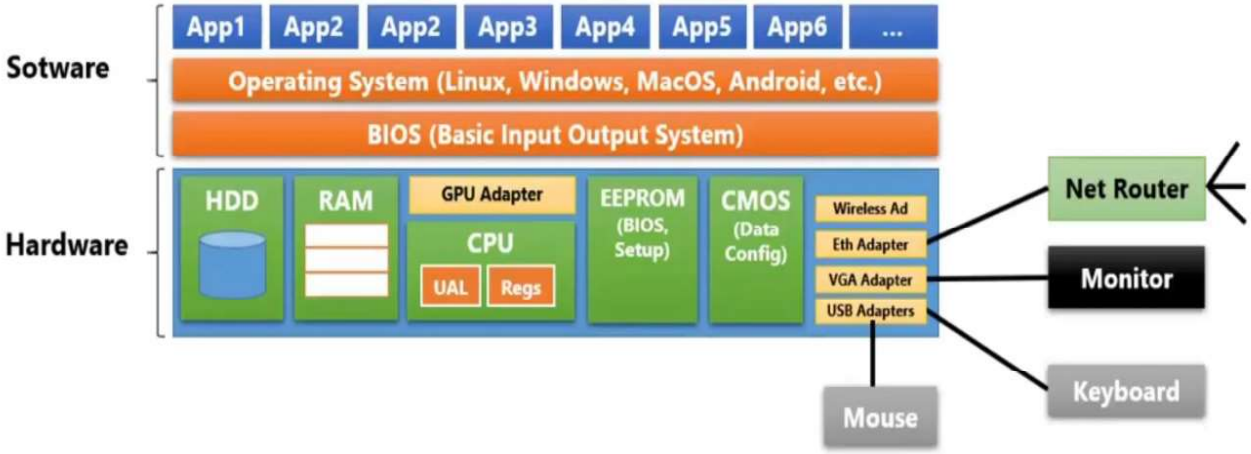
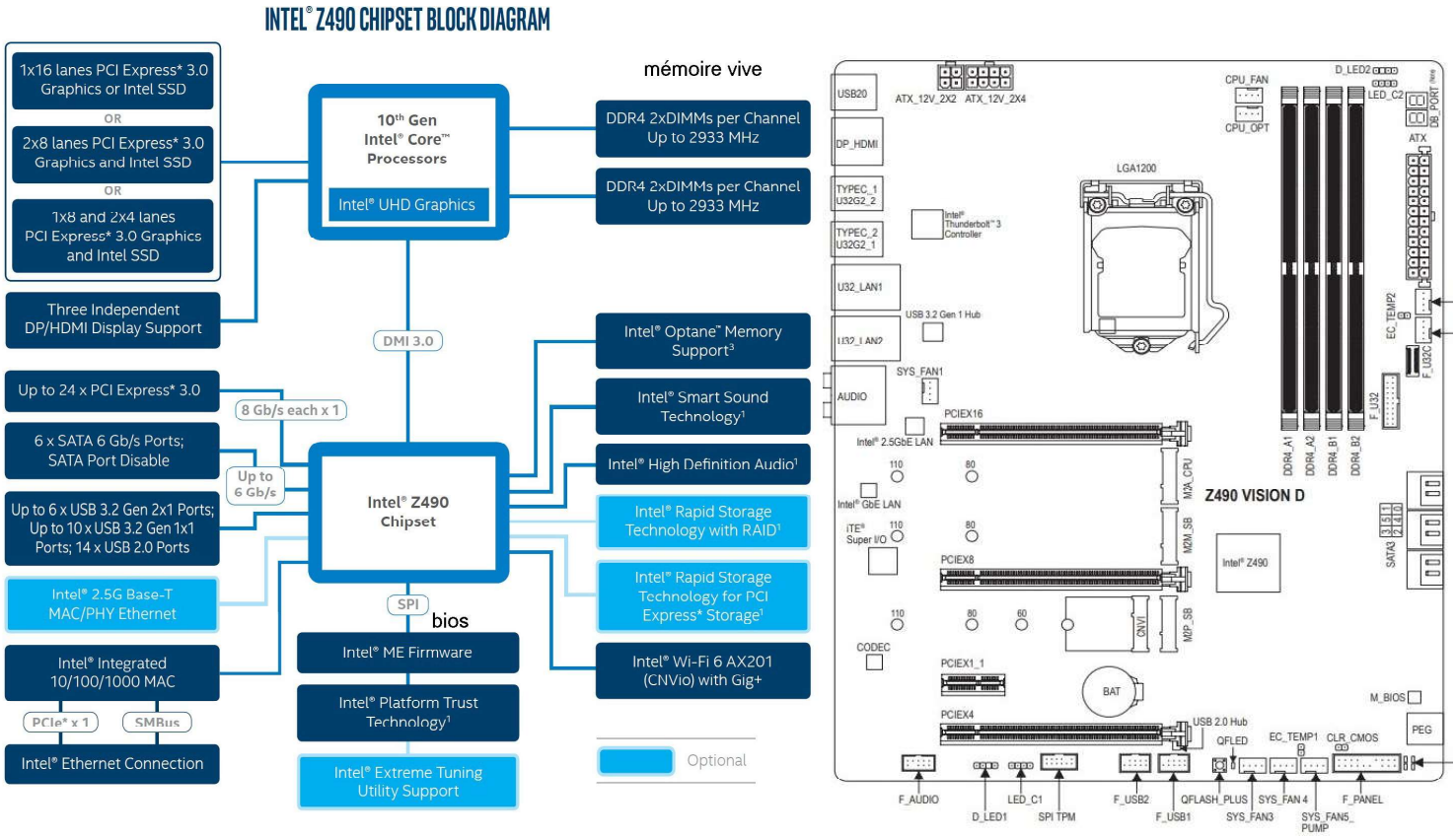
Les infrastructures des machines

1) L'architecture classique

C'est la structure conventionnelle d'une machine d'un utilisateur peu adapté pour la mise en place d'un serveur.

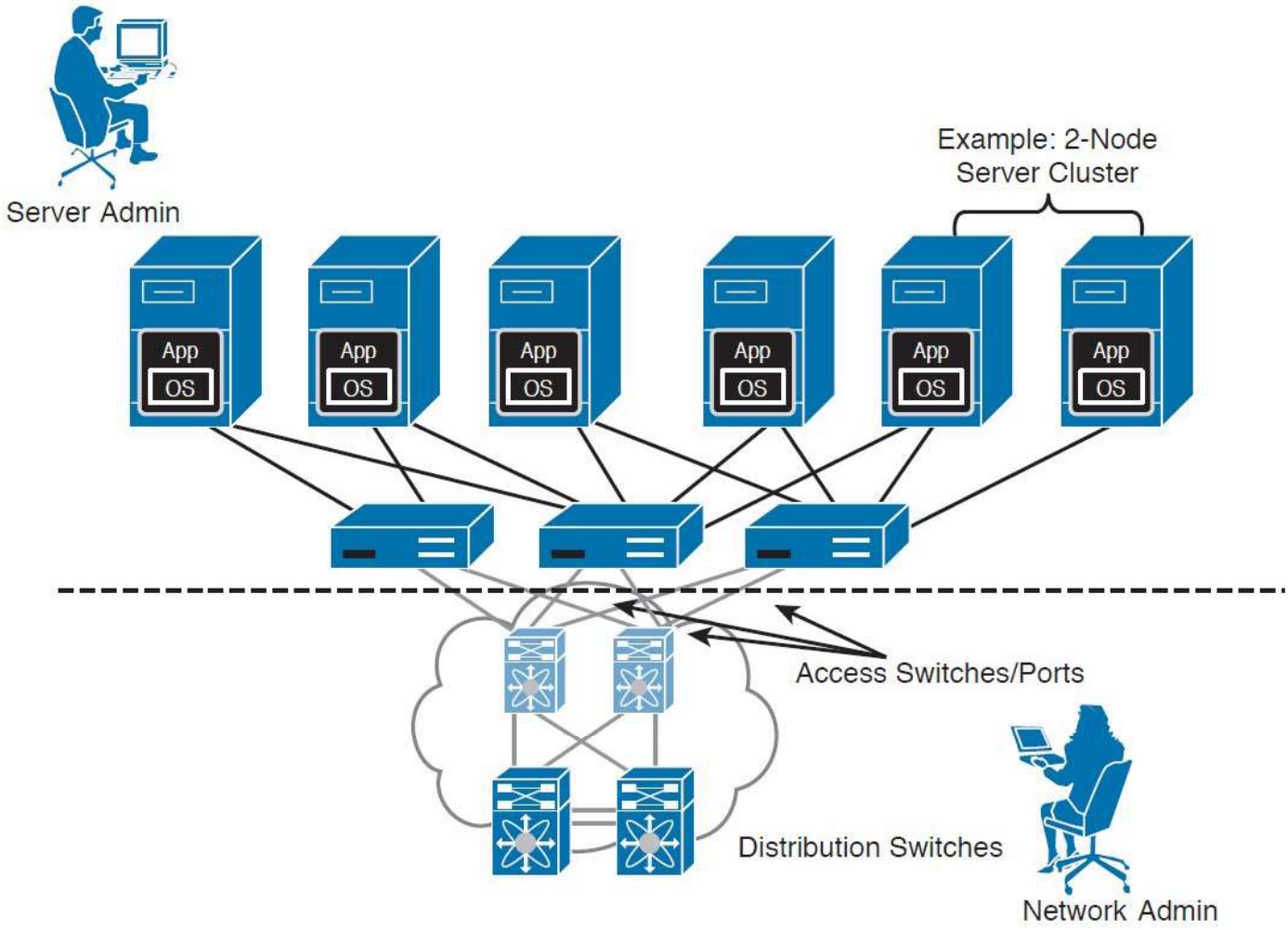


Les ressources processeurs RAM et disque sont très peu optimisées. La migration vers une autre machine ne peut se faire qu'avec une machine identique et est très chronophages (image disque très lourde) . Le matériel est implanté sur une carte mère

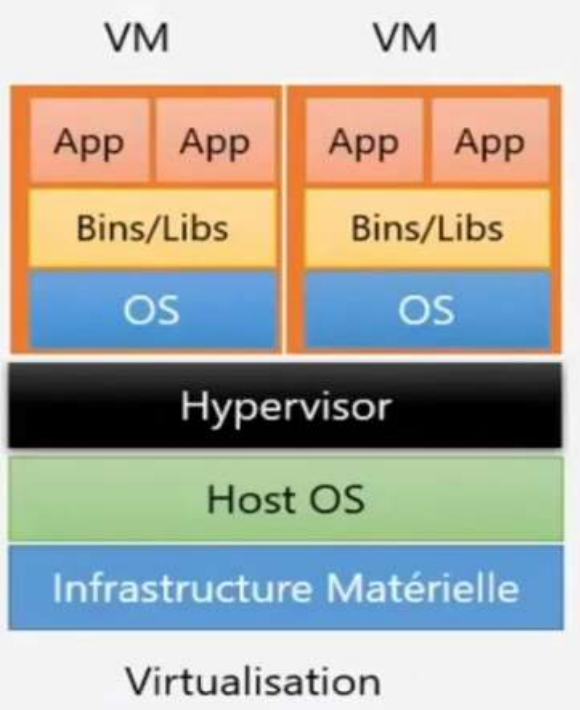


2) La virtualisation

Avant la virtualisation on avait autant de serveur physique que de système d'exploitation.



En virtualisation plusieurs machines virtuelles (VM) **avec des systèmes d'exploitation différents** travaillent sur la même machine grâce à un hyperviseur.



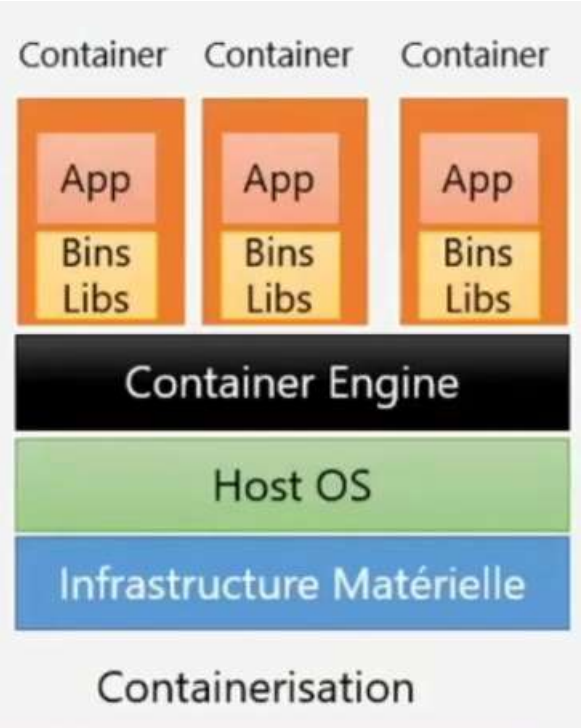
Ces machines virtuelles peuvent migrer facilement vers une autre machine car elles sont quasi indépendantes du matérielle et on n'a pas l'obligation de tout réinstaller grâce à des images disques des VM . La duplication des VM vers d'autre machine reste aisée et permet d'améliorer la résilience du système . Une répartition des charges processeurs attribuée aux VM peut se faire sur plusieurs machines par migration.

On obtient donc une meilleur optimisation des ressources processeurs, RAM et disques.

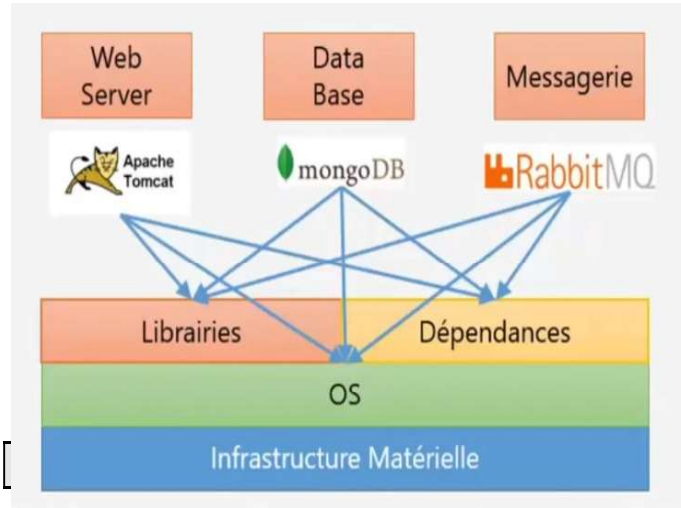
Le temps de démarrage d'une telle infrastructure est plus lente.

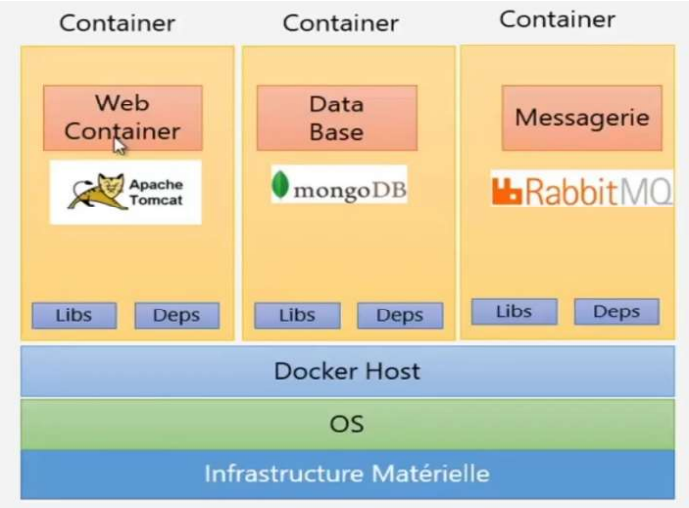
3) La containérisation

Dans ce cas précis on va virtualiser les différentes applications grâce à un moteur de conteneur. Les applications seront virtualisées avec ses dépendances dans un conteneur à partir d'une image. Le conteneur va permettre d'isoler et de packager une application avec juste ce dont elle a besoin pour fonctionner.

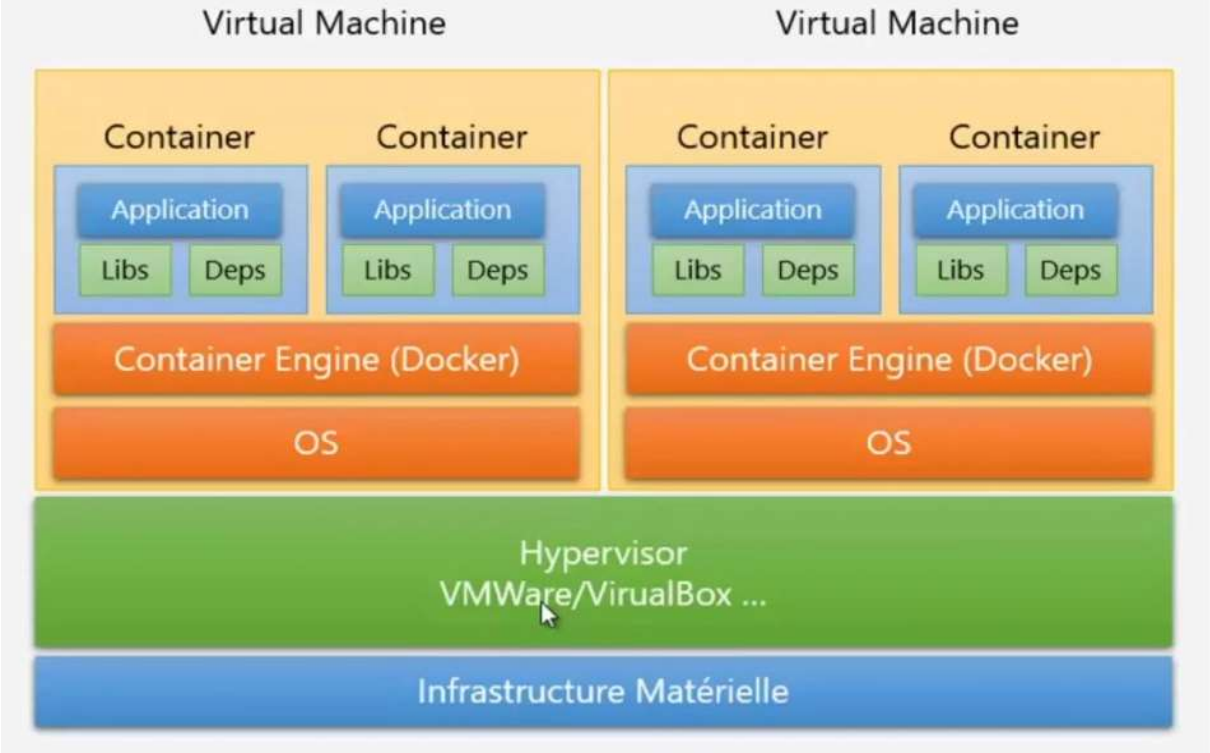


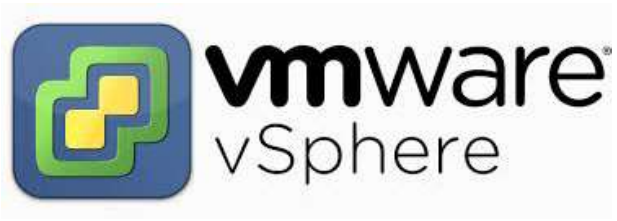
Cette décomposition de l'infrastructure applicative permet d'avoir des petits éléments légers, très facile à déployer sur des machines différentes. Le démarrage de la machine est quasi instantanée. Tous les conteneurs utilisent le même kernel et consomment peu de ressources machines.



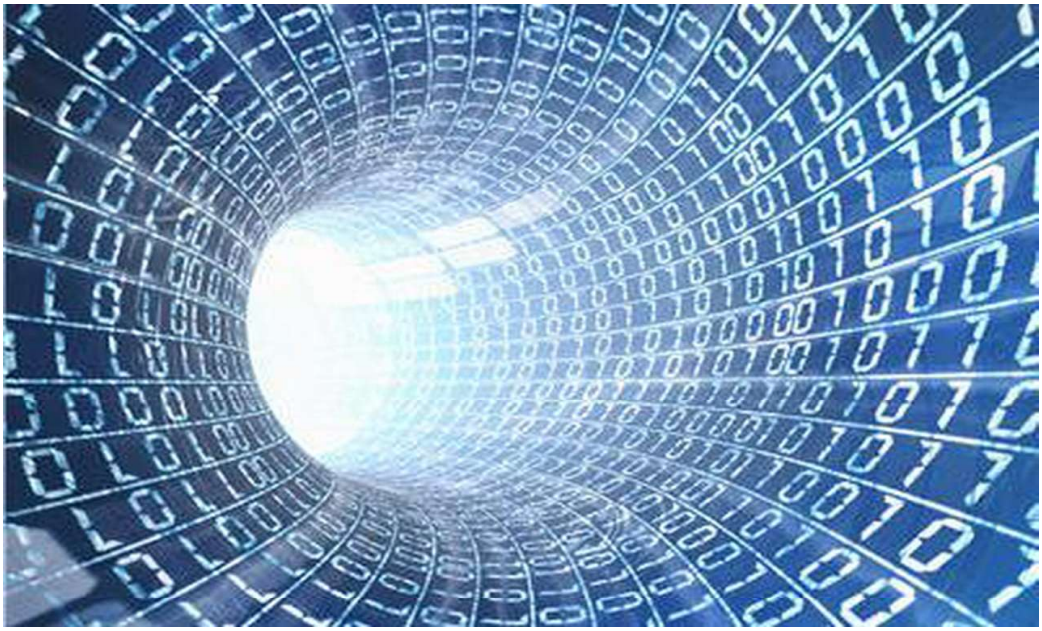


Une solution mixte de virtualisation et de containérisation peut être aussi adoptée.





Les hyperviseurs







Les hyperviseurs

1) Présentation

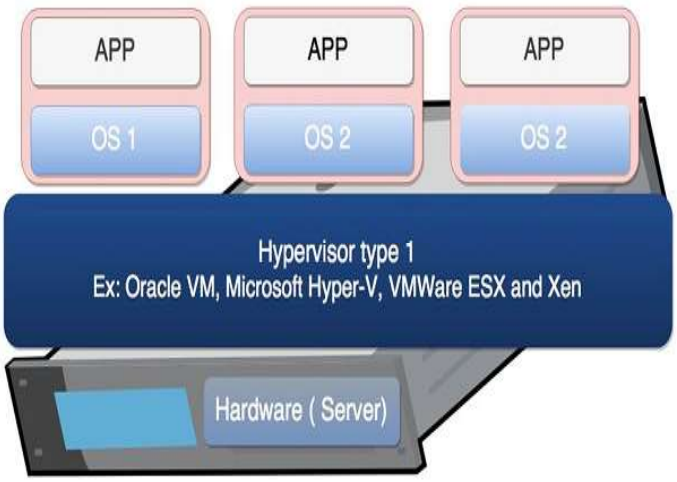
De nos jours, les entreprises ont de plus en plus recourt à la virtualisation de leur infrastructure, que ce soit pour répondre à des problématiques de coûts, de performances ou de souplesse dans le fonctionnement.
Un hyperviseur, dans sa forme la plus basique, est un outil permettant à plusieurs systèmes d'exploitation (Windows, Linux, etc..) de tourner sur une même machine physique.
L'hyperviseur n'aura que pour but d'accueillir ces machines, et d'allouer les ressources nécessaires au fonctionnement de celles-ci.

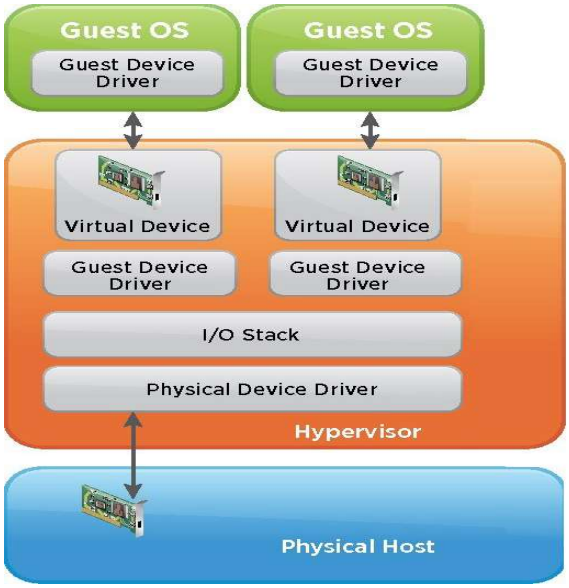
2) Principe d'un hyperviseur

Il existe deux types d'hyperviseur :

2.1) Hyperviseur de type 1

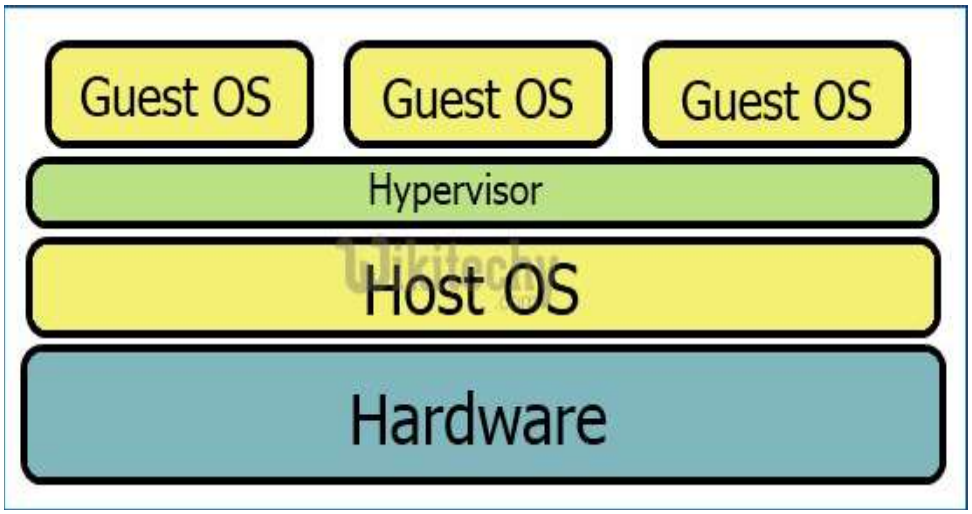
Un hyperviseur de type 1 a comme particularité de s'installer directement sur la couche matériel (à comprendre qu'il est relié directement au matériel de la machine hôte). Il est alors considéré comme outil de contrôle du système d'exploitation, c'est à dire qu'il s'agit d'un noyau allégé et optimisé pour la virtualisation de machines, à contrario d'un OS classique (Windows ou Linux). Au démarrage de la machine physique, l'hyperviseur prend directement le contrôle du matériel, et alloue l'intégralité des ressources aux machines hébergées.
Le gros avantage de ce type d'hyperviseur, c'est qu'il permet d'allouer la quasi-totalité des ressources disponibles aux machines virtuelles, car celui-ci est directement relié à la couche matérielle. Cela est très utile lorsqu'il s'agit de virtualiser de gros serveurs (type Exchange) demandant de conséquentes ressources pour fonctionner correctement.
A contrario, un seul hyperviseur de ce type peut être installé sur une machine physique. Ainsi, si vous décidez de virtualiser beaucoup de machines, ou des machines demandant un nombre de ressources conséquents, il faudra disposer d'une machine physique disposant d'une puissance équivalente à l'intégralité des machines virtualisées, ou prévoir plusieurs machines physiques avec d'autres hyperviseurs.





2.2) Hyperviseur de type 2

Un hyperviseur de type 2 est considéré comme un logiciel, s'installant et s'exécutant sur un système d'exploitation déjà présent sur la machine physique.
Le système d'exploitation virtualisé par un hyperviseur de type 2 s'exécutera dans un troisième niveau au-dessus du matériel, celui-ci étant émulé par l'hyperviseur.
L'avantage d'utiliser ce type d'hyperviseur est la possibilité d'installer et d'exécuter autant d'hyperviseurs que l'on désire sur notre système hôte, ce type n'étant pas relié directement au matériel.
La plupart du temps, les hyperviseurs de type 2 sont utilisés pour virtualiser des OS afin de procéder à des tests de compatibilité et/ou de sécurité.



3) Définitions

La *machine hôte* ou *l'hôte* héberge des *machines virtuelles (VM)*.
L'*hyperviseur* est le composant logiciel qui joue le rôle d'interface entre les machines virtuelles et l'hôte.
Un *cluster* est un regroupement d'hôtes ESX dont les ressources peuvent être gérées, optimisées et supervisées selon des règles spécifiques.

4) Les avantages de la virtualisation

Depuis de nombreuses années, les performances des équipements informatiques n'ont cessé d'évoluer pour atteindre aujourd'hui une puissance extraordinaire. Les applications proposées de nos jours ont besoin de beaucoup de ressources mais paradoxalement n'utilisent qu'une fraction du potentiel de certains serveurs. Selon Microsoft, il est souvent possible de regrouper jusqu'à 5 serveurs sur une seule machine sans perte de performances. La virtualisation apporte donc de nombreux avantages :

Elle permet de **diminuer le nombre de machines physiques**, ce qui entraine un retour sur investissement intéressant :

- En termes d'espace nécessaire, un serveur capable de faire fonctionner différents systèmes d'exploitation sur une seule machine **réduit en moyenne de moitié l'espace réservé aux serveurs** dans une entreprise.

- En plus de cette réduction de place, la diminution du nombre de machines physiques entraine une **réduction de la consommation électrique**.

- Enfin, moins de machines veut dire **moins de contrats de supports matériels** (souvent très cher sur les serveurs, où la maintenance doit intervenir rapidement en cas de panne matérielle).

En plus de ces avantages, la virtualisation permet une gestion simplifiée du parc serveurs.

- Les applications étaient autrefois étroitement liées aux serveurs sur lesquels elles s'exécutaient. La technologie de virtualisation créant une couche d'abstraction entre le matériel physique et les logiciels, elle permet l'exécution et la cohabitation de plusieurs serveurs bien distincts sur une même machine. Ainsi, des applications métiers développées en interne ne s'exécutant que sur un ancien OS (comme NT4 par exemple) peuvent être conservées sans garder les contraintes liées à l'ancien serveur physique**. Le système est donc moins dépendant du matériel** : matériel générique

- La virtualisation permet de réduire **le temps et le coût souvent élevés consacrés à l'administration des serveurs**. La gestion du parc machine est plus facile, ce qui allège la charge des administrateurs.

- Elle simplifie la mise en place de plateformes de tests ou de production en réduisant le temps de mise à disposition d'un serveur.

- Enfin, elle augmente **la disponibilité des serveurs** avec une reprise d'activité plus rapide que pour une machine physique.

- le système est donc isolé du matériel ce qui améliore la tolérance aux pannes et offre un **meilleur contrôle des ressources**

Nous pouvons ajouter à ces caractéristiques un réseau plus sécurisé. En effet, la machine hébergeant les systèmes virtuels n'est **pas visible par l'attaquant**.

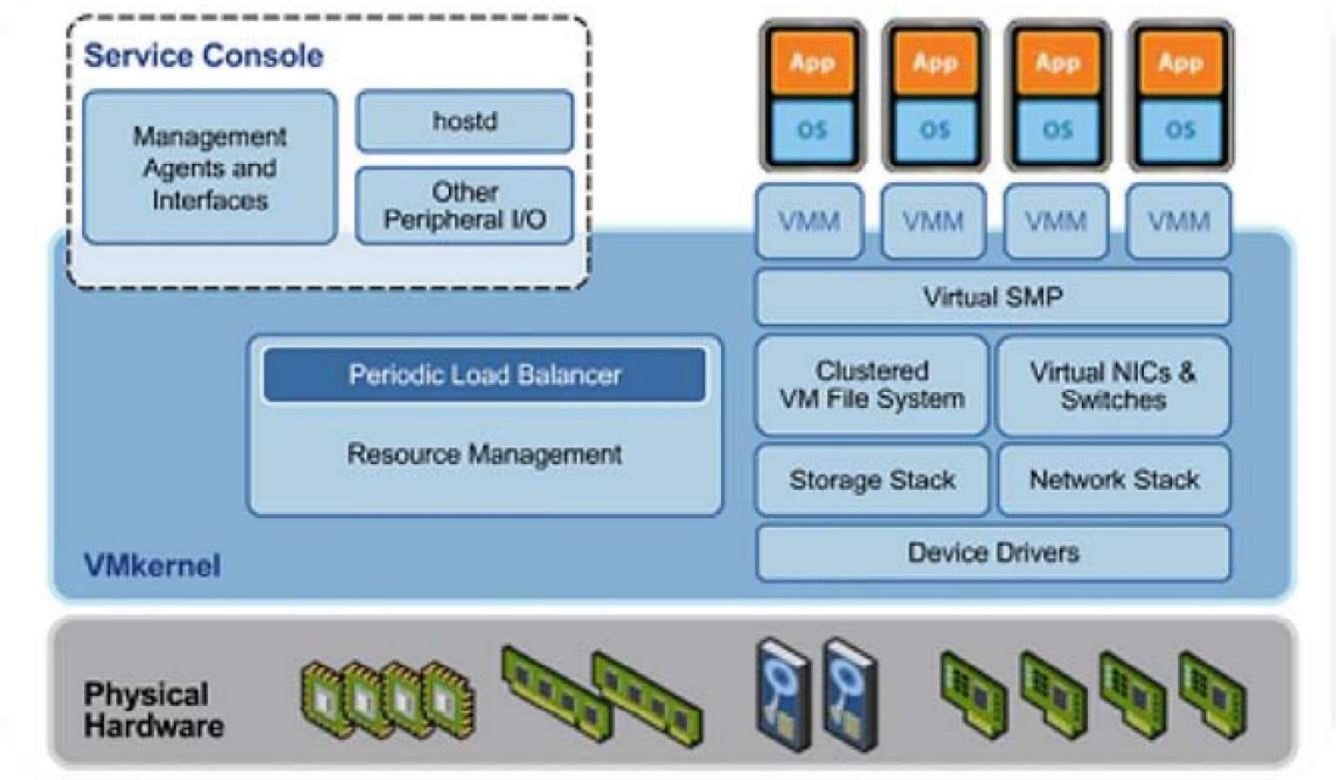
5) **Les principales fonctionnalités de l'hyperviseur de niveau1 VMWARE** vSphere ESXi

ESXi (ESX) est la solution de virtualisation proprement dite. C'est un système d'exploitation à part entière, basé sur un noyau de type POSIX, appelé VMkernel. Ce dernier assume le rôle d'hyperviseur. Il permet d'allouer les ressources matérielles de l'hôte aux différentes machines virtuelles (VM). Le partage de ressources obéit à des règles configurables relativement précises (temps CPU, mémoire vive, priorités réseau, entrées sorties disque, etc.).
Les machines virtuelles peuvent communiquer entre elles grâce à des switchs virtuels (vSwitchs) gérés par la solution. Les vSwitchs peuvent aussi être connectés aux interfaces physiques des serveurs et ainsi permettre la communication entre les machines virtuelles et le réseau local physique de manière transparente.

Très concrètement, ESX permet :

- de cloner une machine en quelques clics ;
- de créer des modèles de machines déployables ;
- de sauvegarder un ou plusieurs états d'une machine virtuelle, pour ensuite pouvoir revenir à des états antérieurs (ce qui s'avère pratique lors des tests ou montées de version) ;

En outre, la mise en « cluster » de plusieurs serveurs ESX rend par exemple possible :
- la migration d'une machine virtuelle d'un serveur à un autre sans interruption de service



La partie qui suit résume les grandes fonctionnalités d'un serveur ESXI

Virtual Machine Monitor :

La partie VMM est responsable de la virtualisation des processeurs
- C'est VMM qui prend le contrôle de la machine virtuelle dès le démarrage
- En somme, cela permet d'exécuter plusieurs environnements identiques sur une seule machine

Gestionnaire de ressource (ressource Management) :

Les responsabilités au sein du Vmkernel :

• Il a pour charge de partitionner les ressources physiques entre les différentes machines. Cela offre la possibilité aux administrateurs de spécifier des réservations et des limites pour les machines virtuelles
• Enfin, c'est ce ressource manager qui ordonnance le temps d'accès au processeur

Periodic Load Balancer

Voici la partie sur l'équilibrage de charge périodique :
La gestion du processeur est faite à deux endroits. En effet, le Vmkernel ordonnance les processeurs indépendamment tandis que le Periodic Load Balancer prévaut et décide sur quel processeur sera réellement ordonnancé la VM. Sa fonction principale est de garantir une bonne répartition du processeur entre les machines virtuelles. Pour cela, il vérifie toutes les 20 millisecondes l'utilisation du processeur et migre les machines virtuelles en conséquence pour garantir cette bonne répartition.

Virtual SMP

Parlons maintenant du Virtual SMP (Symetric Mutli-Proccessing) :
Virtual SMP permet à une machine virtuelle d'utiliser jusqu'à quatre processeurs physiques en même temps. Grâce à cela il devient possible de virtualiser les applications gourmandes en processeur (BDD, serveurs de messagerie).
Avant l'implémentation de virtual SMP, un seul processeur était alloué à plusieurs machines.

Service console

Et enfin une brève description des possibilités offertes par le service console :

- Il offre l'accès en ligne de commande à l'ESX
- Il offre également un accès web à l'ESX
- Enfin, il permet depuis cet accès distant de manager et monitorer voire même de créer des machines virtuelles

6) Les Fonctionnalités avancées de VMWARE

En fonction de la licence acquise, des fonctionnalités plus ou moins avancées sont disponibles : planification de tâches, switchs distribués DVS (switchs partagés entre plusieurs hôtes ESX), duplications et réplications automatiques, déploiement assisté d'hôtes ESX, etc.

vCenter Server

VCenter Server permet la gestion centralisée des hôtes ESX, et rend ainsi transparente l'administration de multiples serveurs en une seule interface consolidée.
Il permet entre autres :
- la gestion de rôles et de droits, pour définir des périmètres d'administration spécifiques à différents groupes d'administrateurs ;
- l'authentification unique (l'administrateur s'authentifie sur VCenter Server et se trouve connecté à l'ensemble des serveurs ESX) ; il est également possible de s'authentifier via un annuaire Active Directory ;
- la gestion de l'optimisation des ressources des serveurs (pour les ressources pouvant être gérées ou allouées dynamiquement) ;
- l'automatisation de tâches d'administration.

Une des spécificités de VMware est que l'administration des hôtes, des VM, mais aussi du stockage et une partie du réseau (vSwitch ou DVS) se fait à partir du serveur vCenter.
VCenter Server s'avère donc incontournable lorsqu'il est question d'administrer plusieurs hôtes ESX.
C'est le point central pour configurer, approvisionner et gérer des environnements informatiques virtualisés. Il va permettre d'administrer plusieurs serveurs ESXi (*cluster*) permettant ainsi de nombreuses solutions en matière de disponibilité.

vSphere Client

Pour l'administration d'un hôte ESX, les seules manipulations graphiques pouvant être réalisées en local sont limitées à sa configuration IP ainsi qu'au changement du mot de passe root. Pour le reste, il est possible d'y ouvrir une session shell et de procéder à la maintenance du serveur par ligne de commandes.
Pour une administration par interface graphique, l'utilisation du client lourd vSphere Client est incontournable jusqu'à ESX 5.0. Ce client permet de se connecter au serveur vCenter ou directement à un hôte ESX à des fins d'administration. Il permet entre autres :

- de monter une clé USB locale sur une VM à travers le réseau ;
- de monter un CD/DVD local, ou une image ISO sur une VM à travers le réseau ;
- de modifier tous les paramètres de configuration d'ESX et des VM;
- d'effectuer la prise en main de bureau à distance des VM (ce qui revient à voir l'écran virtuel d'une VM dans une fenêtre) ;
- d'accéder aux espaces de stockage des serveurs ESX (pour envoi/téléchargement de fichiers ou dossiers).

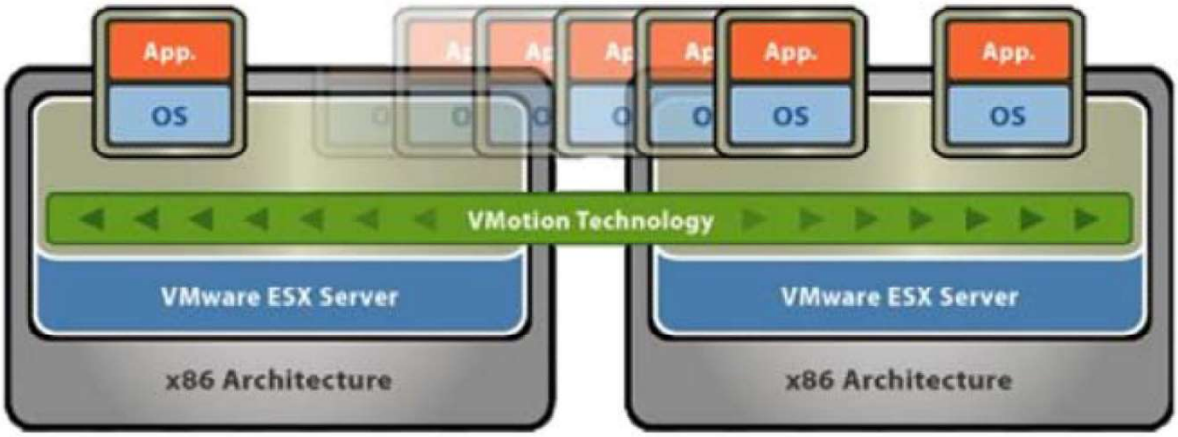
VMotion : déplacement à chaud des machines virtuelles

VMotion est un service qui permet de transférer une machine virtuelle lancée d'un serveur ESX vers un autre sans aucune interruption de service.
Nous sommes, dans ce cas-là, dans le même espace de stockage partagé et dans le même cluster.

Cette migration s'effectue en 3 étapes :

- Premièrement, l'état de la machine est sauvegardé sur un stockage réseau
- Ensuite, la mémoire est transférée au travers du réseau
- Ce n'est qu'à partir de cet instant que le basculement automatique de serveur est effectué

Comme je l'avais précisé dans la partie précédente, l'équilibrage de charge est donc possible grâce à cette technique.

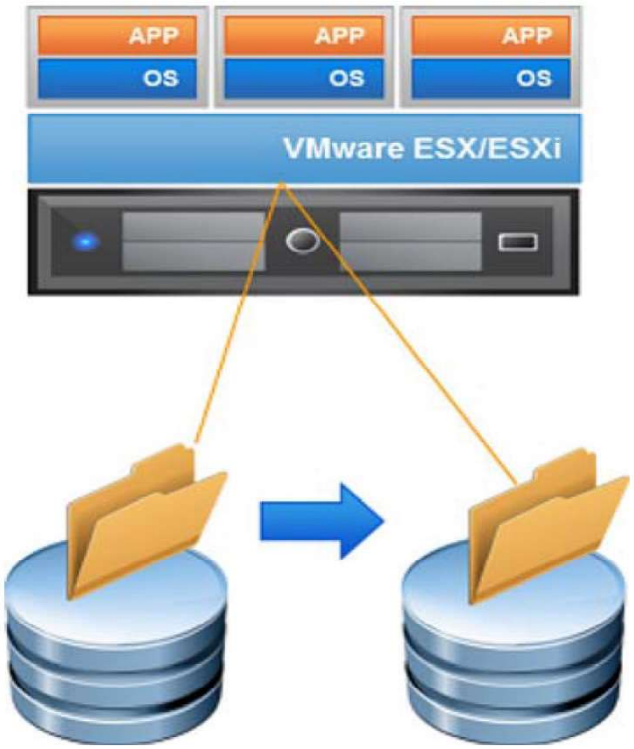


VMware Storage VMotion - changement d'espace de stockage

Après avoir vu le déplacement au sein d'un même espace de stockage, nous allons voir maintenant que VMware offre la possibilité de changer la machine d'espace de stockage:

Voici le détail de cette migration :

- Premièrement, c'est le home directory qui est déplacé
  - fichiers de configuration et fichiers de log
- Ensuite, on procède à une copie du contenu entier du disque sur la destination
- Enfin, il y a une phase d'écriture différentielle des modifications apparues lors de la première copie



VMware vSphere VMFS est un système de fichiers en *cluster* hautement performant optimisé pour les machines virtuelles. Alors que les systèmes de fichiers classiques ne permettent qu'à un seul serveur d'accéder en écriture-lecture à un même système de fichiers à un moment donné, VMFS utilise le stockage partagé afin d'autoriser simultanément plusieurs hôtes VMware vSphere à écrire et lire des données sur le même stockage.

VMware Distributed Resource Scheduler (DRS)

Fonction qui affecte et équilibre la capacité informatique dynamiquement dans les collections de ressources matérielles pour les machines virtuelles (équilibrage de charge entre différents serveurs ESXi). Cette fonction comporte des possibilités de gestion d'alimentation distribuée (DPM) permettant au centre de données de réduire significativement sa consommation d'énergie.

Tolérance aux pannes VMware Fault Tolerance (FT)

Quand la tolérance aux pannes est activée pour une machine virtuelle, une seconde copie de la machine originale (ou primaire) est créée. Toutes les actions réalisées sur la machine virtuelle primaire sont également effectuées sur la seconde machine virtuelle. Si la machine virtuelle primaire devient indisponible, la seconde machine devient active pour une disponibilité continue.

Recommandations de sécurité

Dans une solution de virtualisation, l'hyperviseur contrôle l'accès aux ressources de l'hôte et est responsable du cloisonnement entre les machines virtuelles. Ce composant logiciel est donc critique du point de vue de la sécurité. Comme cela a été évoqué précédemment, une des spécificités de VMware est que l'administration des hôtes et des VM, mais aussi du stockage et une partie du réseau (vSwitch ou DVS) se fait à partir du serveur vCenter.

En vertu du principe de « séparation des rôles » et du principe de « moindre privilège », il est essentiel de bien définir les rôles et privilèges associés aux différents périmètres de responsabilité des administrateurs. À titre d'exemple, il n'est pas concevable que l'administrateur d'une machine virtuelle dispose également des privilèges d'administration de l'hôte qui les héberge. Le cas échéant, si cette machine virtuelle venait à être compromise, les autres machines virtuelles de l'hôte le seraient également