



Virtualisation des serveurs & Cloud Computing

ALI.WALI@ISIMS.USF.TN

SAHAR.KALLEL@ISIMS.USF.TN

Objectifs du cours

- ▶ Comprendre les principes de la virtualisation;
- ▶ Manipuler les concepts de la virtualisation à travers des outils pratiques;
- ▶ Découvrir la notion du cloud computing et ses applications

Plan de cours

- ▶ **Chapitre 1 -Principes de la virtualisation**
 - ▶ I. Introduction
 - ▶ II. Définition
 - ▶ III. Les domaines de la virtualisation
 - 1. La virtualisation d'applications
 - 2. La virtualisation de réseaux
 - 3. La virtualisation de stockage
 - 4. La virtualisation de serveurs
- ▶ IV. Avantages & inconvénients de la virtualisation
- ▶ V. Les différents types de virtualisation
 - 1. la virtualisation complète ;
 - 2. la para-virtualisation;
 - 3. La virtualisation assistée par le matériel ;
 - 4. le cloisonnement.
- ▶ VI . Les Objectifs de virtualisation

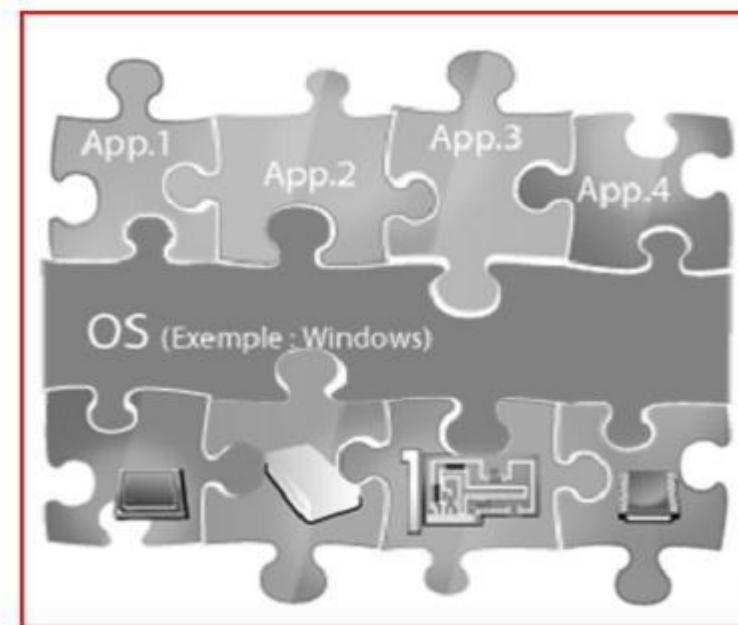
Plan de cours

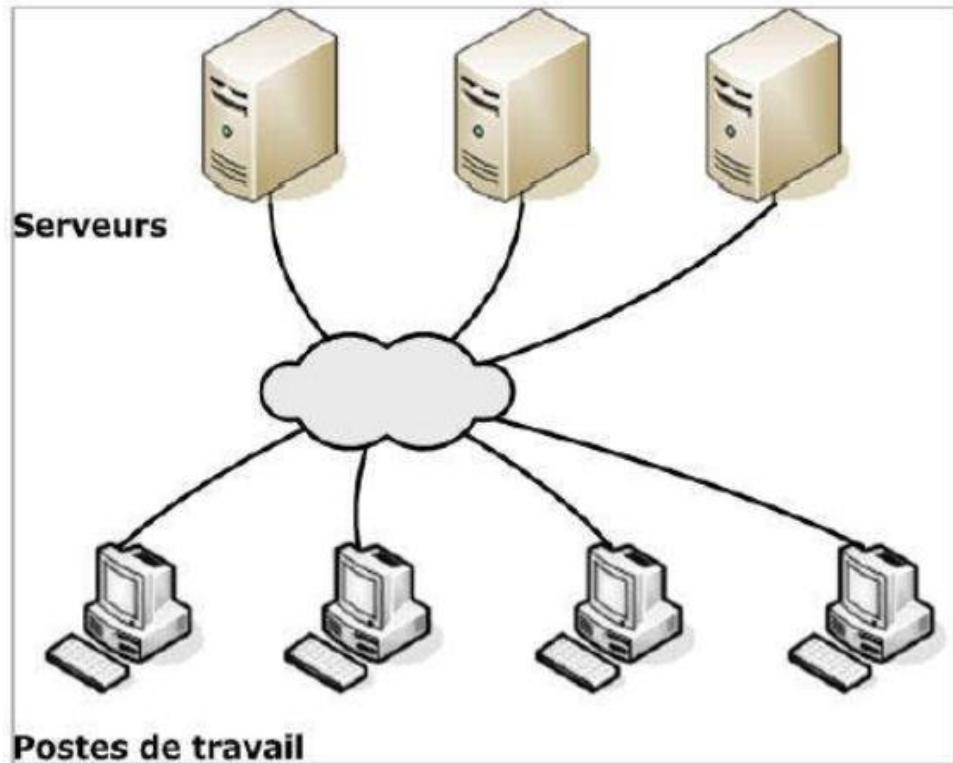
- ▶ **Chapitre 2: Virtualisation: étude de cas**
- ▶ **Chapitre 3: Cloud computing**
 - ▶ I. Introduction
 - ▶ II. Définition du « Cloud Computing» ou informatique en nuage
 - ▶ III. Historique du Cloud Computing
 - ▶ IV. Les différents services de Cloud Computing
 - ▶ V. Les différentes typologies de Cloud Computing
- ▶ **Chapitre 4: Cloud computing: étude de cas**

Chapitre 1: Principe de la virtualisation

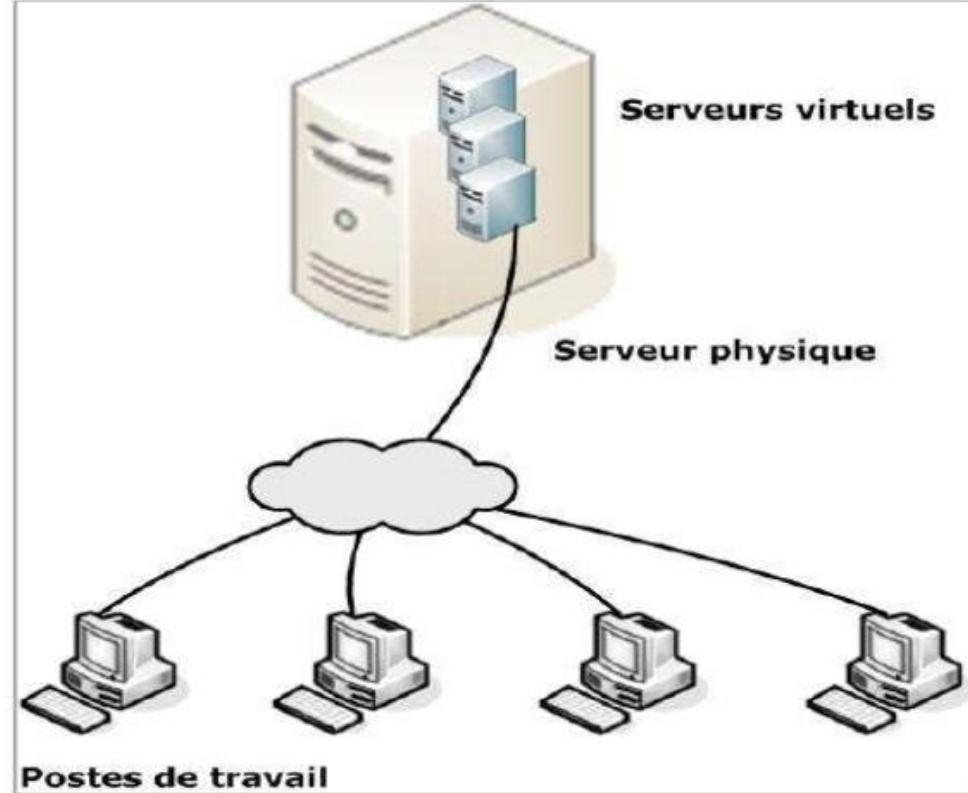
Objectif Général	Comprendre les principes de la virtualisation.
Objectif Spécifiques	<ul style="list-style-type: none">• Savoir définir le concept de la virtualisation.• Prendre connaissance des domaines de la virtualisation.• Déterminer les avantages et les inconvénients de la virtualisation.• Comprendre les différents types de la virtualisation.
Volume horaire	Cours: 10h
Mots clés	virtualisation, domaines, application, stockage, serveur, réseaux, types,...

- A l'origine, le matériel informatique dont nous disposions a été conçu pour n'exécuter qu'un seul système d'exploitation et une application, puis plusieurs applications.





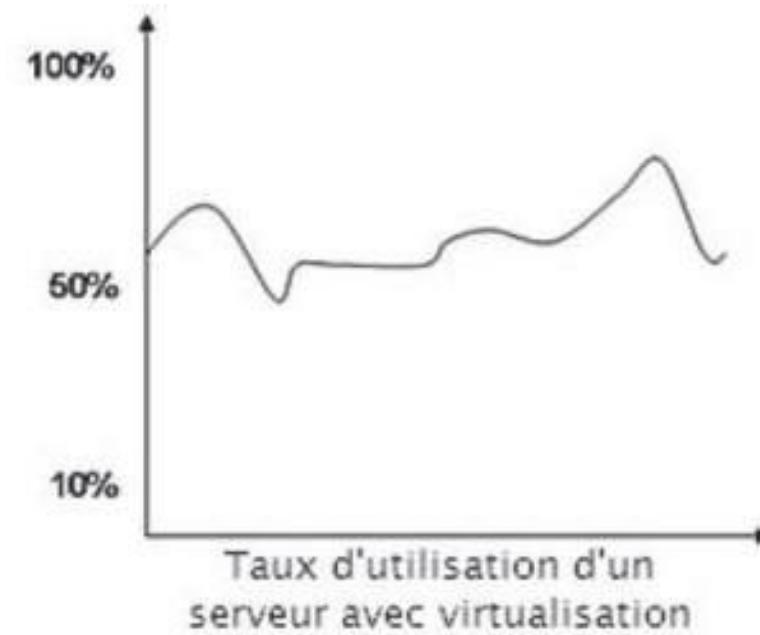
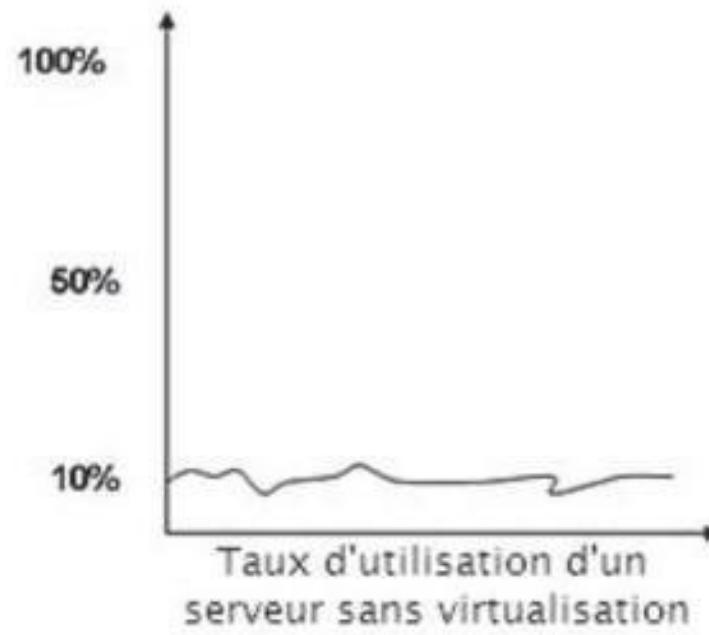
Architecture traditionnelle

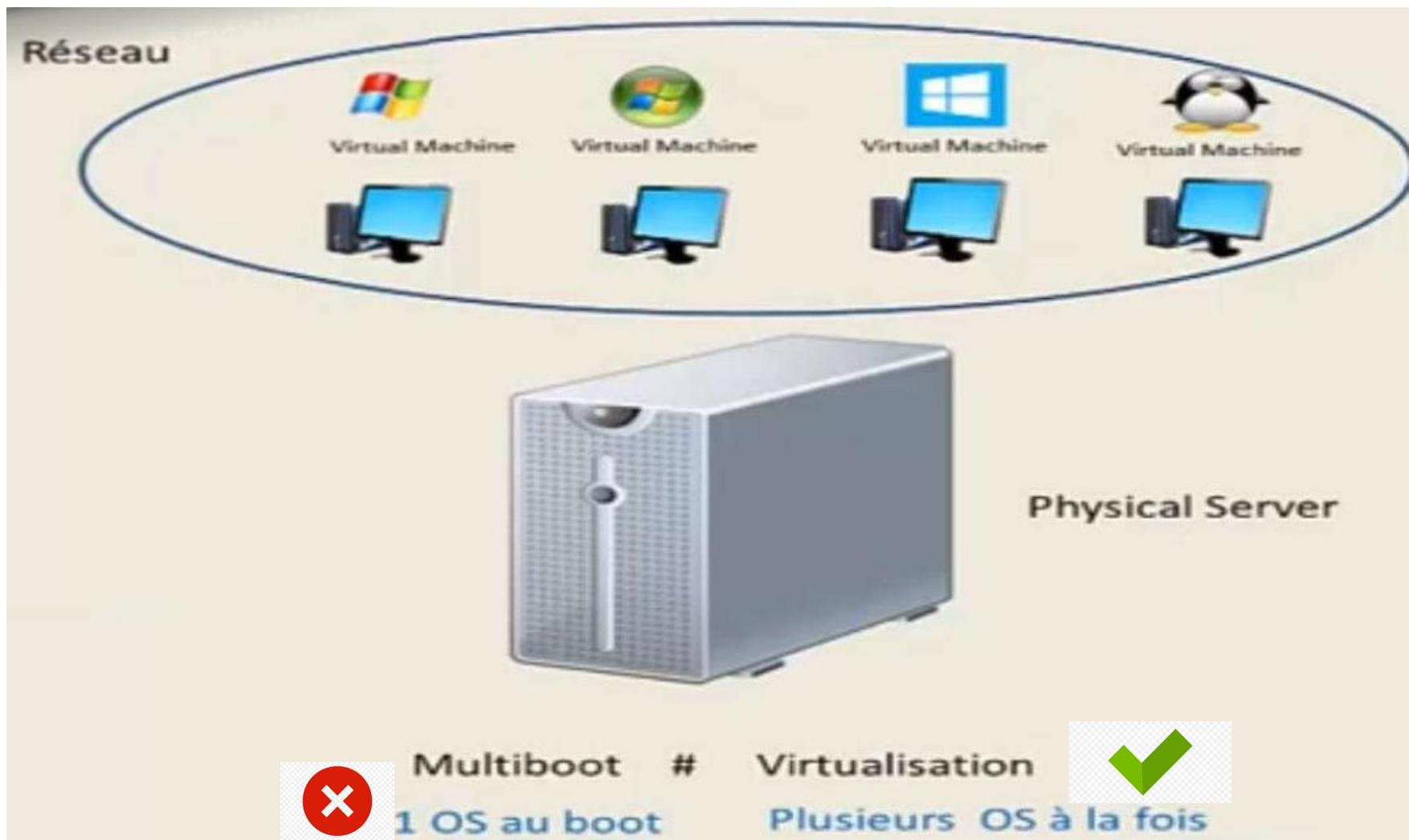


Architecture virtualisée

Le principe de la virtualisation est donc un principe de *partage* : les différents systèmes d'exploitation se partagent les ressources du serveur.

- La plupart des serveurs en entreprise n'exploitent qu'environ 10 à 15 % des ressources matérielle (sans virtualisation).



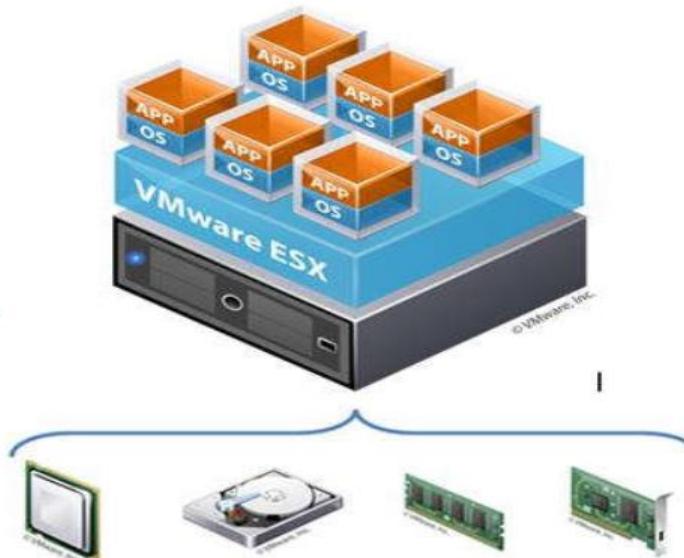
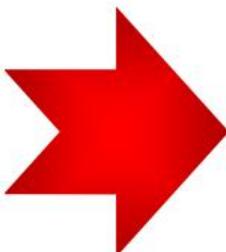


Qu'est-ce que la Virtualisation?

- Ensemble de techniques permettant de faire tourner plusieurs systèmes d'exploitation sur une même machine physique.



- 1 système d'exploitation / machine
- Exécution de **plusieurs** applications / serveur augmente le risque d'interruption de service global
- En général, **1 serveur = 1 application**



Chaque machine possède ses propres applications et OS

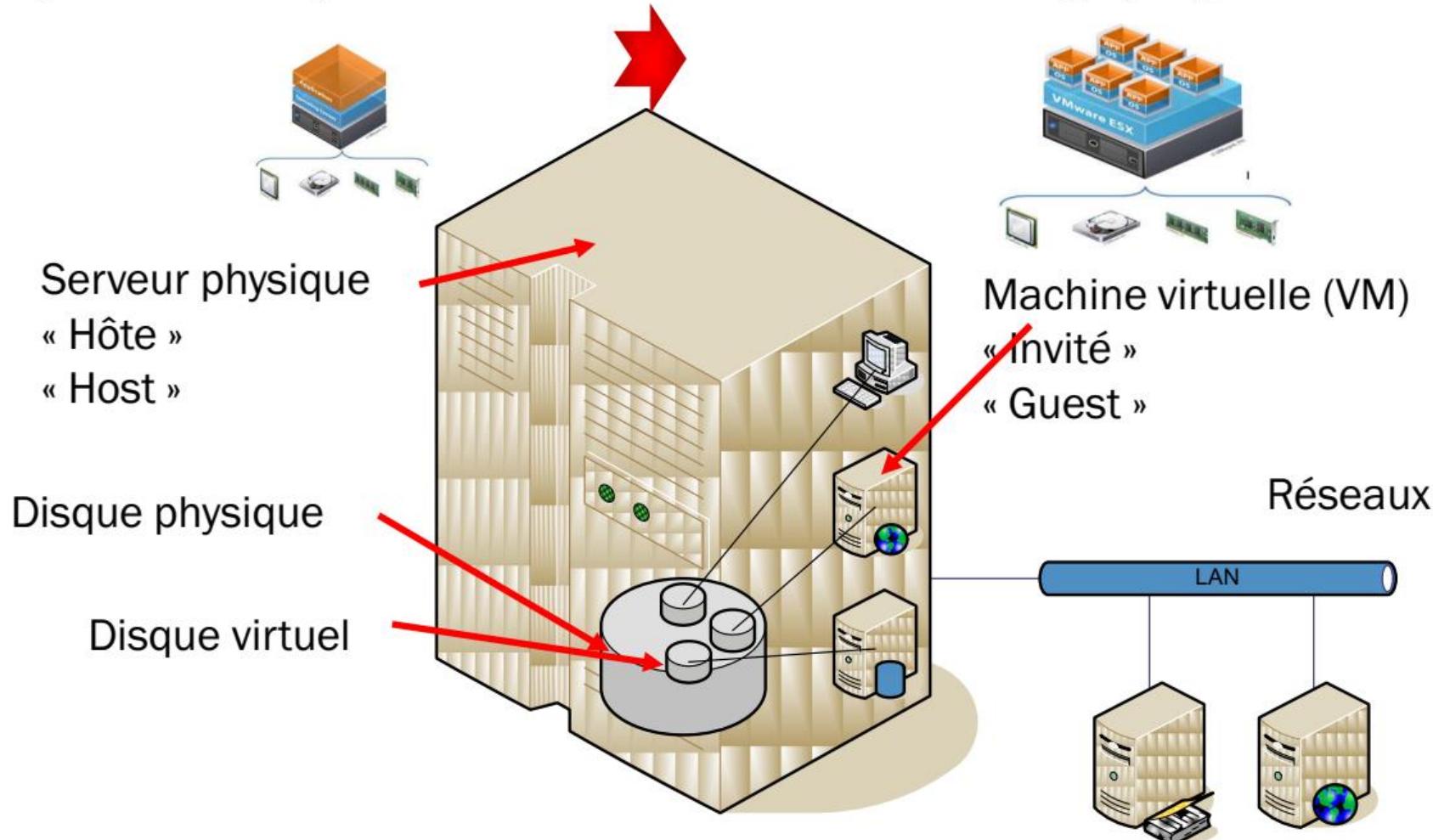
Qu'est-ce que la Virtualisation?

La virtualisation consiste à virtualiser l'environnement matériel
c'est-à-dire:

- Le processeur, la mémoire vive, le disque dur, le réseau et les divers autres périphériques d'entrées/sorties.
- Une machine virtuelle se comporte donc exactement comme un ordinateur physique et contient ses propres ressources matérielles **qui sont alors virtuelles** (logicielles).
- L'autonomie de chaque machine virtuelle rend la solution complètement transparente pour l'utilisateur et toutes autres actions.

Qu'est-ce que la Virtualisation?

- Ensemble de techniques permettant de faire tourner plusieurs systèmes d'exploitation sur une même machine physique.



Qu'est-ce que la Virtualisation?

Chaque **outil de virtualisation** met en œuvre **une ou plusieurs de ces notions** :

- **Une couche d'abstraction matérielle et/ou logicielle**
- Un système d'exploitation **hôte** (installé directement sur le matériel)
- Des systèmes d'exploitation (ou applications, ou encore ensemble d'applications) « **virtualisé(s)** » ou « **invité(s)** »
- Un **partitionnement, isolation** et/ou partage des ressources physiques et/ou logicielles
- Des **images manipulables** : démarrage, arrêt, clonage, sauvegarde et restauration, sauvegarde de contexte, migration d'une machine physique à une autre.
- Un **réseau virtuel** : réseau purement logiciel, interne à la machine hôte, entre hôte et/ou invités

Pourquoi virtualiser?

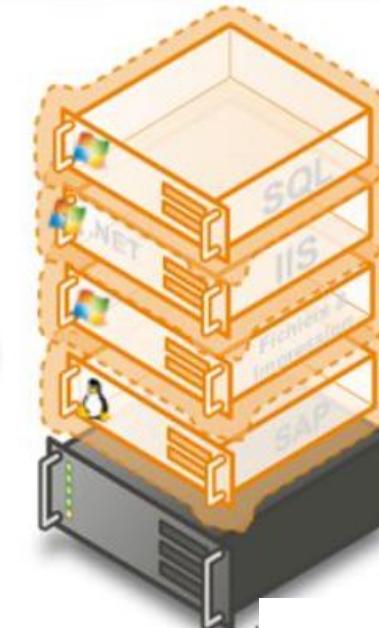
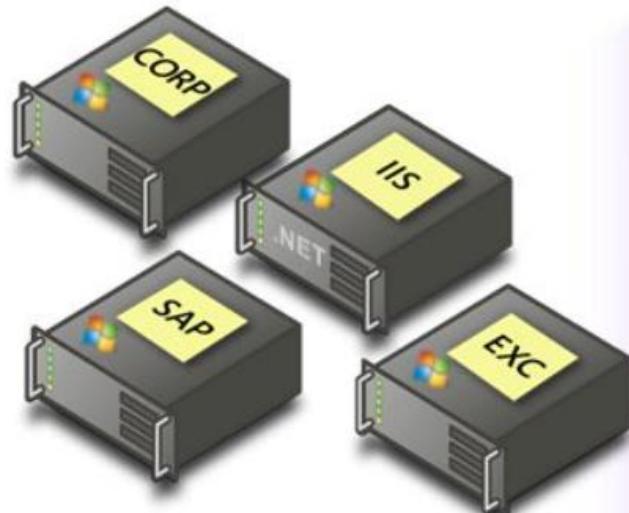
#1: Optimisation des performances et de l'efficacité

Défis :

Coûts des locaux
Surcharge dans l'administration
Faible utilisation par serveur
Coûts : électricité et climatisation
Impact sur l'environnement.

Solution :

Consolidation matérielle
Simplification dans l'administration des systèmes
Rationalisation dans les centre de données
Responsabilités environnementales



Pourquoi virtualiser?

#2: Accroissement de la disponibilité

Défis :

Impact de l'arrêt d'un serveur ou d'une application

Respect des niveaux de service

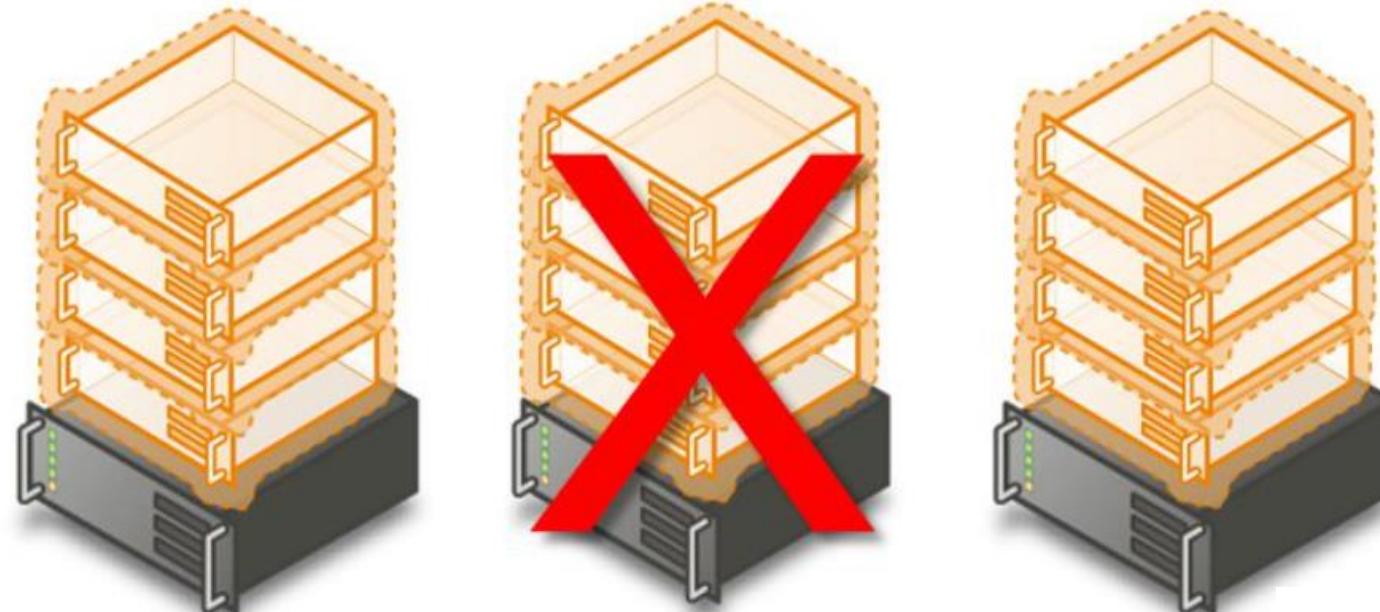
Systèmes critiques pour l'entreprise

Solution :

Continuité métier pour un coût raisonnable

Homogénéité des solutions de tolérance aux pannes

Basculement rapide en cas de panne



Pourquoi virtualiser?

#3: Meilleure flexibilité

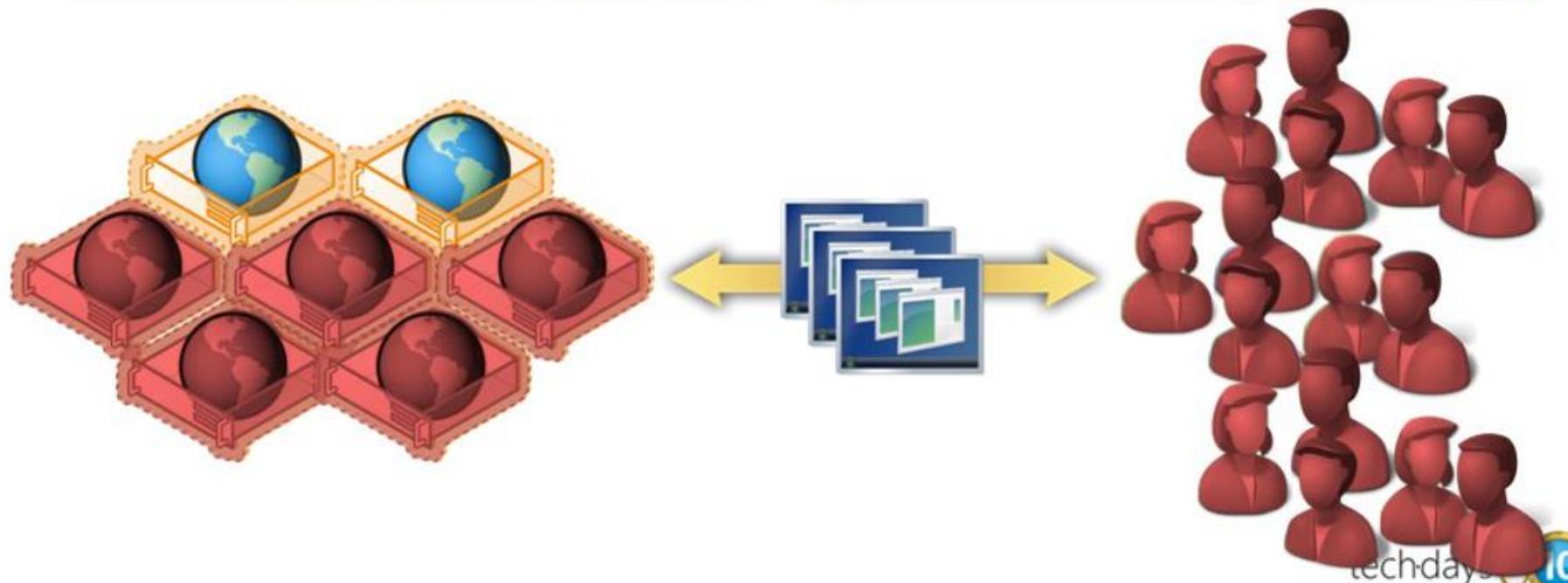
Défis :

Difficulté de faire face à des pics d'activité

Systèmes surdimensionnés et sous-employés

Solution :

Un centre de données capable de s'adapter en fonction de l'évolution planifiée ou non de la demande



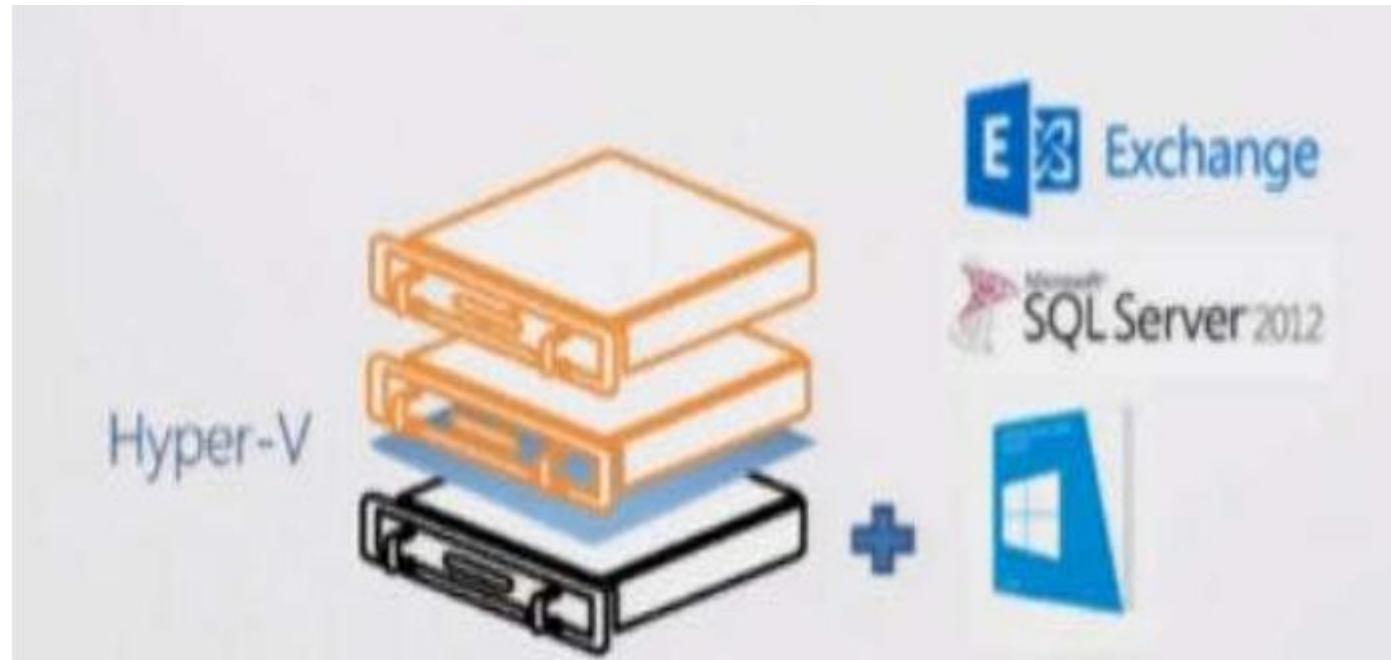
Les formes de la virtualisation

Il existe 3 formes :

- la virtualisation de matériel
- la virtualisation de présentation
- la virtualisation d'application

La virtualisation de matériel

— C'est le fait de faire tourner plusieurs environnements sur le même système physique



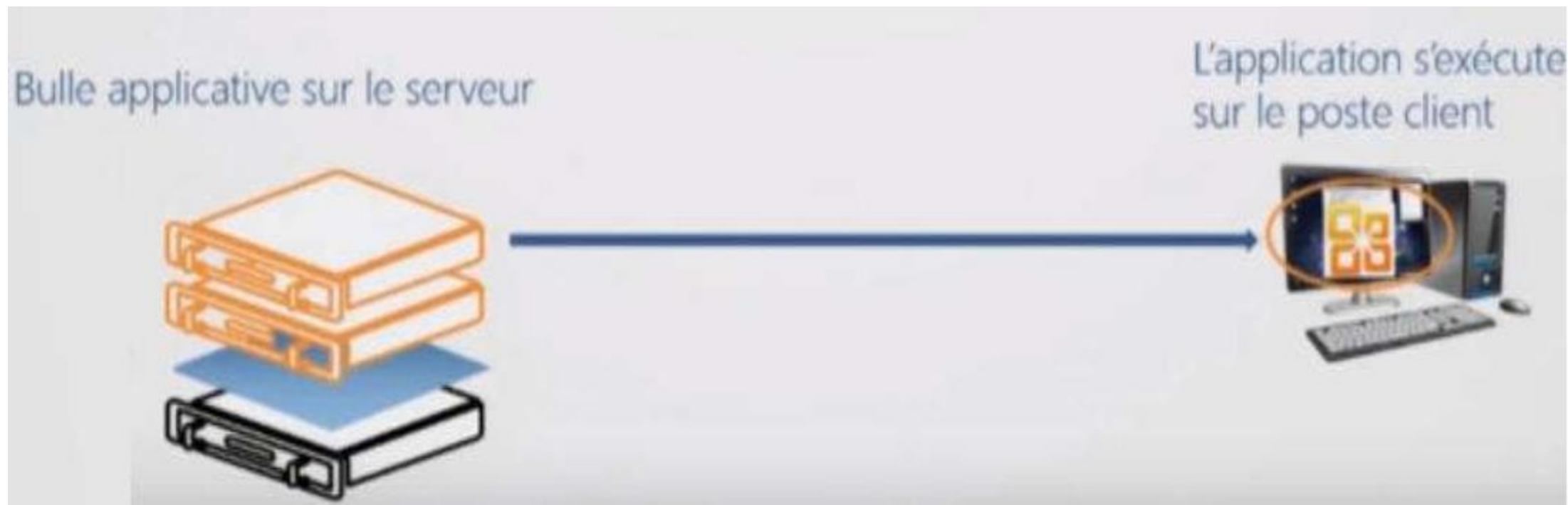
La virtualisation de présentation

Consiste à exécuter des applications de manière centralisé sur des serveurs et déporter l'affichage sur des poste client « Remote control service »

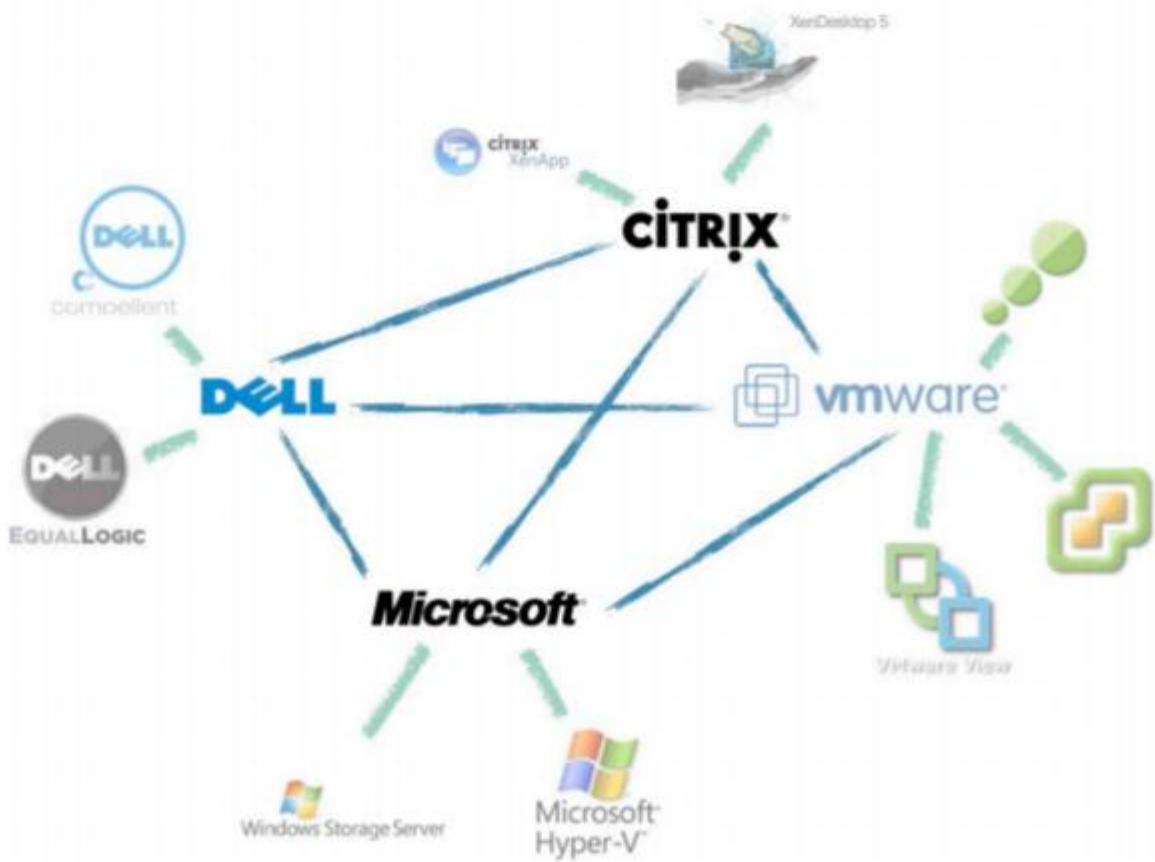


La virtualisation d'application

Permet de distribuer sur un poste client des applications métiers sans perturber le système d'application



Les produits de virtualisation

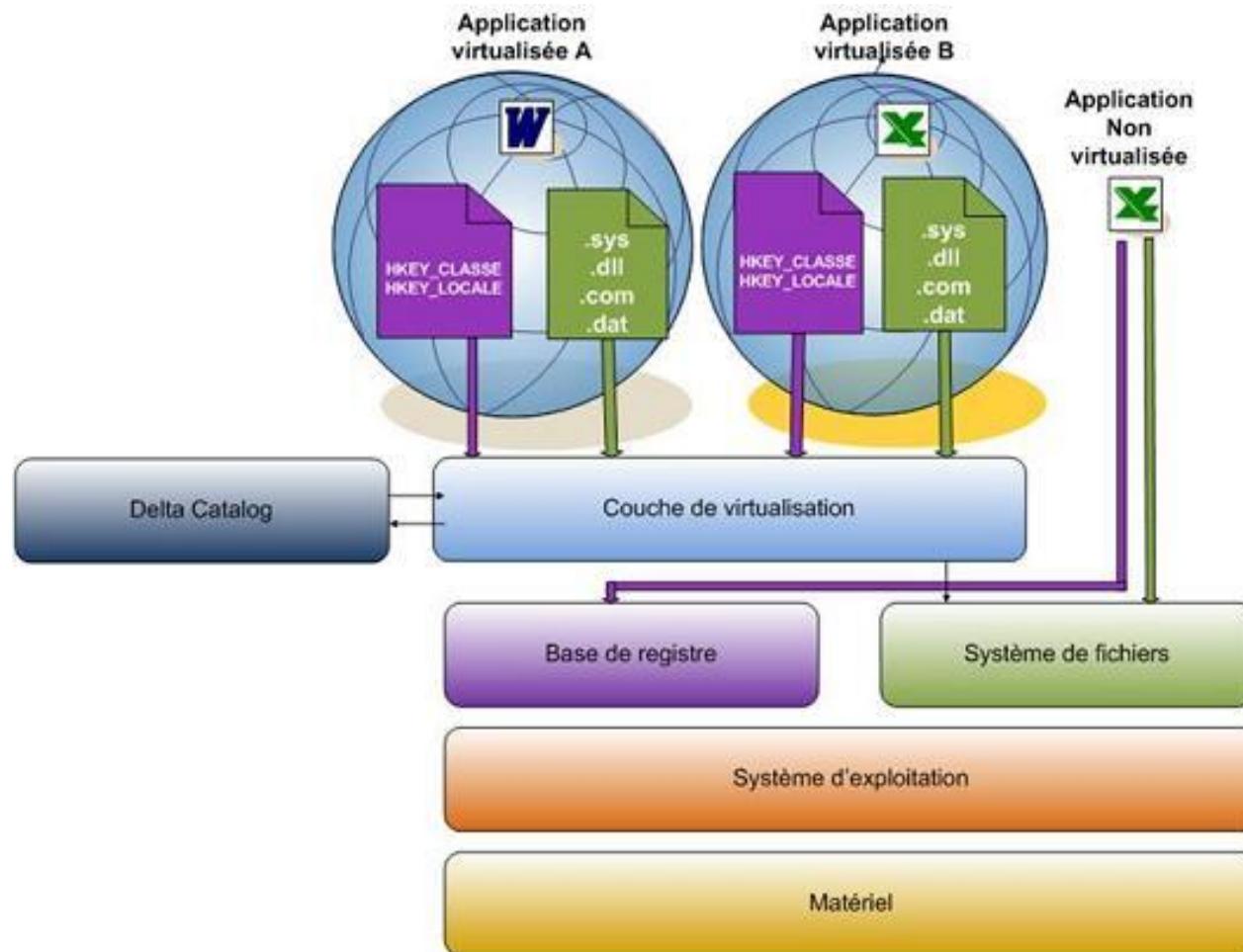


Les domaines de la virtualisation

- La virtualisation d'application consiste à encapsuler dans un même package l'application et son environnement système de manière imperméable au système d'exploitation sur lequel l'application s'exécute.
- Ainsi plusieurs applications peuvent tourner sur un même système sans avoir d'incompatibilités de versions de bibliothèques « dll », de clés de registre et il est même possible de faire tourner plusieurs versions d'une même application sur un même système d'exploitation (exemple : applications Microsoft Office).
- Cette technologie est essentiellement utilisée dans les environnements Windows mais il existe également des outils Linux qui utilisent ce concept (Klik).

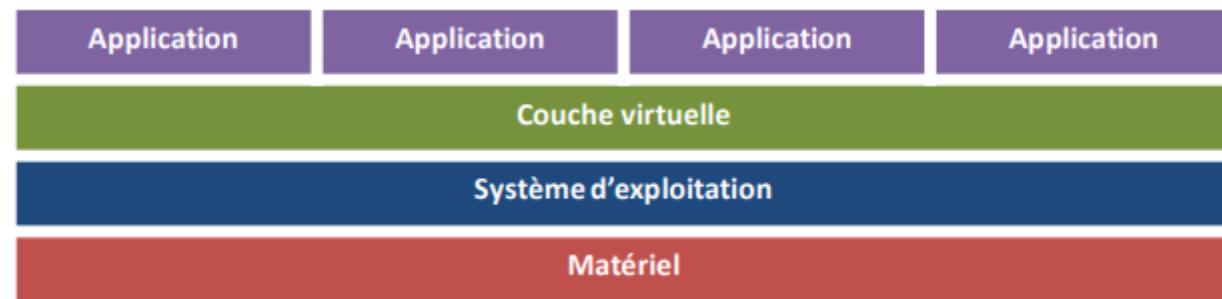
Virtualisation d'application

Les domaines de la virtualisation



Virtualisation d'application

Les domaines de la virtualisation



- On peut dire que la couche virtuelle va ajouter des avantages au système virtualisé en permettant d'exécuter des applications conçues pour d'autres systèmes.

Exemple : Wine est un logiciel qui permet d'exécuter certains programmes Windows sous Ubuntu. <http://www.winehq.org/>

- On peut aussi citer l'avantage gagné au niveau de la protection du système d'exploitation hôte en s'assurant que l'application virtualisée ne viendra pas interagir avec les fichiers de configuration du système.

Les domaines de la virtualisation

- De manière générale, la virtualisation des réseaux consiste à partager une même infrastructure physique (débit des liens, ressources CPU des routeurs,...) au profit de plusieurs réseaux virtuels isolés.
- Un VLAN (Virtual Local Area Network) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

- **Les réseaux virtuels de niveau 1:** appelés réseaux virtuels par port (port based VLAN);
- **Les réseaux virtuels de niveau 2:** appelés réseaux virtuels par adresse MAC (MAC address-based VLAN);
- **Les réseaux virtuels de niveau 3:** Les réseaux virtuels par adresse de sous réseau (Network address-based VLAN) et Les réseaux virtuels par protocole (Protocol-based VLAN).

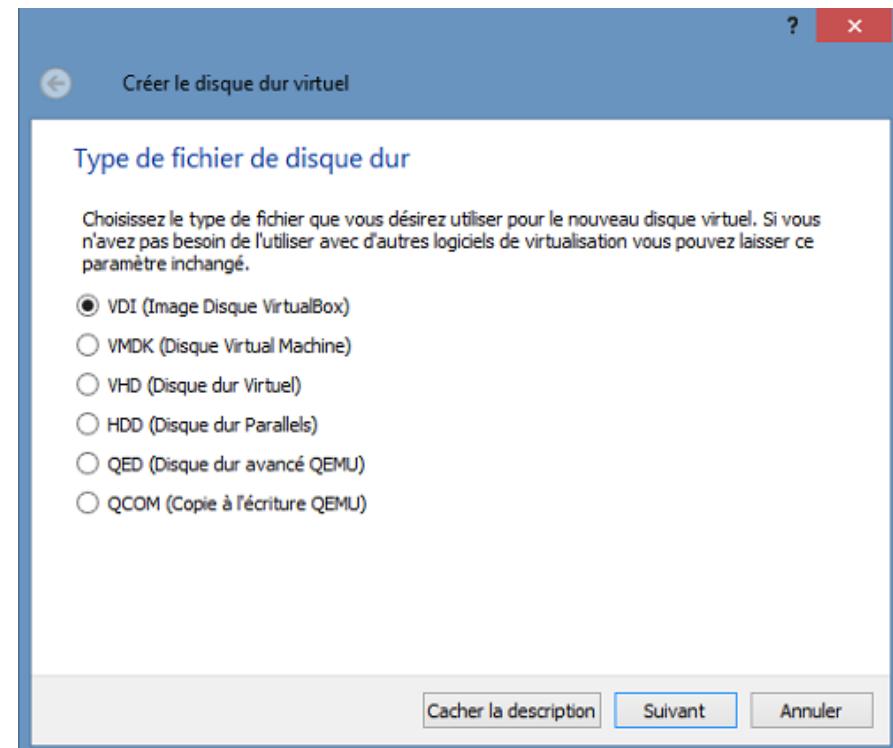
Les domaines de la virtualisation

- Les avantages qu'offrent les réseaux virtuels sont les suivants :
 - Une réduction du traffic de diffusion, puisque celui-ci est à présent contenu au sein de chaque réseau virtuel ;
 - Une sécurité accrue puisque l'information est encapsulée dans une couche supplémentaire ;
 - Une meilleure flexibilité puisqu'une modification de la structure des réseaux peut être réalisée en modifiant la configuration du commutateur.

Virtualisation de stockage

Les domaines de la virtualisation

- Dans une machine virtuelle, les données sont stockées sur un disque dur virtuel.
- Ce disque dur se présente **sous forme de fichier dans le système de fichiers** de l'hôte :
 - VHD chez Microsoft
 - VDI chez Oracle
 - VMDK chez VMWare
 - OVF format ouvert



Virtualisation de stockage

Les domaines de la virtualisation

- Les disques virtuels peuvent être statiques ou dynamiques.
- Dans le cas où le disque est statique, si on crée un disque de 50 Go, le fichier de disque virtuel fera 50 Go sur le système hôte.
- Avec un disque dynamique, le fichier de disque virtuel se remplit au fur et à mesure qu'il est utilisé.
- **Un disque de 50 Go dans lequel il n'y a pas de données ne pèsera dans le système de fichiers hôte grande chose.**

Les domaines de la virtualisation

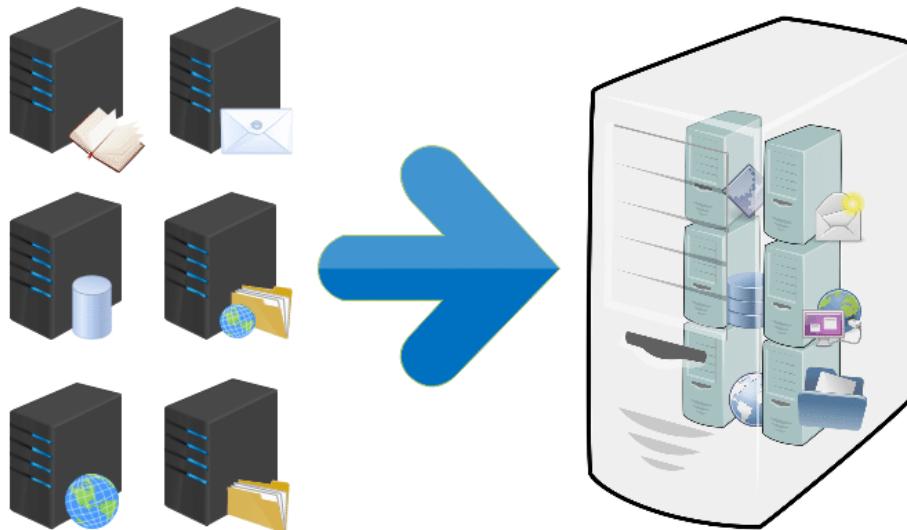
➤ La virtualisation de stockage permet :

- d'adjoindre un périphérique de stockage supplémentaire sans interruption des services;
- de regrouper des unités de disques durs de différentes vitesses, de différentes tailles et de différents constructeurs ;
- de réallouer dynamiquement de l'espace de stockage;
- de fournir des fonctionnalités avancées dans le domaine du **stockage** informatique.
- en particulier de fédérer les volumes en une ressource unique.

Virtualisation de serveurs

Les domaines de la virtualisation

- Cette technique permet aux entreprises d'utiliser des serveurs virtuels en lieu et place de serveurs physiques.
- Si cette virtualisation est faite au sein de la même entreprise, le but est de mieux utiliser la capacité de chaque serveur par une mise en commun de leur capacité.



Virtualisation de serveurs

Les domaines de la virtualisation

- La virtualisation de serveurs permet de :
 - Regrouper plusieurs serveurs physiques sous-employés sur un seul hôte qui exécute des systèmes virtuels ;
 - Réduire la surface au sol, la consommation électrique, le besoin de climatisation et le nombre d'administrateurs ;
 - Réaliser des économies (locaux, consommation électrique, personnel).

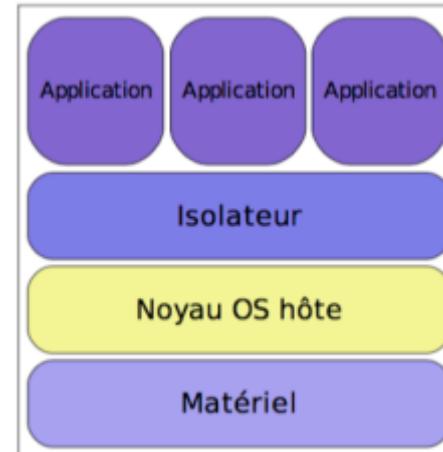
Les 3 variantes d'architecture de virtualisation

- La virtualisation doit s'adapter aux différentes briques technologiques d'une infrastructure.
- 3 variantes d'architecture de virtualisation existent:
 - L'isolateur,
 - L'émulateur,
 - L'hyperviseur et para-virtualisateur

L'isolateur

Les 3 variantes d'architecture de virtualisation

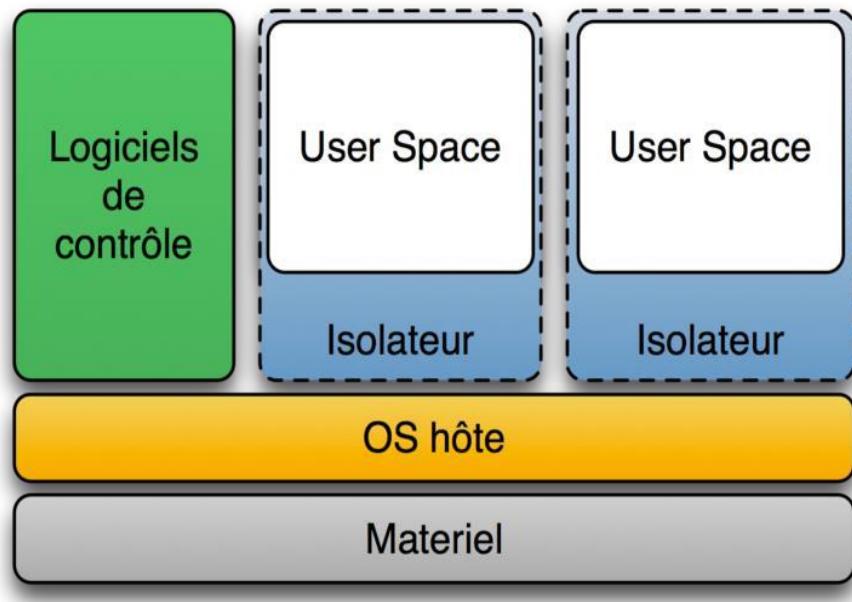
- Un isolateur est un logiciel permettant d'isoler l'exécution des applications dans des contextes ou zones d'exécution, c'est l'archétype de la solution de virtualisation par "juxtaposition".
- L'isolateur permet ainsi de faire tourner plusieurs fois la même application (à base d'un ou plusieurs logiciels) prévue pour ne tourner qu'à une seule instance par machine.



L'isolateur

Les 3 variantes d'architecture de virtualisation

- Cependant, on ne peut pas parler de virtualisation de systèmes d'exploitation car l'isolation ne consiste à virtualiser que des applications.
- Il s'agit de la technique de virtualisation la plus « légère » qui existe.
- On pourrait par contre avoir plusieurs instances de Tomcat qui écoutent sur le même port, plusieurs Apaches sur le port 80 etc.



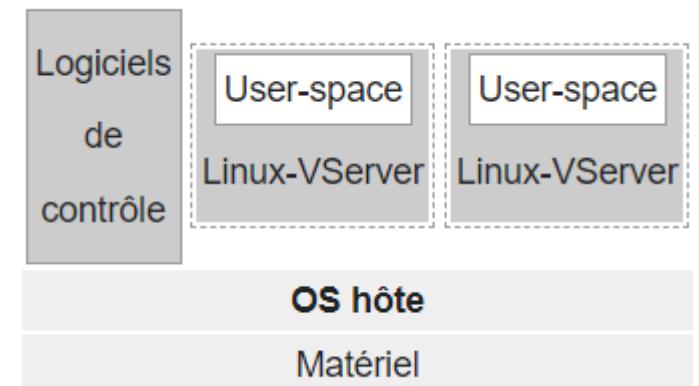
L'isolateur

Les 3 variantes d'architecture de virtualisation

➤ Quelques isolateurs :

- Linux-VServer: isolation des processus en user-space, (Ce projet permet d'exécuter un ou plusieurs environnements d'exploitation « systèmes d'exploitation sans le noyau » ; autrement dit, il permet d'exécuter une ou plusieurs distributions sur une distribution.)
- BSD Jail: isolation en user-space,
- OpenVZ: libre, partitionnement au niveau noyau sous Linux et Windows2003.

C'est la version open-source du logiciel Virtuozzo.



L'émulateur

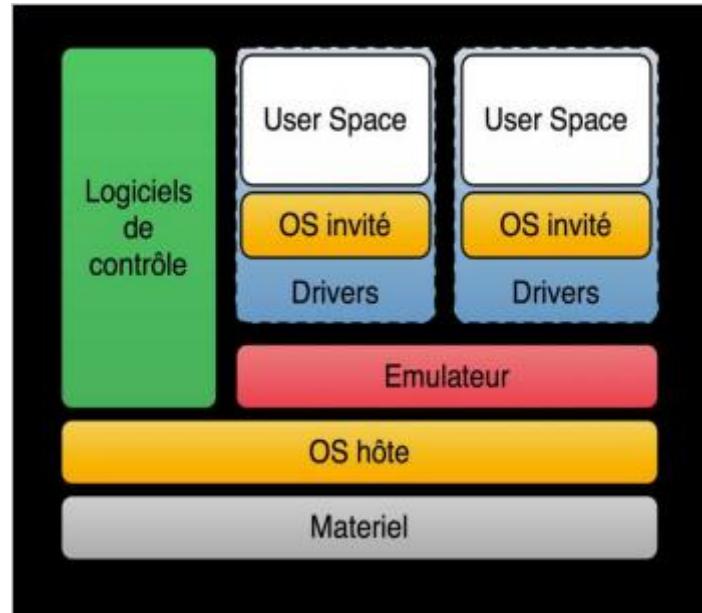
Les 3 variantes d'architecture de virtualisation

- La définition du terme émuler est « simuler, sur un ordinateur, le comportement de ».
- Il faut voir dans l'émulation une **imitation du comportement physique d'un matériel par un logiciel**, et ne pas le confondre avec la simulation, laquelle vise à imiter un modèle abstrait.
- L'émulateur reproduit le comportement d'un modèle dont toutes les variables sont connues, alors que le simulateur tente de reproduire un modèle mais en devant extrapoler une partie des variables qui lui sont inconnues.
- En conclusion, l'émulation consiste à simuler l'exécution d'un programme en interprétant chacune des instructions destinées au micro-processeur.

L'émulateur

Les 3 variantes d'architecture de virtualisation

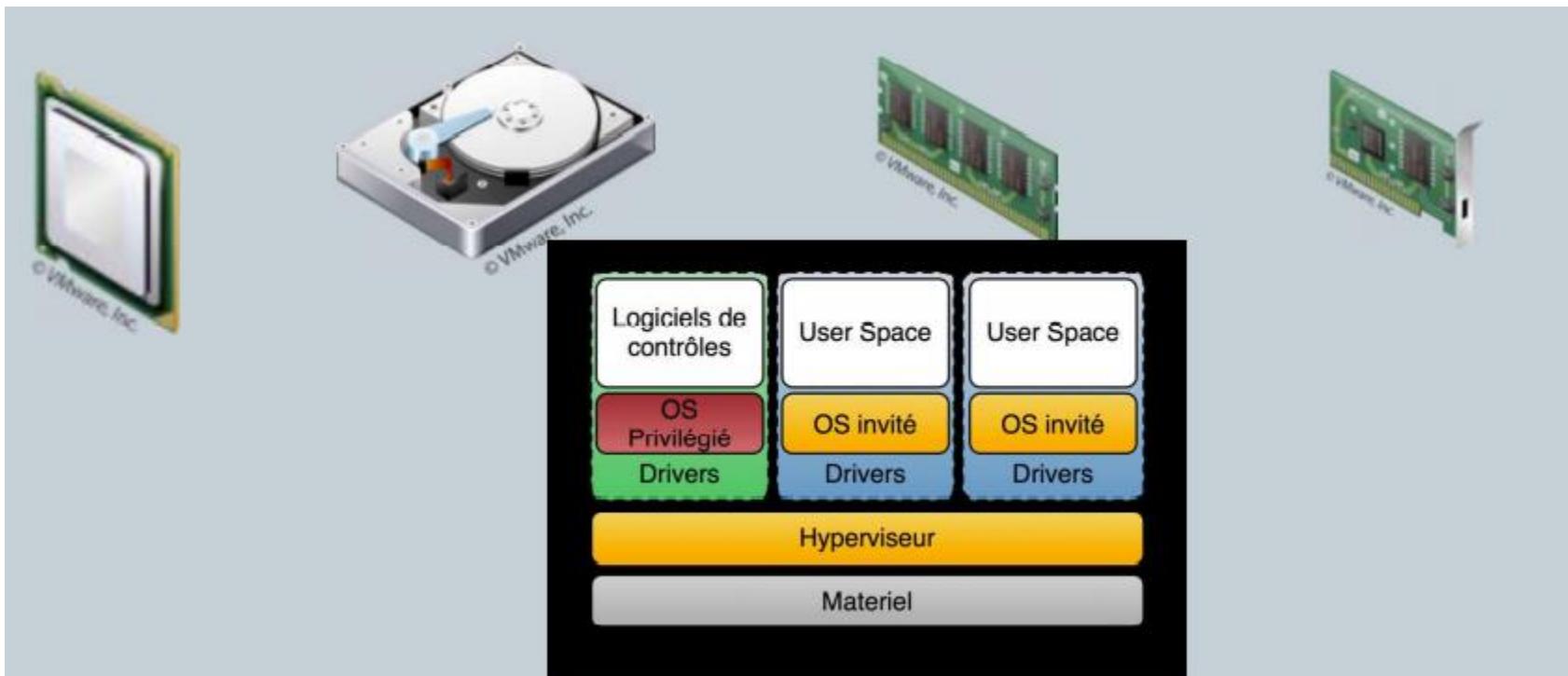
- Avantages:
 - Facilité de mise en œuvre et d'utilisation,
 - très bonne compatibilité d'OS.
- Inconvénients
 - Mauvaises performances, matériel émulé
- Exemples:
 - **BLUESTACKS** (émulateur android sur PC),
 - **NOX PLAYER** (émulateur android sur PC),
 - **QEMU** est un logiciel libre de machine virtuelle, pouvant émuler un processeur et, plus généralement, une architecture différente si besoin.



L'hyperviseur

Les 3 variantes d'architecture de virtualisation

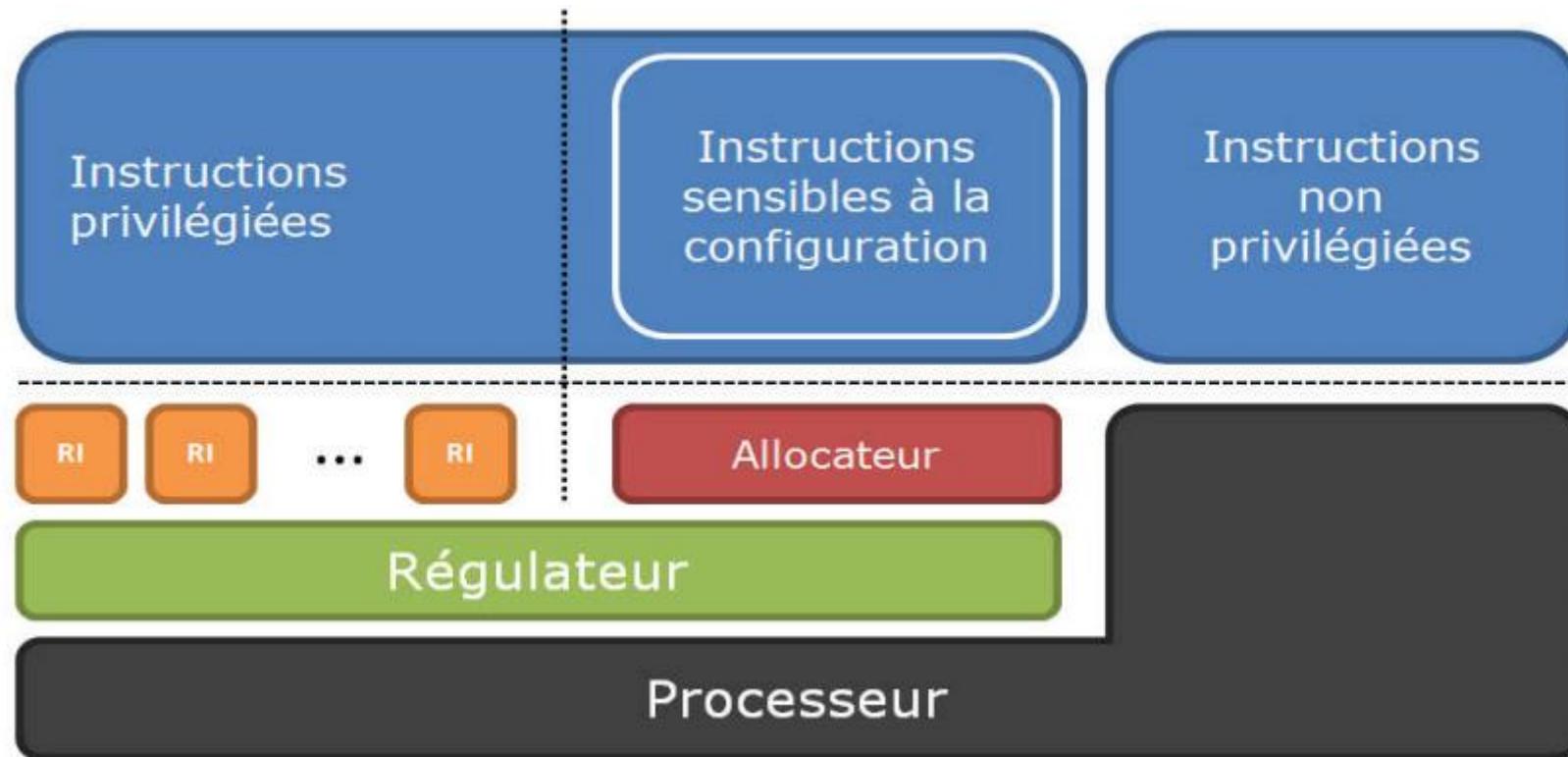
- L'hyperviseur intègre son propre OS (ou micro OS) de taille réduite et de préférence peu consommateur en ressources (VMware ESX, HyperV , Xen Citrix).
- L'Hyperviseur alloue aux machines virtuelles des ressources matérielles.



L'hyperviseur

Les 3 variantes d'architecture de virtualisation

- Composants d'un hyperviseur: L'hyperviseur, ou programme de contrôle, est un logiciel constitué d'un ensemble de modules.



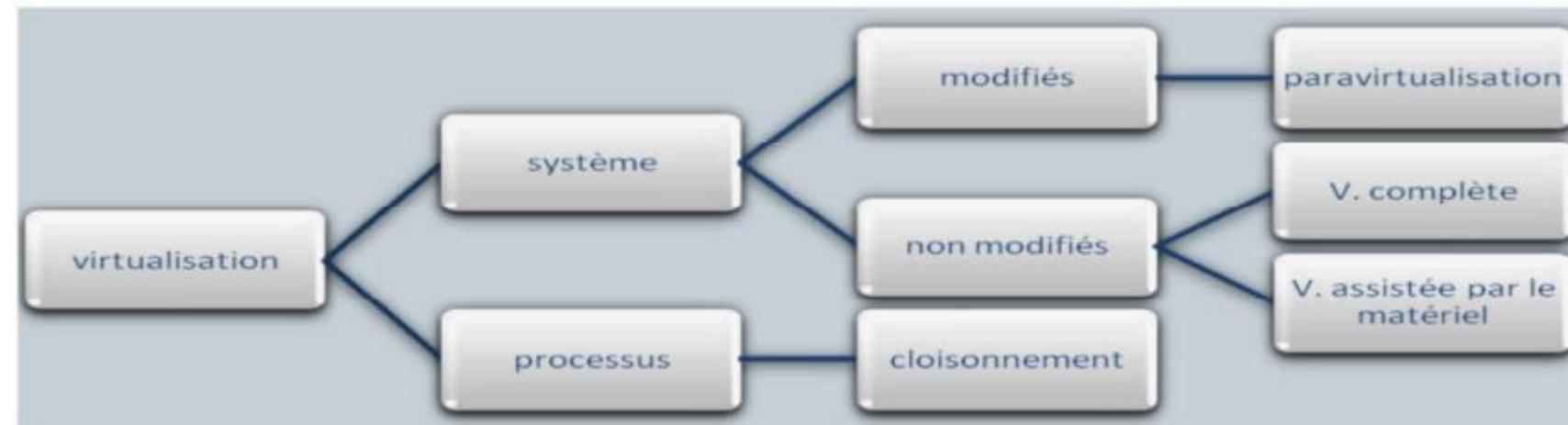
L'hyperviseur

Les 3 variantes d'architecture de virtualisation

- Composants d'un hyperviseur:
 1. Le régulateur (dispatcher) : il peut être considéré comme le module de contrôle de plus haut niveau de l'hyperviseur.
 2. L'allocateur : son rôle est de déterminer quelle(s) ressource(s) doivent être allouées aux applications virtualisées.
 3. Des interpréteurs : à chacune des instructions privilégiées (à l'exception de celles qui sont prises en charge par l'allocateur), on va associer une routine d'interprétation.

Les différents types de virtualisation

- Les technologies les plus répandues sont :
 - la virtualisation complète
 - la paravirtualisation
 - la virtualisation assistée par le matériel
 - le cloisonnement.



Les différents types de virtualisation

- L'hyperviseur émule un environnement matériel complet sur chaque machine virtuelle.
- Chaque VM dispose donc de son propre contingent de ressources hardwares virtuelles donné par l'hyperviseur et peut exécuter des applications sur cette base.
 - ➔ Le système d'exploitation invité n'a pas conscience d'être virtualisé.
- Le matériel physique du système hôte, en revanche, reste caché du système d'exploitation invité
 - ➔ L'OS qui est virtualisé n'a aucun moyen de savoir qu'il partage le matériel avec d'autres OS.
- Cette approche permet l'exploitation de systèmes invités non modifiés.
- Les solutions logicielles populaires pour la virtualisation complète sont Oracle VM VirtualBox, Parallels Workstation, VMware Workstation, Microsoft Hyper-V et Microsoft Virtual Server.

Paravirtualisation

Les différents types de virtualisation

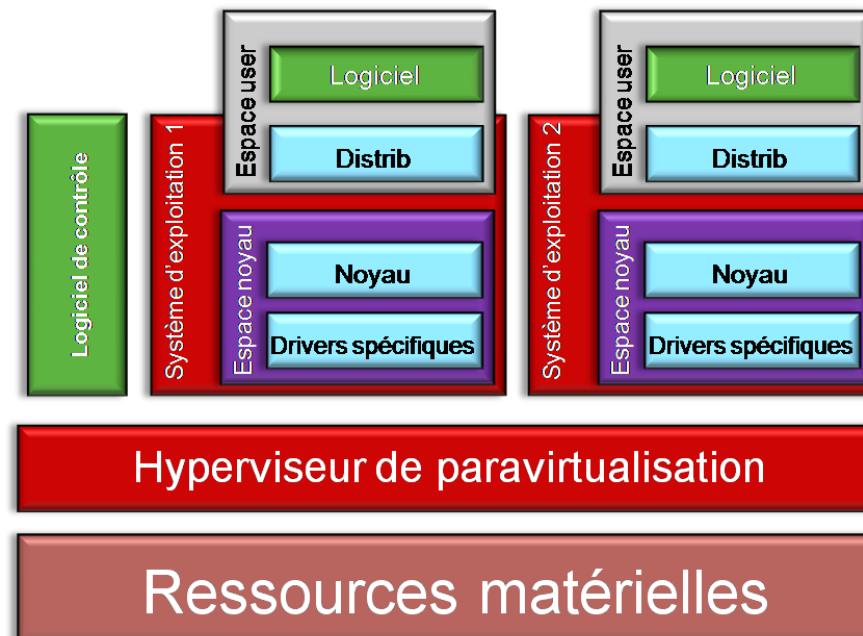
- Alors que la virtualisation complète fournit un environnement matériel virtuel distinct pour chaque machine virtuelle, **avec la paravirtualisation, l'hyperviseur met simplement à disposition une interface de programmation (API) qui permet aux systèmes d'exploitation invités d'accéder directement au matériel physique du système hôte.**
- Cependant, il faut pour cela au préalable que le noyau du système d'exploitation invité ait été porté sur l'API. Ainsi, seuls les systèmes invités modifiés peuvent être paravirtualisés.
- Les fournisseurs de systèmes propriétaires - tels que Microsoft Windows - n'autorisent généralement pas de telles modifications.
- Parmi les hyperviseurs qui permettent les paravirtualisations, on compte Xen et Oracle VM Server for SPARC. Le concept est également utilisé dans le système d'exploitation mainframe z/VM d'IBM.

Paravirtualisation

Les différents types de virtualisation

Par opposition à la virtualisation, on parle de paravirtualisation lorsque **les systèmes d'exploitation** doivent être **modifiés** pour fonctionner sur un hyperviseur de paravirtualisation.

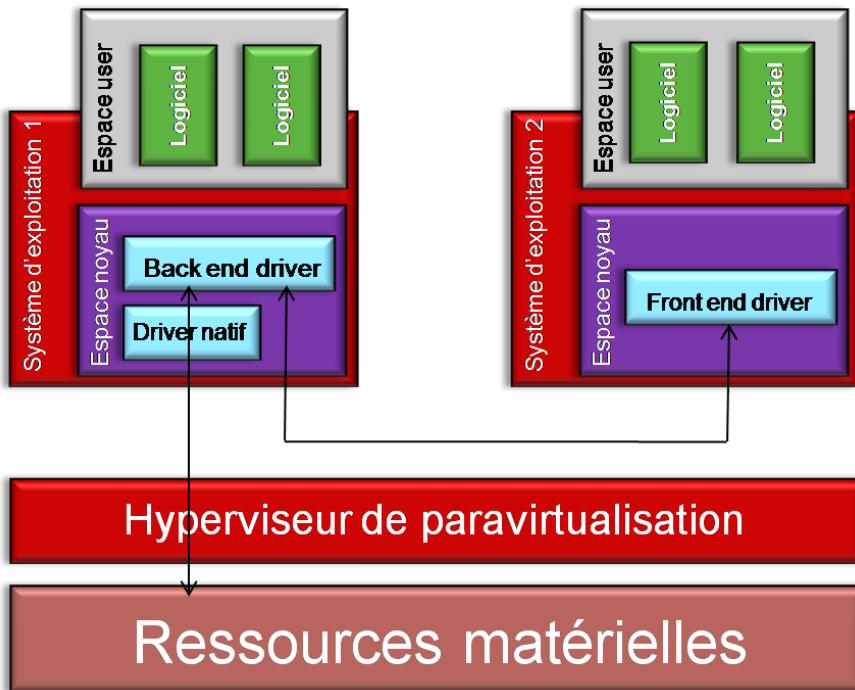
Les **modifications** sont en fait des **insertions de drivers** permettant de rediriger les appels système au lieu de les traduire.



Paravirtualisation

Les différents types de virtualisation

Le mécanisme de redirection des appels système est expliqué ici:



Des drivers **backend** et **frontend** sont installés dans les **OS paravirtualisés**.

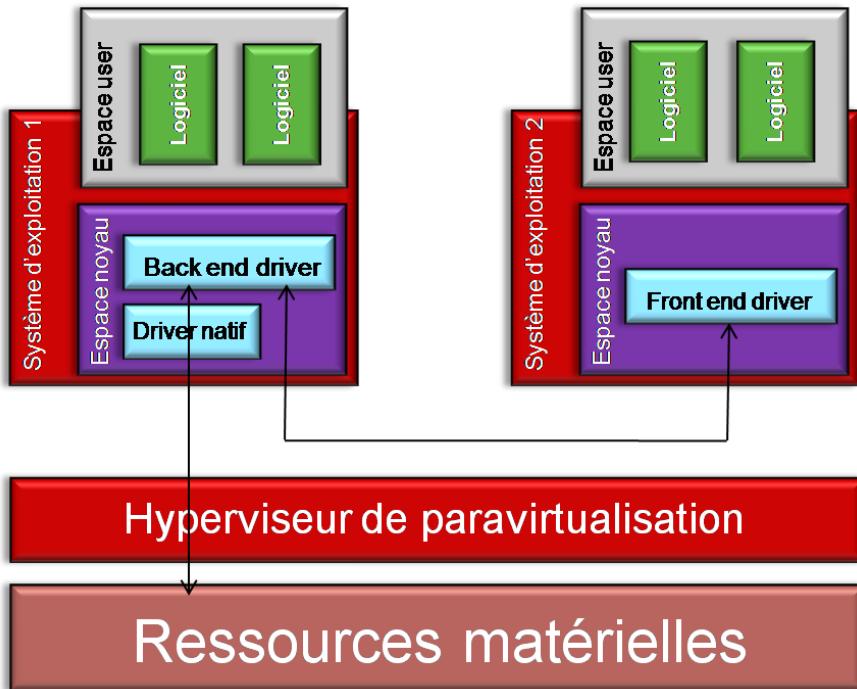
Ils permettent, au lieu de traduire les appels système comme cela est fait dans la virtualisation complète, de ne faire que de **la redirection** (ce qui est beaucoup plus rapide).

Il est donc intelligent d'utiliser un tel mécanisme pour accéder à du matériel potentiellement très sollicité (disque dur, interface réseau...).

Paravirtualisation

Les différents types de virtualisation

Le mécanisme de redirection des appels système est expliqué ici:



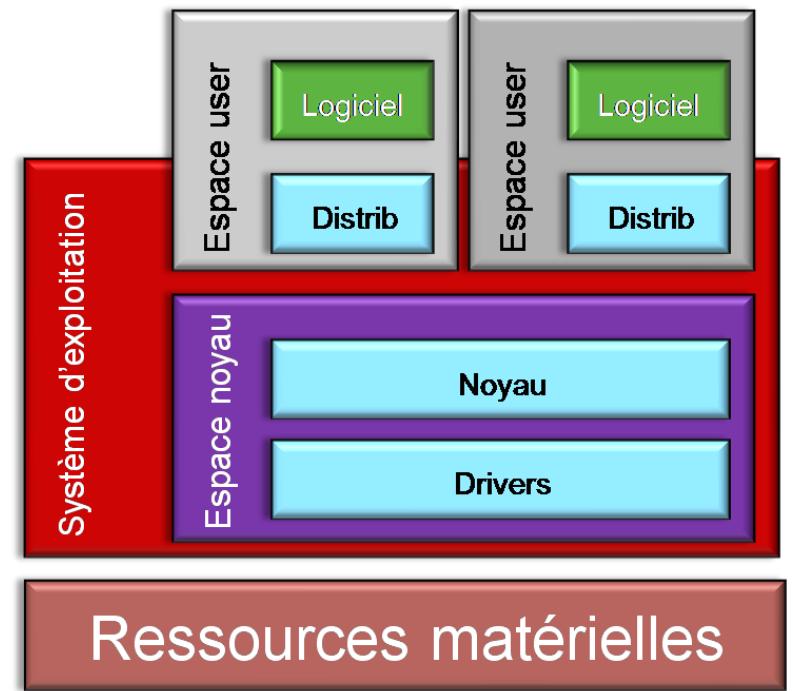
En fait, ce qu'il se passe dans une telle technologie, c'est que le contrôle d'un ou plusieurs matériel(s) est donné à un des OS virtualisé (celui qui contient le driver backend), ici le système d'exploitation 1.

Une fois cela compris, il sera simple d'imaginer que l'OS 2, qui souhaite accéder au hardware, devra passer par son driver front end qui redirigera les appels système vers l'OS 1.

(-) L'inconvénient de cette technique est donc la dépendance d'un OS virtualisé vis à vis d'un autre qui se crée par ce mécanisme de driver. En effet si l'OS 1 tombe en panne, l'OS 2 ne pourra plus accéder au matériel.

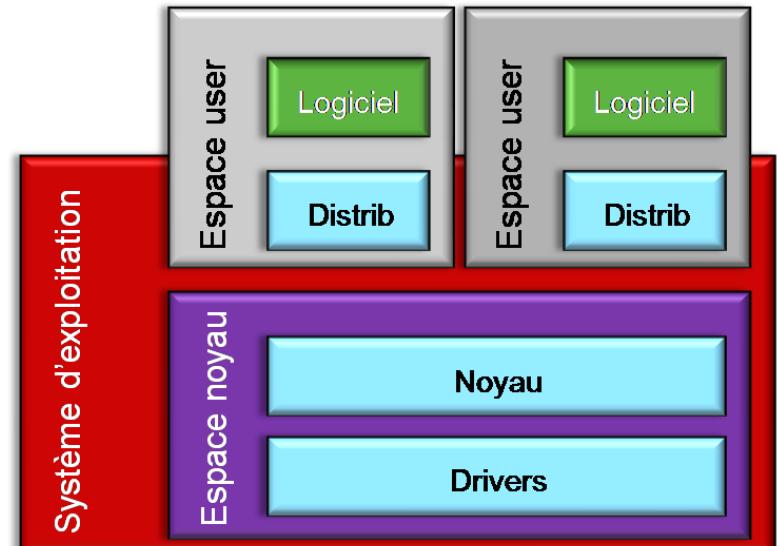
Le cloisonnement/ L'isolation

- L'isolation est une technique permettant d'emprisonner l'exécution des applications dans des contextes.
- Cette solution est très performante (le surcoût d'une application isolée/virtualisée est minime par rapport au temps d'exécution de la même application installée sur un système d'exploitation).
- La performance est donc au rendez-vous, cependant on ne peut pas parler de virtualisation de systèmes d'exploitation car l'isolation ne consiste à virtualiser que des applications.



Le cloisonnement/ L'isolation

- On ne peut pas vraiment parler de virtualisation proprement dit, mais cette technique permet de multiplier les instances d'une même application dans un contexte cloisonné, avec des performances proches de l'exécution native.
- L'environnement ainsi « virtualisé » se retrouve confiné mais pas isolé à 100% du système hôte, notamment au niveau des ressources physiques (et du noyau).
- SUN dispose, par exemple, sur son système Solaris de ce type de technologies - SUN Zone / Containers.
- Les isolateurs sont principalement réservés aux serveurs Linux et sont fortement utilisés pour l'isolation de serveurs LAMP par les fournisseurs de serveurs Web.



Ressources matérielles

Exemples d'isolateur:

Les deux principales solutions pour l'isolation Linux sont OpenVZ et LXC.

Virtualisation – Les types de connexion au réseau

En termes de connexion au réseau, on trouve plusieurs types de connexion au réseau, Parmi ces types de connexion au réseau, on trouve :

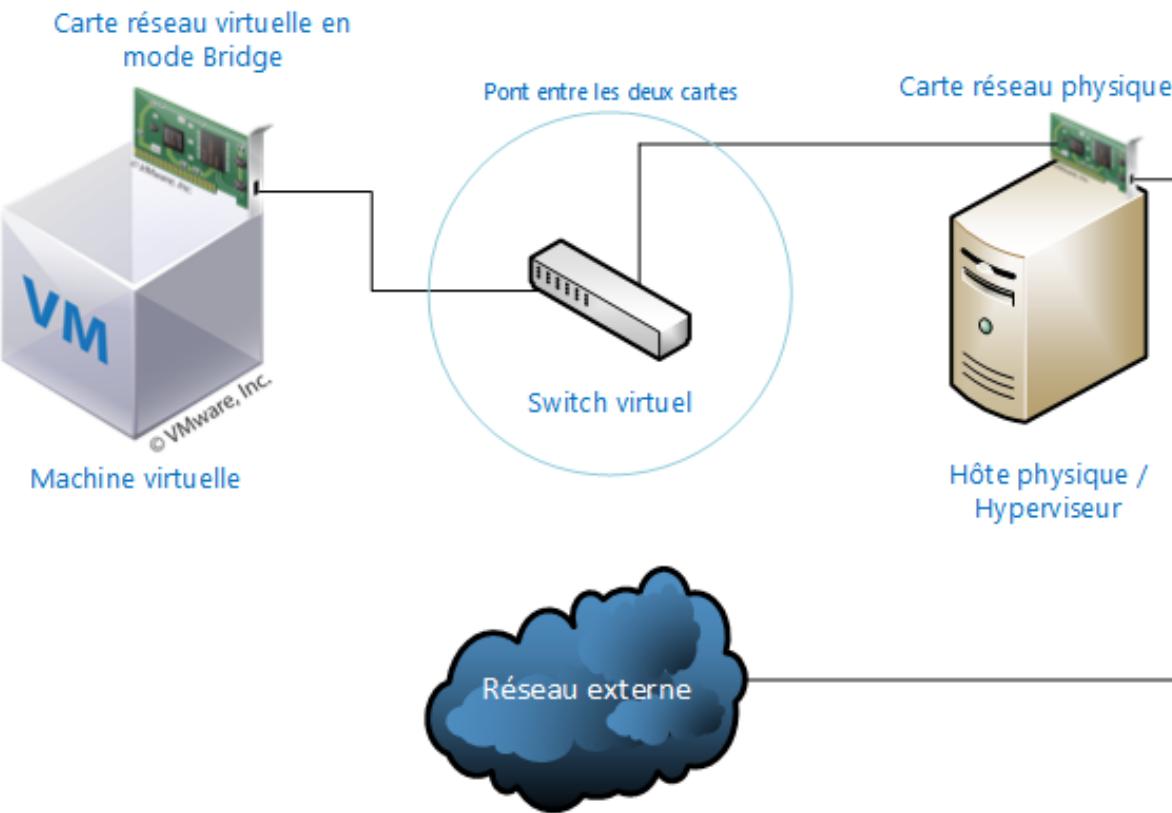
- Bridge
- NAT
- Host-Only
- LAN Segment

Le type Bridge

Virtualisation – Les types de connexion au réseau

➤ Ce mode est le plus utilisé puisqu'il permet de connecter une machine virtuelle directement sur le réseau physique sur lequel est branchée la carte réseau physique de l'hôte.

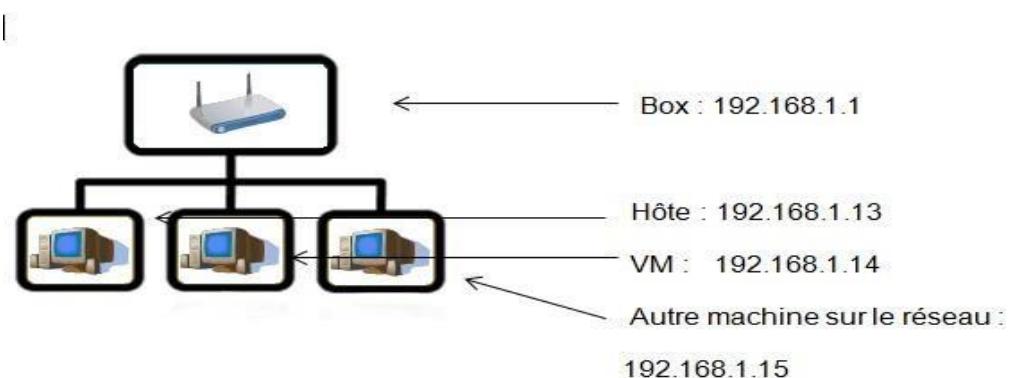
➤ Si l'hôte physique dispose de plusieurs cartes réseaux, on peut choisir de créer un pont ce qui permet une flexibilité dans la configuration et dans la gestion de la connexion réseau



Le type Bridge

Virtualisation – Les types de connexion au réseau

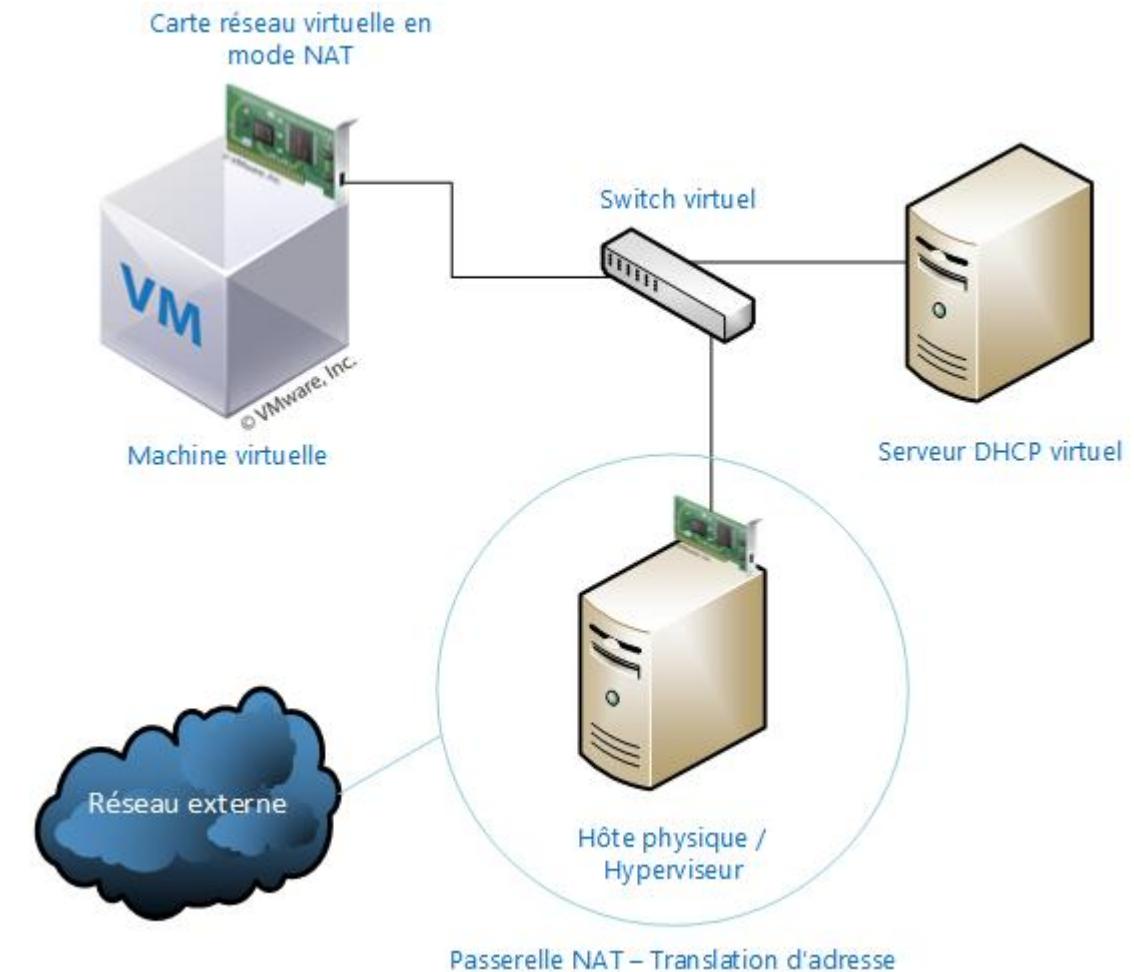
- **Un bridge** c'est-à-dire un pont est créé entre la carte réseau virtuelle de l'application de virtualisation et la carte réseau de votre hôte physique. C'est en quelque sorte un partage de carte réseau, où le système d'exploitation de votre hôte physique partage sa carte physique avec le système d'exploitation de votre ou vos machines virtuelles.
- Vu que la machine virtuelle se retrouvera connectée sur le même réseau que la machine physique, il lui faudra une configuration TCP/IP identique aux autres postes du réseau afin qu'elle puisse communiquer avec le reste du réseau et sortir du réseau.



Le type NAT

Virtualisation – Les types de connexion au réseau

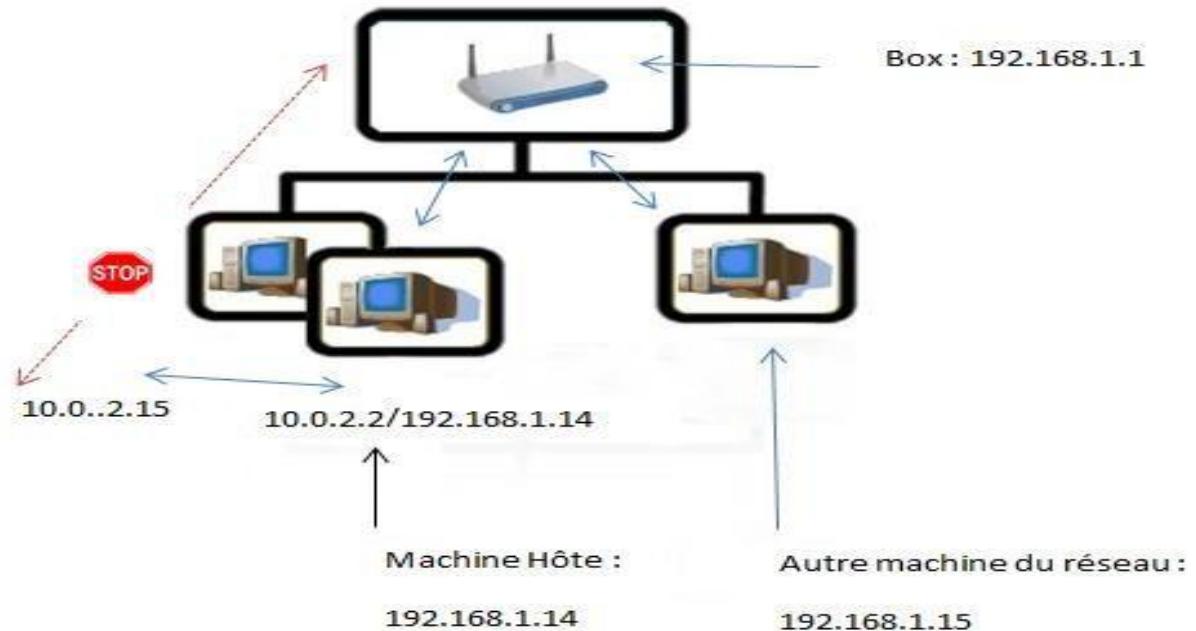
- Ce type de connexion permet à la machine virtuelle d'accéder au réseau de façon totalement transparente puisque c'est l'adresse IP de la machine physique qui est utilisée grâce à la translation d'adresse du processus NAT.
- ➔ Masquer l'adresse IP des clients qui lui sont connectés pour sortir sur le réseau.
- **La machine virtuelle utilise une adresse IP distribuée par l'application de virtualisation via un serveur DHCP, puis elle utilisera votre hôte physique comme passerelle pour sortir du réseau.**



Le type NAT

Virtualisation – Les types de connexion au réseau

55

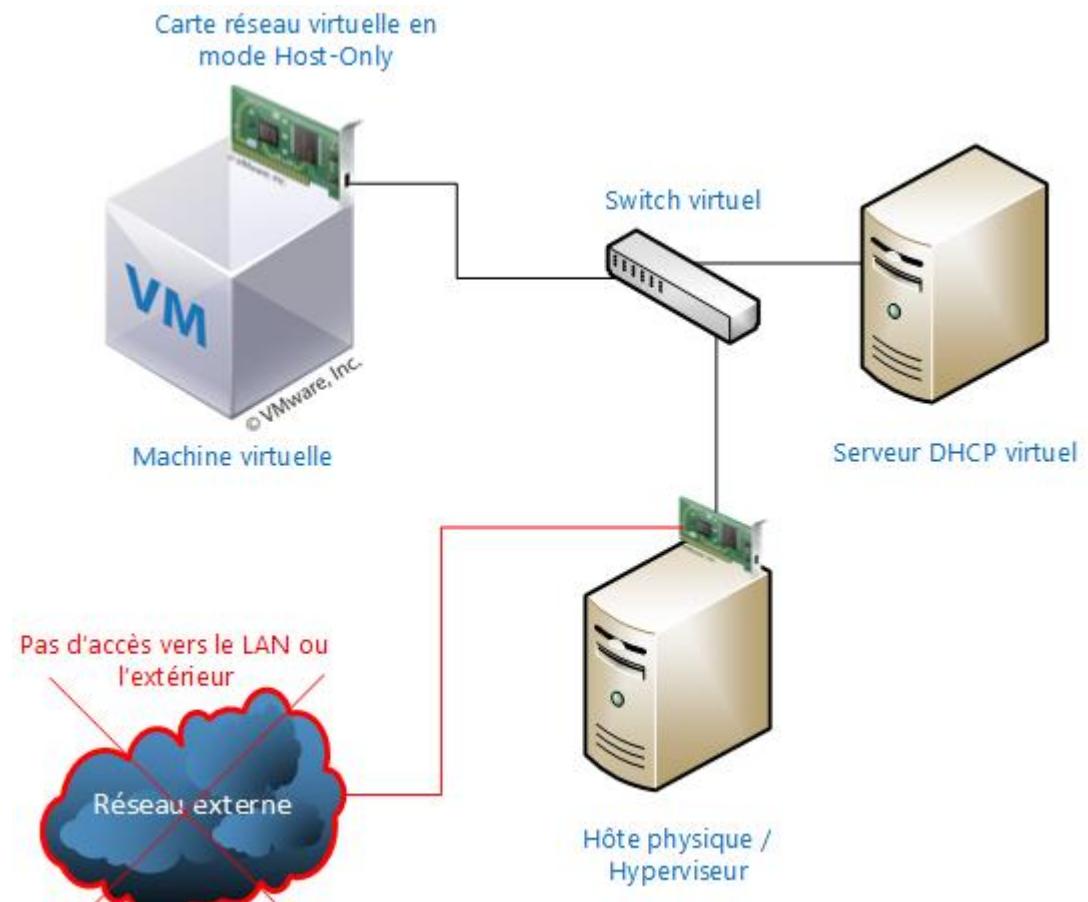


Le type Host-Only

Virtualisation – Les types de connexion au réseau

➤ Ce type de connexion ne permet pas de sortir vers un réseau extérieur, ni d'accéder au réseau local par l'intermédiaire de la carte réseau physique de la machine physique hôte.

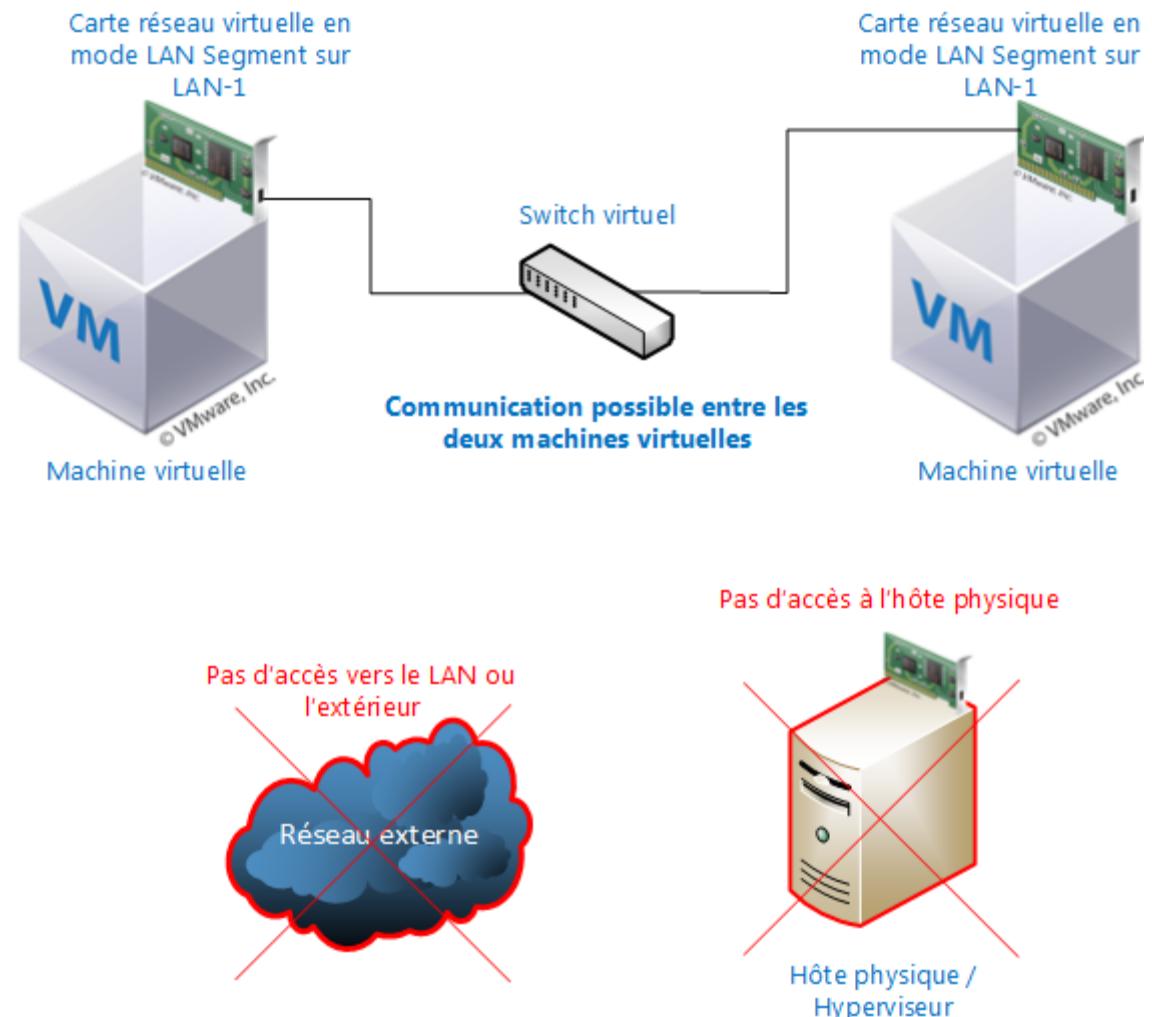
➤ Ce mode permet uniquement d'établir une connexion entre la machine virtuelle et la machine physique. Cela par l'intermédiaire de l'adaptateur virtuel de la machine virtuelle et l'adaptateur virtuel de la machine physique qui obtiendront des adresses IP via le serveur DHCP virtuel de l'hyperviseur.



Le type LAN-Segment

Virtualisation – Les types de connexion au réseau

- Le type LAN Segment permet d'isoler des machines sur un LAN virtuel.
- Par exemple, si un LAN virtuel « LAN-1 » est créé, toutes les machines ayant une carte réseau en mode LAN Segment connectée au « LAN-1 » pourront communiquer ensemble. toutes les machines reliées à « LAN-2 » pourront communiquer ensemble mais ne pourront pas communiquer avec les machines virtuelles du « LAN-1 ».



Virtualisation – Les types de connexion au réseau

➤ En conclusion:

- ✓ le mode Bridge et le mode NAT sont les seuls qui permettent d'accéder au réseau physique sur lequel l'hôte physique est connectée.
- ✓ Les autres modes permettent plus une isolation des machines virtuelles qui peut être intéressante dans une phase de développement, lors de la mise en place d'une maquette, afin de travailler sur un réseau à part, sur un réseau isolé.
- ✓ Toutefois, le LAN Segment peut être utilisé pour isoler certaines machines virtuelles dans un LAN virtuel qui auront pour passerelle une machine virtuelle ayant deux cartes : une dans le LAN virtuel avec les autres machines virtuelles et une en mode Bridge pour sortir sur le réseau.

Les Objectifs de virtualisation

➤ **En conclusion la virtualisation permet donc:**

- ✓ De partager un même serveur physique en N serveurs virtuels, alloués à différents clients.
- ✓ De définir – du moins selon la technologie de virtualisation retenue – la part de ressources allouée à chaque client.
- ✓ De donner à chaque client un contrôle total sur son serveur virtuel :il peut y installer et ré-installer l'OS.

La haute disponibilité

Les Objectifs de virtualisation

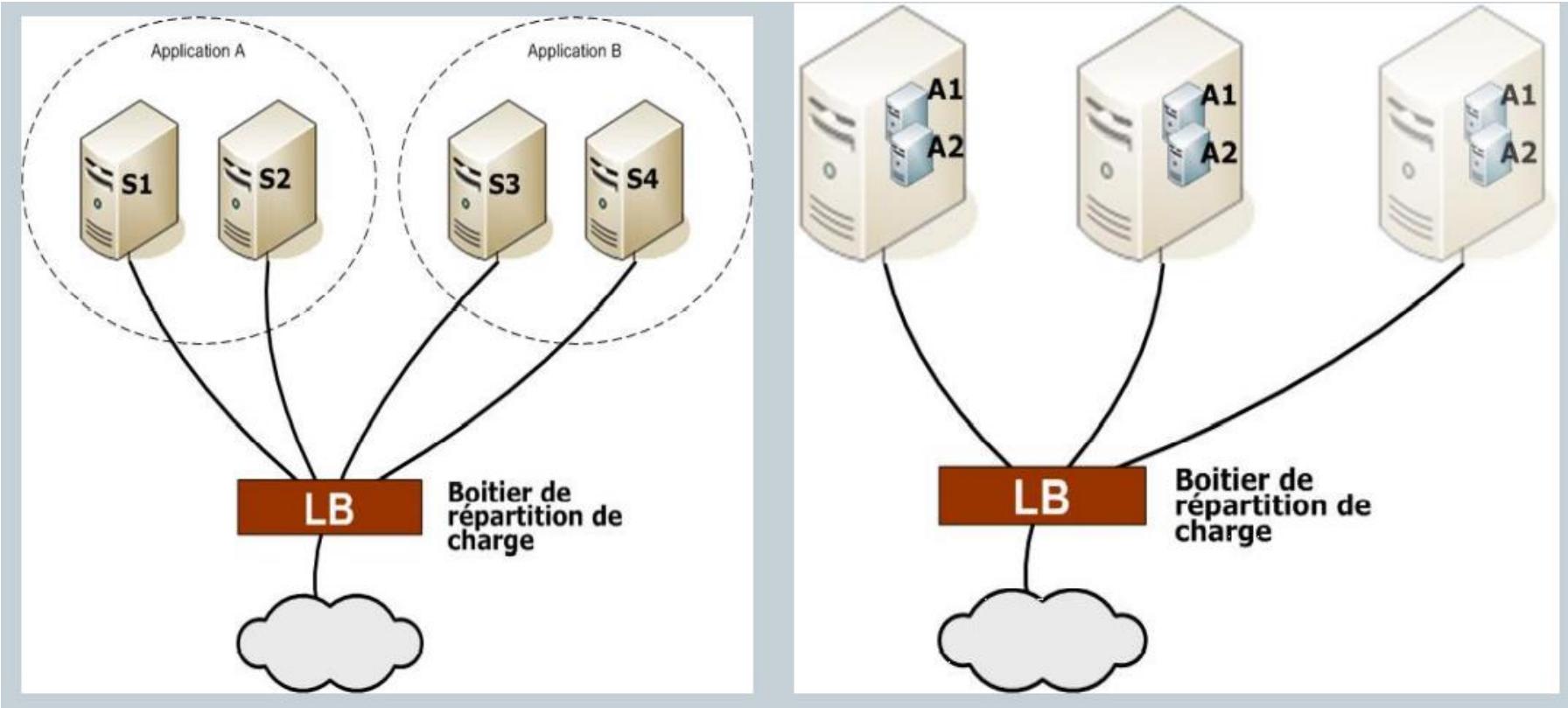
- En matière de haute disponibilité ou de haute capacité d'accueil, les mécanismes centraux sont devenus classiques et bien maîtrisés : répartition de charge (load balancing) et reprise automatique sur incident (failover).
- **Répartition de charge:** La répartition de charge est à la base un moyen d'augmenter la tenue en charge d'une application, en l'hébergeant sur plusieurs serveurs qui se partagent les visiteurs.

C'est le cas typique d'un grand site web recevant plusieurs centaines de milliers de visiteurs par jour, dont le trafic est réparti sur quelques serveurs.

Répartition de charge

Les Objectifs de virtualisation

- Au lieu de 4 serveurs, on n'en a plus que 3, voire 2. Et au lieu d'une répartition sur 2 serveurs, on a une répartition sur 3.



Reprise
automatique

Les Objectifs de virtualisation

- Un autre usage de la virtualisation dans une optique de haute disponibilité de service peut consister à avoir sur plusieurs serveurs physiques les mêmes environnements virtuels (synchronisés régulièrement).

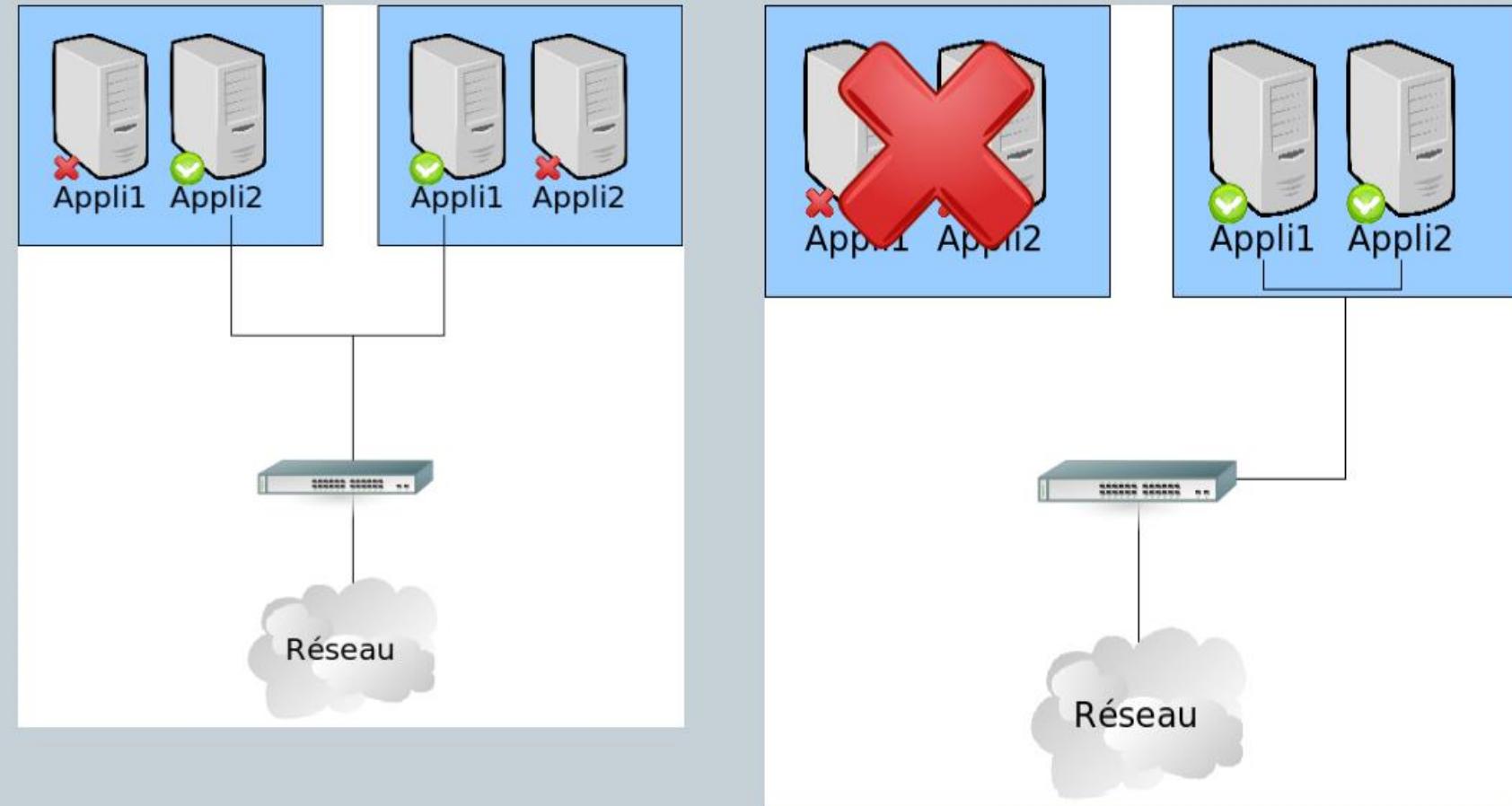
- Les différents serveurs physiques se partagent les différents serveurs virtuels, et si un des serveurs physiques tombe en panne, les machines dont il avait la responsabilité sont relancées sur les autres serveurs.

Reprise
automatique

63

Les Objectifs de virtualisation

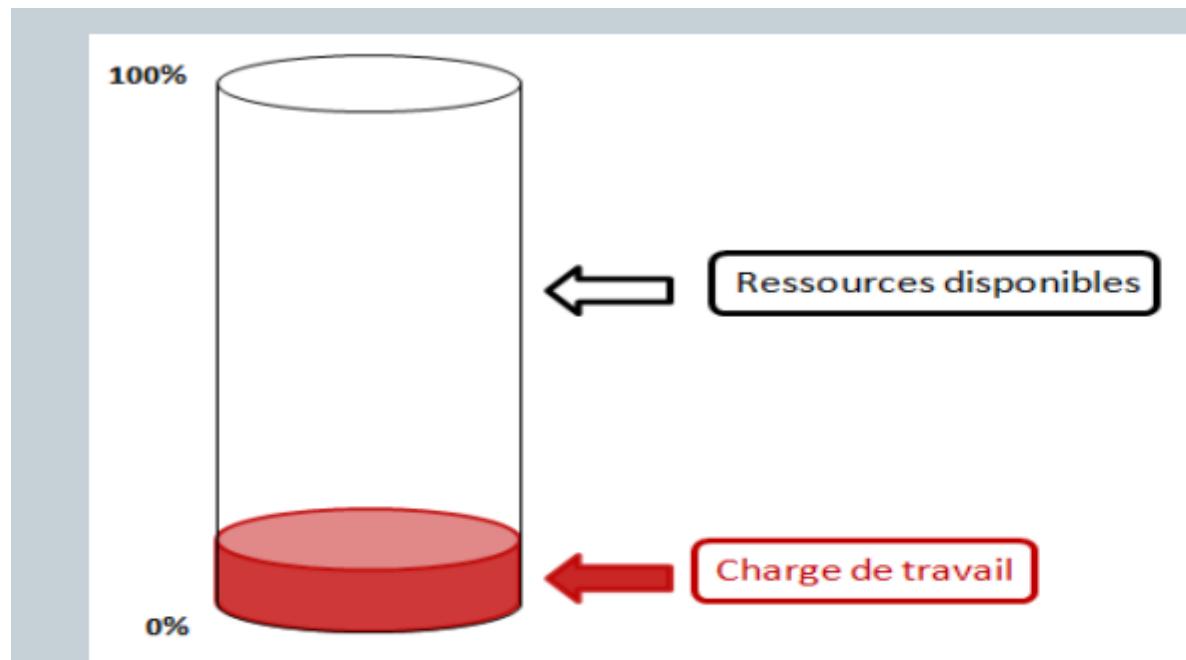
Après une panne d'un des serveurs :



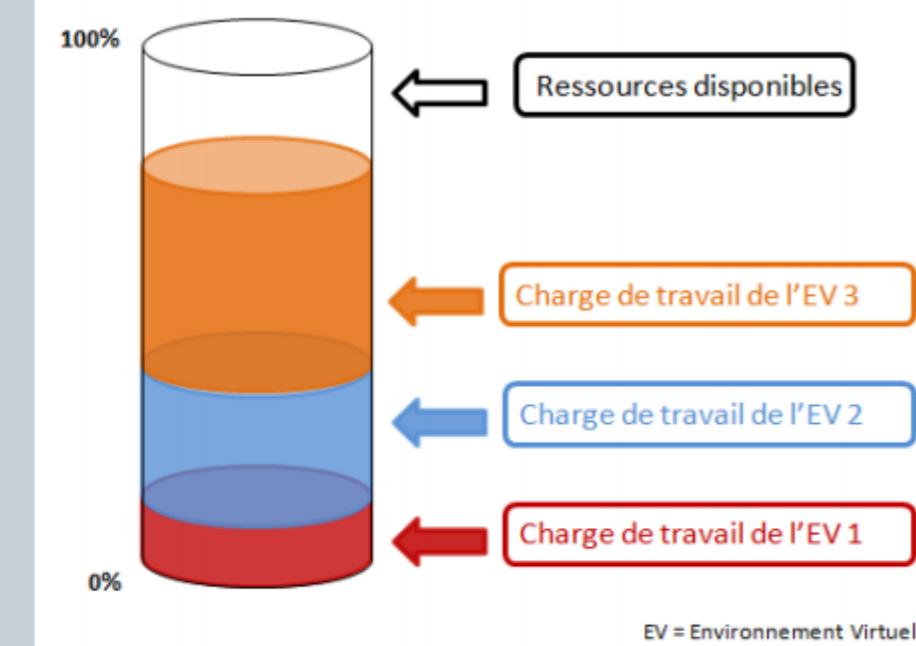
Optimisation de l'infrastructure

Les Objectifs de virtualisation

La virtualisation permet d'optimiser la charge de travail des serveurs physiques
→ Une réduction de l'infrastructure physique et des économies d'énergies



Rendement d'un serveur en l'absence de virtualisation



Rendement d'un serveur en présence de virtualisation

Firewall, VPN

65

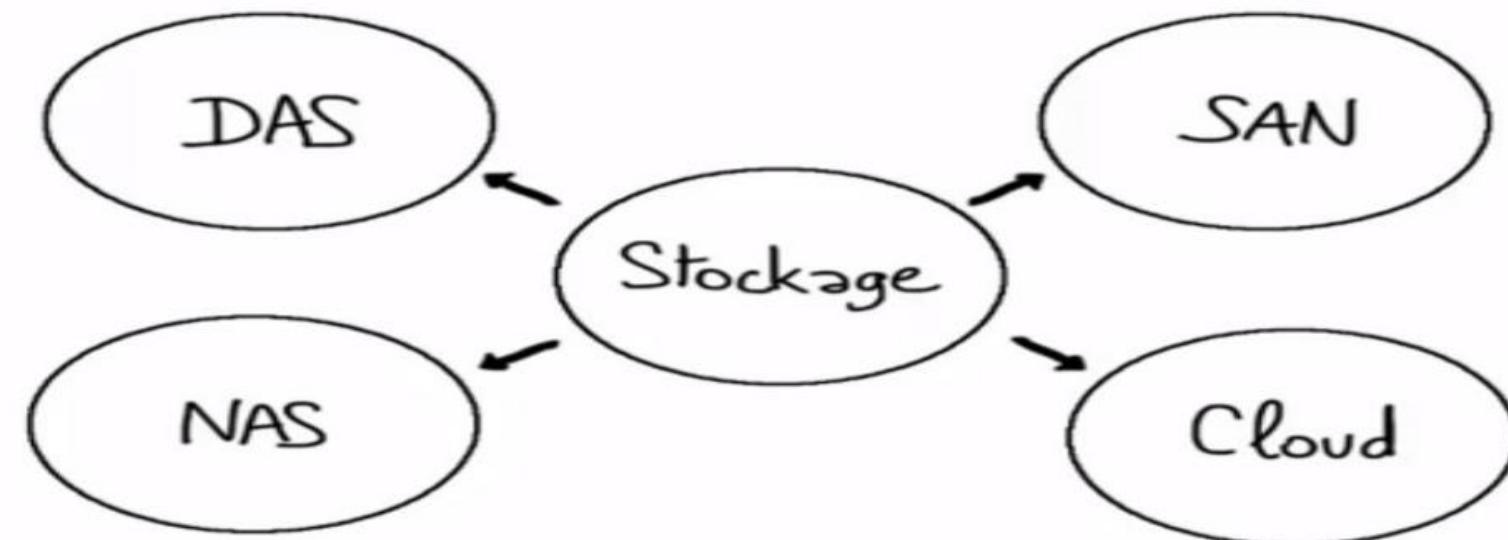
Les Objectifs de virtualisation

Les capacités réseau de certaines solutions de virtualisation permettent même de mettre en place des serveurs virtuels ayant la main sur les interfaces réseau, ce qui permet l'utilisation d'un composant virtuel pour servir de firewall, de système de détection d'intrusions, de endpoint VPN, totalement isolé du matériel, et donc moins sensible en cas d'attaque.

LE STOCKAGE

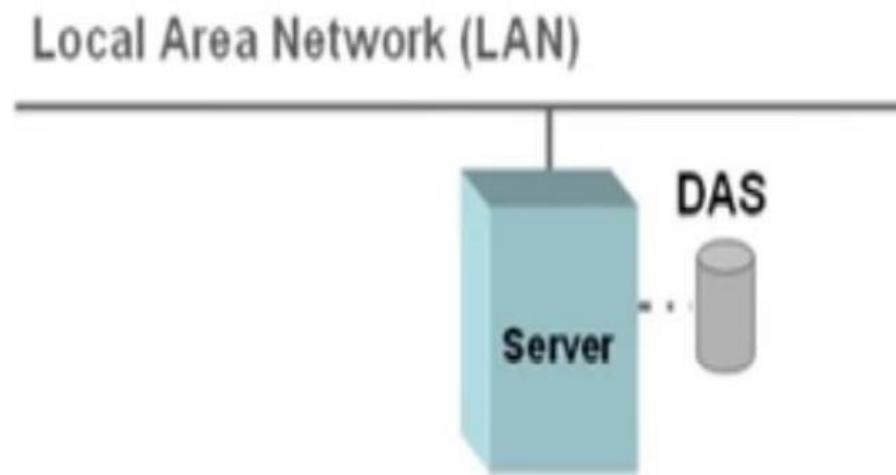
Quelque soit la technologie utilisée, une machine virtuelle se compose de deux éléments :

- Des ressources
- Des données

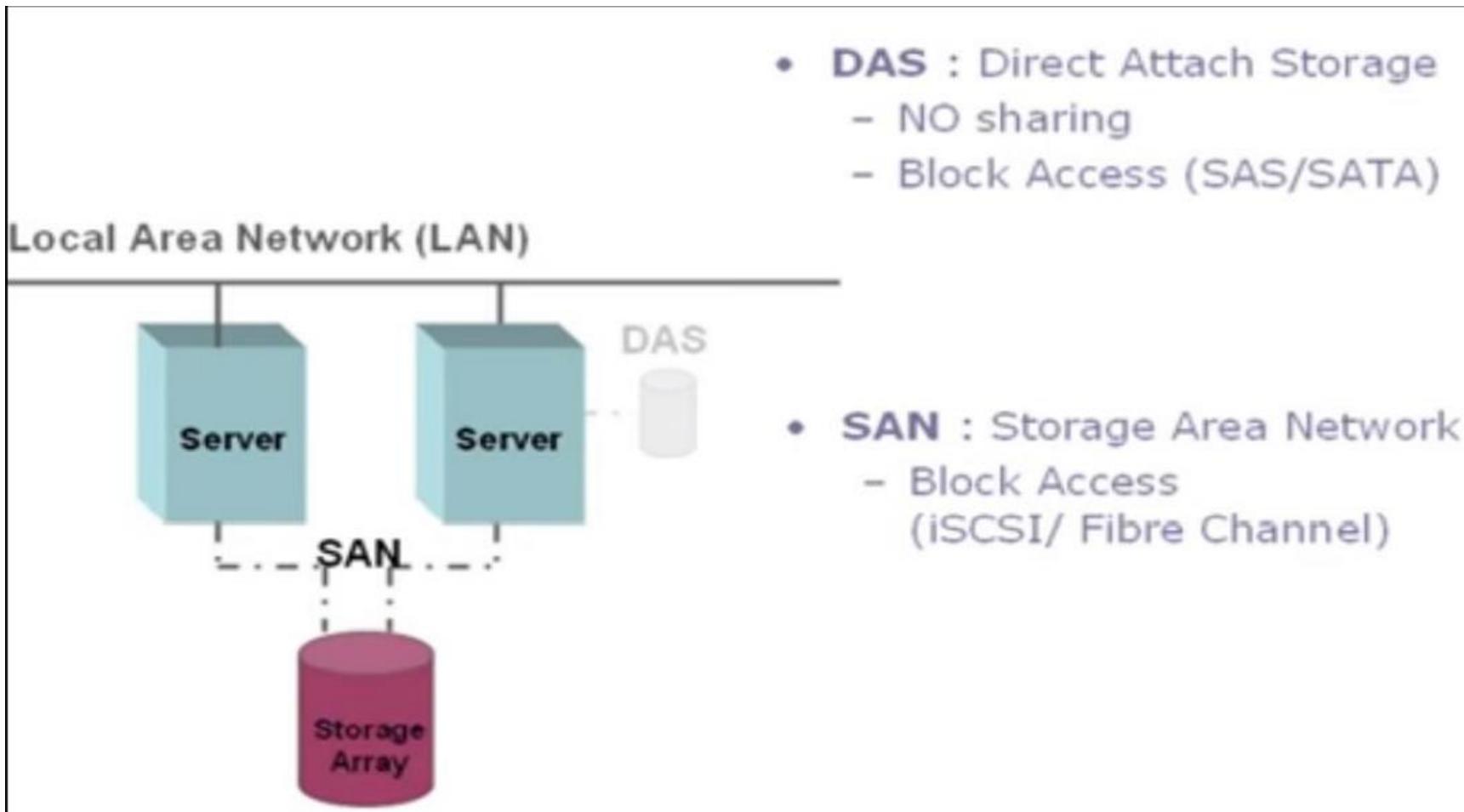


Les trois méthodes de stockage

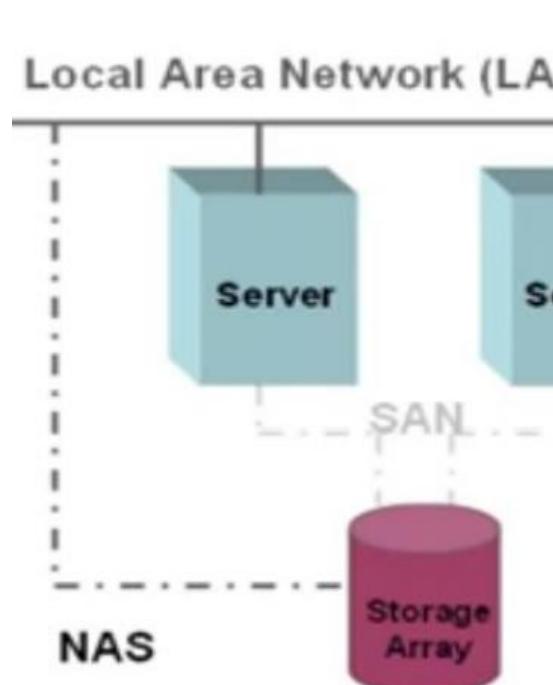
- **DAS** : Direct Attach Storage
 - NO sharing
 - Block Access (SAS/SATA)



Les trois méthodes de stockage

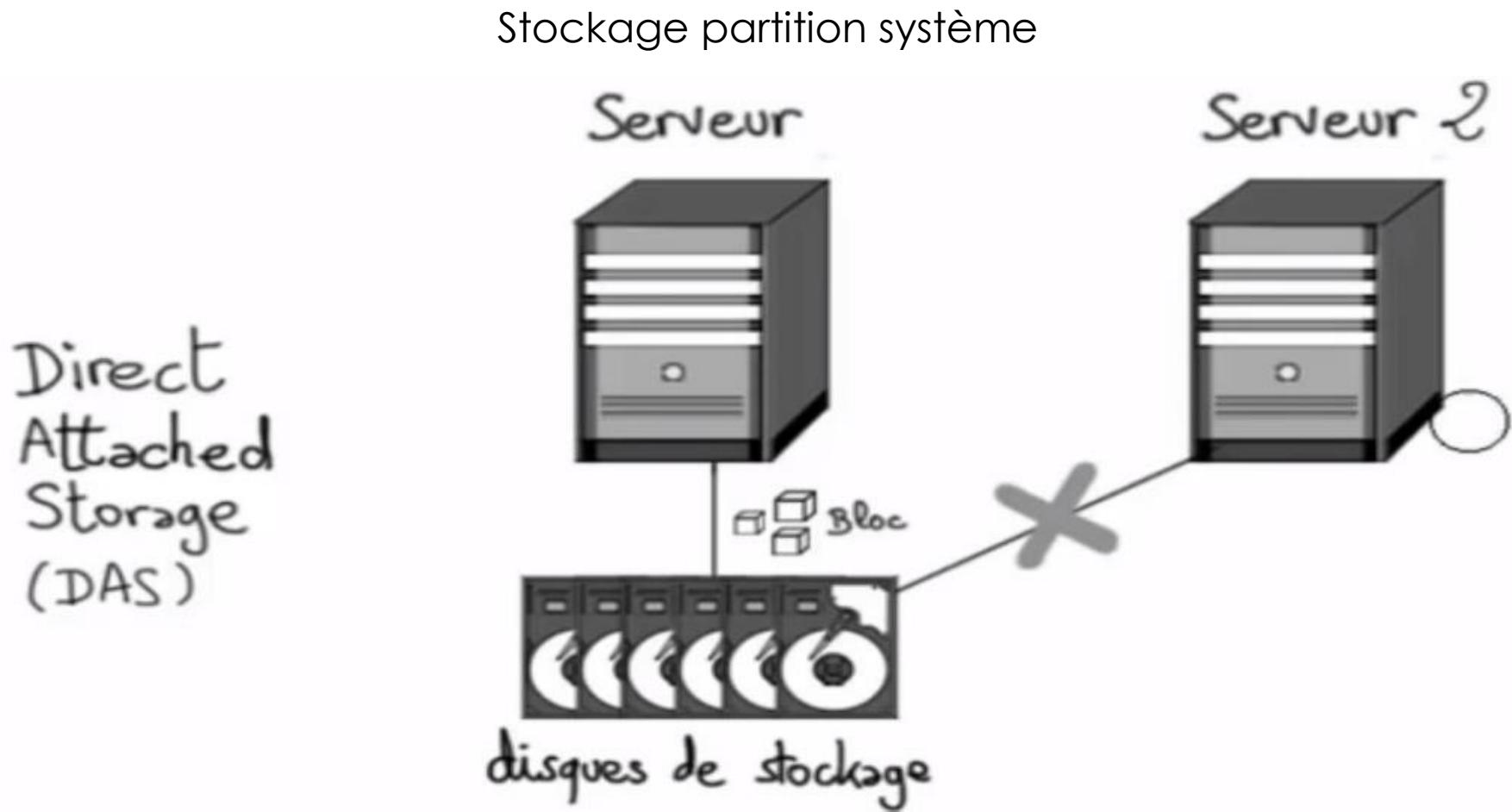


Les trois méthodes de stockage



- **DAS** : Direct Attach Storage
 - NO sharing
 - Block Access (SAS/SATA)
- **SAN** : Storage Area Network
 - Block Access (iSCSI/ Fibre Channel)
- **NAS** : Network Attached Storage
 - File Access (Windows CIFS/ Unix NFS)

LE DAS

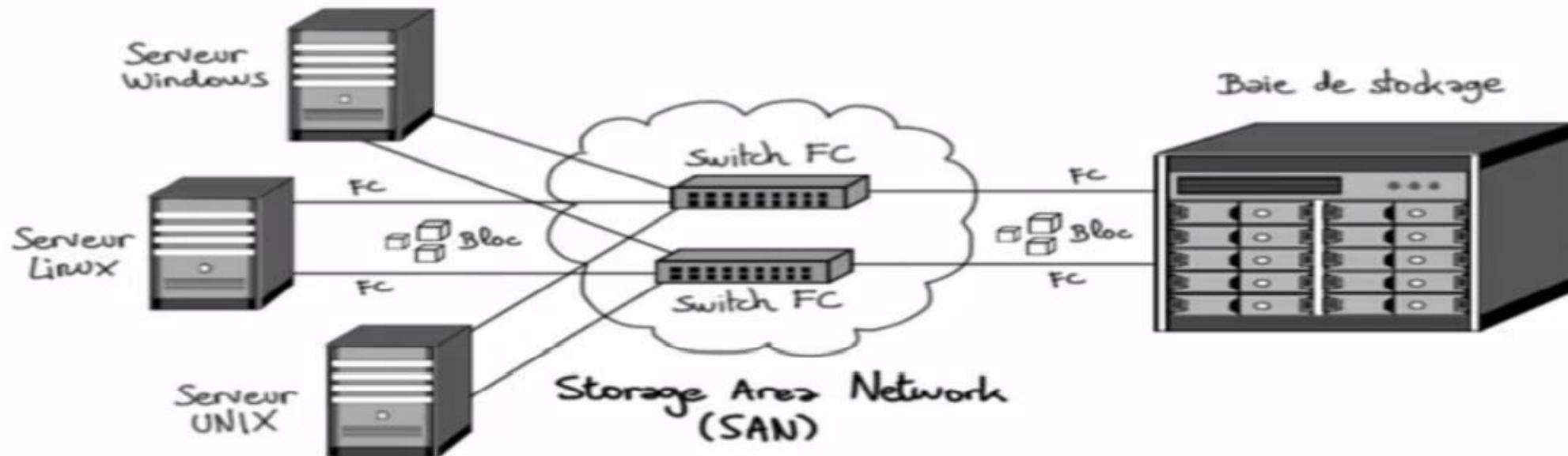


SAN stockage (Storage Area Network)

Un SAN, ou réseau de stockage (Storage Area Network), est un réseau sur lequel circulent les données entre un système et son stockage.

Stockage des données applicatif

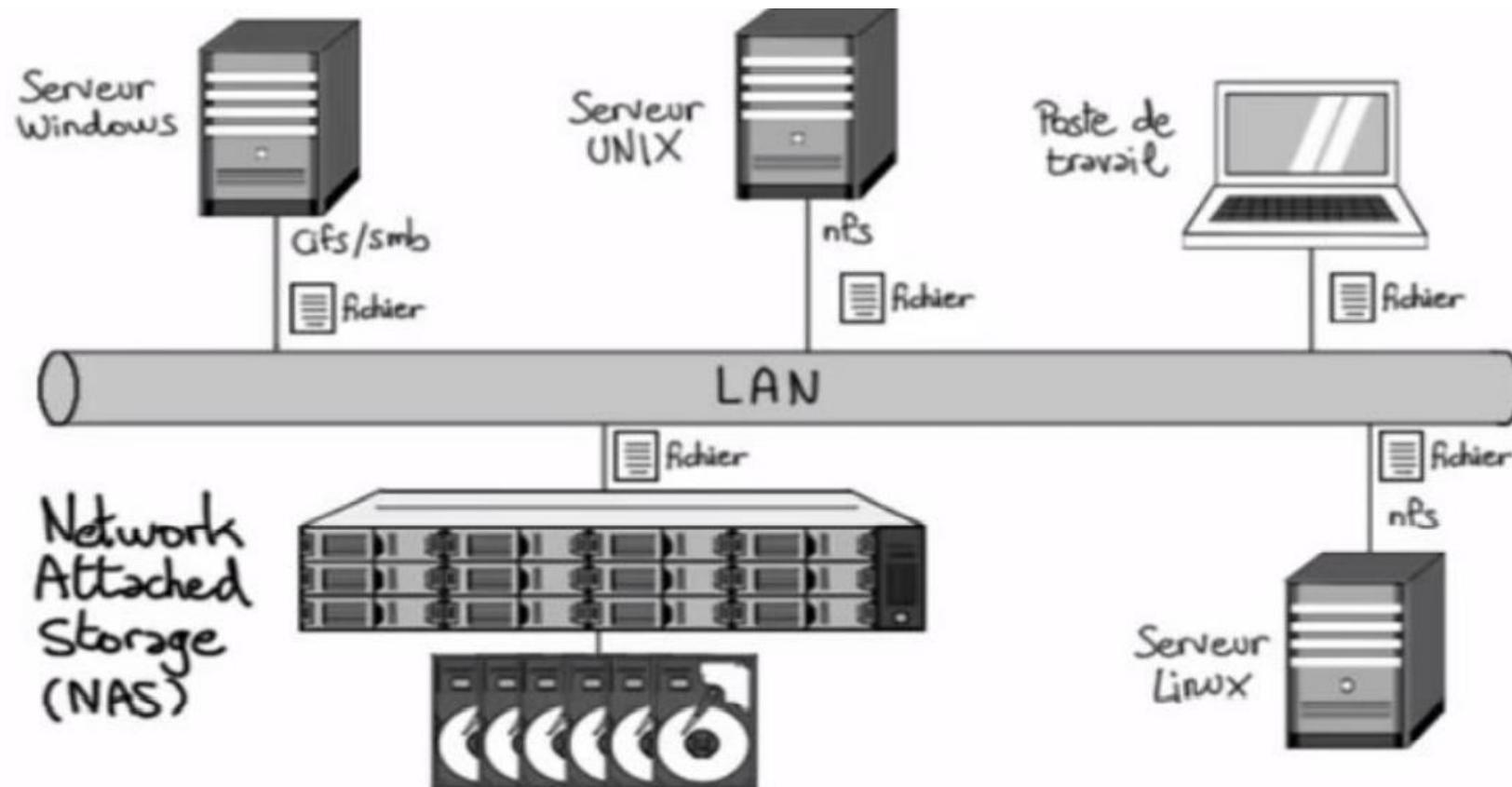
Les deux principaux protocoles d'accès à un SAN sont **iSCSI et Fibre Channel**.



SAN stockage (Storage Area Network)

- **iSCSI** est un protocole d'accès disque fonctionnant sur un réseau Ethernet, il permet d'implémenter un réseau de stockage en profitant de la connectique et des équipements de commutation standards.
- **Fibre Channel** Basé sur des fibres optiques il assure une latence et un débit bien meilleurs que iSCSI, à un prix bien sûr plus élevé. Son principe d'utilisation est le même qu'un SAN iSCSI.

stockage en réseau le NAS

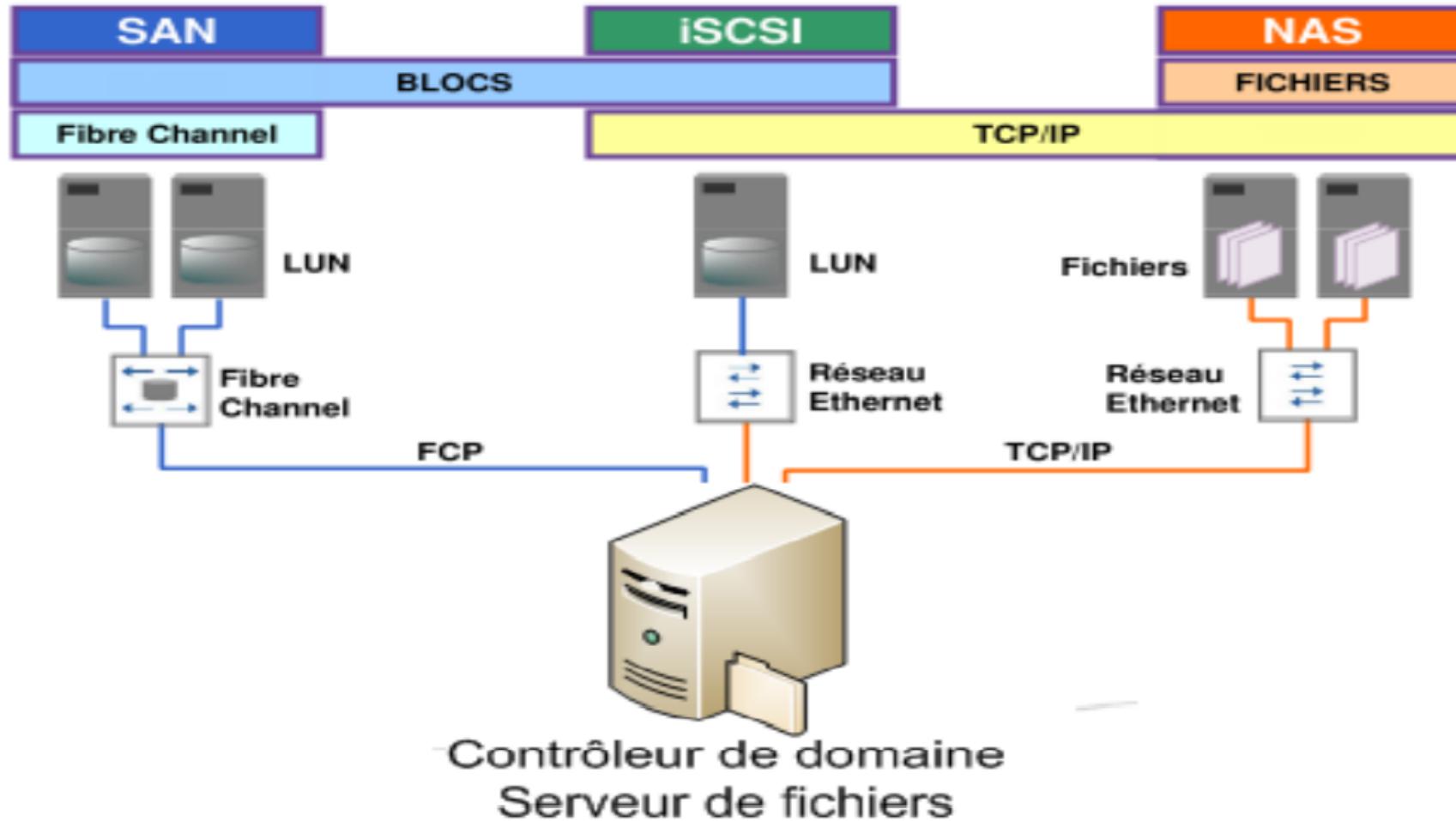


stockage en réseau le NAS

➤ NAS et NFS

- Un NAS, ou stockage réseau (**Network-Attached Storage**) est simplement un serveur fournissant leurs fichiers à d'autres serveurs par le réseau.
- NFS est le standard universel pour l'accès aux fichiers sur un réseau, c'est le protocole le plus utilisé dans les NAS.

Les technologies de stockages



Qu'est-ce que le cloud computing?

- En tant que gérant ou administrateur IT, **vous devez:**
 - Acheter, installer et maintenir régulièrement de nouveaux serveurs, logiciels et plateformes de développement.
 - Optimiser, dimensionner et étendre le système d'information de l'entreprise à la demande, en fonction de l'utilisation attendue



Qu'est-ce que le cloud computing?

Réfléchir à votre consommation d'électricité:

N'utiliser que des ressources dont vous avez besoin, par exemple le processeur, la bande passante, le stockage, la mémoire vive, etc.



Le nuage d'informatique est comme les centrales électriques où on peut obtenir les ressources très rapidement et facilement

Historique du Cloud Computing

- Inventé en 2002 par Amazon, un leader du e-business, qui avait investi dans un parc de machines immense, dimensionné pour absorber la charge importante des commandes faites sur leur site au moment des fêtes de Noël
 - **Problème:** Les serveurs sont inutilisés le reste de l'année.
 - **Solution:** Ouvrir toutes ces ressources inutilisées aux entreprises, pour qu'elles les louent à la demande
-  **Migration des serveurs, des logiciels et des plateformes de développement dans le **Cloud Computing****



Le cloud computing

- Le cloud computing est une technologie qui permet de déposer des données sur des serveurs localisés à distance et d'y avoir accès n'importe quand et depuis n'importe quel appareil connecté à internet.



- Tous types de données peuvent y être conservées : mails, images, notes, logiciels, documents bureautique...

Le cloud computing

Il n'existe pas de définition officielle ou standardisée du *Cloud Computing*

- **Définition de NIST**

- « Le cloud computing est un modèle qui permet un accès réseau à la demande à un pool partagé de ressources informatiques configurables (réseaux, serveurs, stockage, applications et services) qui peuvent être provisionnées rapidement, distribuées avec un minimum de gestion et payées à l'usage»

Quelle utilisation?

- On distingue surtout deux grandes utilisations du cloud:
 - le stockage de données en ligne grâce à des sites internet spécialisés (ou non) qui proposent un espace de stockage.
 - les services en ligne: certains logiciels, applications et jeux vidéo sont accessibles directement sur internet sans avoir à installer quoique ce soit sur son ordinateur.

Quelle utilité?

- Partage
- Sauvegarde
- Accessibilité
- Mobilité
- Pas d'installation

Les déclinaisons

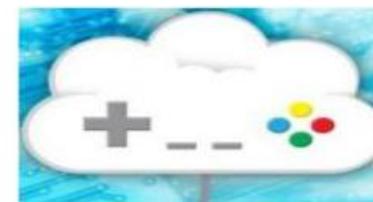
CLOUD PRINTING

les imprimantes sont connectées à internet ,
on peut imprimer de n'importe où et depuis n'importe
quel appareil connecté.



CLOUD GAMING

Lorsqu'une personne souhaite jouer
à un jeu vidéo, c'est un serveur distant qui lance le jeu.



CLOUD LEARNING

Dispositif de formation à distance.



Les types de cloud



Les caractéristiques du cloud

Caractéristiques principales

Réseaux à bande
passante élevée

Elasticité
Souplesse

Services
mesurés

Services à la
carte

Partage des ressources

Modèles de services

SaaS

Software as a Service

PaaS

Platform as a Service

IaaS

Infrastructure as a Service

Modèles de déploiement

Public

Privé

Hybride

Communautaire

Les caractéristiques essentielles du cloud

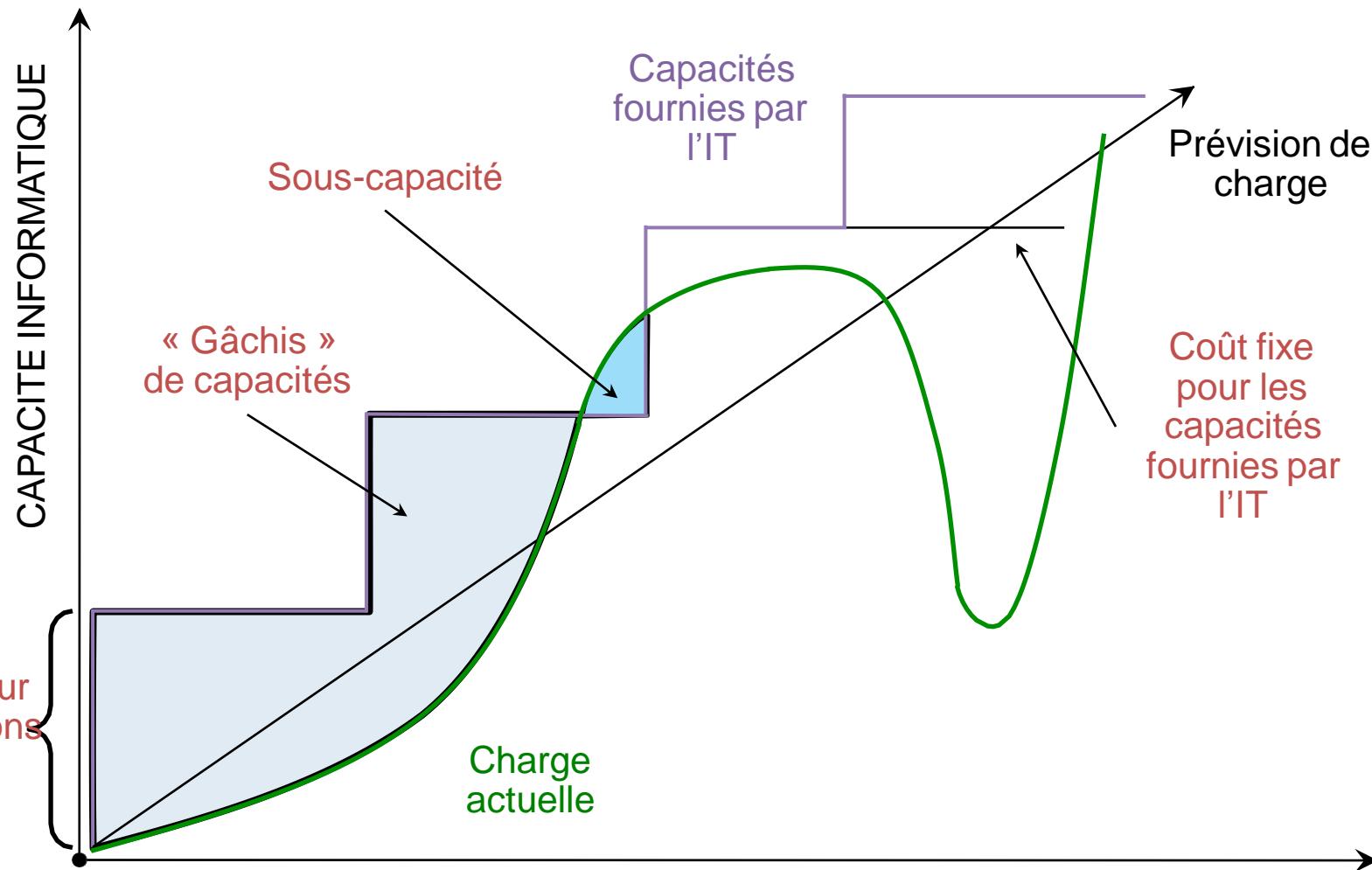
- Elasticité « Rapid elasticity »
- Ressources en libre-service « self-service »
- Accès réseau ubiquitaire « Location independence »
- Mise en commun des ressources « Ressource pooling »
- Service mesurable et facturable « Pay-as-you-go »

Elasticité

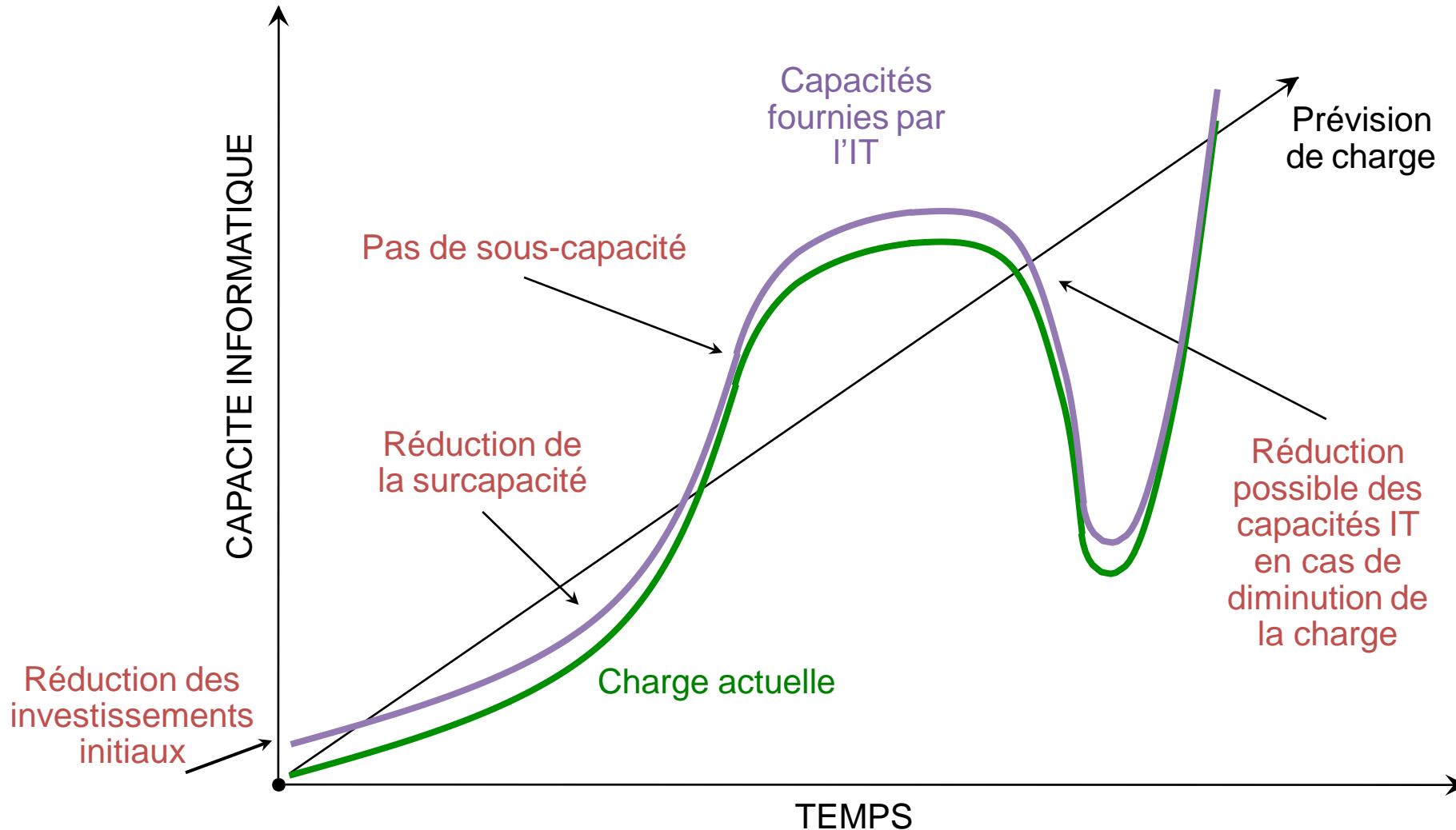
- Adaptation rapide des ressources à une variation du besoin



Sans Cloud : Faible optimisation



Avec Cloud : Optimisation dynamique



Libre service

- Ressources en libre-service « self-service » offertes à la demande sans intervention humaine



Accès réseau ubiquitaire

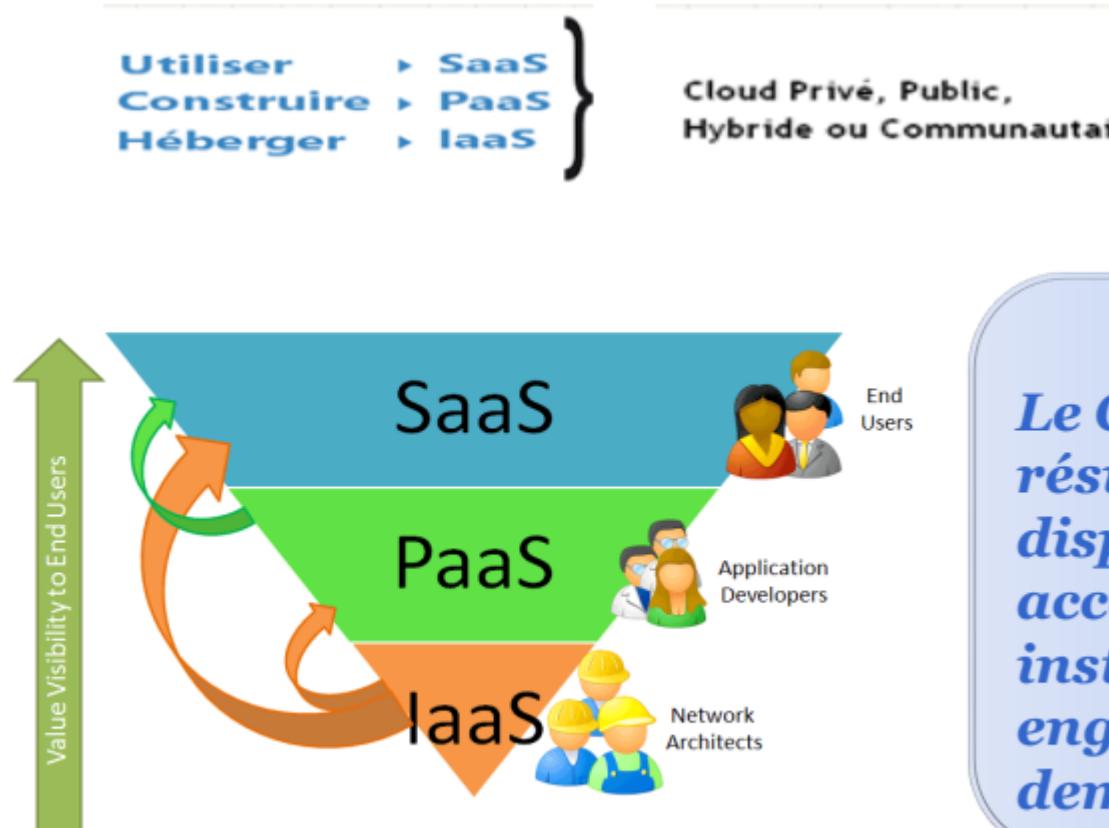


Paiement à l'usage

- Service mesurable et facturable à l'utilisation
 - « Pay-as-you-go »

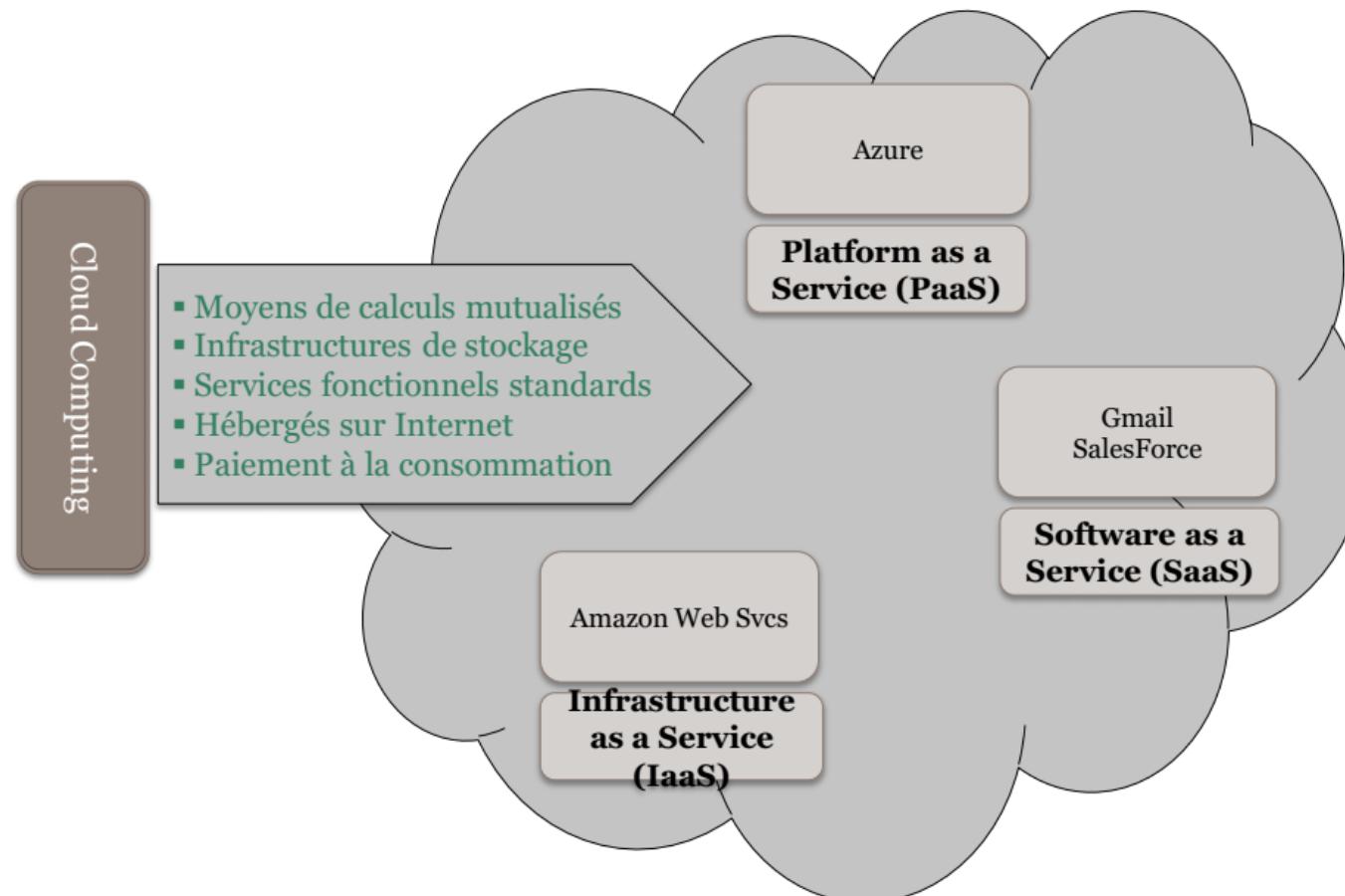


Les principaux services du cloud

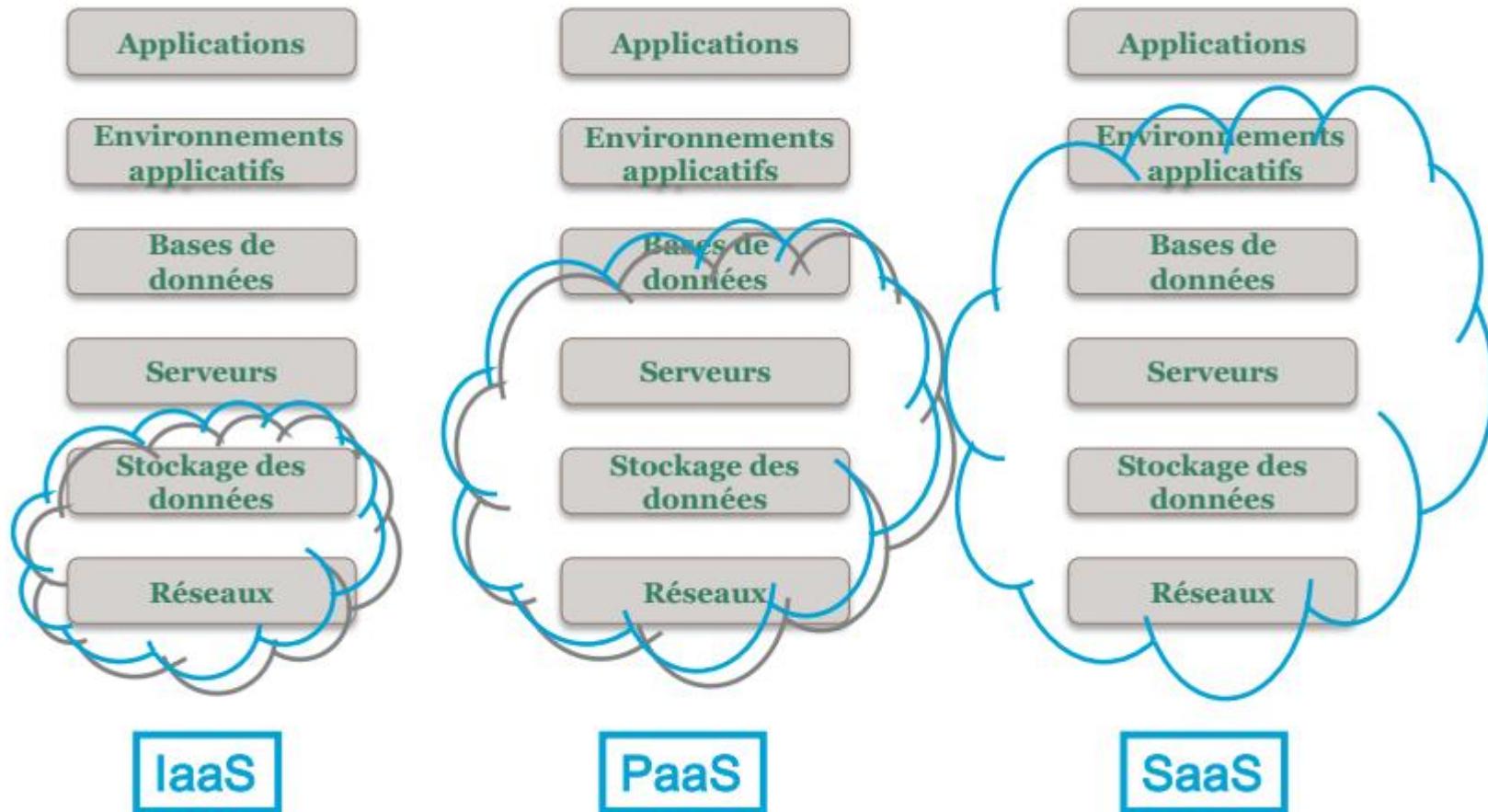


Le Cloud Computing se résume en : Services disponibles et accessibles à tous, instantanément, sans engagement et à la demande.

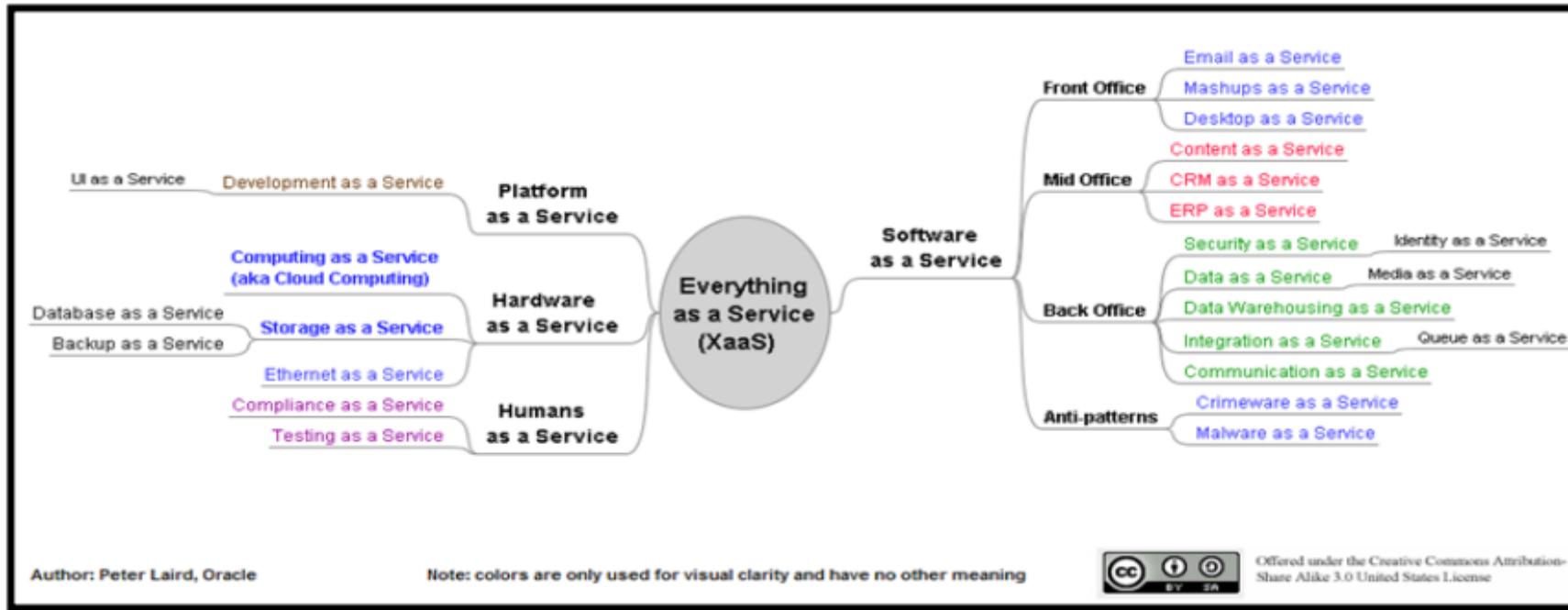
Modèle de service



Les trois grands services du cloud



Les trois grands services du cloud



Le «Cloud Computing» se décline déjà selon 3 tendances:

- SaaS: Software as a Service
- Paas: Platform as a Service
- IaaS: Infrastructure as a Service

Les acteurs du marché

Avec l'expansion du marché du Cloud Computing, on voit apparaître un nombre croissant d'acteurs.

Fournisseurs principaux	SaaS	PaaS	IaaS
	CRM		
	ERP		
	SCM		
	CCC	 	Stockage & Sauvegarde
	DCC		Calcul
	Int.aaS		Cloud Privés

CRM : Customer Relationship Management

ERP : Enterprise Resource Planning

SCM : Supply Chain Management

CCC : Content Communication and Collaboration

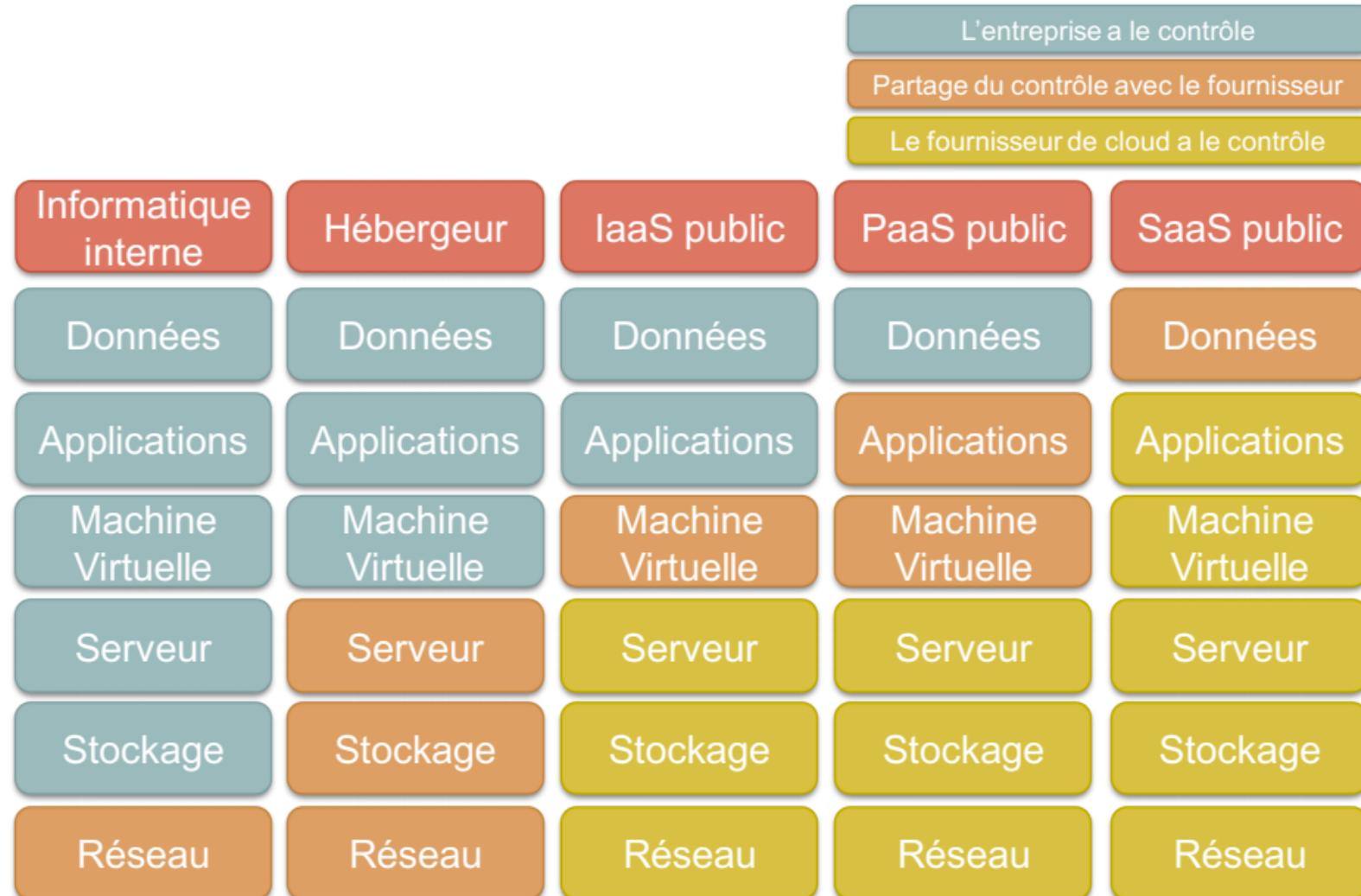
DCC : Digital Content Creation

Int.aaS : Integration-as-a-Service

Les acteurs du marché

SaaS	<ul style="list-style-type: none">• Le Gestionnaire de Relation Client (CRM)• La comptabilité et la finance• La visioconférence• La gestion des ressources humaines• Les communications unifiées• La messagerie et les logiciels collaboratifs	
PaaS	<ul style="list-style-type: none">• Plateformes propriétaires de développement d'applications	
IaaS	<ul style="list-style-type: none">• Espace sécurisé dans une salle machine• Machines virtuelles ou machine physique• Unités de calculs	

Qui contrôle quoi?



SaaS (Software as a Service)

- Concerne la mise à disposition d'applications d'entreprise : CRM, outils collaboratifs, messagerie, Business Intelligence, ERP, etc.
- Le fournisseur offre une fonction opérationnelle et gère de façon transparente pour l'utilisateur l'ensemble des aspects techniques requérant des compétences informatiques. Le client garde la possibilité d'effectuer quelques paramétrages de l'application.
 - ✓ Salesforce CRM, Microsoft Dynamics CRM on line (Gestion Relation Client).
 - ✓ Google Apps(Outils bureautiques):Google documents, Agenda, meet...
 - ✓ BaseCamp(Gestion de projets)– La tendance est au travail en mode projet et il est important d'y avoir accès en continué.
 - ✓ FaceBook, Viadeo(Réseaux sociaux): nouveau mode de communication.

PaaS (Platform as a Service)

- PaaS propose à l'utilisateur d'avoir accès à une véritable plate-forme de développement (langage de programmation, outils de développements, modules).
 - ✓ Force.Com (SalesForce), Titan(Microsoft Dynamics CRM)(Gestion Relation Client).
 - ✓ Google App Engine(Développer un site web dynamique)
 - ✓ Intuit(Comptabilité)

IaaS (Infrastructure as a Service)

Concerne la mise à disposition de ressources informatiques (puissance CPU, mémoire, stockage...).

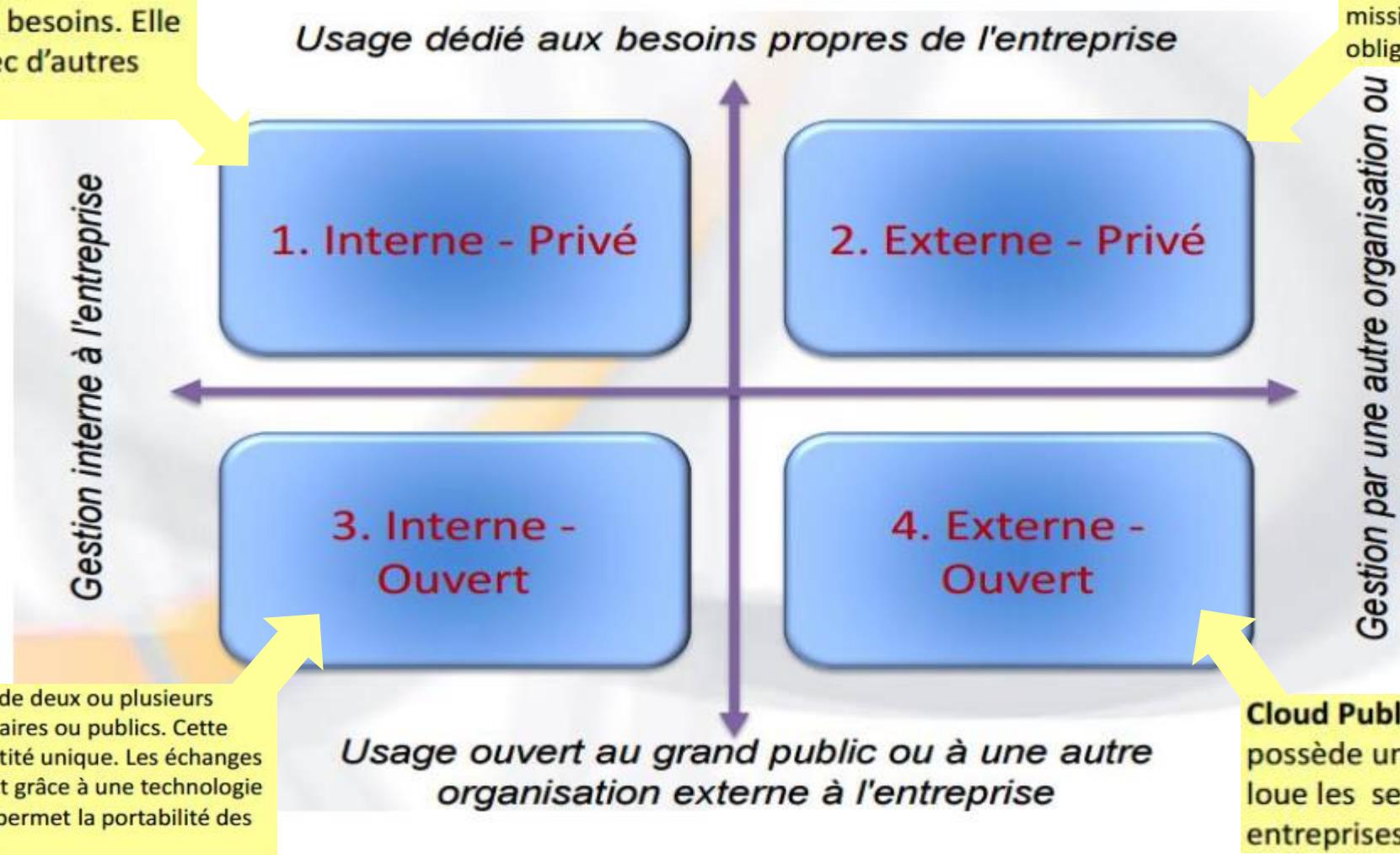
PaaS proposait des plateformes de développement mutualisées, IaaS propose des plateformes de production mutualisées.

- **Microsoft**
- **Azure**: Virtualisation du système, des outils de développement et des applications.
- **IBM**
- **Blue Cloud** – Système Open source(Red Hat Entreprise Linux)+applications (Websphere, DB2...).
- **Amazon S3** : Offre un stockage illimité
- **Elastic Compute Cloud (EC2)** : Images serveur

Les 4 modèles de déploiement

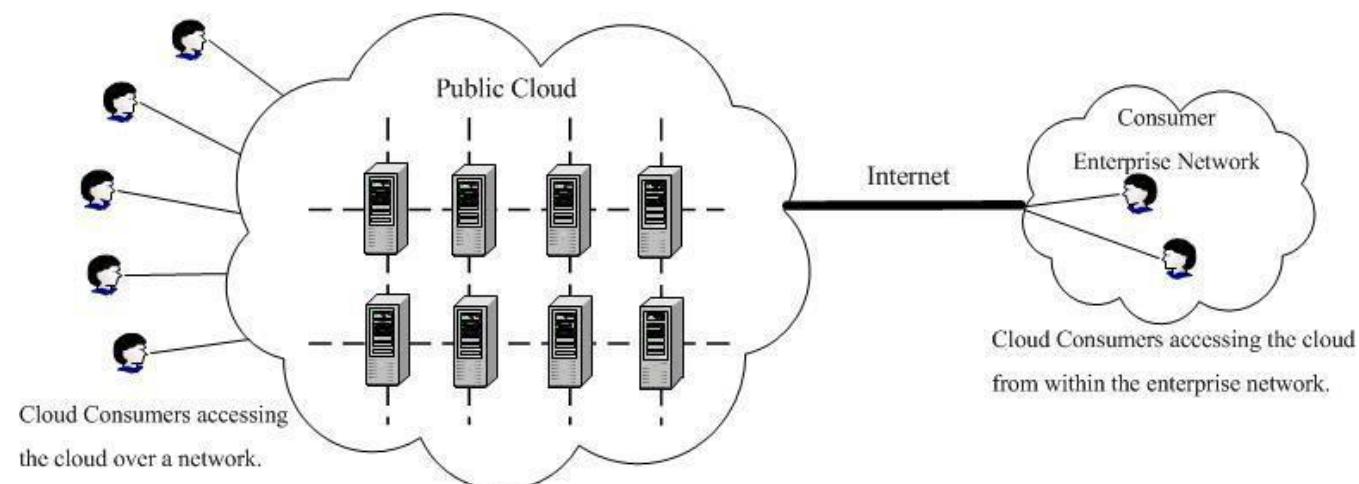
Cloud Privé : une seule et unique organisation loue ou possède son infrastructure, et la gère uniquement pour ses besoins. Elle ne la partage pas avec d'autres organisations

Cloud communautaire : l'infrastructure est partagée par plusieurs organisations et concerne une communauté spécifique qui partage des intérêts communs (une mission, des exigences de sécurité, des obligations légales, etc)



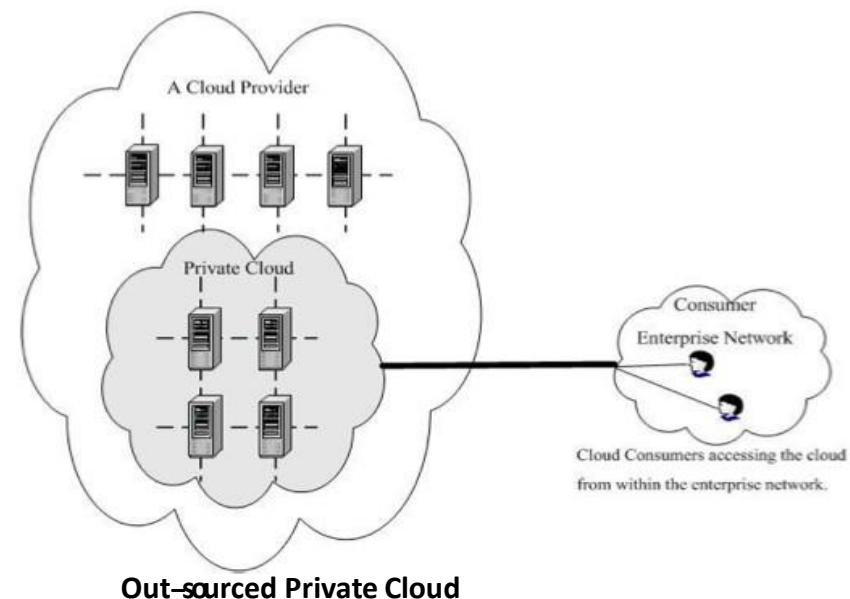
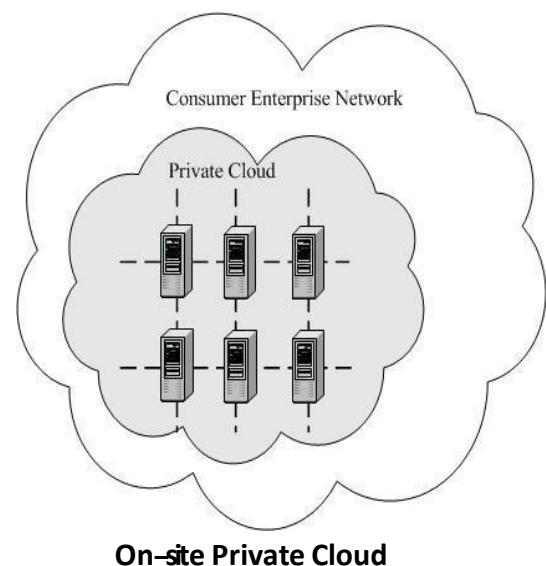
Cloud Public

- Le cloud est **externe à l'organisation**, accessible via **Internet**, géré par un **prestashop externe** propriétaire des infrastructures, avec des ressources partagées entre plusieurs sociétés.
- Les fournisseurs Cloud mettent à la disposition de leurs clients des services et des infrastructures mutualisées, extensibles et disponibles en permanence.



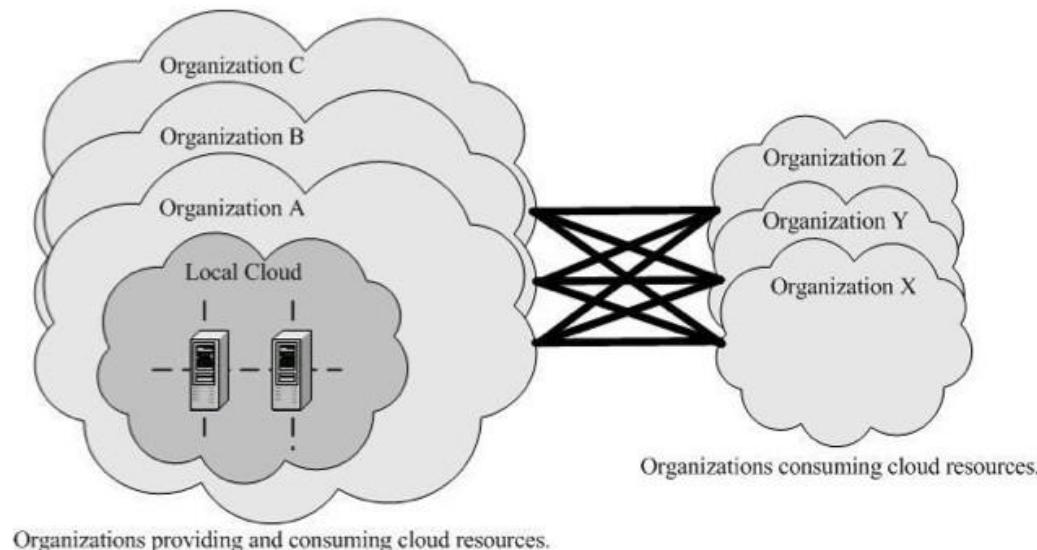
Cloud Privé

- Cloud interne à la DSI (propriétaire des infrastructures) ou entièrement dédié et accessible via des réseaux sécurisés, hébergé chez un tiers, mutualisé entre les différentes entités **d'une seule et même entreprise**.
- Ouvert aux partenaires privilégiés de l'entreprise (fournisseurs, bureaux d'études, grands clients, institutions financières, prestataires-clés...)



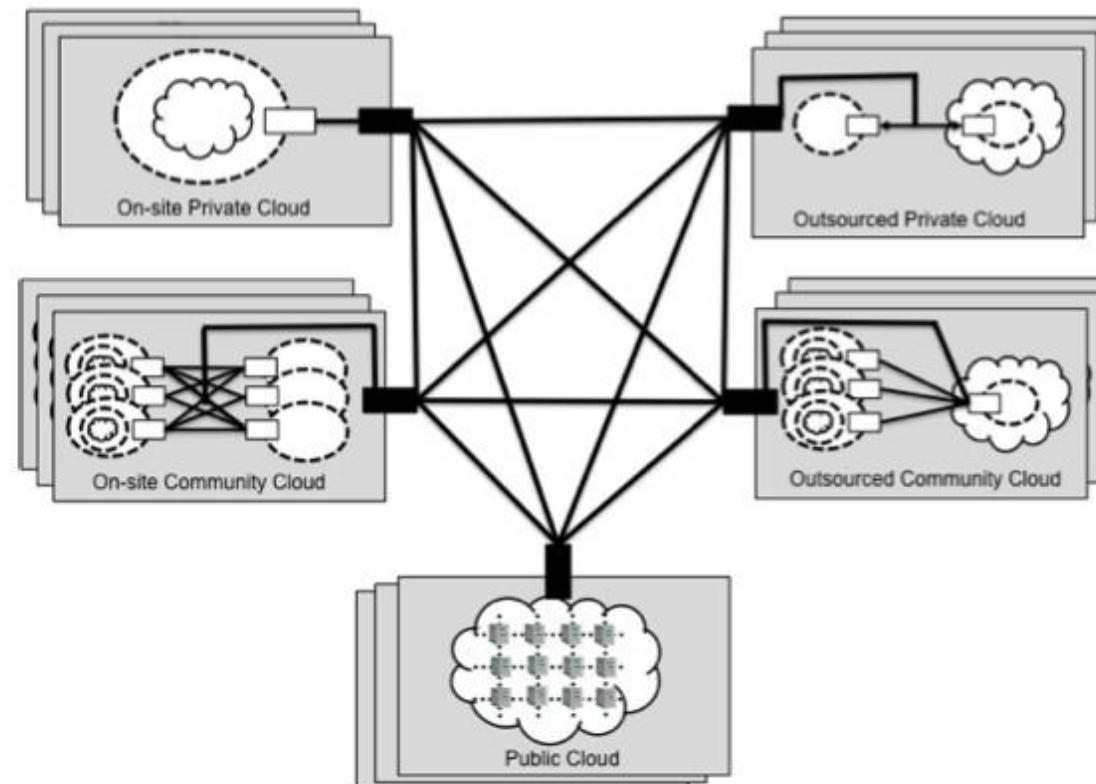
Cloud communautaire

- Il s'agit d'une variation du modèle de Cloud Public incluant uniquement les membres de plusieurs entreprises.
- Les ressources et les services sont partagées à l'échelle d'une communauté (ex: à l'échelle d'un état, d'une ville, d'une académie, ...).

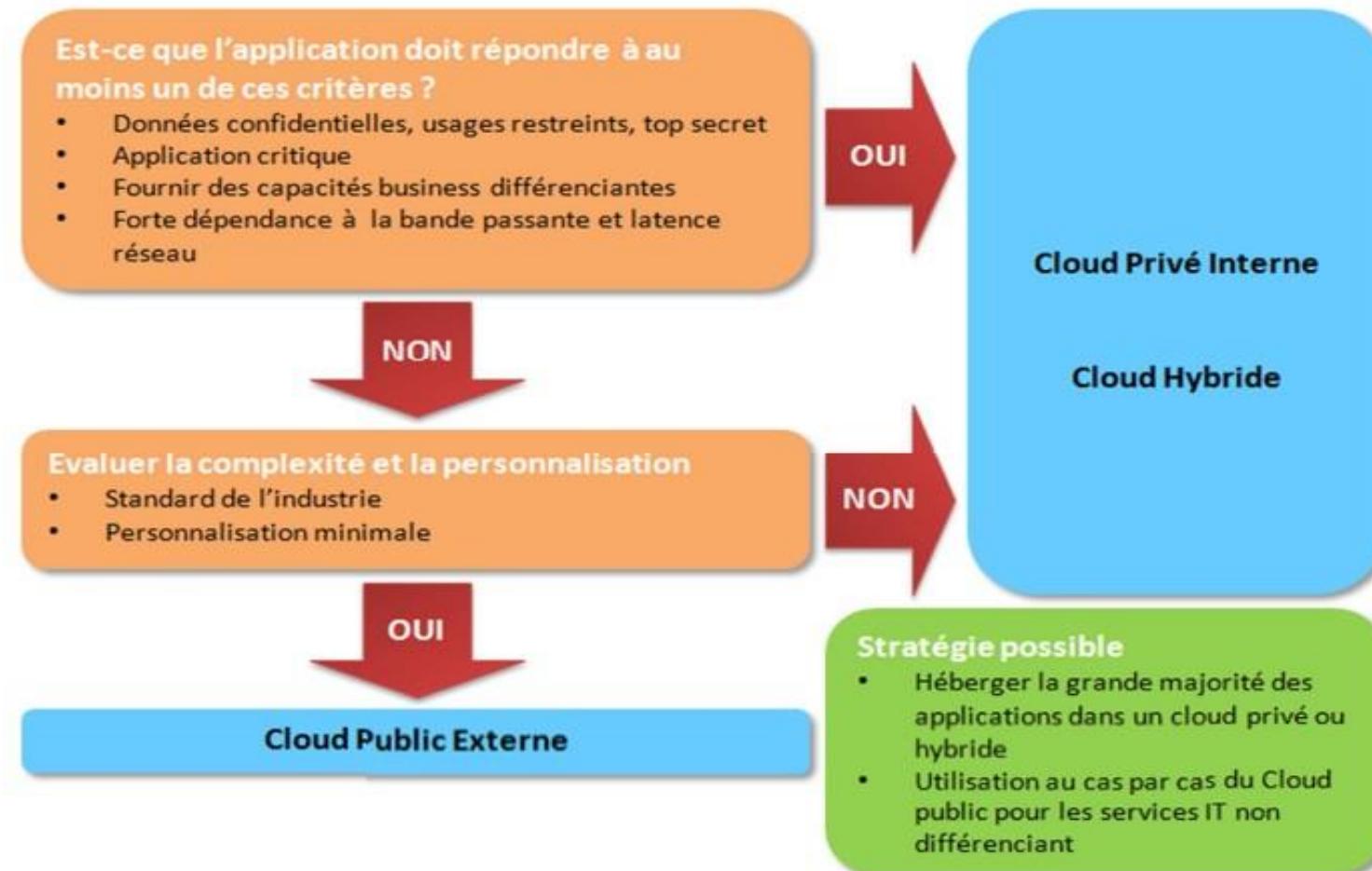


Cloud hybride

- Un Cloud Hybride est la combinaison de Cloud Privé et de Cloud Public.

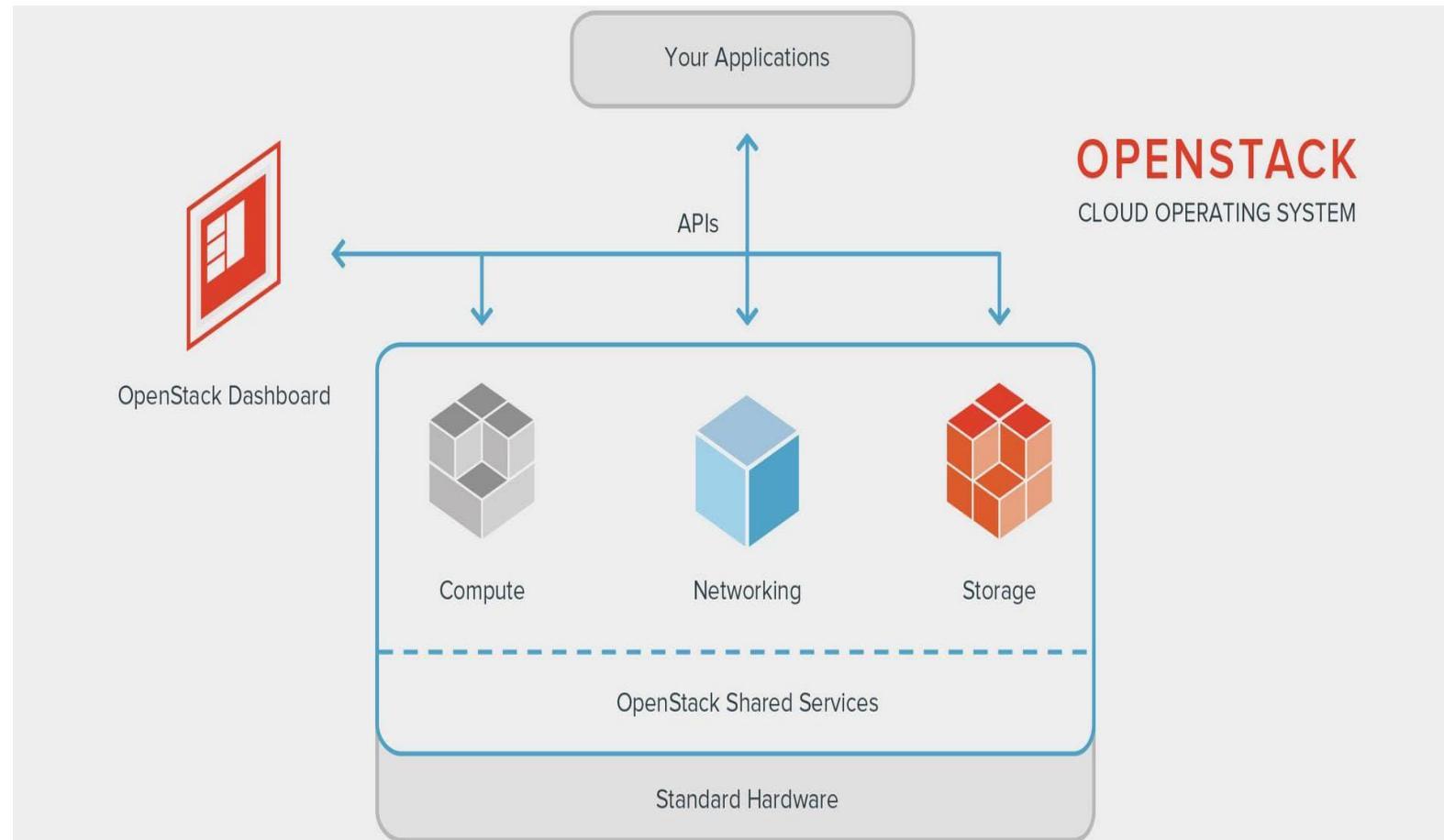


Privé ou Public ?



Openstack

Qu'est-ce que OpenStack ? Et de quoi est-il composé ?



Openstack

Qu'est-ce que OpenStack ? Et de quoi est-il composé ?

- OpenStack est un ensemble de logiciels open source permettant de déployer des infrastructures de cloud computing (**infrastructure en tant que service IaaS**).
- La technologie possède une architecture modulaire composée de plusieurs projets corrélés (Nova, Swift, Glance...) qui permettent de contrôler les différentes ressources des machines virtuelles telles que la puissance de calcul, le stockage ou encore le réseau inhérents au centre de données sollicité.

LES CONCEPTS INFRASTRUCTURE AS A SERVICE

- Compute
- Storage
- Network

Compute

- Instance
- Image
- Flavor (gabarit)
- Paire de clé (SSH)

Instance

- Dédiée au compute
- Durée de vie typiquement courte, à considérer comme éphémère
- Ne doit pas stocker de données persistantes, Disque racine non persistant
- Basée sur une image

Image Cloud

- Image disque contenant un OS déjà
- Instanciable à l'infini
- Sachant parler à l'API de metadata

Flavor

- Instance type chez AWS
- Définit un modèle d'instance en termes de CPU, RAM, disque (racine), disque éphémère
- Le disque éphémère a, comme le disque racine, l'avantage d'être souvent local donc rapide

Paire de clé

- Clé publique + clé privée SSH
- Le cloud manipule et stocke la clé publique
- Cette clé publique est utilisée pour donner un accès SSH aux instances

Ressource stockage

Le cloud fournit deux types de stockage :

- Block
- Objet

Stockage Block

- Volumes attachables à une instance
- Possibilité d'utiliser n'importe quel système de fichiers
- Possibilité d'utiliser du LVM, du chiffrement, etc.
- Compatible avec toutes les applications existantes
- Nécessite de provisionner l'espace en définissant la taille du volume

Stockage Partagé?

- Le stockage block n'est pas une solution de stockage partagé comme NFS
- NFS se situe à une couche plus haute : système de fichiers
- Un volume est a priori connecté à une seule machine

BOOT FROM Volume

Démarrer une instance avec un disque racine sur :

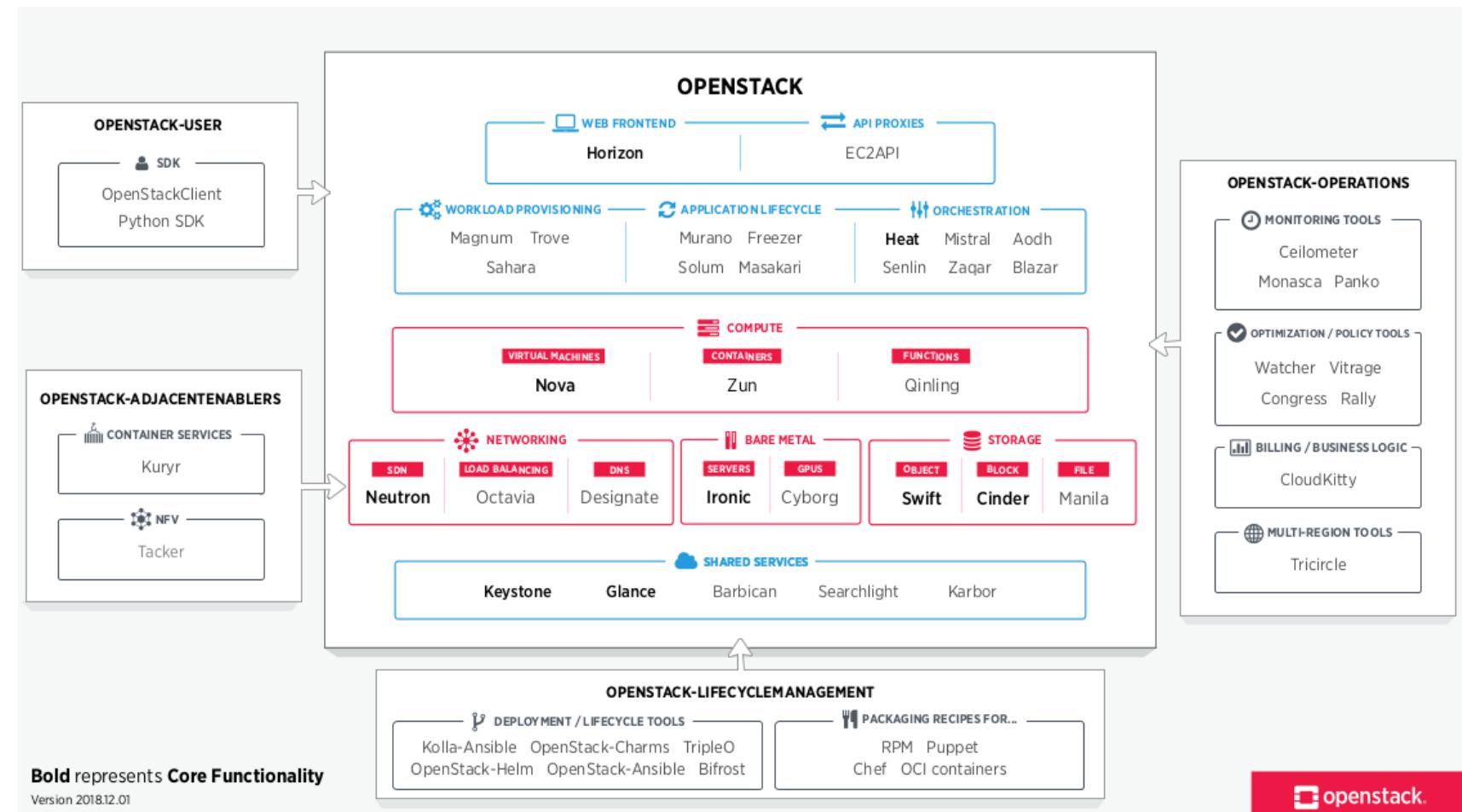
- un volume Persistance des données du disque racine
- Se rapproche du serveur classique

Network

- Réseau L2
- Port réseau
- Réseau L3
- Routeur
- IP flottante
- Groupe de sécurité

Openstack

- OpenStack est composé d'une série de logiciels et de projets au code source libre qui sont maintenus par la communauté incluant: Nova, Swift, Glance, Horizon, Neutron... etc.
- La figure suivante donne une visibilité plus ou moins complète sur ces derniers.



Openstack

- Ces logiciels sont regroupés dans des couches selon les fonctionnalités dont ils disposent.
Chaque couche colorée en rouge représente un type d'infrastructure.
- Les couches colorées en bleu représentent des services à un aspect plus logique (plus abstrait).
- Pour plus de détail voir le lien ci-dessous:

<http://sysblog.informatique.univ-paris-diderot.fr/2019/03/24/quest-ce-que-openstack-et-de-quoi-est-il-compose/>

Openstack

OPENSTACK EST UN LOGICIEL OPENSOURCE PERMETTANT DE DÉPLOYER DES CLOUDS PRIVES ET PUBLICS

- Contrôler et automatiser les pools de ressources
- Optimiser l'allocation de ressources
- Donner le contrôle aux admins et aux utilisateurs via le portail - Garantir la conformité
- Permettre aux développeurs de rendre leurs applications «cloud aware» grâce aux APIs

Openstack

- **OpenStack Compute** : provisionner et contrôler un large réseau de machines
- **OpenStack Object Storage** : créer une plateforme de stockage de plusieurs Petabytes hautement disponible à l'aide de serveurs standards
- **OpenStack Image Service** : gérer et organiser un large catalogue d'images de machines

Utiliser Openstack

- Toutes les fonctionnalités sont accessibles par l'API
- Les clients (y compris Horizon) utilisent l'API
- Des crédentials sont nécessaires
- API OpenStack : utilisateur + mot de passe + projet (tenant) + domaine
- API AWS : access key ID + secret access key

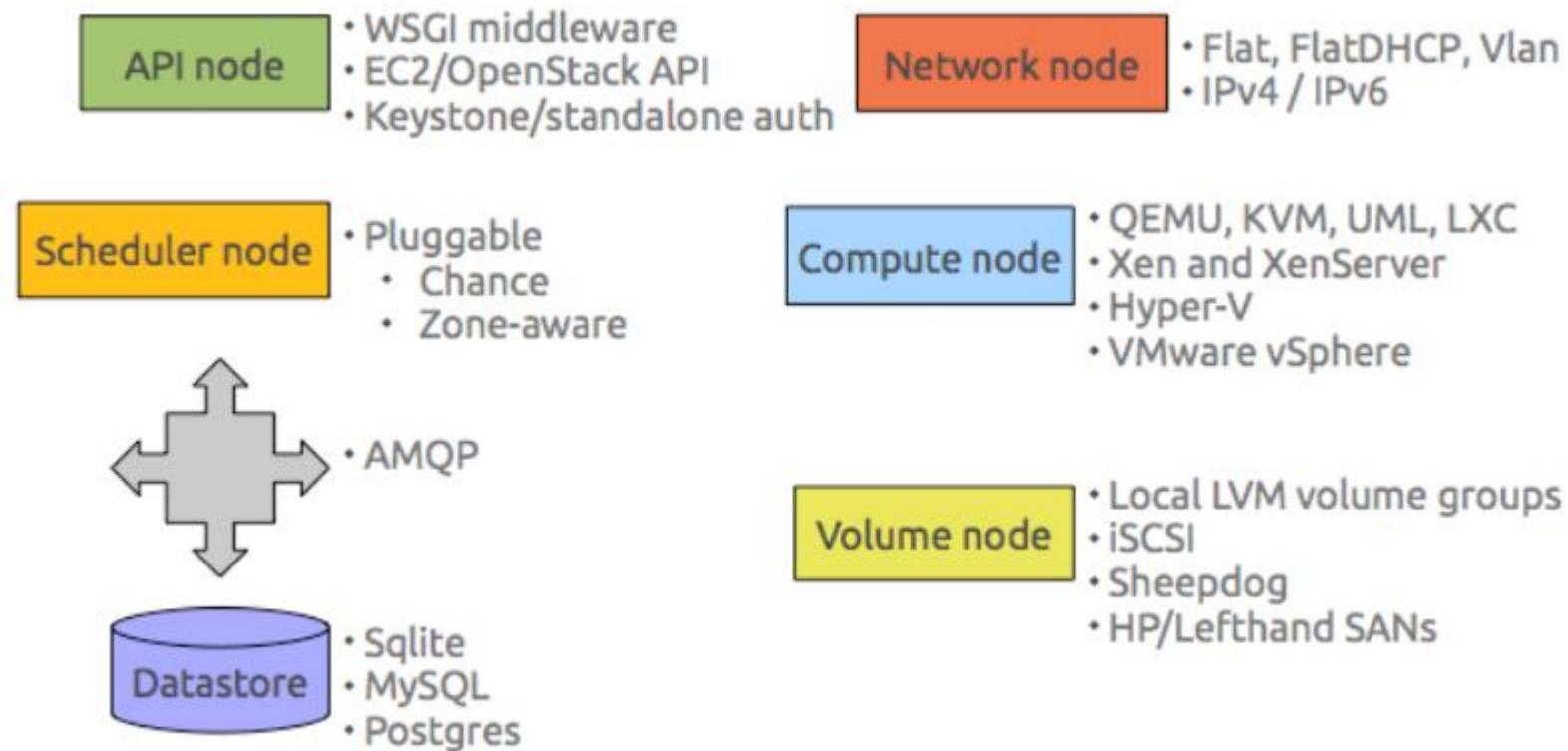
KEYSTONE : AUTHENTIFICATION, AUTORISATION ET CATALOGUE DE SERVICES

- Annuaire des utilisateurs et des groupes
- Gère des domaines
- Liste des projets (tenants)
- Catalogue de services
- Gère l'authentification et l'autorisation
- Fournit un token à l'utilisateur

Nova

- Gère le cycle de vie d'instances de compute dans un environnement OpenStack
- Les responsabilités incluent la génération dynamique, la planification et la mise hors service de machines virtuelles à la demande
 - Provisioning et gestion de machines virtuelles
 - Contrôle direct par API
 - Framework modulaire
 - Multi-hyperviseur

Une conception très modulaire: Nova



Propriété d'une instance

- Éphémère, a priori non hautement disponible
- Définie par une flavor
- Construite à partir d'une image
- Optionnel : attachement de volumes
- Optionnel : boot depuis un volume
- Optionnel : une clé SSH publique
- Optionnel : des ports réseaux

Glance : Registre d'image

- Registre d'images et de snapshots
- Propriétés sur les images
- Est utilisé par Nova pour démarrer des instances

Glance supporte un large éventail de types d'images, limité par le support de la technologie sous-jacente à Nova

API

Ils consistent à gérer

- Instances
- Flavors (types d'instance)
- Keypairs
- Indirectement : images, security groups (groupes de sécurité), floating IPs (IPs flottantes)
- Reboot / shutdown Snapshot
- Lecture des logs Accès VNC
- Redimensionnement
- Migration (admin)

SWIFT (OBJECT STORAGE)

Swift (OpenStack Object Storage)

- Solution de stockage évolutive
- Stockage d'objets
- Interface REST
- Pas de Single Point of Failure
- Pas de taille limite d'objet
- Coefficient minimum de réPLICATION de 3, dans des «zones» séparées
- Stable et déployé en production
- Utilise des serveurs standards

Le service Neutron

- Le service Neutron d'OpenStack permet de gérer et manipuler les réseaux et l'adressage IP au sein d'OpenStack.
- Avec Neutron, les utilisateurs peuvent créer leurs propres réseaux, contrôler le trafic à travers des groupes de sécurité (security groups) et connecter leurs instances à un ou plusieurs réseaux.
- Neutron gère aussi l'adressage IP des instances en leur assignant des adresses IP statiques ou par l'intermédiaire du service DHCP.
- Il fournit aussi un service d'adresse IP flottante que l'on peut assigner aux instances afin d'assurer une connectivité depuis Internet.

Le service Neutron

L'API permet notamment de manipuler ces ressources :

- Réseau (network) : niveau 2
- Sous-réseau (subnet) : niveau 3
- Port : attachable à une interface sur une instance, un load-balancer, etc.
- Routeur
- IP flottante, groupe de sécurité

IP flottantes

- En plus des fixed IPs portées par les instances
- Allocation (réservation pour le projet) d'une IP depuis un pool
- Association d'une IP allouée à un port (d'une instance, par exemple)
- Non portées directement par les instances

Les groupes de sécurité

- Équivalent à un firewall devant chaque instance
- Une instance peut être associée à un ou plusieurs groupes de sécurité
- Gestion des accès en entrée et sortie
- Règles par protocole (TCP/UDP/ICMP) et par port
- Cible une adresse IP, un réseau ou un autre groupe de sécurité

Neutron : Autres Fonctionnalités

Outre les fonctions réseau de base niveaux 2 et 3, Neutron peut fournir d'autres services :

- Load Balancing
- Firewall : diffère des groupes de sécurité
- VPN : permet d'accéder à un réseau privé sans IP flottantes
- QoS

Que peut-on faire avec OpenStack ?

- En raison de la gratuité de la licence, l'utilisation d'OpenStack est particulièrement rentable. Une fois le système mis en place, il est facile à administrer.
- En utilisant les serveurs virtuels des services d'hébergement, **une petite solution de Cloud computing peut être mise en place pour 30 à 60 dinars par mois.**
- Ainsi, OpenStack peut être utilisé comme plateforme pour des applications de Cloud privées comme un serveur d'imagerie médicale par exemple.
- Il permet également de réaliser des projets extraprofessionnels ou des boutiques en ligne.

Installation d'OpenStack

- Sur une distribution Linux UBUNTU voir ce lien
<https://ubuntu.com/openstack/install>
- Ou ce lien pour l'une des distributions Linux que vous préférez
<https://docs.openstack.org/install-guide/>

Les alternatives à OpenStack

- Ceux qui ne souhaitent pas utiliser OpenStack peuvent créer eux-mêmes les services nécessaires grâce à des serveurs virtuels et des stockages en ligne.
- L'utilisation de solutions comme Owncloud ou Nextcloud est également envisageable.

Quelques fournisseurs de solutions similaires :

- **OpenNebula (gratuit)**
- **VMWare (payant)**
- **Microsoft AzureStack (payant)**
- **Google Anthos (payant)**

Documentation

- <https://www.youtube.com/watch?v=Kfj5XiNdJN0>
- [https://www.editions-
eni.fr/open/mediabook.aspx?idR=d6582c7c07a1449b28b4cd0fa5f276
80](https://www.editions-eni.fr/open/mediabook.aspx?idR=d6582c7c07a1449b28b4cd0fa5f27680)
- [https://www.redhat.com/fr/services/training/cl010-red-hat-openstack-
technical-overview?section=Programme](https://www.redhat.com/fr/services/training/cl010-red-hat-openstack-technical-overview?section=Programme)