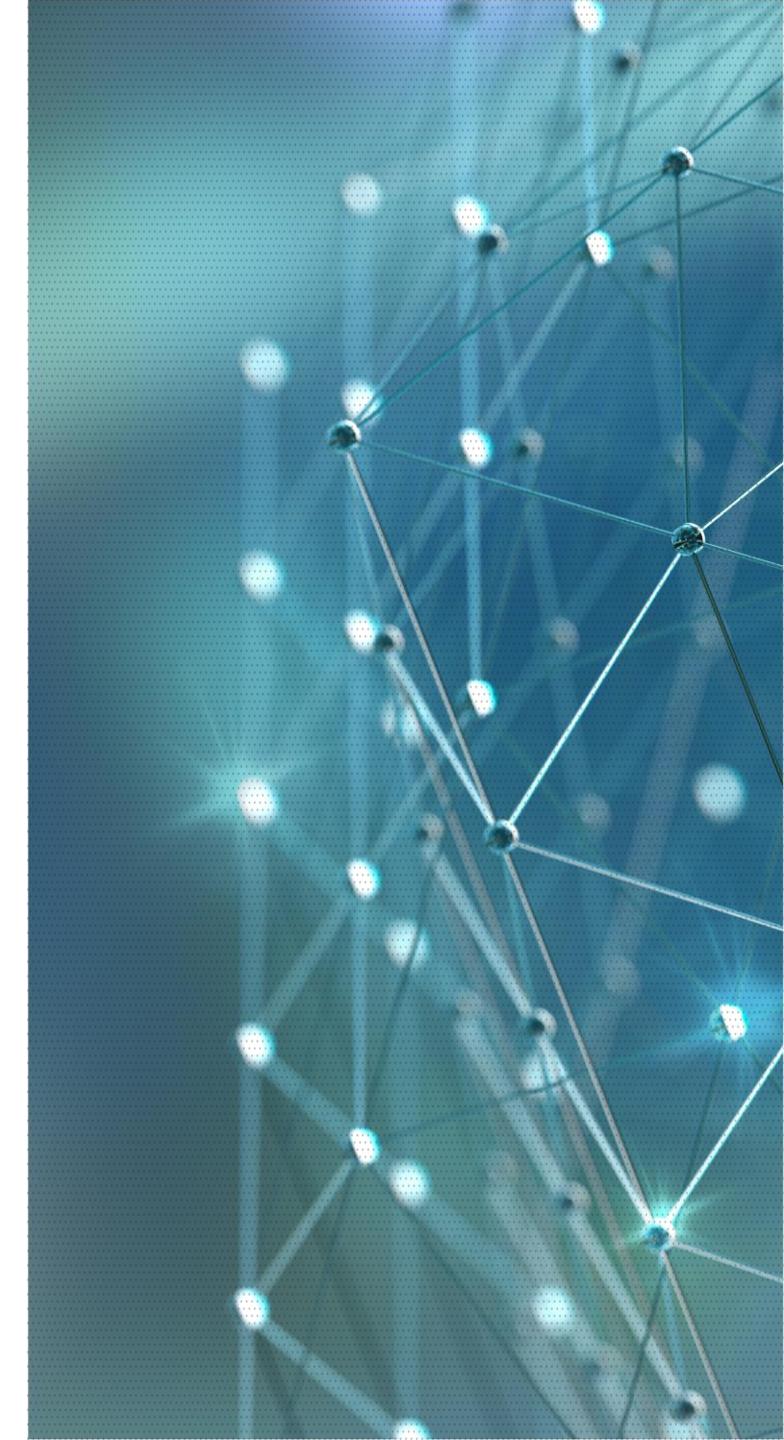


Un tour d'horizon des solutions des acteurs du marché du Cloud

Software as a Service

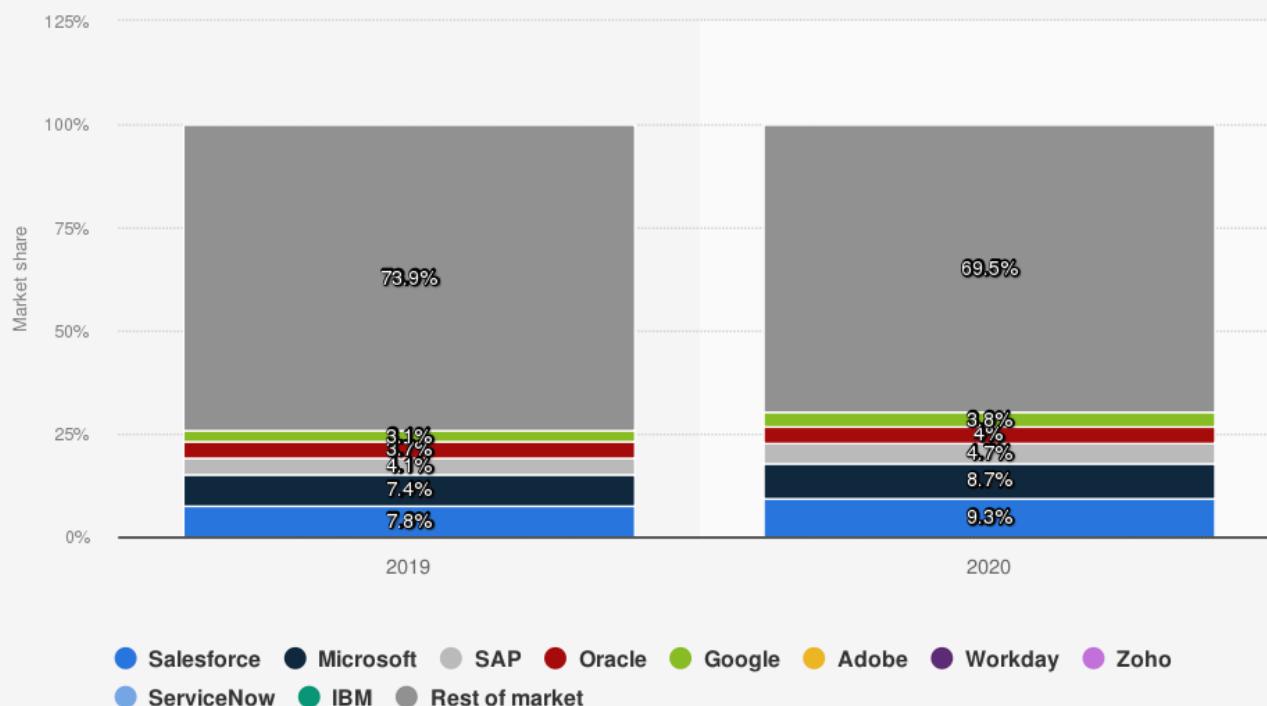
Infrastructure as a Service

Platform as a Service



Les acteurs du SaaS

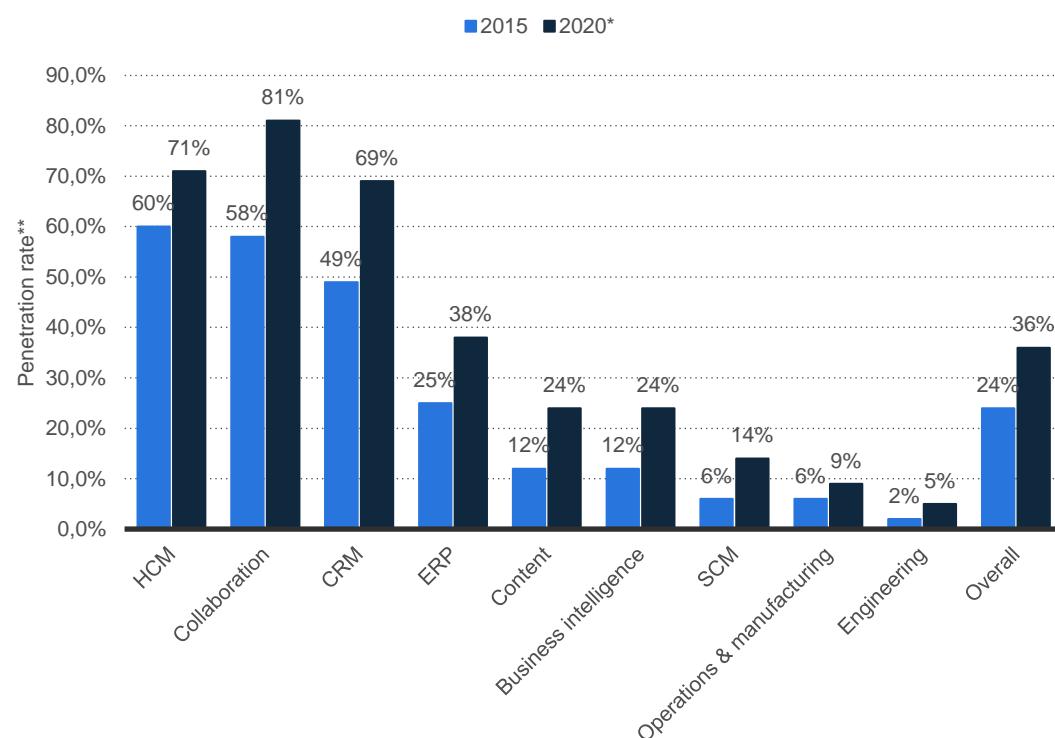
Public cloud software as a service (SaaS) market share worldwide in 2019 and 2020, by vendor



Source
IDC
© Statista 2022

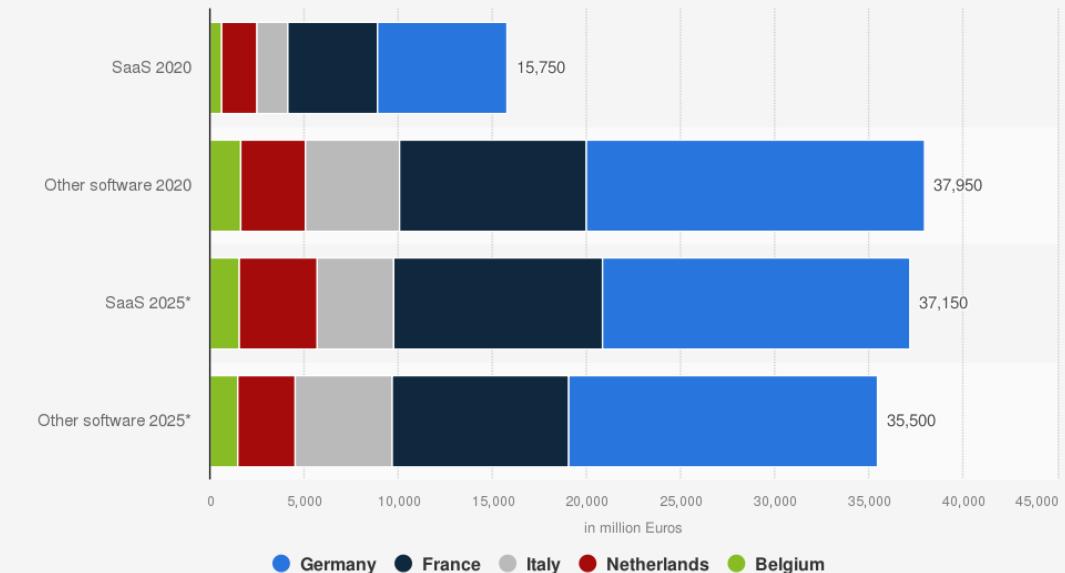
Additional Information:
Worldwide; IDC; 2019 and 2020

Ratio SaaS/Classique 2015 et 2020



Source: Various sources ((Altman Vilandrie & Co.) [ID 782240](#)

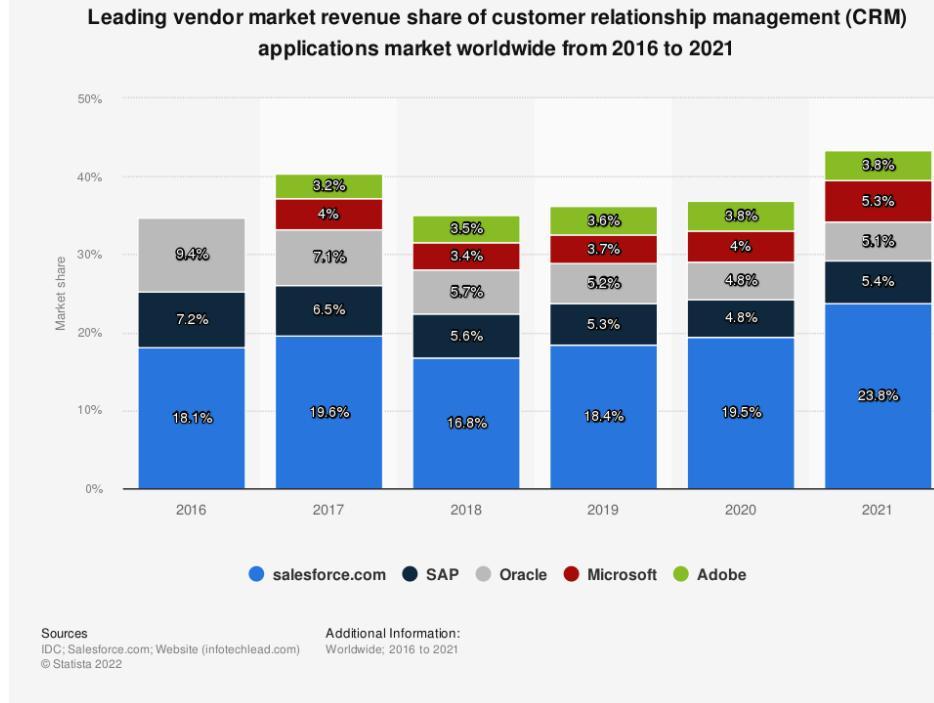
Market revenue of software as a service (SaaS) versus other software in Europe 2020 and 2025, by country (in million euros)



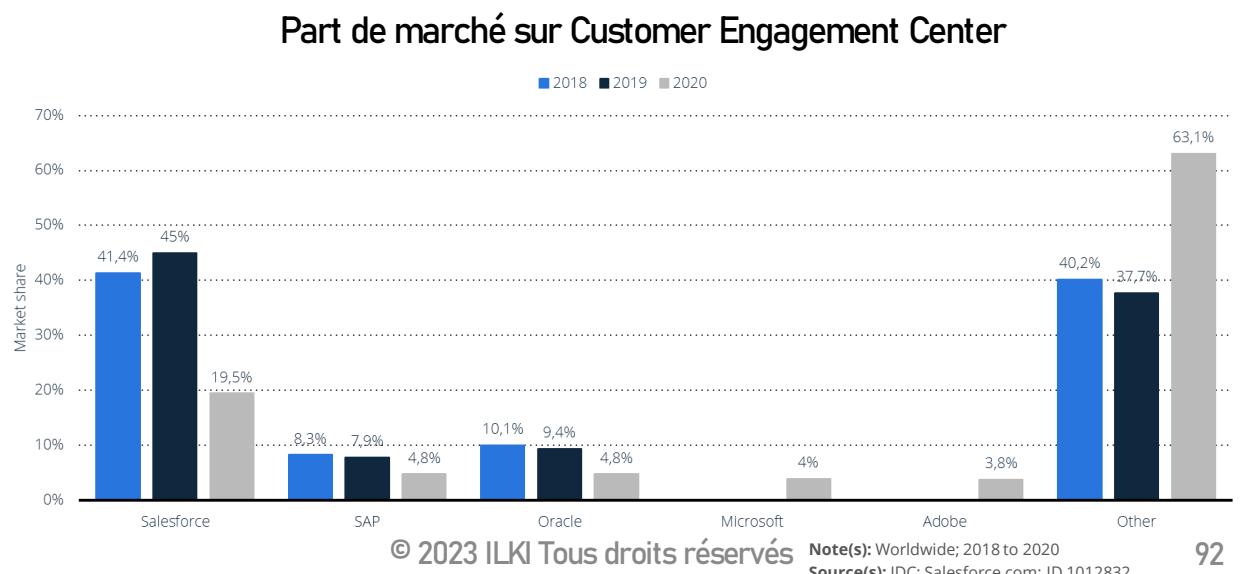
Sources
Reply; Statista estimates; teknowlogy Group
© Statista 2022

Additional Information:
Belgium; France; Germany; Italy; Netherlands; Reply; Statista estimates; teknowlogy Group; 2020

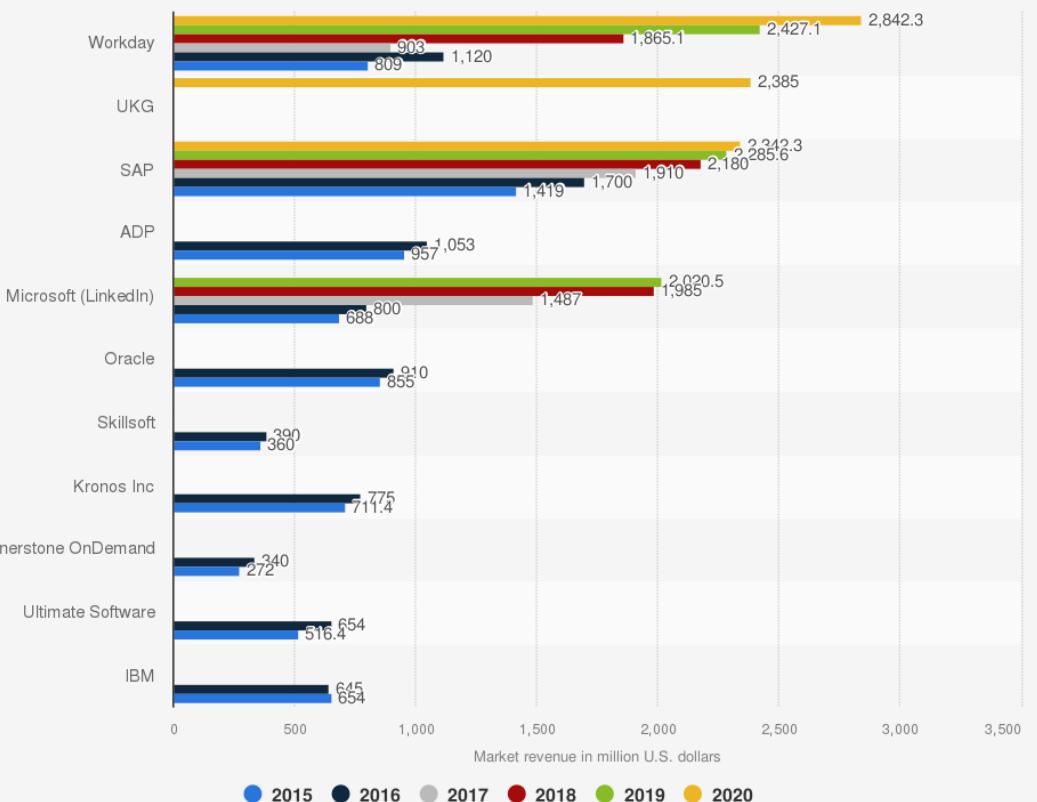
CRM: vente et service client



Part de marché sur Sales Force Automation



Human capital management (HCM) applications market revenue worldwide from 2015 to 2020, by leading vendor (in million U.S. dollars)*



UKG = Ultimate Kronos Group

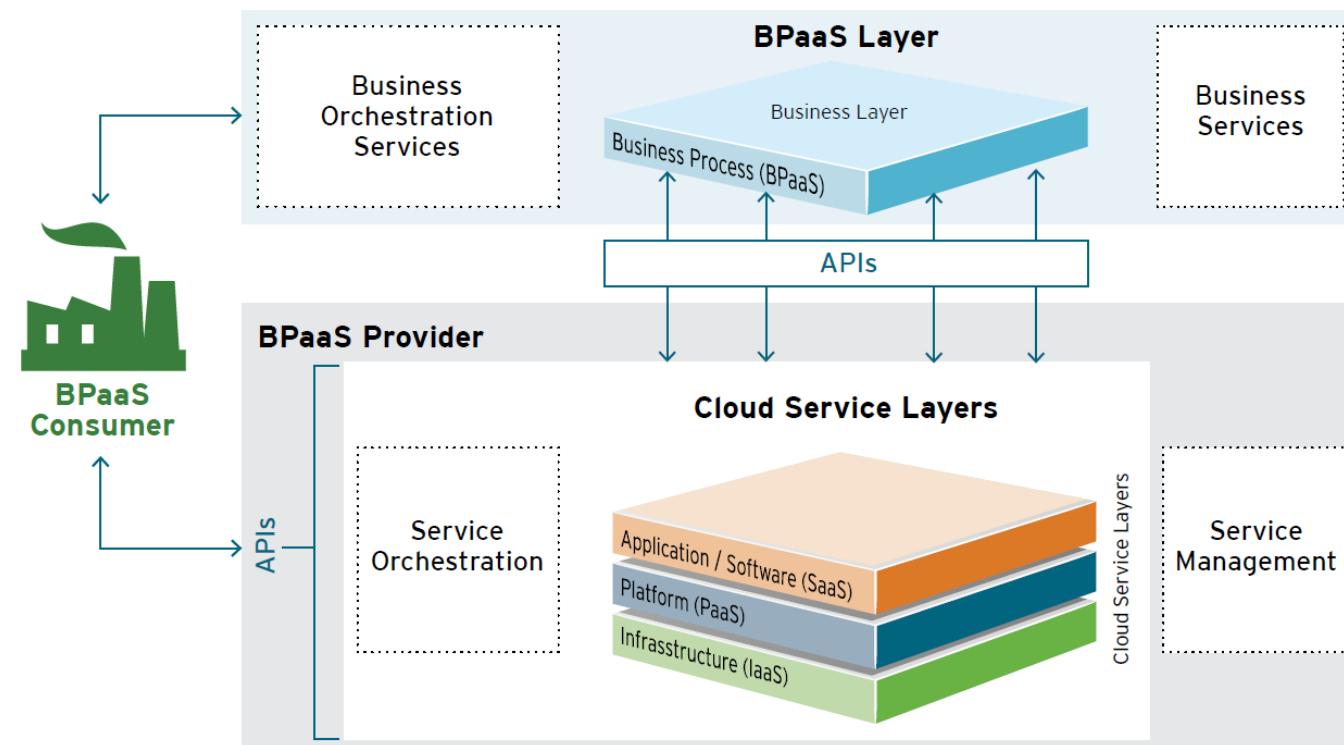
- **Principes**
 - Capacité « as a service » de créer, déployer et gérer des applications d'analyse dans le cloud basées sur des données à la fois dans le cloud et on-premises
 - Connectivité et ingestion de sources de données : capacités qui permettent aux utilisateurs de se connecter à des données structurées et non structurées contenues dans divers types de plates-formes de stockage (relationnelles et non relationnelles), à la fois on-premises et dans le cloud
- **Plusieurs mondes**
 - Les acteurs venant du on-premises proposant également du cloud : Tableau (racheté par Salesforce)...
 - Les acteurs natifs du cloud permettant l'ingestion de données on-premises : Birst (racheté par Infor), Domo, SAP, GoodData, IBM, Looker (racheté par Google)...
 - Les grands cloud provider veulent se positionner : AWS (Quicksight), Microsoft (PowerBI et Azure), Google, Alibaba...
- **La notion de multicloud devient de plus importante**
 - Qlick et SAP le mettent en avant
 - Elasticité et coûts

- D'indiscutables atouts
 - ✓ Orienté processus versus organisation
 - ✓ Cohérence transversale des données de l'entreprise
 - Ralliement aux meilleures pratiques de la gestion (diminution du développement spécifique)
 - Décloisonnement des structures et fluidification des échanges
 - Essentiel : optimisation de l'efficacité des processus
- Des obstacles incontournables
 - Complexité stratégique : direction du projet, impliquer l'organisation, l'informatique et la culture d'entreprise
 - Peu adapté en général à la souplesse exigée par l'e-business aujourd'hui (paradoxe)
 - Difficultés techniques trop souvent minorées
- Le challenge des éditeurs :
 - Une très grande majorité des grands comptes est déjà équipée contre une minorité d'ETI ;
 - Les ETI hésitent sur les coûts de mise en œuvre et le manque de souplesse ;
 - La désimbrication/orchestration et le cloud en mode SaaS sont l'avenir des ERP.

- Encore un énième mot-valise de la même forme que DevOps ?
 - Certes encore peu usité...
 - A priori contradictoire car le fournisseur de SaaS s'occupe de tout !
- Mais le mot a beaucoup de sens
 - Le fournisseur de SaaS ne s'occupe pas toujours de tout... → sauvegarde par exemple
 - ✓ Il y a beaucoup (trop) de fausses applications SaaS...
 - On a besoin de superviser les applications SaaS pour remonter d'éventuelles alertes
 - Les applications SaaS nécessitent de sécuriser leur accès → fédération d'identités
 - Les applications SaaS aussi communiquent entre elles !
 - ✓ Besoin d'API gateway, API Chaining, Webhook (IFTTT, Zapier...) et sécurisation
 - Permet justement la désimbrication des services Cloud

Le Business Process as a Service

- Les services techniques et les services aux entreprises sont orchestrés, mais à différents niveaux.
- Particulièrement agile et proche des besoins de l'entreprise.
- Évolutif et facturable.



Des moyens de garantir ce niveau d'abstraction

- **Low-Code et No-Code**
 - Salesforce, ServiceNow, Outsystems, RunMyProcess...
 - Zapier, Bubble, Webflow...
- **RPA : Robot Process Automation**
 - Low-code pour créer des scripts d'automatisation
 - Intégration avec les applications d'entreprise
 - Orchestration et administration, y compris la configuration, la surveillance et la sécurité
 - Acteurs : UI Path, Automation Anywhere, Blue Prism, WorkFusion...
- **Ici aussi les grands veulent rentrer**
 - Microsoft Power*, Google...
- **Point d'attention principal : la gouvernance**

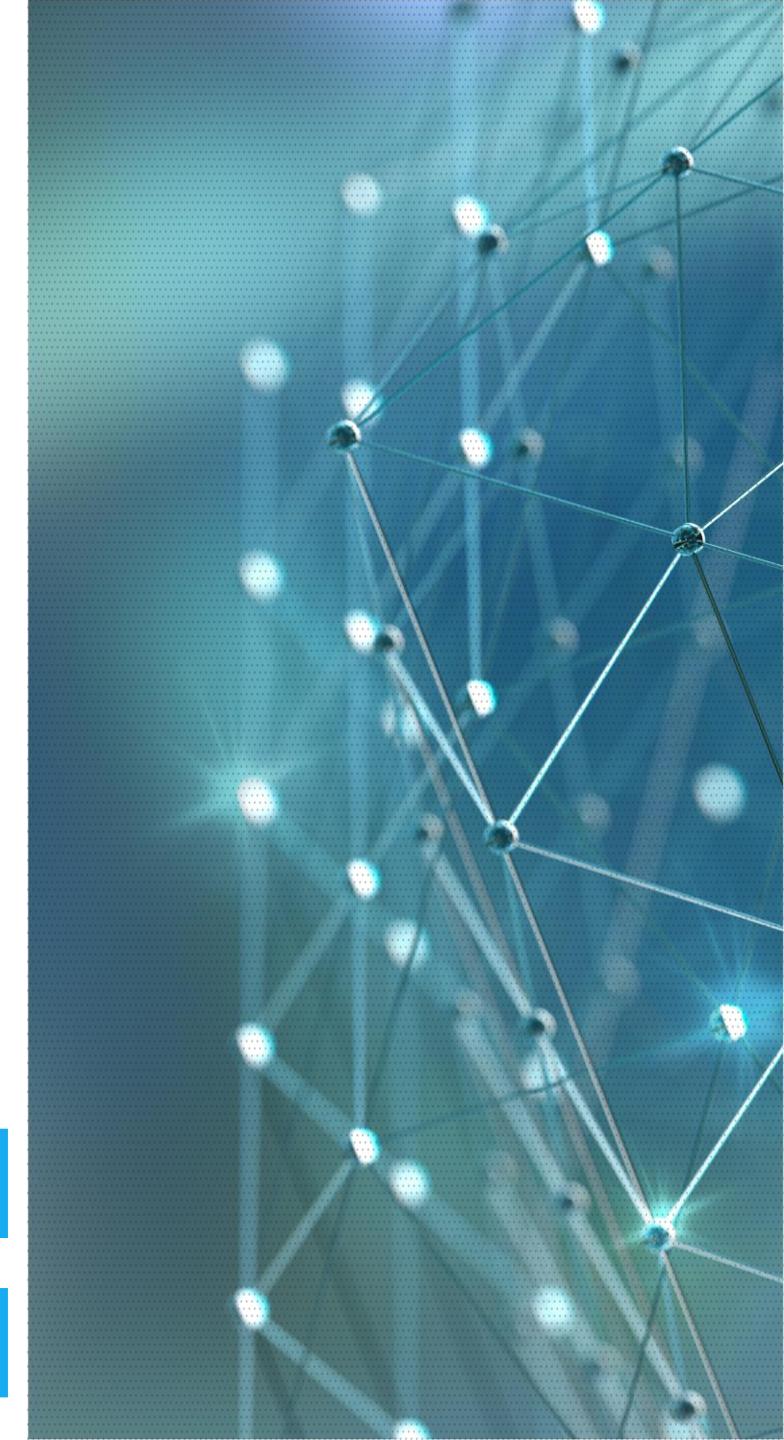
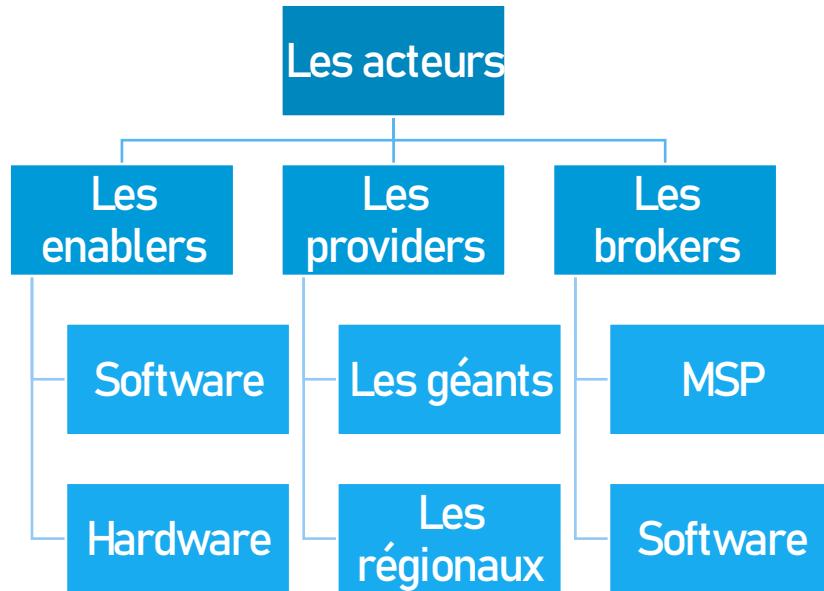


Un tour d'horizon des solutions des acteurs du marché du Cloud

Software as a Service

Infrastructure as a Service

Platform as a Service



Gartner Magic Quadrant

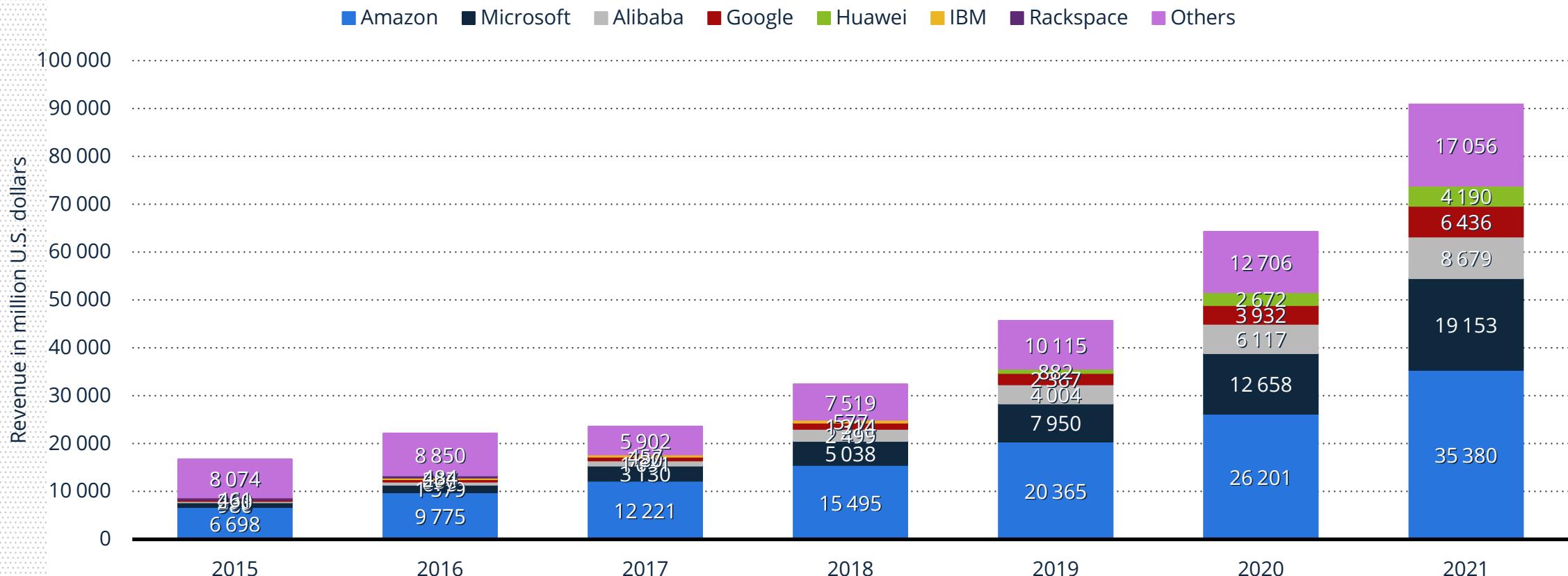
Magic Quadrant for Cloud Infrastructure and Platform Services



Source: Gartner (May 2018)

As of July 2019 © Gartner, Inc

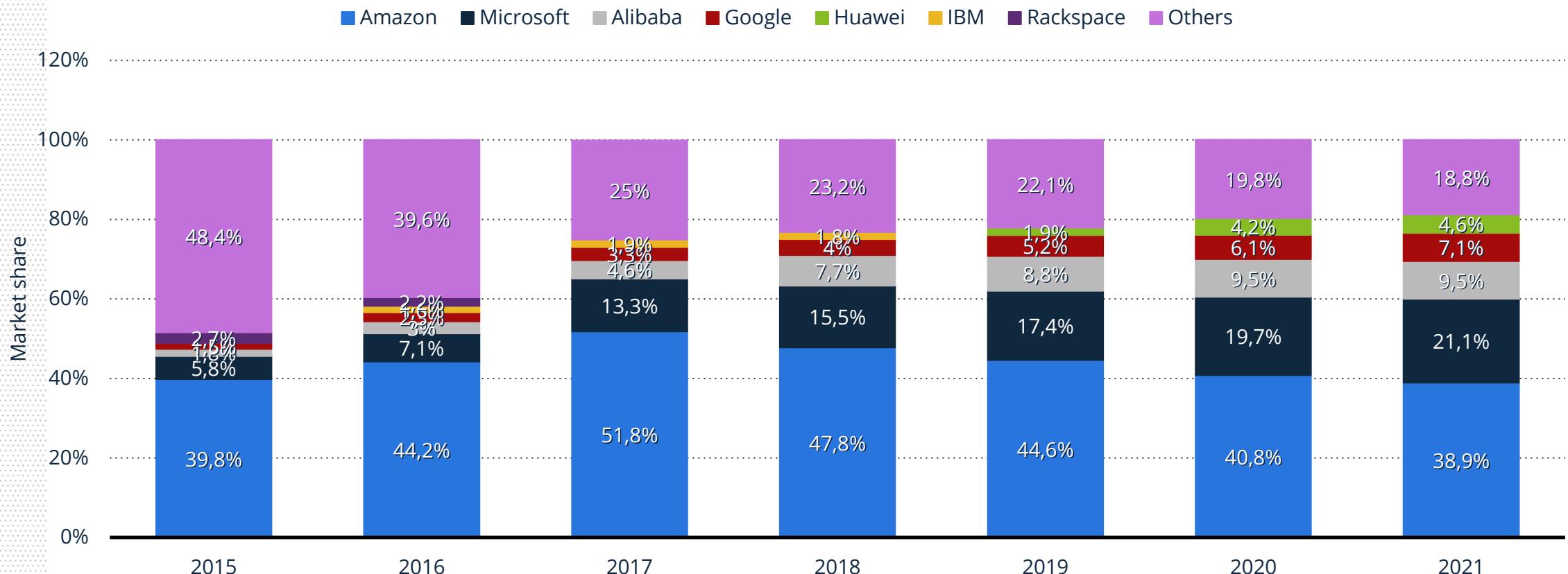
Le marché - CA



Note(s): Worldwide; 2015 to 2021

Source(s): Gartner

Le marché – parts de marché



Note(s): Worldwide; 2015 to 2021

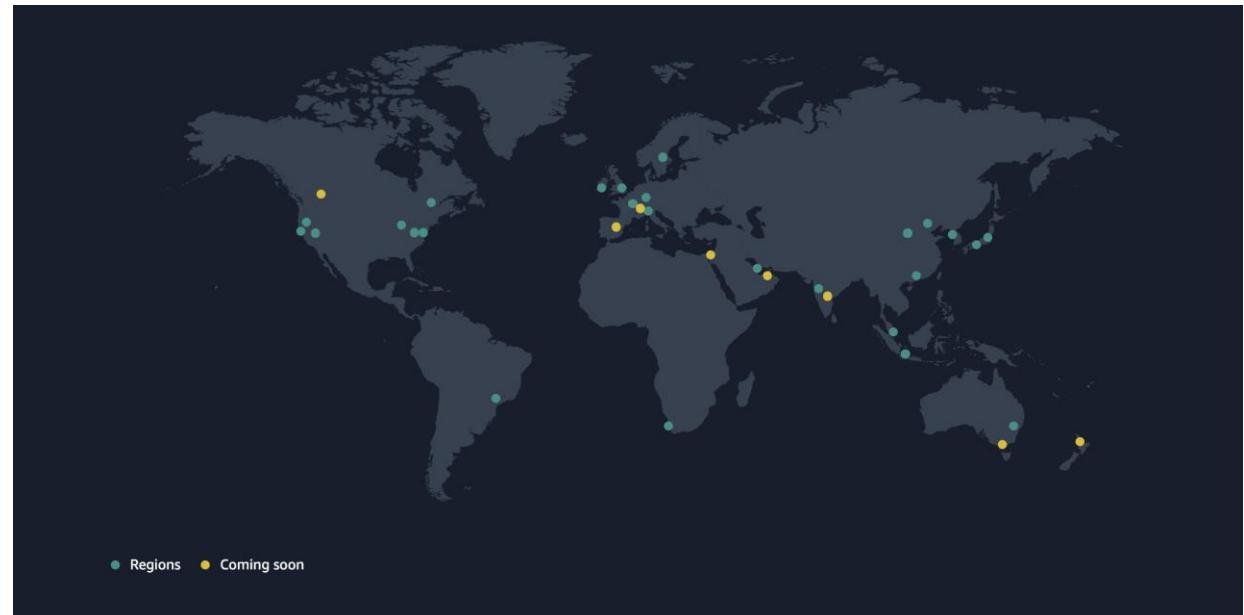
Source(s): Gartner

- Leader avec près 40% de parts de marché
 - Incontesté ?
- Une offre des plus complètes IaaS+PaaS
 - Compute : EC2 (Nitro, Graviton), Container, Lambda, Fargate, VMware...
 - Storage : S3, EBS, Glacier...
 - Réseau : VPC, Direct Connect, CloudFront..
 - Et beaucoup d'autres : base de données, monitoring, migration, gouvernance, sécurité...
 - Tout pour développer : CodeCommit, CodeBuild, CodeDeploy, CodePipeline ...
 - ✓ Et des services applicatifs pour IA, IOT, ML, mobile, multimedia, VR, jeux, blockchain, robotique...
- Très large marketplace
- Multiples régions découpées en Availability Zones
 - Présent en France
- Nombreuses options de paiement (as you go, réservations, spot...)



Infrastructure globale AWS

- S'appuie sur :
 - Des régions (Regions)
 - ✓ 27
 - ✓ Localisations géographiques
 - ✓ Constituées au minimum de deux zones de disponibilités
 - Des zones de disponibilités (Availability Zones)
 - ✓ 87
 - ✓ Clusters de data centers
 - ✓ Isolées les unes des autres en cas de panne de l'une d'entre elles
 - Des emplacements de réseaux périphériques (Local zones)
 - ✓ Point de présence local AWS pour réduire les temps de latence

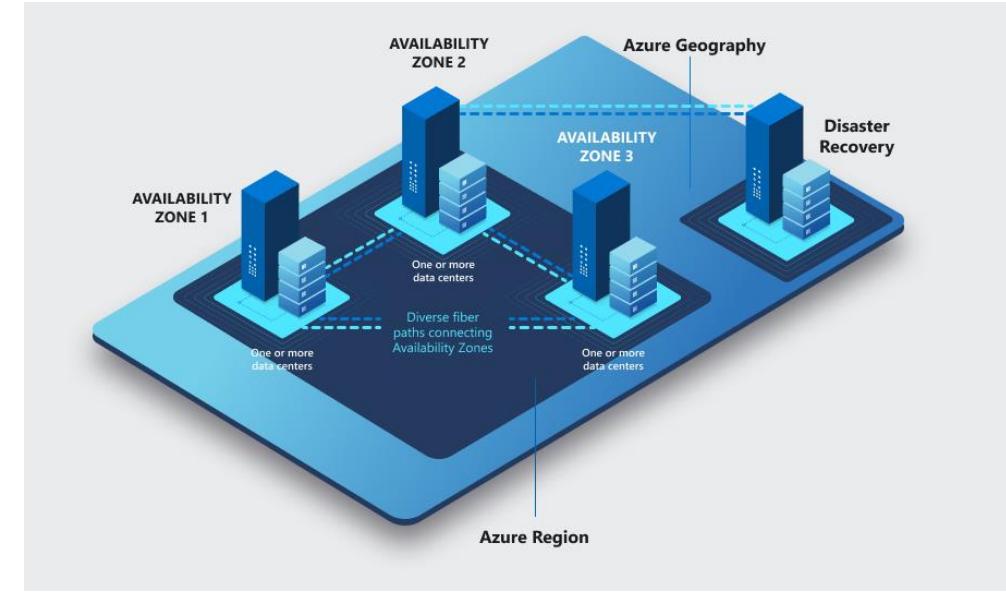


<https://aws.amazon.com/fr/about-aws/global-infrastructure/> (septembre 2022)

- Numéro 2 incontesté
 - Malgré un départ assez tardif
- Une offre large
 - Compute : VM, Containers, Functions, Serverless...
 - Stockage : Blob, SMB, Disk...
 - Réseau : Virtual Network, Express Route, CDN...
 - Et beaucoup d'autres : base de données, monitoring, migration, gouvernance, sécurité...
 - Mais à chaque fois, un peu moins qu'AWS...
 - Pour développer : Visual Studio Team Services & application center, Dev/test lab (templates)...
 - ✓ Avec des services applicatifs autour de App Service (Web & mobile apps), IoT, Media, AI, ML, Blockchain, VR/AR...
- MarketPlace moins large qu'AWS
- Multiples régions découpées en Availability Zones
 - Présent en France

Azure regions et zones de disponibilité

- <https://infrastructuremap.microsoft.com/explore>
- Azure Geographies
 - Une ou plusieurs régions
 - Pas technique
- Azure Regions
 - Ensemble de datacenters
- Azure Availability Zone
 - Datacenter



Amérique	Europe	Moyen-Orient	Afrique	Asie-Pacifique
Brésil Sud	France Centre	Qatar Central	Afrique du Sud Nord	Australie Est
Centre du Canada	Allemagne Centre-Ouest	Émirats arabes unis Nord		Inde centrale
USA Centre	Europe Nord			Japon Est
USA Est	Norvège Est			Centre de la Corée
USA Est 2	Sud du Royaume-Uni			Asie Sud-Est
États-Unis - partie centrale méridionale	Europe Ouest			Asie Est
Gouvernement américain - Virginie	Suède Centre			Chine Nord 3
USA Ouest 2	Suisse Nord			
USA Ouest 3				

Alibaba cloud

- Numéro 3 mondial
 - Aliyun sur Chine
 - 42% de part de marché en Chine
 - Chiffre d'affaires à 90% en Chine
 - En dehors de la Chine, Alibaba Cloud est le plus généralement utilisé dans la région Asie/Pacifique à la recherche d'une plate-forme pour les charges de travail agiles (Gartner)
- Large offre
 - Basé sur Xen et KVM (Elastic Compute Service)
 - Stockage blocs (Cloud disks)
 - Stockage objet (Alibaba Object Storage Service)
 - Service CDN
 - Service de conteneurs basé sur Docker (Cloud Container Service)
 - Cloud privé possible
 - Variété de services de couche IaaS-PaaS, y compris services de base de données (ApsaraDB)...
- Datacenters
 - Plusieurs régions en Chine (13)
 - États-Unis (côtes Est et Ouest), Allemagne, Royaume-Uni, Australie, Hong Kong, Indonésie, Philippines, Japon, Inde, Malaisie, Singapour, Thaïland, Corée, Emirats arabes unis.
 - <https://www.alibabacloud.com/global-locations>



Google Cloud Platform

- N°4 mondial avec 7% de parts de marché
- Leader de Kubernetes
- Une offre avec une croissance très élevée
 - Compute, Storage, Réseau...
 - Et beaucoup d'autres : base de données, monitoring, migration, gouvernance, sécurité...
 - Tout pour développer bien sûr avec Kubernetes
 - ✓ Et des services applicatifs pour IA, ML, multimedia...
- Un nombre de régions encore limité
 - Europe : Belgique, Londres, Pays-Bas, Zurich, Francfort, Finlande, Varsovie, Madrid
 - La France enfin ouvert !



DISPONIBLES DANS
35 RÉGIONS 103 ZONES 173 EMPLACEMENTS EN PÉRIPHÉRIE DU RÉSEAU PLUS DE 200 PAYS ET TERRITOIRES

BIENTÔT DISPONIBLE ! Google Cloud va continuer à se développer dans les régions suivantes : Berlin (Allemagne), Dammam (Royaume d'Arabie saoudite), Doha (Qatar), Malaisie, Mexique, Nouvelle-Zélande, Thaïlande et Turin (Italie).

- Début difficile
- Rachat de Softlayer en 2013
- En Europe : Londres, Paris, Francfort, Amsterdam, Oslo, Milan
- Différentes offres
 - Mise en valeur de 3 offres
 - ✓ IBM Cloud for VMware Solutions
 - ✓ IBM Cloud Pak for Applications
 - Modernisation d'applications (monolithe vers cloud native)
 - ✓ Red Hat OpenShift on IBM Cloud
 - Mais toujours la vision de proposer tout type de cloud
 - ✓ IBM Cloud Virtual Server for Classic Infrastructure et for VPC
 - ✓ IBM Cloud Bare Metal = Serveurs physiques
 - Avec possibilité d'intégrer des hyperviseurs : Xen, Hyper-V, vSphere...
 - ✓ IBM Cloud Kubernetes Service
 - ✓ IBM Cloud Functions (event-driven) et Cloud Code Engine (serverless)
 - Mais toujours IBM Cloud Foundry



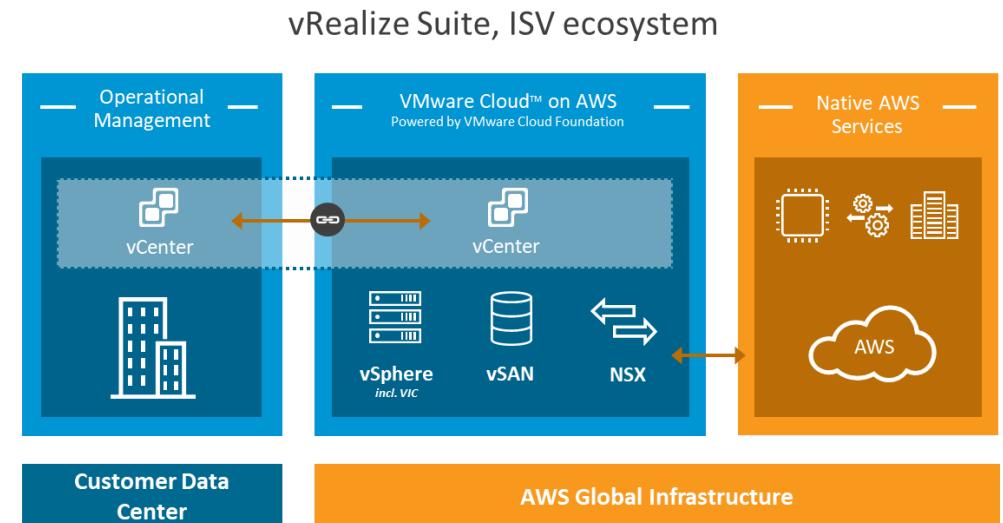
- Oracle Compute Cloud Service
 - Fin 2015
 - Première génération à base de Xen
- Oracle Cloud Infrastructure
 - Fin 2016
 - ✓ Seconde génération à base de KVM
 - Rachat de Ravello (nested-virtualization)
 - Europe : UK, Allemagne, Pays-Bas
- Serveurs physiques ou virtuels
- Services
 - Compute, Network, Storage (objet et bloc)
 - One-click Oracle database, RAC et Exadata
 - Containers
 - FaaS
- Verbatim
 - Gartner 2018 : "Oracle is primarily targeting customers that want to run Oracle software on cloud IaaS, particularly those that prefer to run on bare-metal servers"
 - Gartner 2019 :
 - ✓ "Oracle's cloud strategy is anchored by its applications, database and other middleware"
 - ✓ "Oracle is unlikely to ever be viewed by the market as a general-purpose provider of integrated IaaS and PaaS offerings"
 - Gartner 2020 : "With the significant enhancements made during the past year, Oracle is now well-positioned to handle broad lift-and-shift use cases (not just those limited to Oracle applications) and hybrid workloads. Oracle has a future focus on expanding the worldwide geographies it serves with competitive capabilities. »
 - Gartner 2021
 - ✓ Most Gartner clients consider OCI mainly for lift and shift of Oracle-centric workloads rather than as a general-purpose provider for all workloads, despite OCI being capable of such.



Les géants : beaucoup de points communs

- Américains ou chinois
- Des régions partout dans le monde avec des zones de disponibilités
 - Voir des zones locales
 - Voir des « extensions » de datacenter (AzureStack / AWS Outposts)
- Des offres complètes
 - Infrastructures : compute, storage, network...
 - Middleware : base de données, analytique...
 - Développement : tout pour développer et composer avec de multiples librairies disponibles (IA, ML, IoT...)
 - Des outils de sécurité, gouvernance, migration, gestion des coûts, management, IaC, automatisation...
- VMware s'associe avec les géants : AWS, Azure, Google, Oracle...

- Démarrage de la stratégie de VMware avec AWS
 - Partenariat signé en fin 2016
 - Première région AWS Q3 2017
 - ✓ Arrivée en France depuis mars 2019
 - Fonctionnalités
 - Déploiement de Cloud Foundation sur des serveurs bare metal
 - Serveurs certifiés et compatibilité garantie
 - Managés par VMware
 - Intégration aux services AWS
 - Les 4 cas d'usage officiels
 - Migration vers le cloud
 - Extension de datacenter
 - PSI
 - Modernisation d'application



Les acteurs européens restent régionaux

- Présents dans chaque pays d'Europe
 - OVHCloud en France
 - Aruba en Italie
 - Ionos en Allemagne
 - CloudSigma en Suisse
 - EBRC au Luxembourg...
- Les opérateurs ont essayé avec plus ou moins de succès
 - Deutsch Telekom versus Orange...
- Mais avec des offres bien moins complètes individuellement comparées aux géants
- Vers un regroupement européen ?
 - Initiative Gaia-X (cf. plus loin)

Vers un cloud souverain européen ?

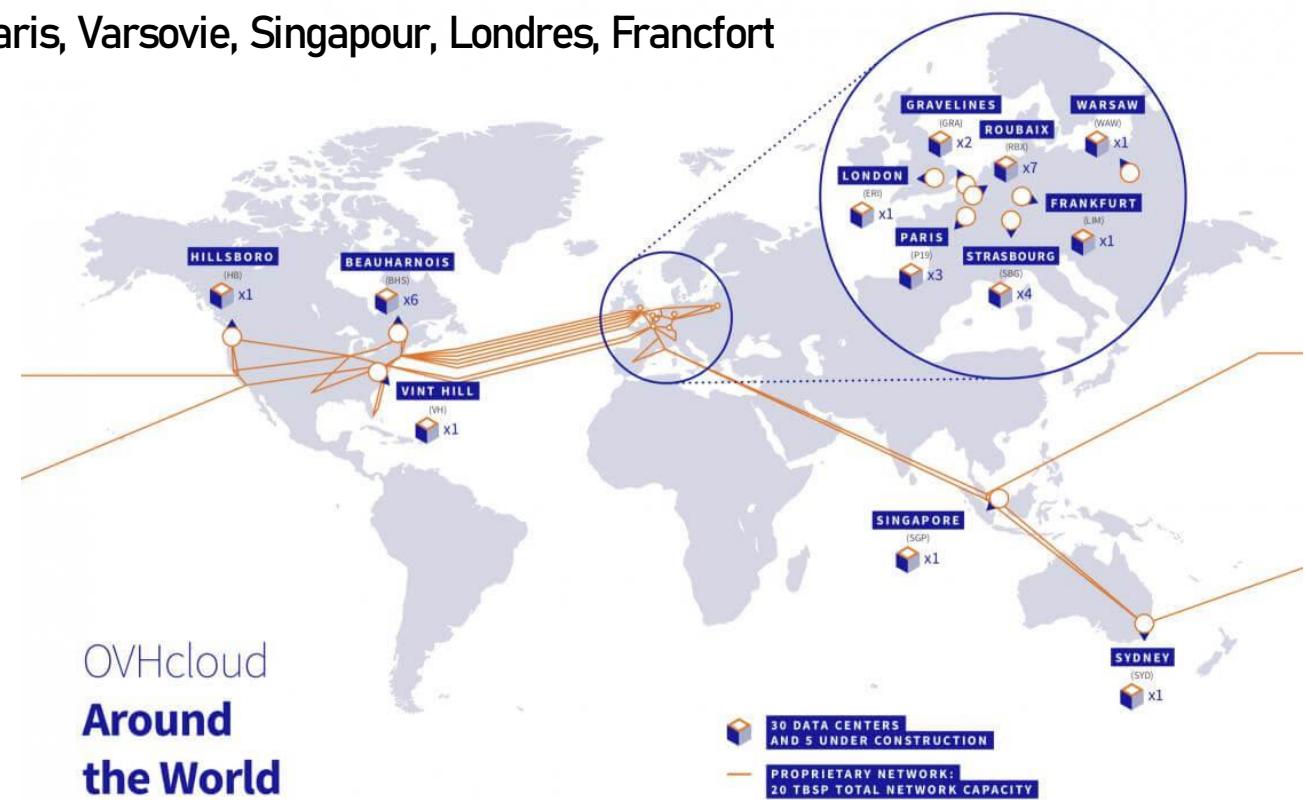
- Initiative Gaia-X
 - Gouvernements allemand et français
- Fondation* Gaia-X depuis le 15/09/2020
 - Certains parlent de « Métacloud souverain » ?!?!
 - Amadeus, Atos, Beckhoff, Bosch, BMW, CISPE, DE-CIX, Deutsche Telekom, Docaposte, EDF, Fraunhofer, German Edge Cloud, Institut Mines Telecom, International Data Spaces Association, Orange, 3DS Outscale, OVHcloud, PlusServer, Safran, SAP, Scaleway et Siemens.
 - ✓ CISPE = Cloud Infrastructure Services Providers in Europe
 - <https://cispe.cloud/code-of-conduct/>
 - Annonce par OVHcloud et T-Systems d'un cloud dédié aux OIV en 2021
 - Aucune nouvelle depuis...
 - Guillaume Poupart (ANSSI) parle de Cloud de Confiance
 - Cloud de confiance : le retour de la vengeance du cloud souverain ?
 - Cf. Plus loin...

* AISBL = association internationale sans but lucratif

Les acteurs américains sont bien présents et les européens tentent de se fédérer

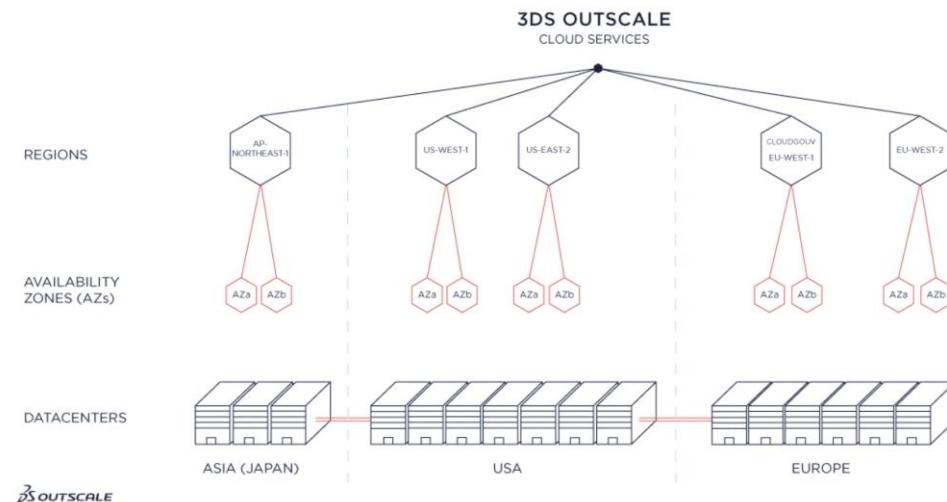
- Le cloud public est dominé par Amazon et Microsoft
 - Présents dorénavant en France
 - Google grandit très vite
 - ✓ Et arrive en France
 - OVH est l'acteur français le plus avancé
 - ✓ Malgré les évènements récents...
- Le marché du cloud privé hébergé devient de plus en plus mature et certains acteurs sont réellement avancés
 - Laisser à d'autres la gestion des couches d'infrastructure sans valeur ajoutée
- Les européens commencent à essayer de tenter de débuter de se fédérer...
- Le marché évolue vers l'hybridation et le multi-cloud
 - De l'importance de l'automatisation et de l'orchestration

- Chiffres clés
 - 632 millions
 - Introduction en bourse en octobre 2021
 - Licorne
- Datacenters : Roubaix, Gravelines, Strasbourg, Paris, Varsovie, Singapour, Londres, Francfort
 - Rachat de vCloud Air :
 - ✓ 7 datacenters aux US
 - ✓ 2 en Europe
 - ✓ 1 en Australie
 - Datacenters en France
 - ✓ Certifiés HDS et PCI DSS
- Technologies
 - Serveurs OVH
 - Stockage OVH
 - ✓ NAS ZFS/NFS avec cache SSD
 - ✓ Rachat de d'OpenIO
 - Portail OVH
- Offres
 - Cloud privé hébergé
 - Cloud public
 - Bare Metal Cloud



Outscale → 3DS Outscale

- Dassault Systèmes
- Cloud Management par TinaOS
 - « Propriétaire mais basé sur des briques Open Source... »
 - « Compatibilité » Amazon EC2
- Datacenter en France, USA, Asie
- Serveurs Cisco UCS + baies Netapp + NVIDIA (vGPU)
- Offre
 - Stockage : bloc ou objet
 - Réseau : LB, VPN, DirectLink
 - Disponible on-premises

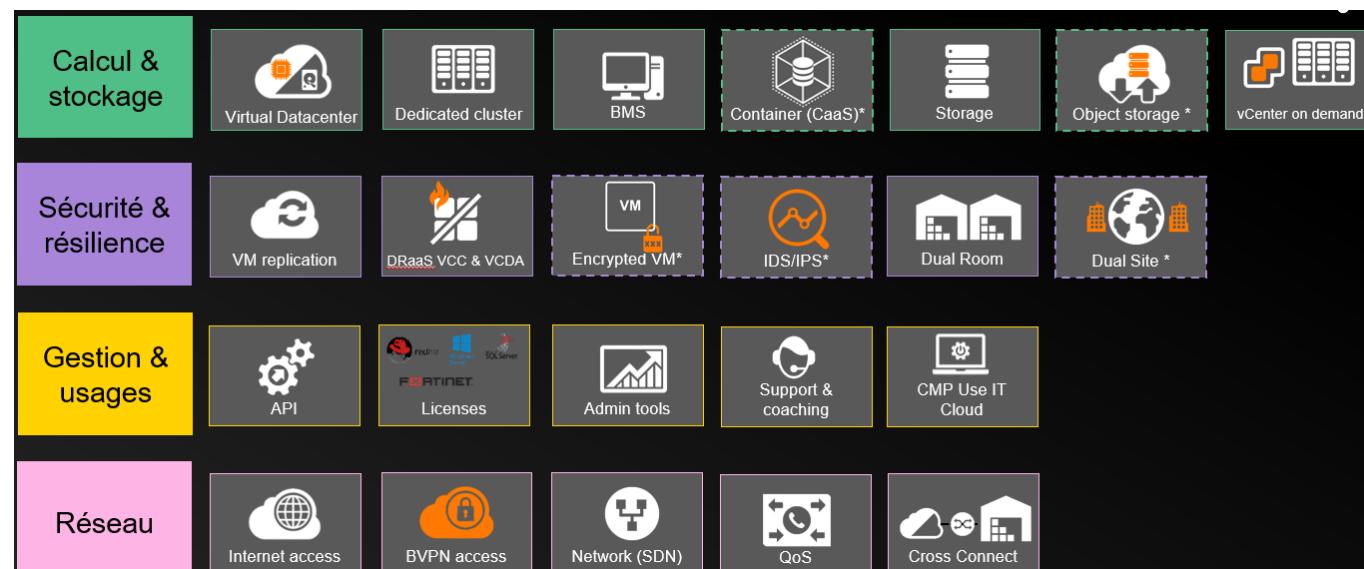


Et Orange ?

- De Cloudwatt à Orange Flexible Engine
 - Basé sur Openstack et Huawei
 - Membre de Cloud Alliance (Huawei Cloud, Telefonica Cloud, T-Systems)
 - ✓ 1 seul contrat Flexible Engine donne accès à toutes les ressources de la Cloud Alliance
 - ✓ Une seule facture, pour l'utilisation de Flexible Engine et de la Cloud Alliance
- Bilan en 2022
 - Cloudwatt
 - ✓ Fermé...
 - Flexible Computing Advanced
 - ✓ Basé sur vCloud Director...
 - Flexible Computing Engine
 - ✓ Prometteur mais...
 - Orange Cloud de confiance
 - ✓ Regroupement des entités Cloud, sécurité, collaboratif...
 - ✓ Vers l'hybridation et le MSP
 - Accord avec Cap Gemini : Bleu
 - Orange Cloud Avenue début 2022



Flexible Engine Régions

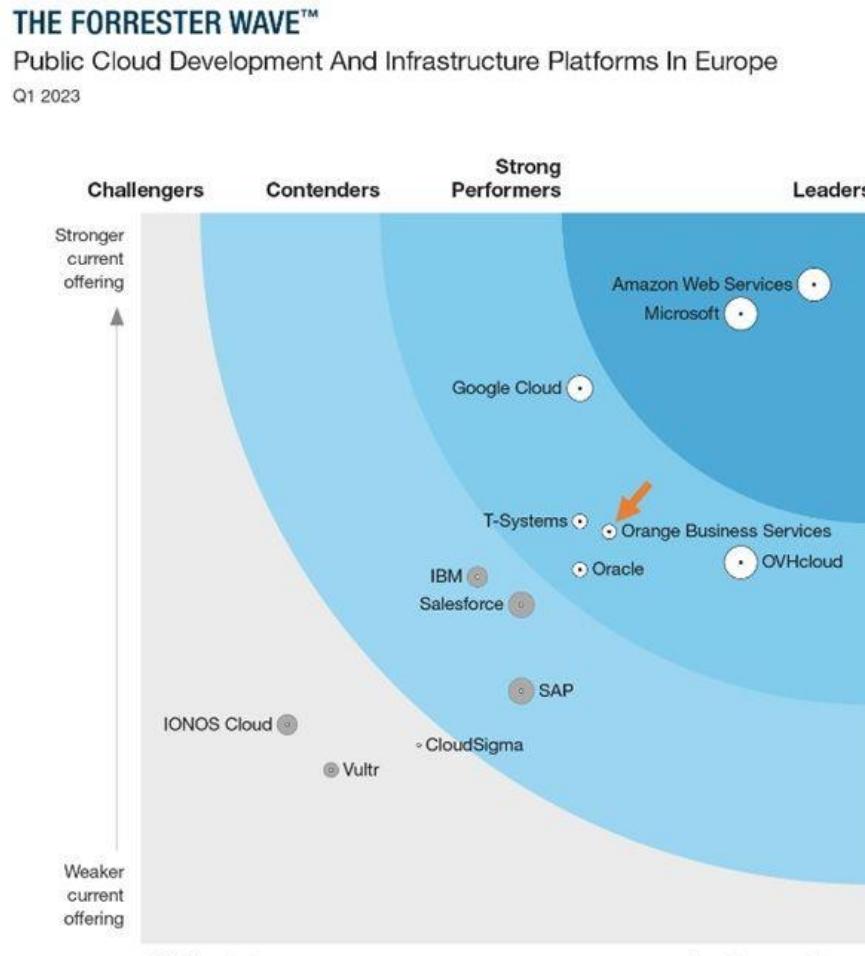


- Précédemment Online SAS
- Hébergeur français
- Fondé par Xavier Niel en 1999
 - Filiale à 94,8 % du groupe Iliad
- Datacenters majoritairement en Ile de France

- Les principaux services
 - Serverless
 - Containers
 - Storage and database
 - Virtual machines
 - Elastic metal



Le marché Européen



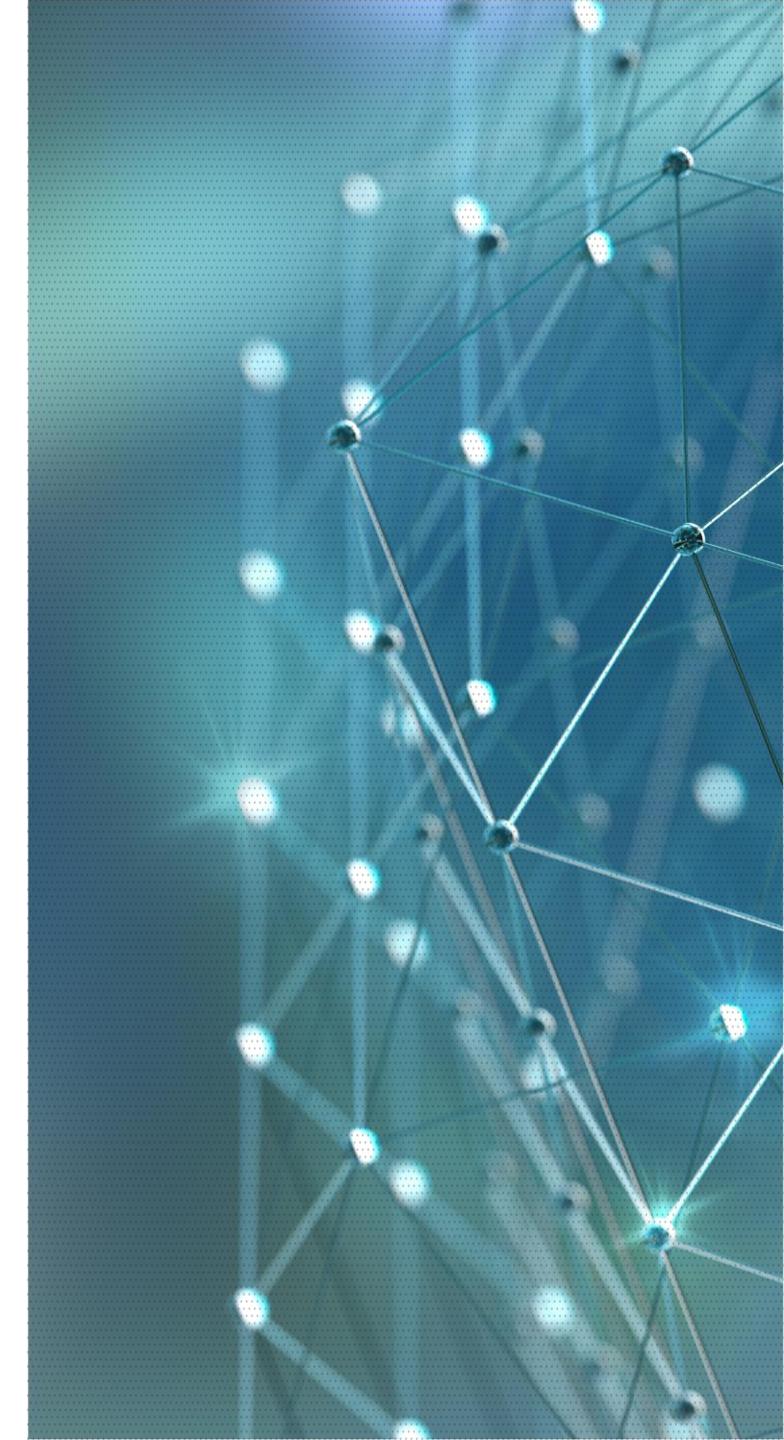


Un tour d'horizon des solutions des acteurs du marché du Cloud

Software as a Service

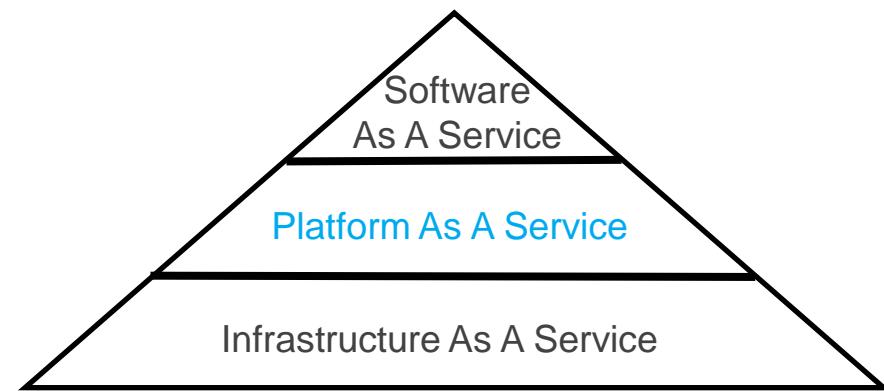
Infrastructure as a Service

Platform as a Service

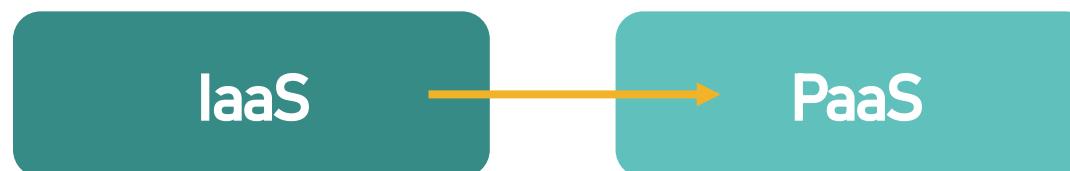


Le CaaS le remplaçant du PaaS?

IaaS, PaaS, aPaaS, SaaS

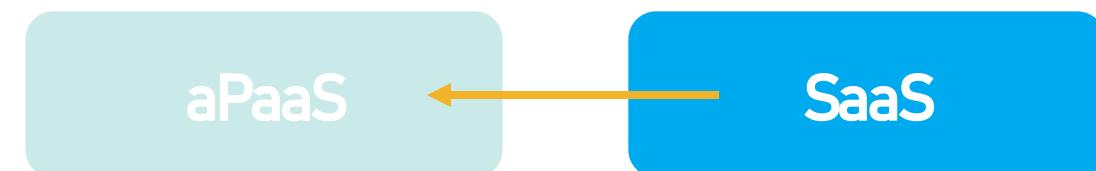


Quand l'infrastructure
s'intéresse au
développement



Google App Engine, Azure App Service, AWS Elastic Beanstalk...

Quand l'application
s'intéresse au
développement



Salesforce, Mendix, OutSystems...

Infrastructure

Applications

■ Et le iPaaS ?

- Suite de services permettant de développer et gérer l'intégration d'applications
- Plutôt orienté B2B
- Informatica, Boomi, Workato, MuleSoft, Jitterbit...

PaaS spécialisés ?

- Vers une spécialisation des PaaS ?

IoT

- AWS IoT Core + FreeRTOS/IoT Greengrass
- Azure IoT + Cloud IoT Edge
- Salesforce Thunder
- ...

IA

- IBM Watson
- Salesforce Einstein
- ...

AutoML

- Datarobot
- Dataiku
- Databricks
- ...

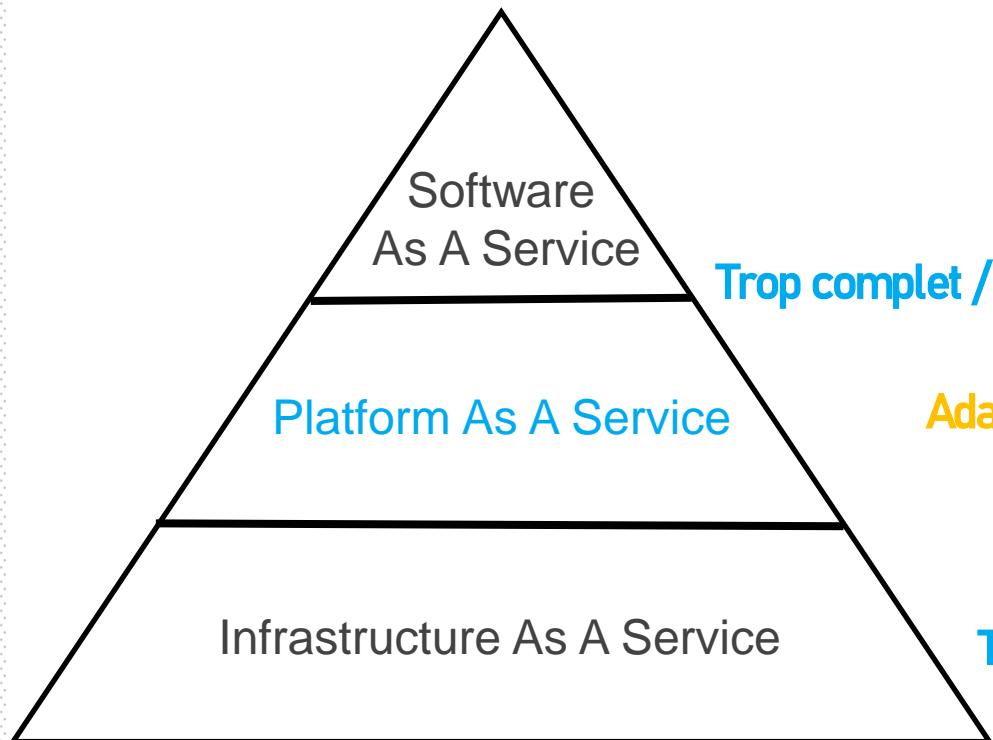
Salesforce et le PaaS

- **Salesforce et le PaaS = une histoire d'amour ?**
 - L'historique Force.com refondu en Lightning
 - Fuel issu du rachat de ExactTarget en 2013
 - Salesforce Analytics, orienté sur l'univers Salesforce
 - Thunder (iPaaS) et IoT Cloud, orientés IoT
 - MuleSoft qui a été rachetée par Salesforce en 2018
- **Et enfin Heroku (2011), le PaaS le plus généraliste, prisé des starts up**
 - Permet à la fois la connexion vers des services « classiques » Salesforce mais également d'autres services spécialisés tels que l'API Einstein Vision (IA) ou Prediction.io (Machine Learning)
- **A noter que Salesforce a également pris très tôt le virage de Kubernetes (2015)**
 - Les aidant dans la transformation des monolithes vers les microservices

Container vs PaaS

- **PaaS - Platform as a Service**
 - Abstraction de la complexité des couches d'infrastructures
 - Repose sur un format de type container (ex : Cloud Foundry garden/warden)
 - Le développeur *commite* son code, active le pipeline CI/CD et l'artefact se retrouve disponible sur la plateforme PaaS
- **Intégration des containers de type Docker dans les offres PaaS**
 - Openshift intègre nativement le format de container Docker comme son format par défaut depuis 2014 mais à développer son propre moteur avec CRI-O
 - Redhat est toujours le 2^{ème} contributeur Kubernetes après Google
 - Les offres Pivotal et IBM Cloud Platform basées sur CloudFoundry proposent l'usage de containers Docker directement depuis ces frameworks en sus des formats natifs Garden/Warden
 - L'offre Suse Cloud Application Platform basée également sur Cloud Foundry utilise désormais par défaut le format Docker
 - IBM Cloud Platform basé sur Kubernetes et Docker Containerd

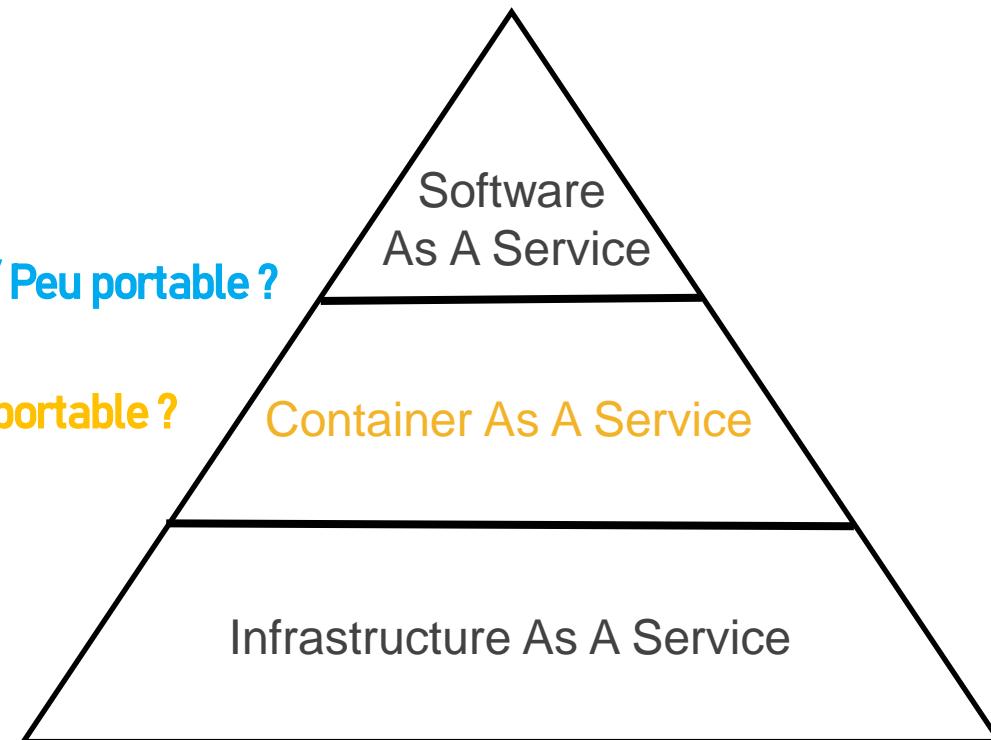
CaaS/PaaS: l'évolution



Trop complet / Trop peu flexible / Peu portable ?

Adaptable / évolutif / portable ?

Trop bas niveau ?



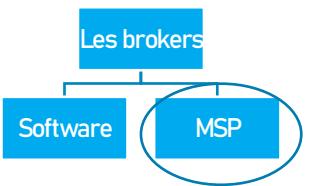
Le PaaS devient un sous-ensemble
du CaaS

CaaS/PaaS : évolution du CaaS vers le PaaP Platform-as-a-Product

- L'adoption de Kubernetes s'accompagne de certaines difficultés
 - Compétences Cloud Native des OPS et des DEV
 - Évolution rapide et constante des différents outils tiers impliquant des mises à jour fréquentes (monitoring, logs, registre, moteur de container, CI/CD, service mesh...)
 - Séparation des responsabilités infrastructures (OPS/SRE) versus applications (PO/DEV)
 - Adapter son CaaS aux besoins de ses développeurs en sélectionnant les outils adéquats
- Plus qu'un modèle de service, une organisation et des process
 - Les OPS gèrent l'infrastructure et la chaîne d'outils dédiés aux DEV
 - Les OPS sélectionnent les outils en fonction des besoins des DEV – propre à chaque entreprise
 - Les outils masquent la complexité de l'infrastructure du point de vue des DEV
 - Les DEV consomment ces outils sans considération pour l'infrastructure sous-jacente
 - Les DEV accélèrent leurs développements sur la base de patterns de code réutilisables et adaptés à la Platform-as-a-Product construite à cet effet
 - Les évolutions des besoins des DEV s'accompagnent de l'enrichissement progressif de la chaîne d'outils pour satisfaire ces nouveaux besoins

<https://samnewman.io/blog/2023/02/08/dont-call-it-a-platform/>

Les Managed Service Providers



Le premier des brokers est le MSP

Managed Services Providers

Fournisseurs de services managés

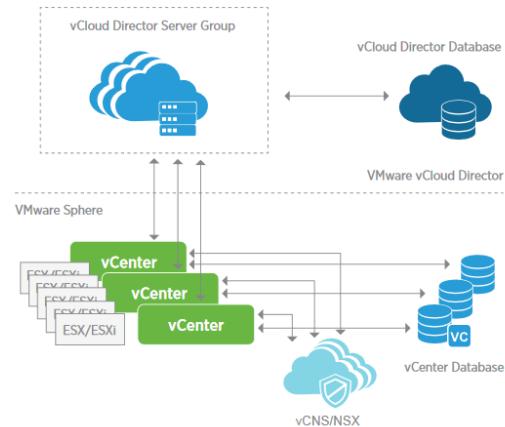
Infogéreur de clouds

Ajout de plus-value sur le cloud et notamment le management ou l'hybridation

- Soit des acteurs du cloud hybride
 - Le MSP délivre des services de management, de réseau, d'application...
 - ✓ Peut comprendre des offres d'autres fournisseurs - y compris des fournisseurs de services d'application, des sociétés d'hébergement et des fournisseurs de services réseau - qui complètent leurs offres traditionnelles avec des services de gestion associés
 - Plusieurs acteurs français sont bien positionnés en Europe sur ce créneau
 - ✓ ATOS, Capgemini, OBS, Claranet, Sopra Steria...
- Soit des acteurs du cloud public
 - Un MSP d'infrastructure de cloud public est un fournisseur qui offre à la fois des services professionnels et de management liés aux opérations d'infrastructure et de plate-forme pour un ou plusieurs fournisseurs IaaS + PaaS intégrés
 - ✓ AWS, Azure, Google, Alibaba
 - Plusieurs acteurs français sont positionnés dans le monde sur ce créneau
 - ✓ ATOS, Capgemini...

La multiplication des MSP/CSP

- Beaucoup d'acteurs français, de tailles très diverses, sont en réalité des MSP mais en utilisant plutôt sous le nom de fournisseurs de cloud et/ou d'infogéreurs de cloud
 - En proposant d'héberger les architectures de leurs clients
 - ✓ Datacenters loués ou privés
 - ✓ Et en les manageant
 - En proposant des cloud privés hébergés
 - ✓ Principalement basé sur vCloud Director
 - ✓ Principalement basé sur Nagios
 - Avec une offre de services associée
 - ✓ Supervision, exploitation, administration
 - ✓ Catalogue de services
 - En proposant de plus en plus de l'hybridation
- Certains sont plus avancés
 - Pour les partenaires VMware Cloud provider
 - ✓ Utilisation de Cloud Foundation
 - ✓ Vmware Cloud Services
 - vSphere on-premises, AWS, Azure
 - Axians vPack : Serveurs + VMware CloudFoundation
 - ✓ Services managés à la carte
 - Minimum jusqu'à l'hyperviseur inclus
 - Supervision, sauvegarde, PSI...
 - Modèles de facturation variés : acquisition + service managés ou « pay as you go »
- Exemples : Cloudtemple, Cheops, LinkByNet(Accenture), Inetum, Axians...



- Réservé aux services providers
- vSphere & NSX
- vDC Virtual Data Center
- vCloud Availability for vCloud Director
- Plug-in Terraform

Quelle plus-value précisément ?

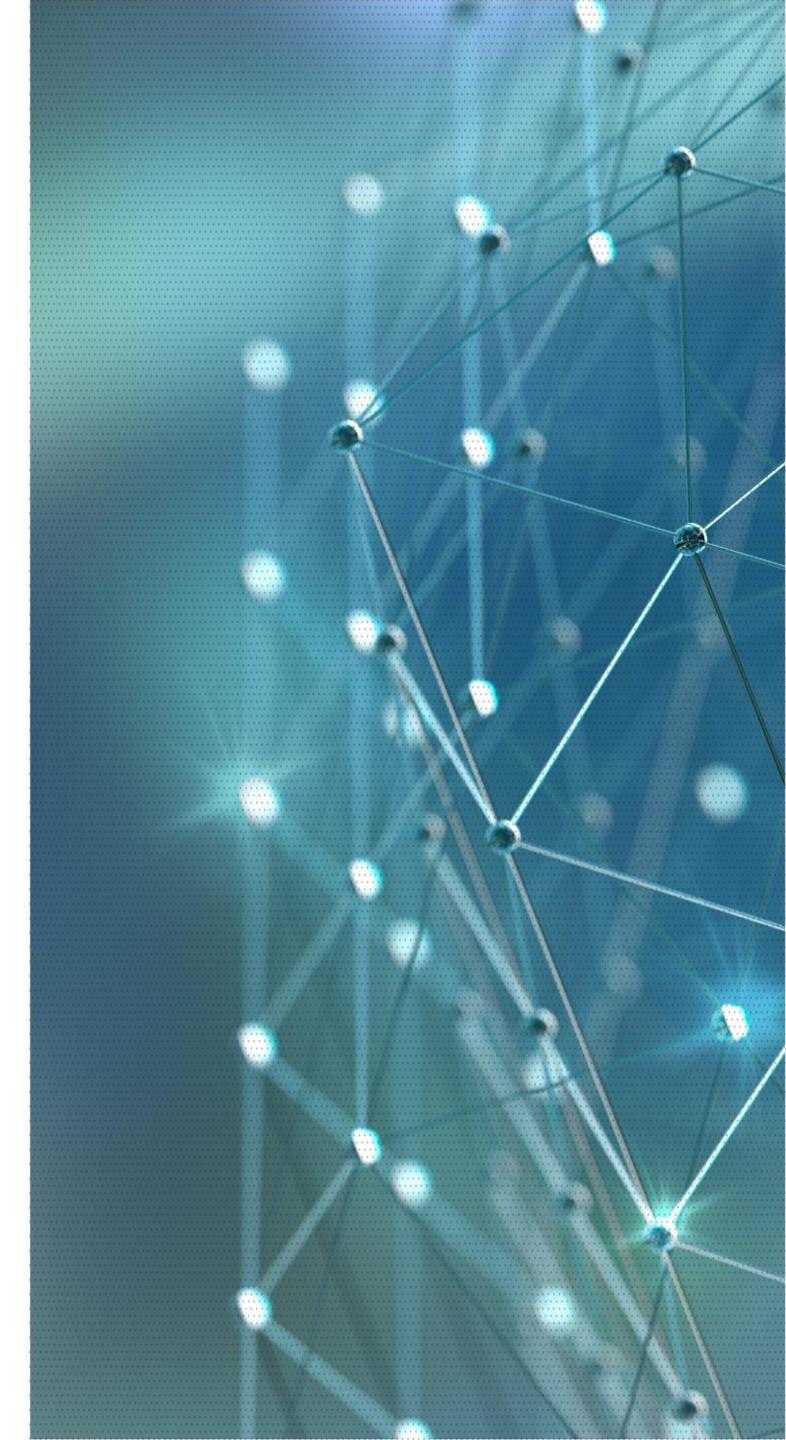
- La plus importante de la plus-value d'un MSP est le SLA
- Le SLA référent des cloud provider publics est la disponibilité du service
 - Les engagements des Cloud Providers sont faibles
 - ✓ Les pénalités en cas de sinistre sont faibles
 - ✓ Elles ne sont pas négociables
 - Le contrat avec le Cloud Provider représente un marché d'offre (mass customisation)
 - ✓ Même pour les grands clients le contrat est standard et sera mis en place « online »
 - ✓ Le fournisseur peut changer les termes et conditions, c'est au client de tracer les changements
- Un contrat de MSP représente un marché de demande (sur mesure)
 - Se négocie de gré à gré -> le contrat est sur mesure
 - Clause d'auditabilité possible
 - Les SLA peuvent être variés : Gestion de la disponibilité, Gestion des incidents et des problèmes, Gestion des changements, Gestion de la sécurité, Industrialisation et amélioration continue, Gouvernance...
 - Des pénalités peuvent/doivent être prévues avec possibilité de résiliation en cas de non tenue chronique et répétée des dysfonctionnements
 - Point d'attention : comment définir les coûts d'un MCO d'un MSP sur un périmètre fluctuant d'un Cloud provider ?

Sommaire

- **Introduction**
- **Cloud Computing**
 - Fondamentaux, bénéfices et enjeux
 - Comprendre les aspects juridiques et la sécurité
- **L'impact du Cloud**
 - L'évolution de la structure des entreprises
 - L'évolution des métiers
- **Un tour d'horizon des solutions des acteurs du marché du Cloud**
 - Software as a Service
 - Platform as a Service
 - Infrastructure as a Service
- **Comment construire son cloud privé**
- **Conclusion**



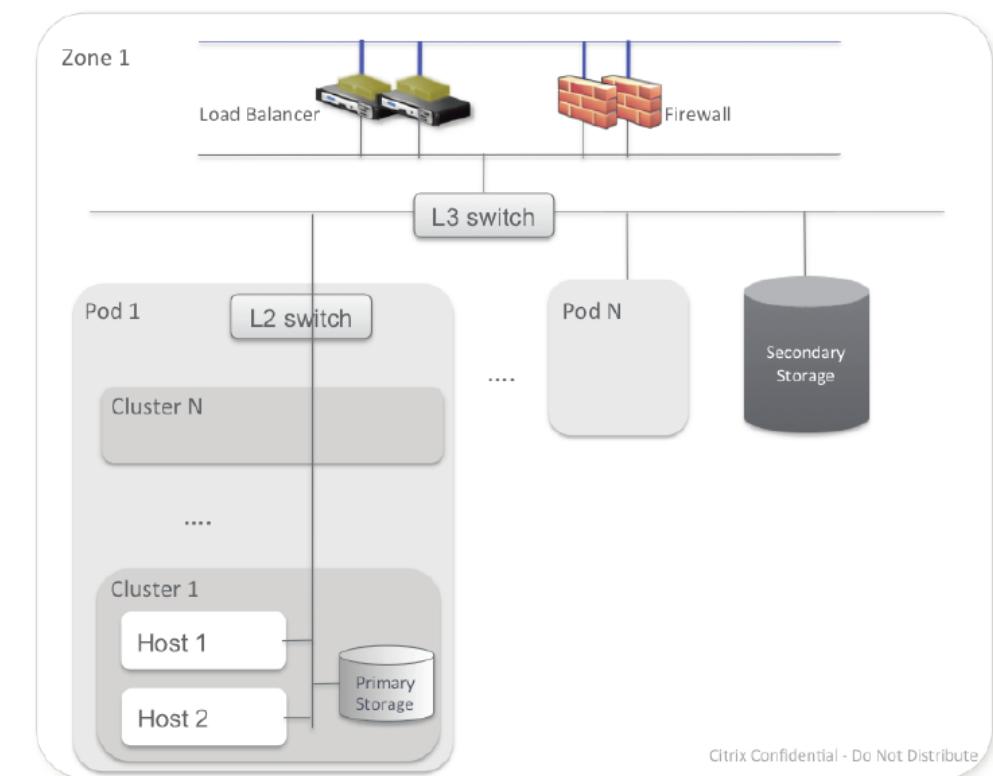
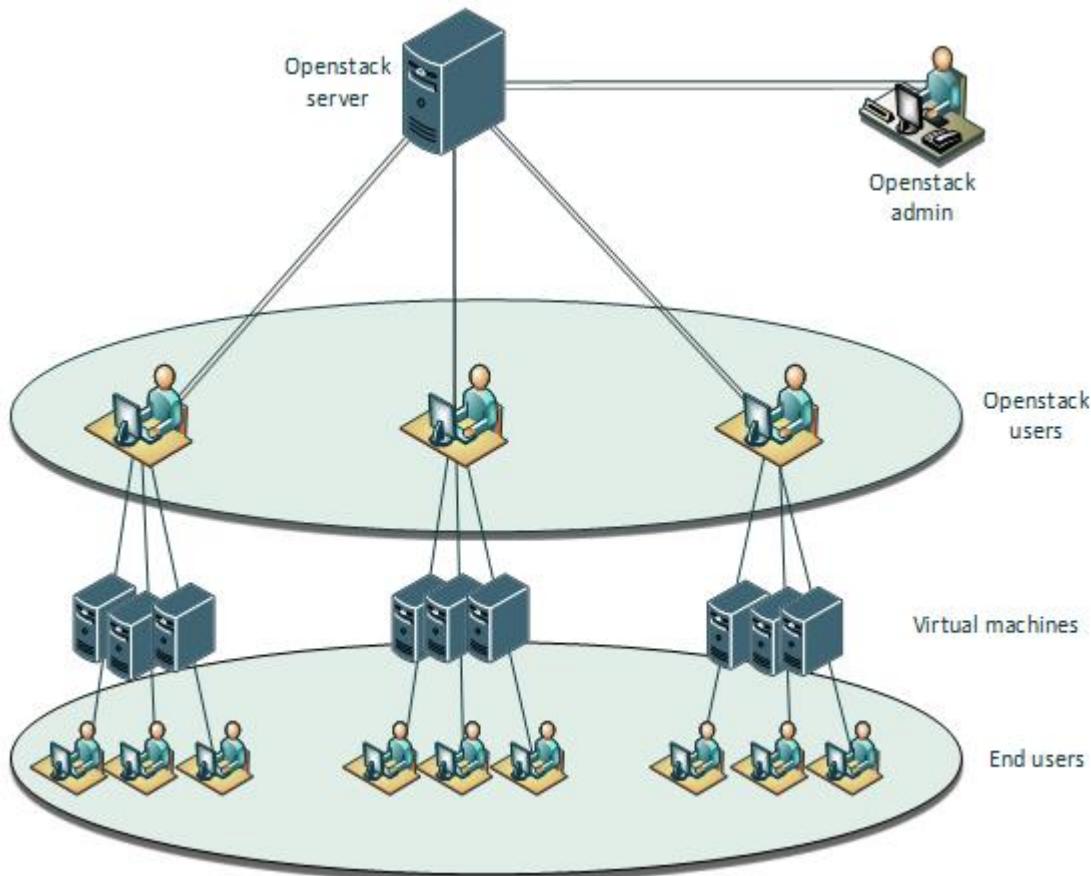
Comment construire son cloud privé



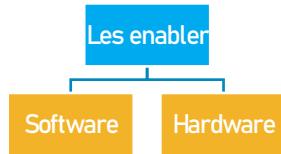
Modélisation

Rappels :

- Dans le cloud public, la notion de tenant peut être vue comme une entreprise cliente
- Dans le cloud privé, la notion de tenant peut se rapprocher d'un environnement applicatif ou d'un service de l'entreprise



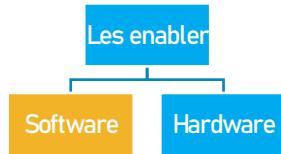
Citrix Confidential - Do Not Distribute



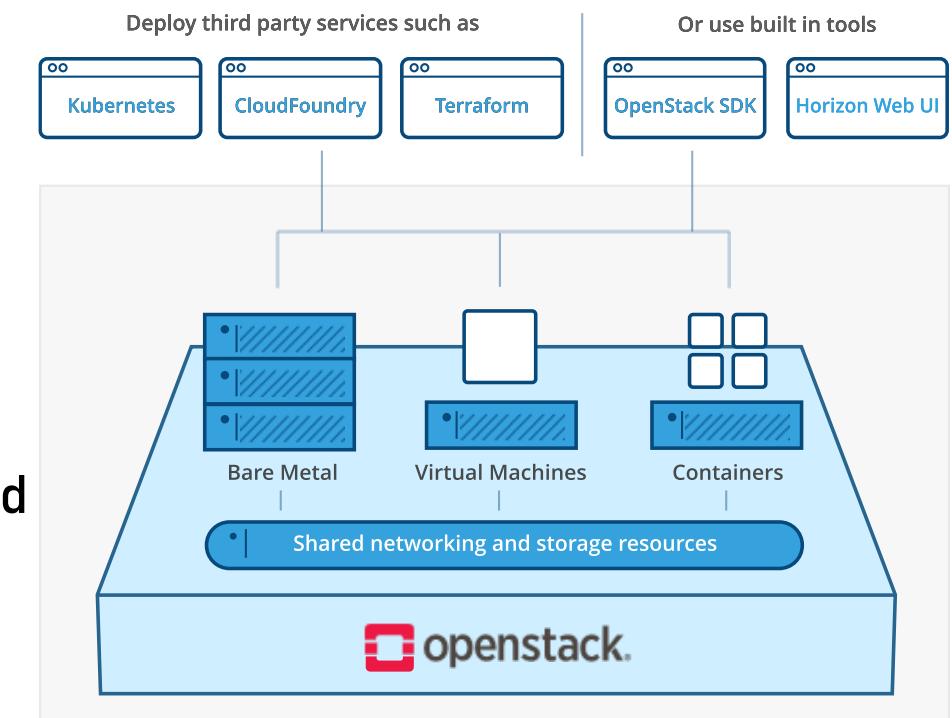
Le logiciel s'impose comme facilitateur

- **Software**
 - Openstack
 - ✓ Cloud Operating System
 - VMware Cloud Foundation
 - ✓ Software Defined Data Center
- **Hardware = converged system**
 - Vous rappelez-vous de VCE ? vBlock ?
 - Pick one : DellEMC VxBlock, PowerOne, Readystack, Cisco & Netapp Flexpod, Huawei, IBM...
 - Une innovation commerciale et non technique
 - Encore des manques d'intégration des outils par rapport aux promesses
 - Beaucoup sont/ont été basés sur des partenariats qui peuvent être mouvants ou impliquant des problématiques de support

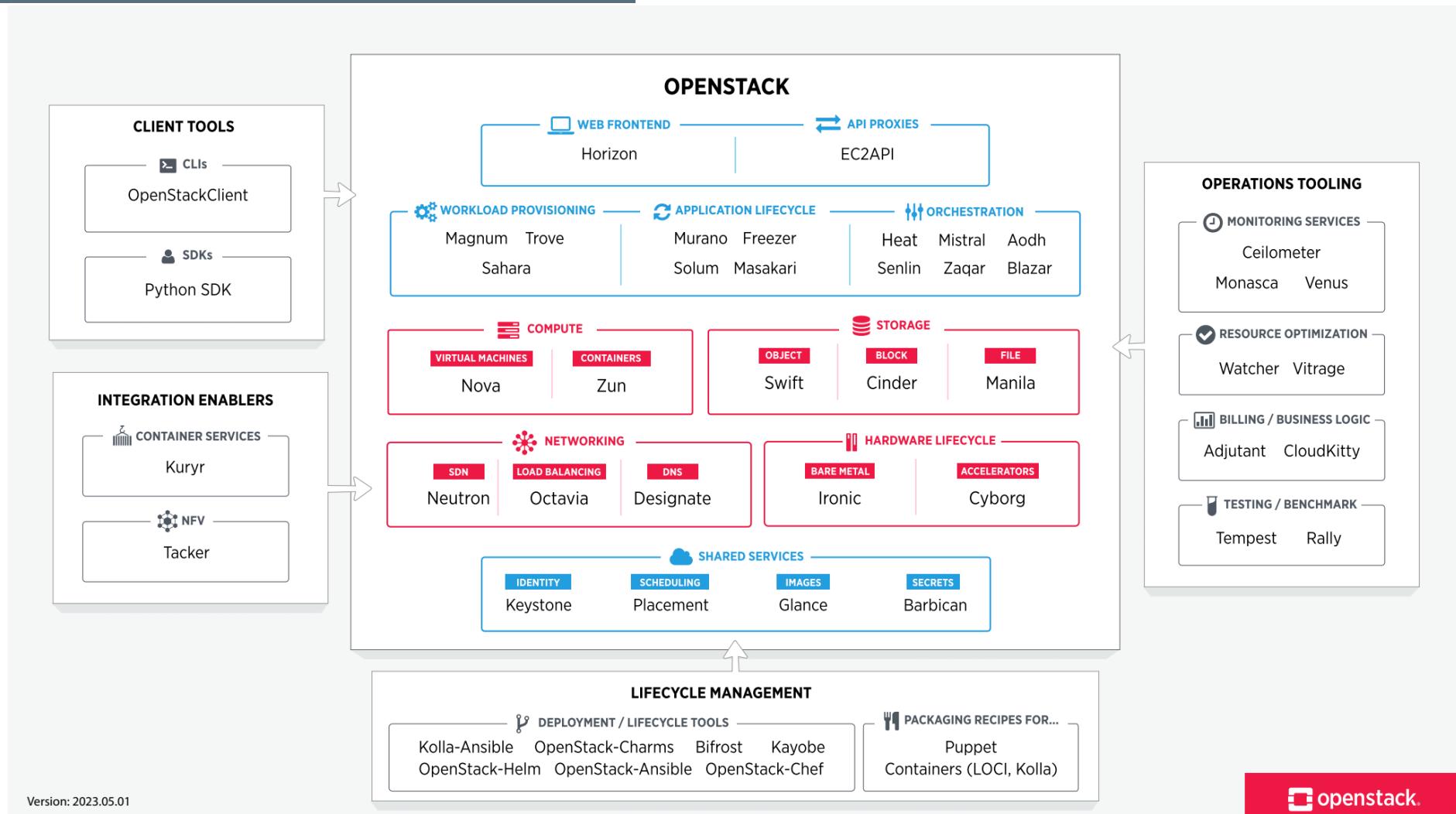
Openstack



- Projet Open Source initié par la NASA et Rackspace en juillet 2010
- Objectif initial :
 - Favoriser l'adoption et permettre à tous de créer des clouds privé/public
 - Réduire le lock-in
 - Opensource (License Apache 2.0)
- Openstack Foundation depuis 2012
 - Platinum : Red Hat, Huawei, Ericsson, Tencent, Ant group (Alibaba), Facebook, FiberHome, Microsoft, Wind River (IoT)
- Une évolution vers Open Infrastructure
 - “Four Opens: Open Source, Development, Design and Community”



Openstack Landscape



Blan

- Points forts
 - Open Source (pas de verrouillage)
 - Multi-hyperviseurs
 - Modulaire
 - Dynamisme et soutien d'une grande communauté
 - Plusieurs distributions avec un mécanisme de certification
- Points faibles
 - Certains composants restent peu matures
 - Pas d'outil de billing natif (Cloudkitty = rating)
 - Un essoufflement puis une évolution du positionnement
- Remarques
 - Beaucoup utilisé par des opérateurs telecom
 - ✓ Pour les fonctions réseau et notamment NFV
 - En France, des grands comptes publics
 - ✓ Souvent clients RedHat historiques



Cloud public

VMware on AWS, Google Cloud VMware Engine...



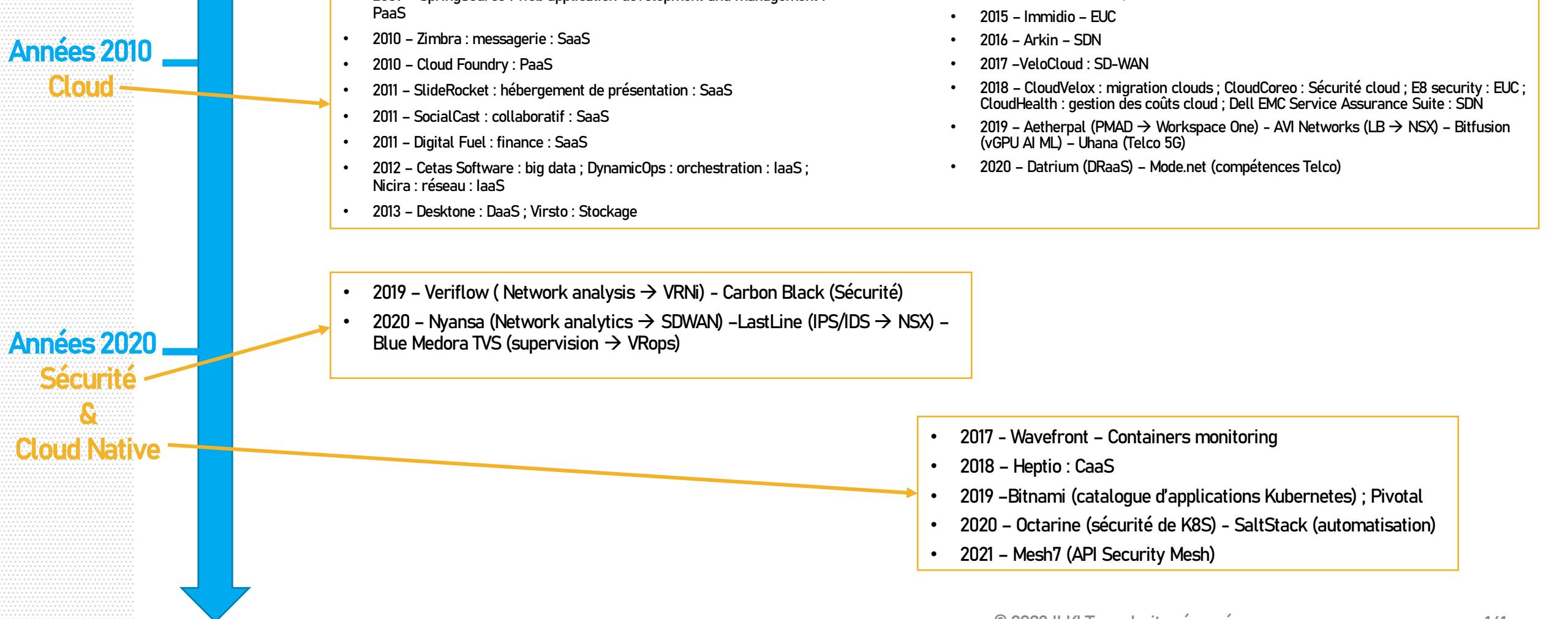
Cloud privé et hybride

Cloud Foundation, vSAN, NSX, velocloud...

Multi-cloud Operations : vRealize Suite (Operations, Automation...), CloudHealth...

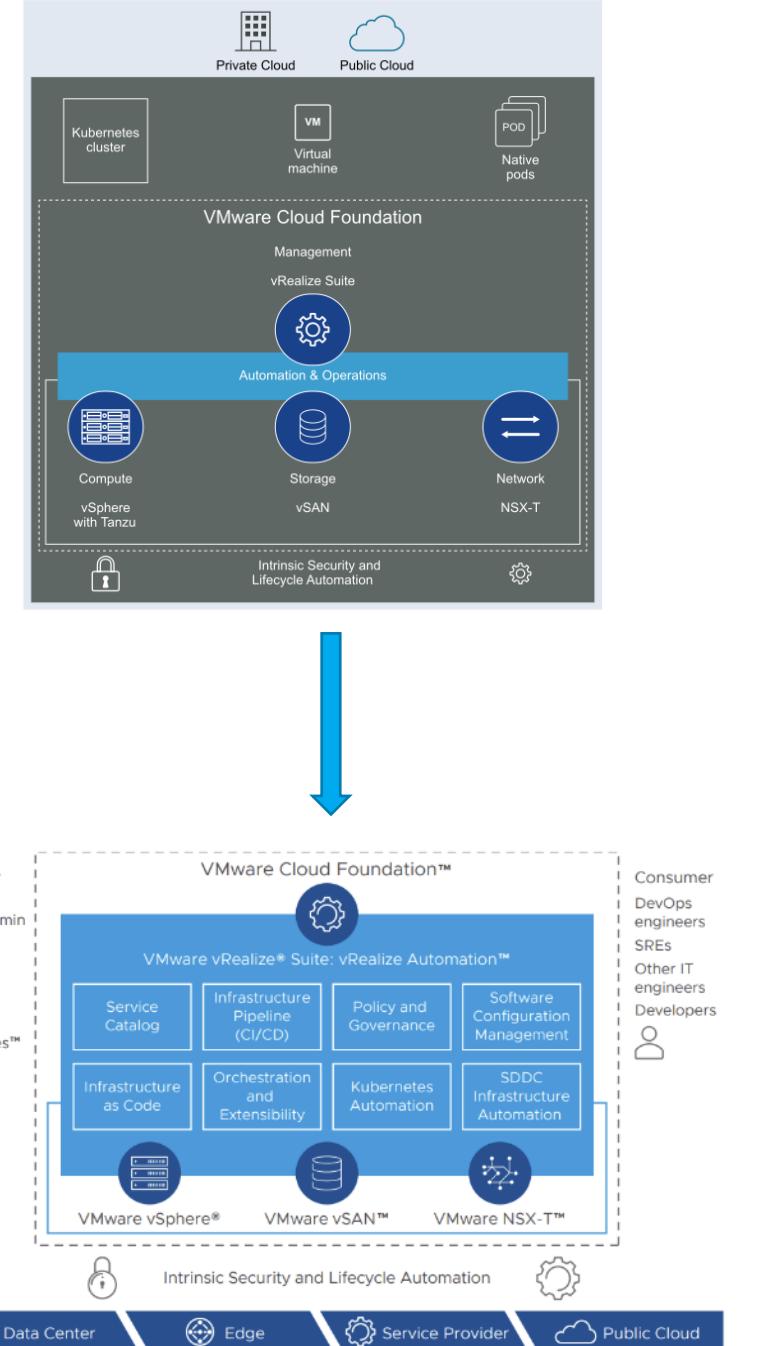
App modernization : Tanzu (Kubernetes, Containers...)

VMware : des années 2010 aux années 2020



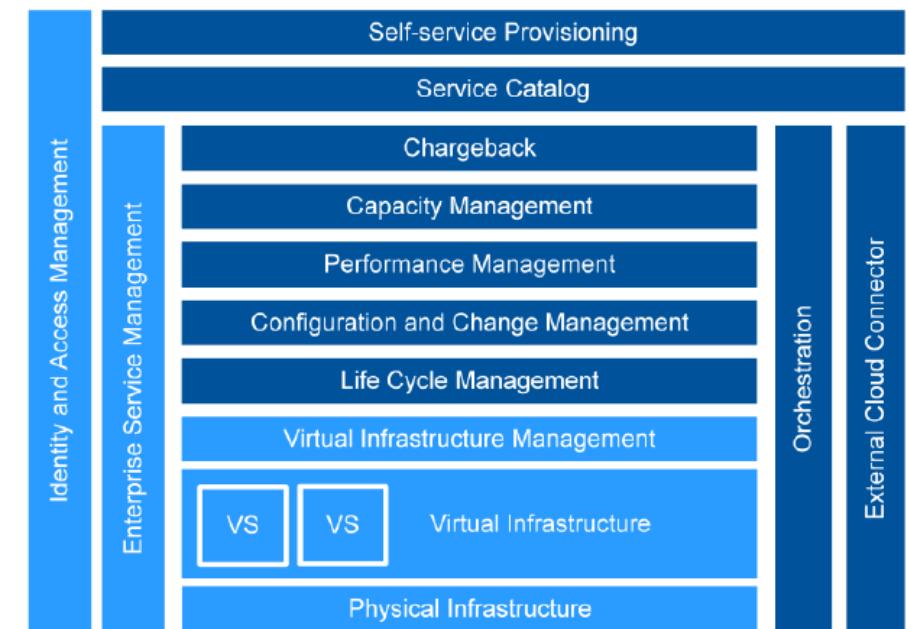
VMware Cloud Foundation

- Simplement : vSphere + VSAN + NSX + SDDC Manager
- Une brique devenue brique de base
 - ReadyNodes Integrated Systems (QCT, Lenovo, HPE, Dell, Hiachi, Fujitsu) ou Composable systems (HPE Synergy, Dell PowerEdge MX)
 - Hybrid cloud : VMC on AWS, Google Cloud VMware Solution, Azure VMware solutions, Oracle Cloud VMware solution
 - VMware Cloud provider avec un VCP Program : Rackspace, OVH, CenturyLink
 - System Integrator : TCS, Wipro, Atos, DXC, HCL
- Evolution du licensing pour intégrer vRealize



Cloud privé

- Ce n'est pas qu'un projet technique
 - Catalogue de services notamment
- Mais la dimension technique existe
 - Ne pas confondre Cloud privé et virtualisation++
 - ✓ Self Service, élasticité, measured service
 - Virtualisation du réseau
 - Automatisation
 - Orchestration
 - Hybride



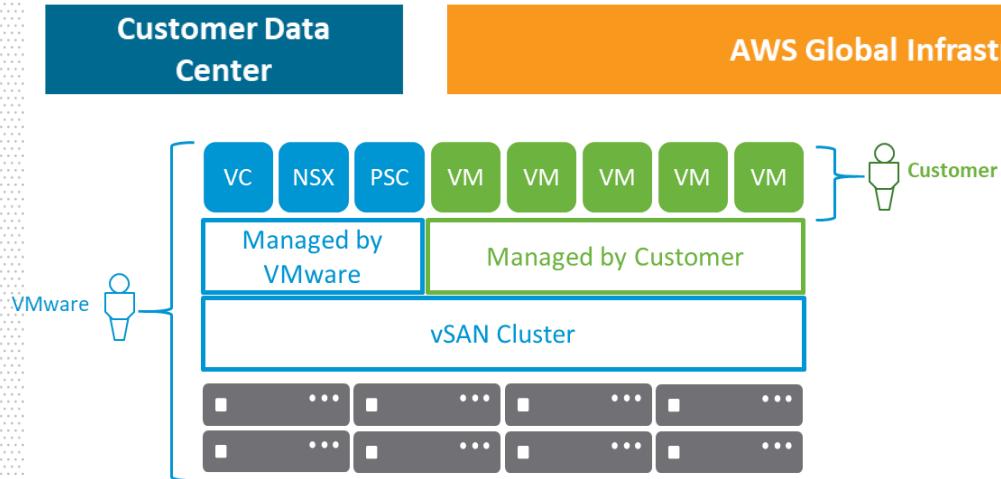
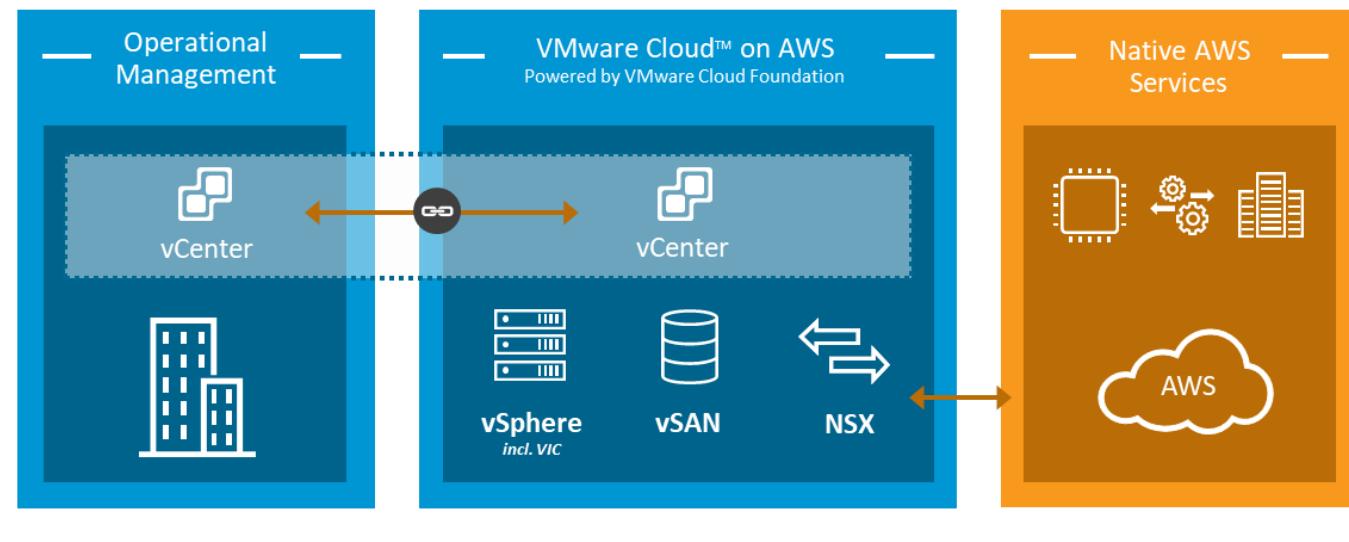
Source : Gartner

Cloud privé virtuel

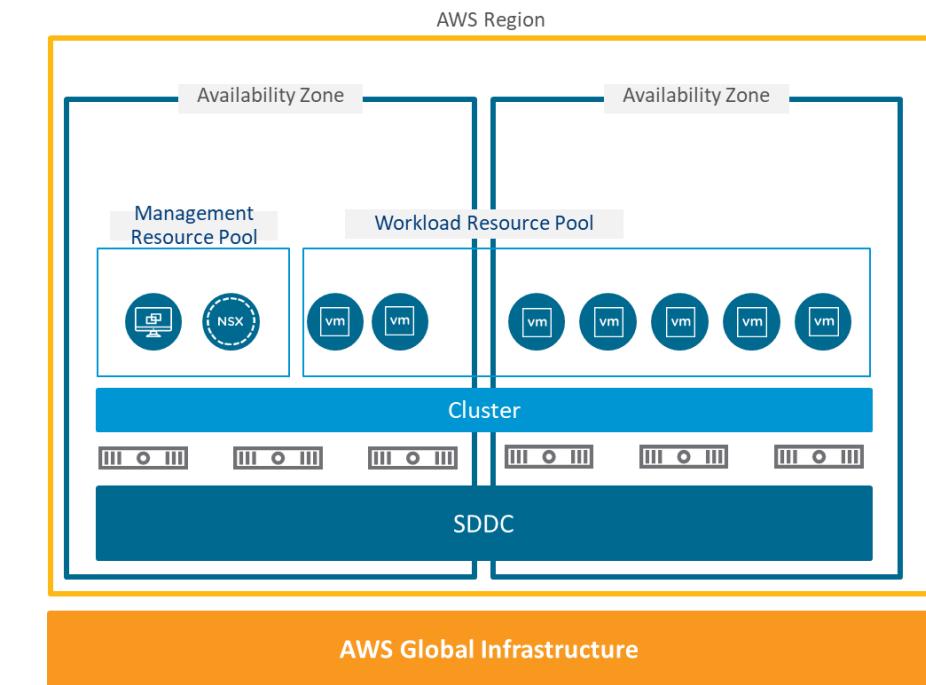
- Démarrage de la stratégie de VMware avec AWS
 - Partenariat signé en fin 2016 et première région AWS Q3 2017
- Puis avec Google
 - Annonce d'un partenariat mi-2019
 - ✓ En fait, managé par CloudSimple...
 - Acquisition de CloudSimple en novembre 2019...
 - ✓ Qui était l'infogéreur de la solution équivalente chez... Microsoft Azure...
 - Mai 2020 : Google Cloud VMware Engine
- Et Microsoft ?
 - Après moultes péripéties...
 - ✓ Azure VMware Solution en septembre 2020
 - "Azure VMware Solution is developed, operated, and supported by Microsoft, backed and cloud verified by VMware."
 - ✓ Disponible aux US, UK, Japon, North & West Europe, Allemagne, Suède, Canada, Brésil, Australie, Asie et France

Architecture globale VMCon AWS

vRealize Suite, ISV ecosystem



- No root ESXi access
- No VIB installations
- No VDS configuration access
- No direct management VM access



Serveurs

Host Specifications

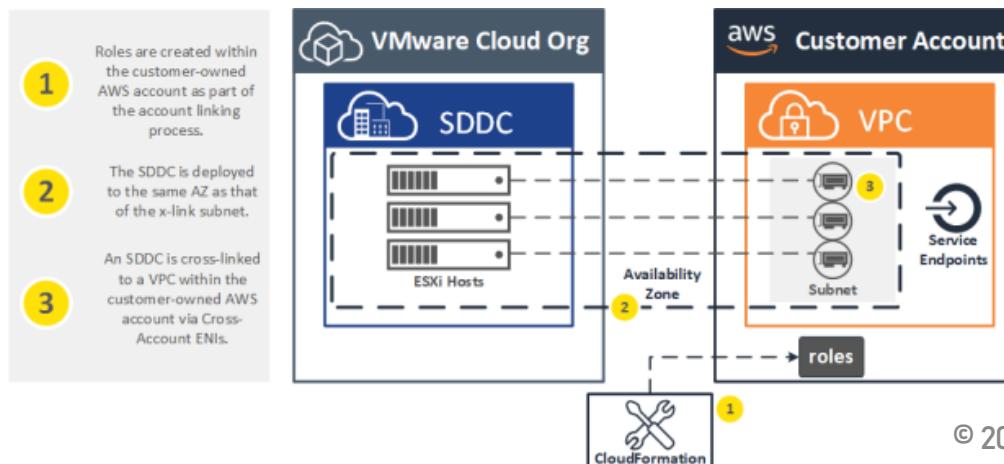
Cores / host	36	48
Memory / host (GiB)	512	768
Storage	NVMe (~10.7 TiB raw storage capacity)	NVMe (~45.8 TiB raw storage capacity)

i3.metal

Good for general purpose clusters. Provides good balance between compute and storage capabilities for most typical workload types.

i3en.metal

This capability is optimized for data-intensive workloads requiring high random I/O access such as relational databases and workloads that require end to end security.



<https://aws.amazon.com/blogs/architecture/augmenting-vmware-cloud-on-aws-workloads-with-native-aws-services/>

Deux offres disponibles

Hôte unique

Vous démarrez ? Profitez de cette option abordable pour démarrer votre expérience du Cloud hybride

Pour un usage hors production uniquement

Inclut :

- Logiciels VMware SDDC : vSphere, vSAN, NSX-T, vCenter Server
- VMware HCX
- Instances bare metal Amazon EC2 dédiées
- Support mondial VMware

Vendu séparément :

- VMware Site Recovery
- VMware Cloud Disaster Recovery
- VMware vRealize Automation Cloud
- VMware vRealize Operations Cloud
- VMware vRealize Log Insight Cloud
- VMware vRealize Network Insight Cloud
- VMware Tanzu Standard

Non pris en charge :

- Gestion du cycle de vie par VMware (mises à jour, correctifs et mises à niveau)
- Haute disponibilité (HA) et clusters étendus
- Contrat de niveau de service (SLA)

Production

Conçu pour les environnements d'entreprise de production

Inclut :

- Logiciels VMware SDDC : vSphere, vSAN, NSX-T, vCenter Server
- VMware HCX
- VMware Tanzu : TKG Service + TMC Essentials
- Instances bare metal Amazon EC2 dédiées
- Support mondial VMware
- Gestion du cycle de vie par VMware (mises à jour, correctifs et mises à niveau)
- Prise en charge de la haute disponibilité (HA) et des clusters étendus
- Contrat de niveau de service (SLA)

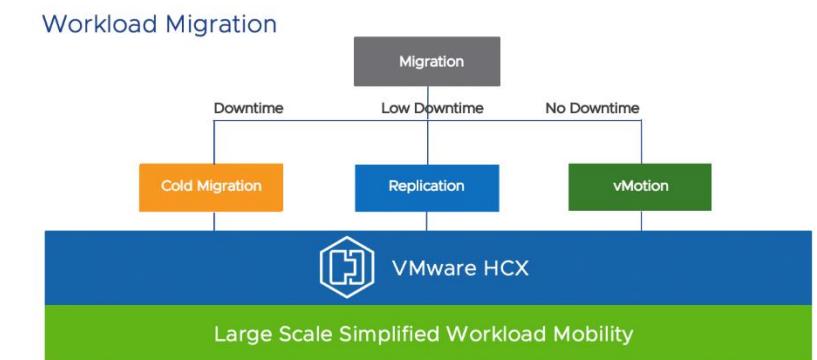
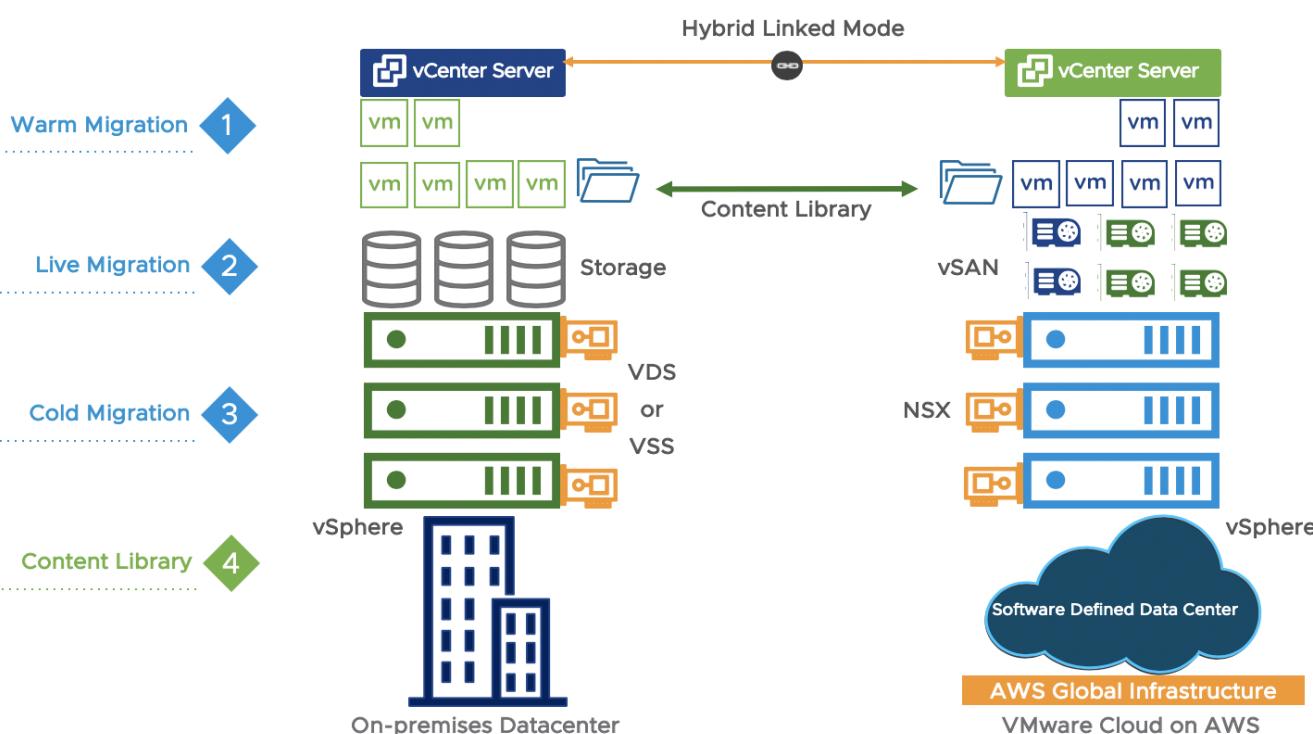
Vendu séparément :

- VMware Site Recovery
- VMware Cloud Disaster Recovery
- VMware NSX Advanced Firewall
- VMware vRealize Automation Cloud
- VMware vRealize Operations Cloud
- VMware vRealize Log Insight Cloud
- VMware vRealize Network Insight Cloud
- VMware Tanzu Standard

* Exemple AWS Europe (Paris)

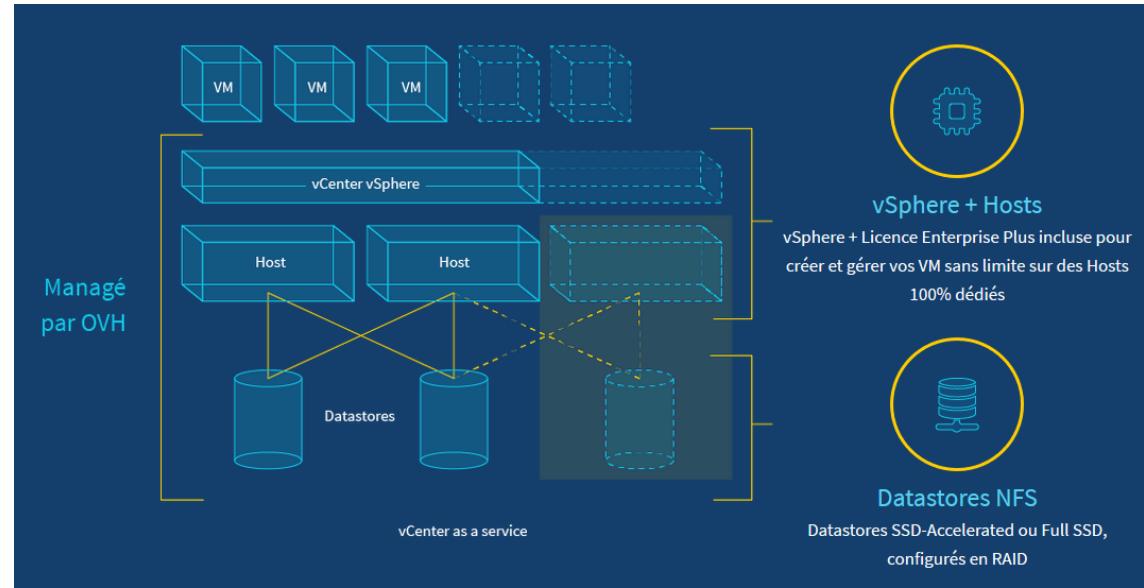
	Single Host	Production Host	
		i3.metal	i3en.metal
Durée d'utilisation	30 jours maximum Un seul hôte simultanément	Sans limitation	
Prix* par heure par hôte (on demand)	€5,76 / heure	€6,89 / heure	€17,59 / heure
Prix* par an par hôte en réservation	N/A	€42 902,98 / 1 an (30%)	€115 284,29 / 1 an (26%)
Prix* pour 3 ans par hôte en réservation	N/A	€89 628,53 / 3 ans (50%)	€248 076,45 / 3 ans (46%)

Hybridation & migration



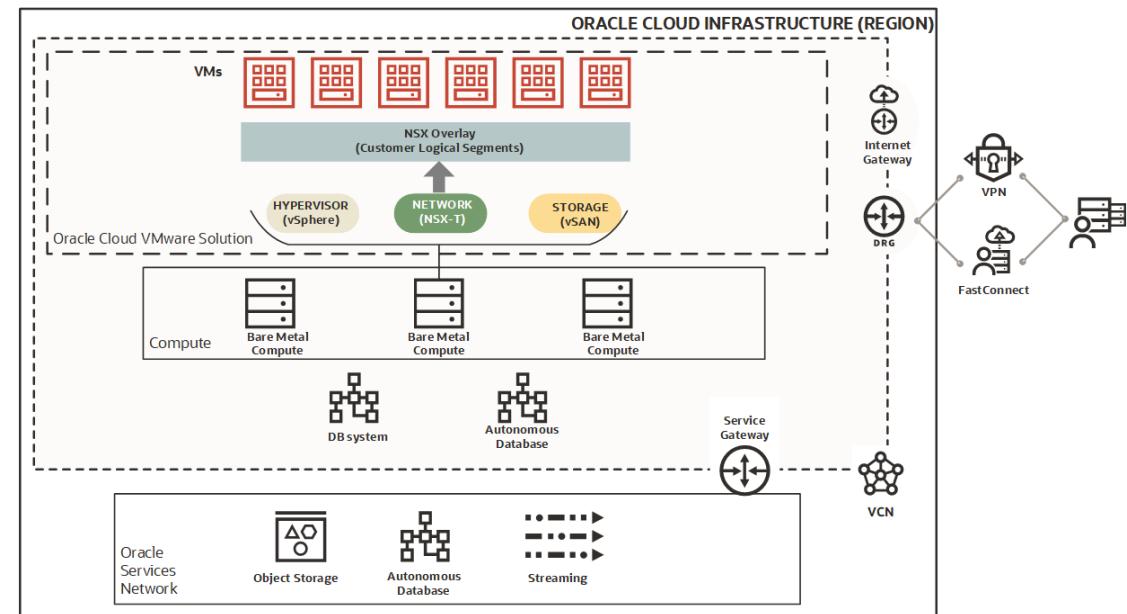
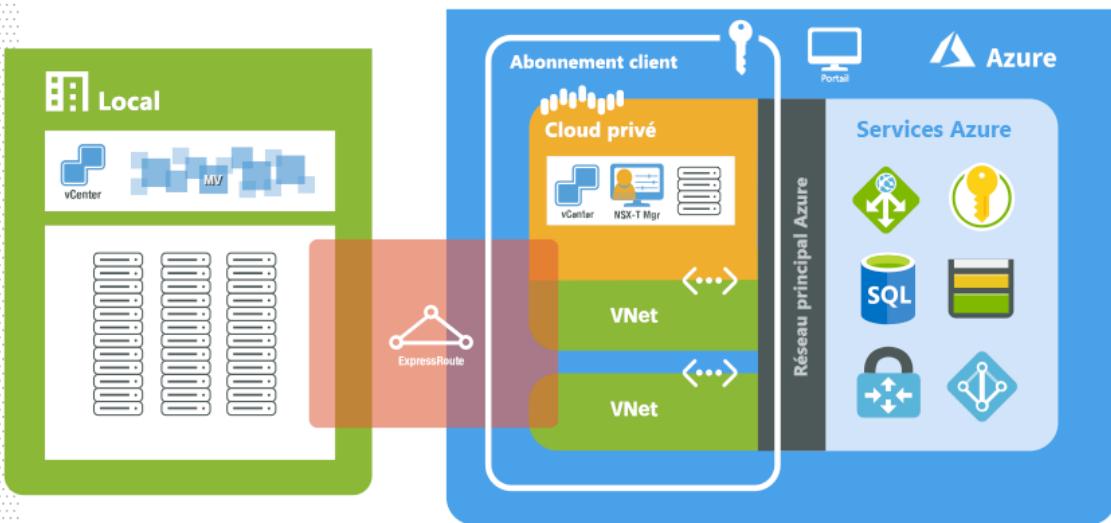
Hosted Private Cloud

- Historiquement vSphere as a Service
 - Serveur physique hôte avec vSphere préinstallé
 - Gestion manuelle des VM
- Hosted Private Cloud
 - Premier Hosted Private Cloud
 - ✓ vSphere, NSX et vRops
 - ✓ Pack de démarrage composé de 2 hôtes minimum
 - Premier VSAN
 - ✓ VSAN en sus
 - ✓ 3 hôtes minimum



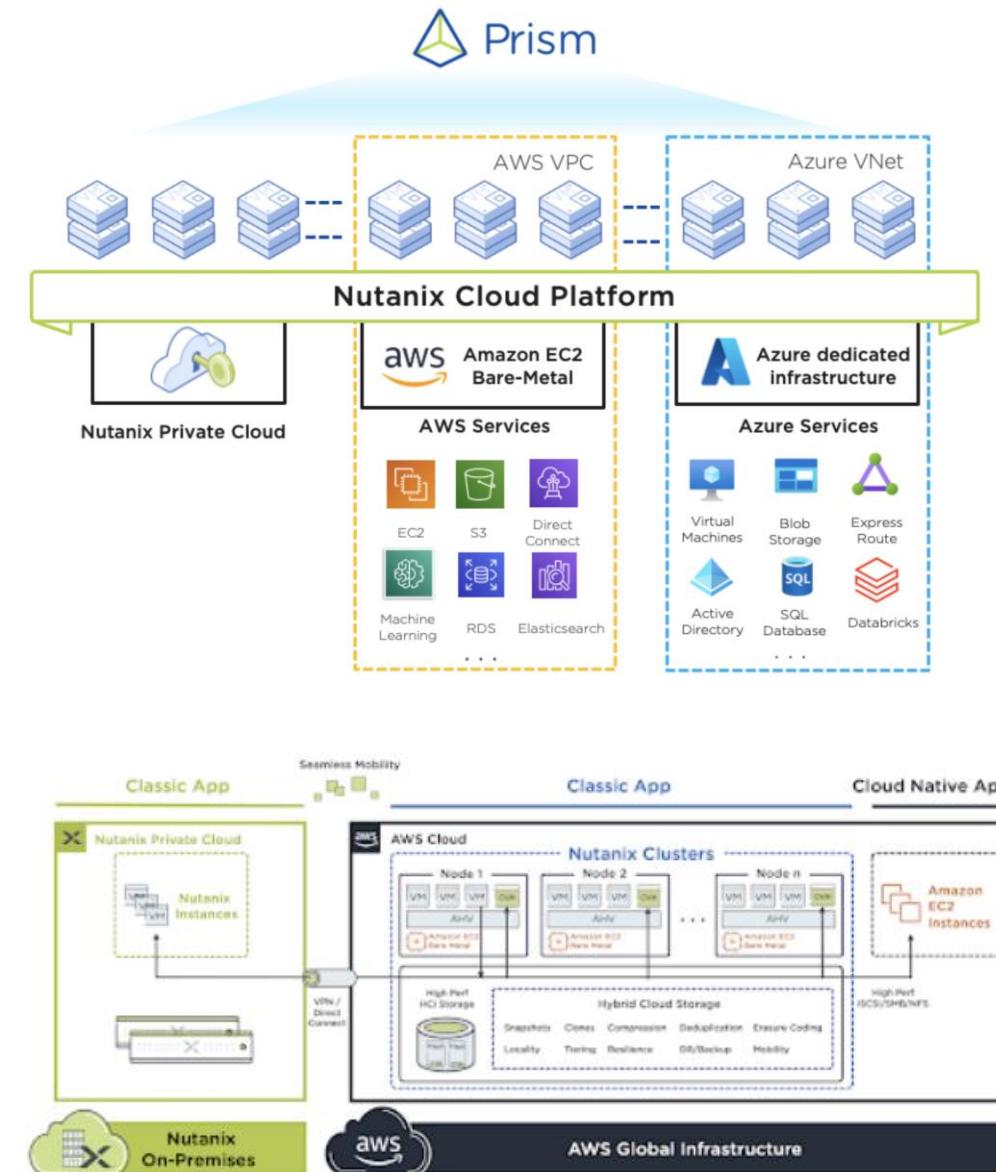
Premier Hosted Private Cloud packs	Standard	Avec certification PCI-DSS	HDS and Health data (Business or Enterprise support required)
PRE 48 (2 hôtes avec chacun 48 Go de RAM et 12 coeurs)	1 171 € HT/mois	1 743 € HT/mois	1 289 € HT/mois
PRE 96 (2 hôtes avec chacun 96 Go de RAM et 12 coeurs)	1 511 € HT/mois	2 309 € HT/mois	1 663 € HT/mois
PRE 192 (2 hôtes avec chacun 192 Go de RAM et 16 coeurs)	1 811 € HT/mois	2 809 € HT/mois	1 993 € HT/mois
PRE 384 (2 hôtes avec chacun 384 Go de RAM et 32 coeurs)	2 711 € HT/mois	4 309 € HT/mois	2 983 € HT/mois
PRE 768 (2 hôtes avec chacun 768 Go de RAM et 32 coeurs)	3 711 € HT/mois	5 975 € HT/mois	4 083 € HT/mois

Les autres offres



La réponse de Nutanix

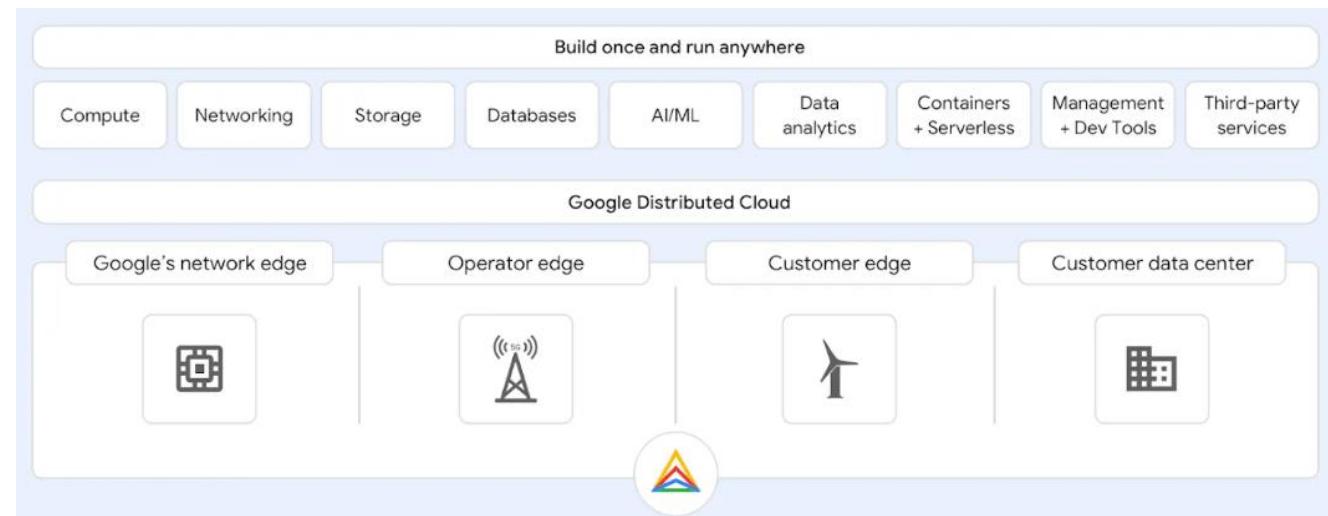
- Nutanix clusters (NC2)
 - Basés sur les offres bare-metal AWS et Azure
 - ✓ Limitations sur les types d'instances et les régions
 - ✓ Potentiellement GCP dans le futur
 - Exécution d'AOS, AHV et Prism
 - ✓ Nutanix Objects bientôt pris en compte
 - Fonctionnalité d'hibernation disponible (uniquement AWS pour le moment)
- Deux philosophies
 - Gestion Nutanix à la charge du client (AWS, Azure...)
 - Service de cluster managé



Cloud privé : des offres des acteurs du cloud public ?

Des nouvelles offres « convergées » ?

- Les gros acteurs du cloud public s'y mettent
- Objectif : étendre leur cloud dans votre datacenter
 - Microsoft Azure Stack
 - AWS Outposts
 - Google Distributed Cloud



Microsoft Azure Stack

- Depuis octobre 2017
 - Historiquement
 - ✓ Achat de la plate-forme matérielle au constructeur
 - ✓ Puis facturation à l'usage par Microsoft
 - « Conçu pour les grandes entreprises »
- Refonte complète en 2020 en trois gammes
 - Azure Stack Hub
 - ✓ Dell-EMC, Lenovo, HPE, Cisco
 - Azure Stack Edge
 - ✓ Microsoft
 - Azure Stack HCI
 - ✓ S2D

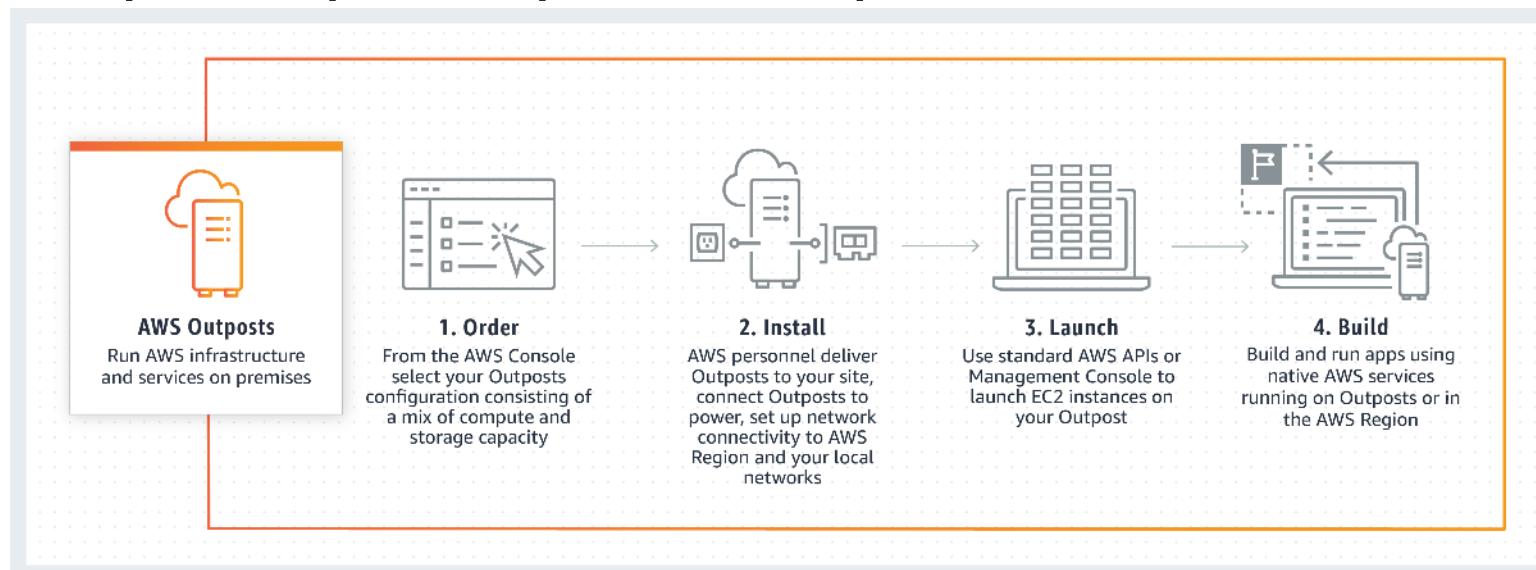


AWS Outposts

■ Historique

- La grande annonce de RelInvent 2018
- Confirmée en 2019...
- Disponibilité générale en fin 2019/2020...
- Valable pour EC2 et VMware

■ 3 ans avec no upfront / partial upfront / All upfront



Des nouvelles offres « convergées » ?

- Les autres acteurs du cloud public s'y mettent mais différemment
 - IBM Cloud Private
 - ✓ Pour développer les futures applications cloud native
 - ✓ Customer-managed
 - Oracle at Customer
 - ✓ Exadata managed par Oracle
 - ✓ Base de données
 - Google GKE on-prem
 - ✓ Google Kubernetes Engine on VMware
- Une exception française
 - Outscale Tina as a Service
 - ✓ Serveurs Cisco UCS + baies Netapp + NVIDIA (vGPU) + KVM

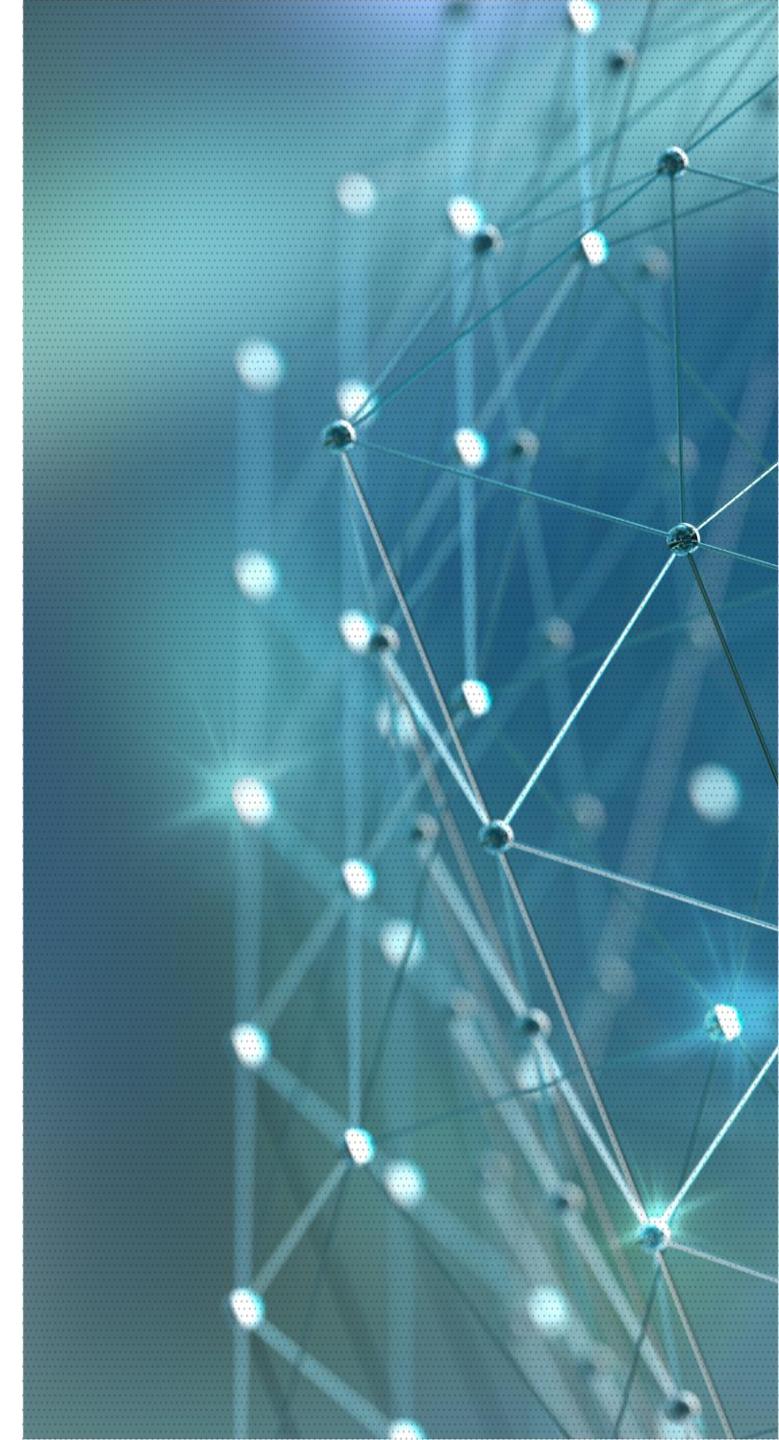


Conclusion

- Il est possible de construire son propre cloud privé avec une hybridation
 - Mais attention ! Construire un cloud privé n'est pas qu'un projet technique
 - ✓ Catalogue de services notamment
 - ✓ Mais la dimension technique existe
 - Ne pas confondre Cloud privé et virtualisation++
 - Virtualisation du réseau
 - Automatisation
 - Orchestration
- Peut-on parler d'Edge Computing ?
 - Ne pas confondre Edge Computing et Cloud privé !
 - Rappelez-vous de la définition
 - ✓ Edge computing
 - Littéralement, traitement (computing) en bordure du réseau
 - Sujet à part entière pour l'IoT ou la 5G (Mobile Edge Computing)
 - Terme également utilisé dans le cloud hybride généralement par abus de langage



Conclusion



Questions



Didier MEIER

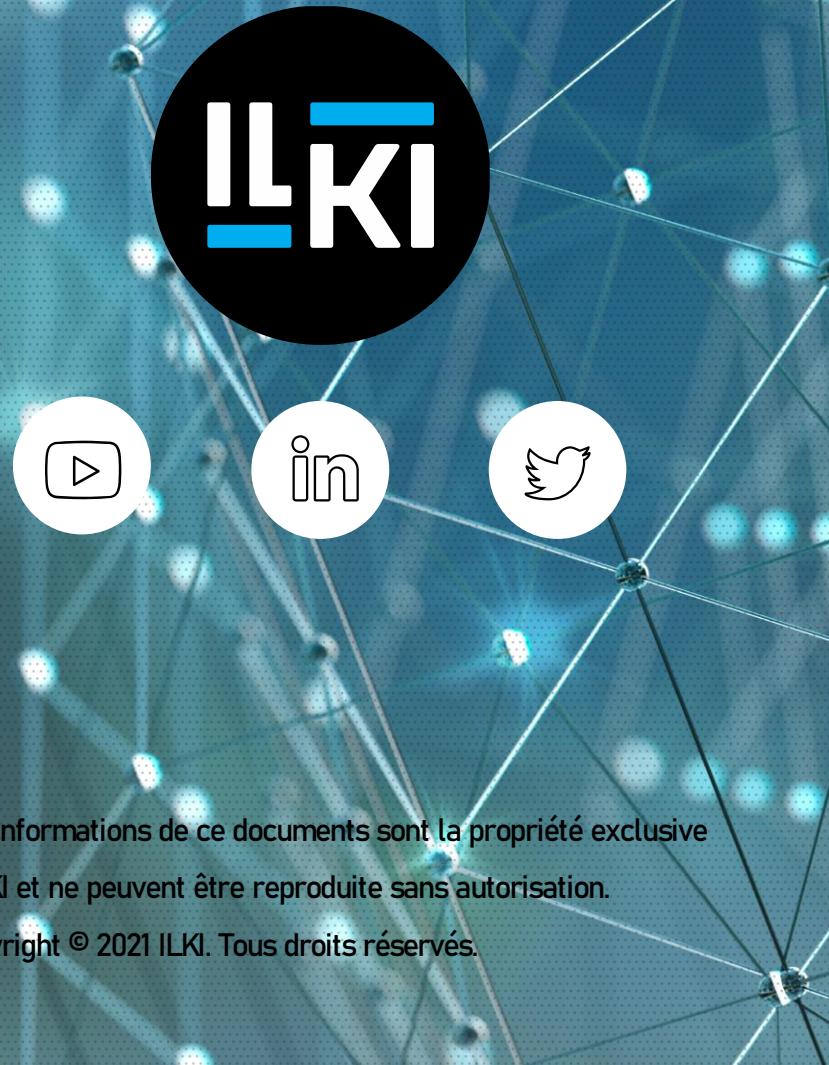
Consultant Cloud & IoT - Associé

Directeur des Opérations - Responsable des
Formations et de l'offre IoT

didier.meier@ilki.fr

www.ilki.fr

Questions



À propos d'ILKI

ILKI accompagne les entreprises dans leurs transitions technologiques en faisant évoluer leurs système d'information en intégrant : Cloud computing, Cloud Native, Digital workplace... Sa mission est d'aider les organisations à mieux appréhender les problématiques techniques, méthodologiques, organisationnelles et financières liées à ces transitions technologiques.

Pour plus d'informations

www.ilki.fr