THALES
Building a future we can all trust

Virtualisation

VISITTHIDETH Lau Jacky

www.thalesgroup.com

OPEN

Programme

Cours Virtualisation

Cours Containers

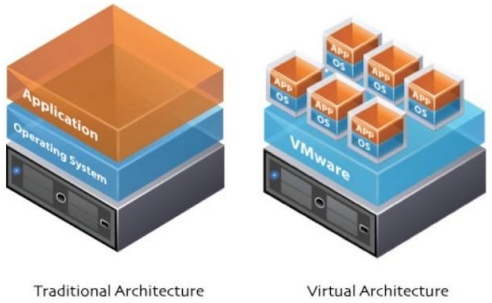
Concept Virtualisation

Virtualisation :

- Créer plusieurs environnement au sein d'une même machine hôte
- Permettre d'isolé des environnements systèmes et réseaux

Solution omniprésentes dans tous les domaines

Métiers en vogue : DevOps, SRE, Ingénieur Système et Réseaux, Administrateur Système, Ingénieur Cloud



Traditional Architecture Virtual Architecture

Origine de la virtualisation

- Développée au **centre scientifique de Cambridge d'IBM et en collaboration avec le MIT**

- Système expérimental **CP/CMS** (Control Program / Cambridge Monitor System) qui est devenu par la suite le **produit hyperviseur**

- **Vmware** développe et popularise à **la fin des années 1990**, un système propriétaire de virtualisation logicielle d'architecture x86 (32 bits)
- Plus d'autre solution de virtualisation open-source sont apparu tels que **Xen, KVM, QEMU, Bochs, Linux-VServer, Oracle VM VirtualBox**

Pourquoi virtualiser ?

Economiser de l'argent

Répartition de charges

Haute disponibilité

Provisionning et flexibilité

Green IT

Les limites de la virtualisation

Retour sur investissement

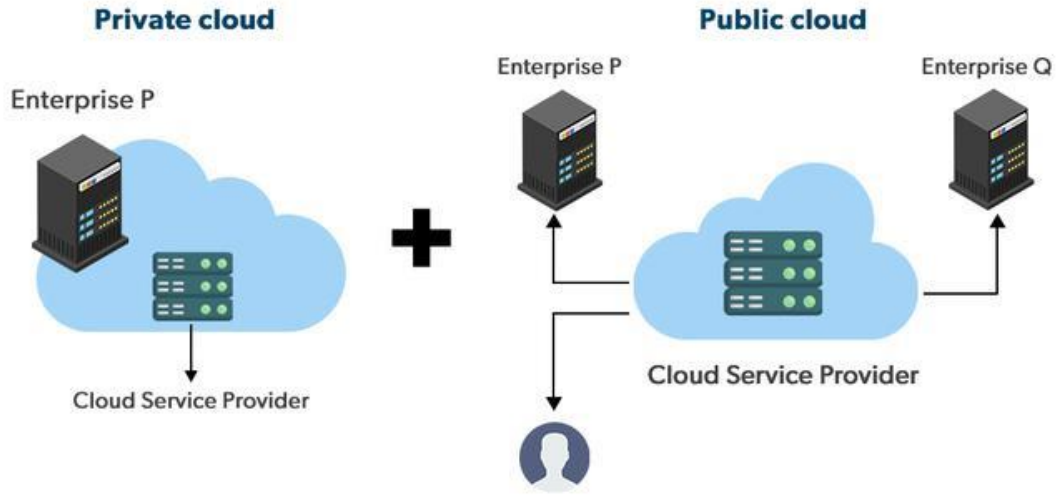
Complexité

Sécurité

Cloud et Virtualisation

- Le cloud est une couche de présentation afin de déployer des Vms ou des containers rapidement
  - Cloud = Virtualisation + API (images , réseaux, accounting)
- Solution privilégié dans le :
  - Cloud Opensource : OpenStack (RedHat)
  - Cloud Privé : Vcloud (Vmware)
- D'autre solutions comme Ovirt(RedHat) ou Proxmox fournissent une API pour piloter un hyperviseur comme KVM.

Cloud Public et Cloud Privé



Vmware, Proxmox, OpenStack,…

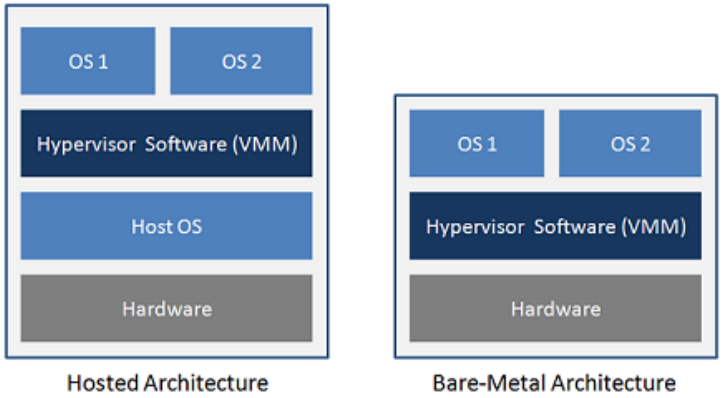
AWS, Google Cloud Platform, Azure, OVH,…

Vmware, Proxmox, OpenStack,…

OPEN

THALES
Building a future we can all trust

Types d'hyperviseur



Hyperviseur de type 1 :

Architecture Bare-metal, l'hyperviseur est installé directement sur le matériel

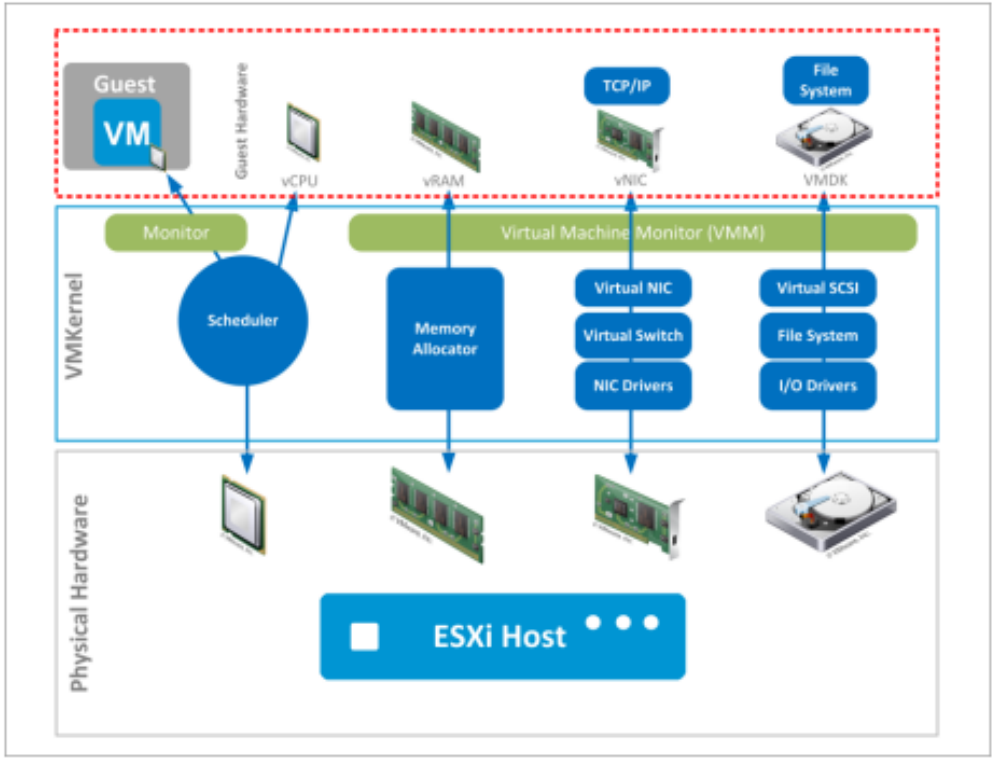
- Ex: Vmware ESXi, Hyper-V, KVM, Xen

Hyperviseur de type 2 :

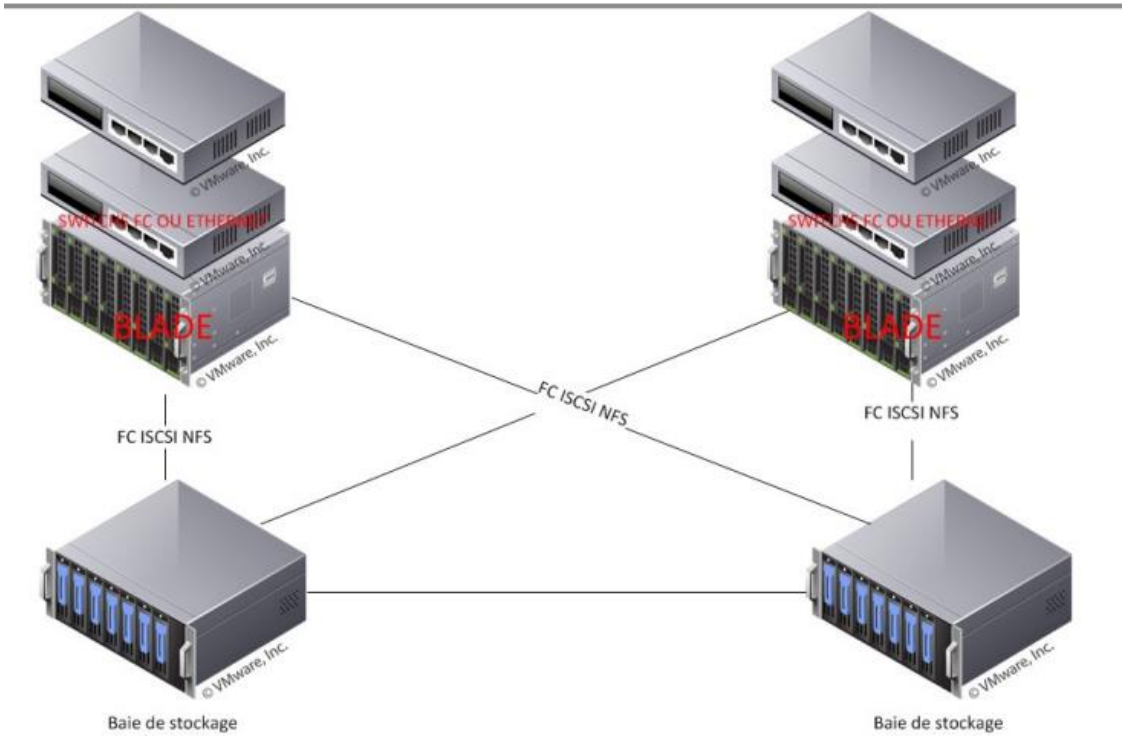
Architecture hébergé, l'hyperviseur est installé sur un système d'exploitation traditionnel en tant qu'application

- Ex: VirtualBox, Vmware Workstation

Composantes d'un hyperviseur

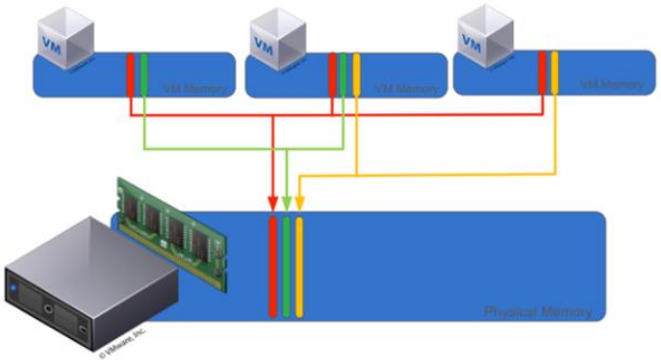


Architecture Scale In



OPEN

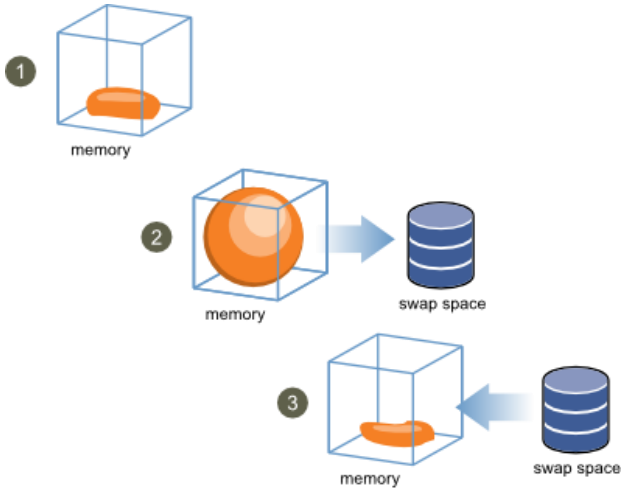
Gestion de la mémoire RAM – Transparent Page Sharing



- **Overcomitment de la mémoire** : La somme des mémoires des machines virtuelles peut dépasser la mémoire totale de la machine physique
- Le Transparent Page Sharing (TPS) consiste à faire pointer les pages mémoires virtuelles identique vers la même page mémoire de la machine physique
- Sous KVM, ce mécanisme se nomme Kernel samepage merging

- Depuis la version ESXi 5.0, TPS est désactivé pour des raisons de sécurité mais peut toujours être réactivé
- Le gain en terme de mémoire peut varier de 5% à 30%

Gestion de la mémoire RAM – Ballooning Vmware, Xen, KVM

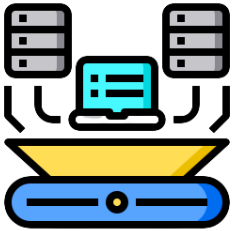


- Le **ballooning** est un **mécanisme de défense de l'hyperviseur pour éviter la surcharge de la mémoire RAM**

- Une fois l'**hyperviseur** en manque de RAM, les VMs ne se rendent pas compte de ceci car elles ne voient que leur propre RAM attribuée. Il faut ainsi pouvoir les mettre au courant de ce manque de l'hôte et ainsi leur demander de faire des sacrifices (SWAP) pour le bon fonctionnement de l'infrastructure

- Tout ceci est rendu possible grâce à l'installation des **VMware Tools** qui peuvent agir sur le Guest OS par le biais du balloon driver (*vmmemctl*).

Partage des ressources CPU/RAM sous Vmware ESXi



Pour une VM, les paramètres de partage des ressources CPU/RAM sont :

- **Limit** : Plafond (en MHz pour les CPU et MB pour la RAM)
- **Reservation**: En cas de contention de ressource, on alloue ces ressources réservées
- **Share**: Plus une VM aura de share et plus elle aura accès aux ressources (CPU idle time ou mémoire)

Chaque VM dispose d'un swap couvrant la différence entre limit et reservation

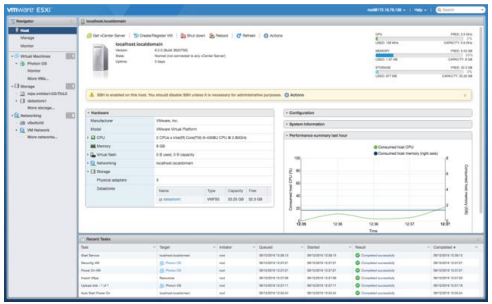
Overhead de la virtualisation réseau

1. Un paquet arrive sur une interface réseau d'une carte ethernet
2. L'hyperviseur (virtual switch) examine le paquet et détermine à quelle machine virtuelle il doit délivrer le paquet (analyse adresse mac et vlan).
3. Le paquet est copié et est délivré à la carte virtuelle de la Vm.

Architecture VMWARE

OPEN

Gestion des ESXI

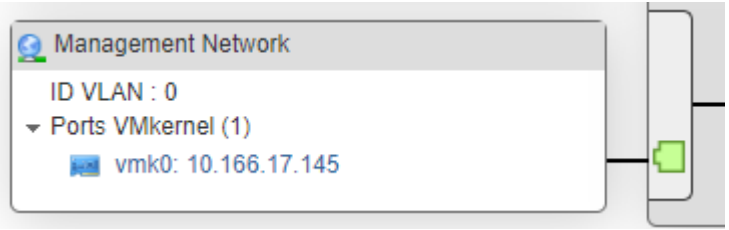


- **Vmware ESXi** est un **hyperviseur de type 1 développé par Vmware**
- C'est le **système d'exploitation phare de Vmware**, un peu comme RedHat, Debian ou Ubuntu
- ESX vient de l'abréviation d'Elastic Sky X et plus récemment ESXi pour « integrated »
- Accessible via :
  - SSH (désactivé par défaut) : Bash + ESXiCli
  - HTTPS
  - Shell

Qu'est ce que le VMKernel ?

Le Vmkernel est un module ESXi qui prend en charge :

- La gestion des Vm (ordonnancement CPU,mémoire)
- L'émulation soft de la couche réseau (cartes , switch)
- La communication avec la couche stockage (ISCSI, FC, NFS)
- Interface de management accessible par HTTP

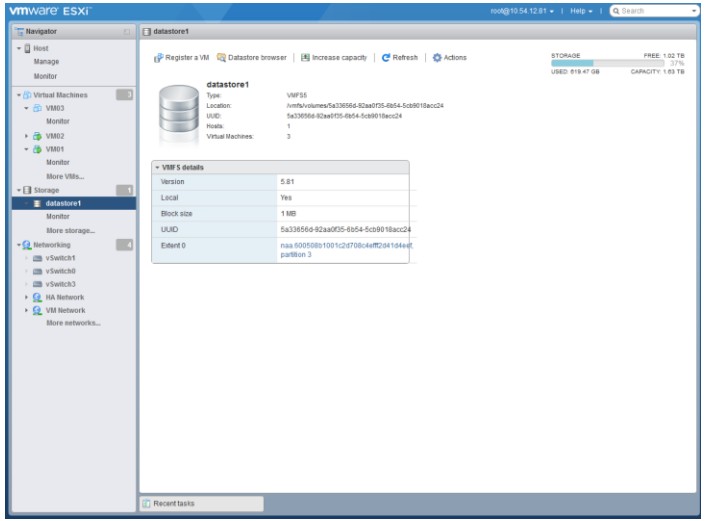


OPEN

THALES
Building a future we can all trust

Datastore

- Un **datastore Vmware** est un volume de stockage qui va fournir des « tranches » de disques pour les VM.
- Il s'appuie sur **un stockage centralisé (FC, ISCSI, NFS) ou distribué (VSAN)**



OPEN

THALES
Building a future we can all trust

Virtualisation du stockage

VMFS est le système de fichiers clustérisés de Vmware et utilisé sur les datastores

Il est essentiel car il permet à plusieurs serveurs ESX de « monter » le système de fichiers dans lequel sont stockées les VM

Les différents formats de fichiers d'une VM sont :

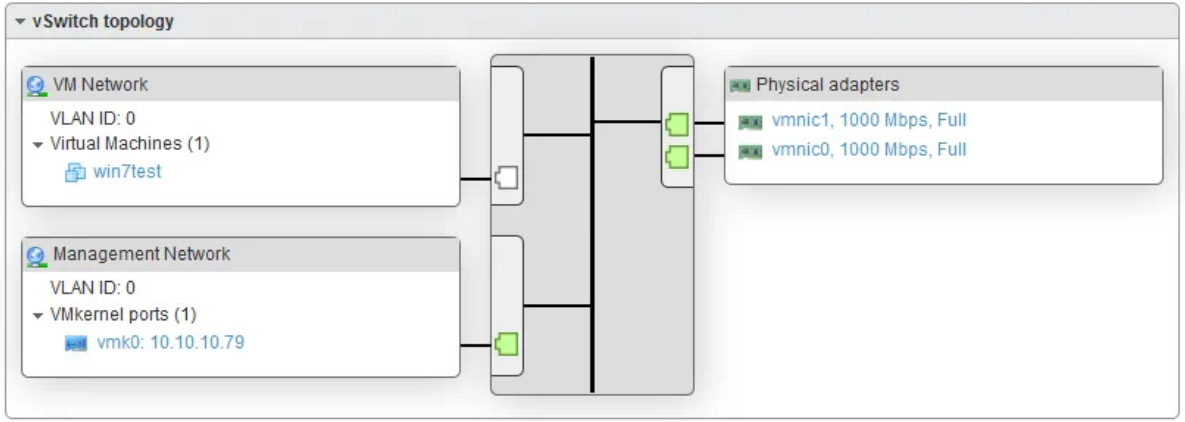
- .ovf : Description des caractéristiques de la VM (CPU, RAM,…)
- .vmdk : Image disque de la VM
- .nvram : Mémoire RAM non-volatile

Vswitch

- Vmware permet de rattacher des machines virtuelles entre elles par le biais de vSwitch (Virtual Switch)
- Ce vSwitch est similaire à un switch physique mais sans spanning-tree
- Il ne gère pas le routage et peut être considéré comme un switch de niveau 2

Fonctionnement Switch

Réseau virtuel



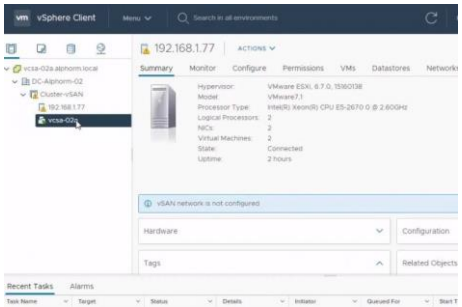
Réseau physique

- **Ports VMKernel** : Ports utilisés pour accéder à l'interface Web d'ESXi et effectuer des opérations liées à la virtualisation (vMotion, replication, fault tolerance,…)
- **Ports Group** : C'est un groupe de ports virtuels qui permet d'associer un groupe de VM et un vSwitch.
- **Uplink ports** : Port qui fait le lien avec une carte réseau physique et le vSwitch. Un uplink est associé à une interface réseau du serveur.

OPEN

THALES
Building a future we can all trust

Gestion Infra Vmware Vsphere vCenter



Vmware Vsphere vCenter est la solution d'orchestration de Vmware pour gérer un parc d'ESXi

C'est la solution qui a rendu célèbre Vmware et qui est devenu populaire dans les entreprises et dans le cloud

Accessible via :

- HTTPS (Vsphere vCenter Web Client)
- SSH (Bash + PowerCli)
- Shell

OPEN

THALES
Building a future we can all trust

Le déploiement automatique, un sujet à la mode

CI/CD

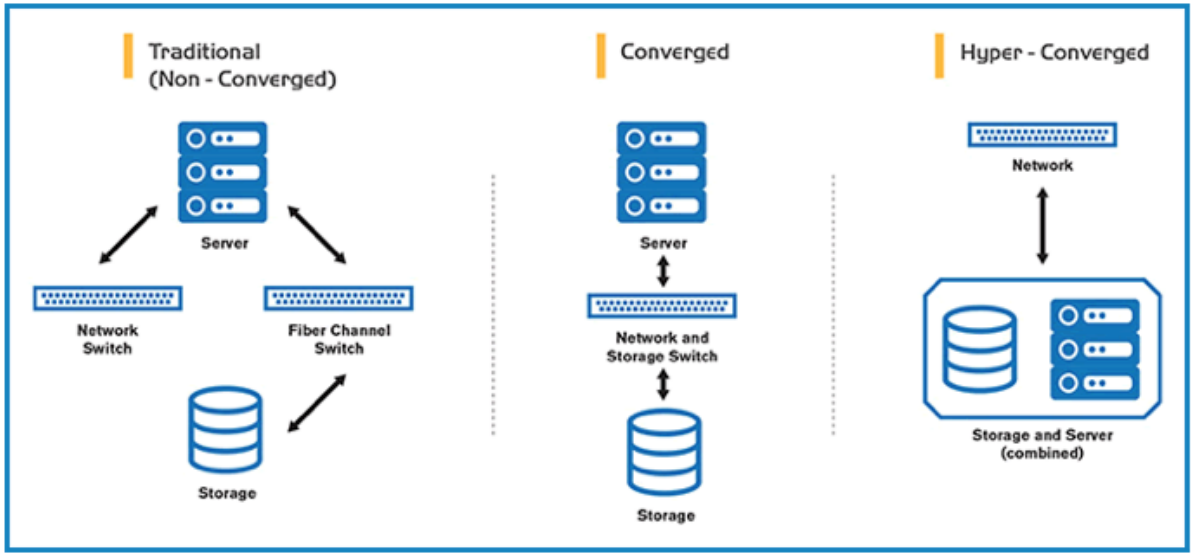
Plan de reprise d'activité

Cohérence du parc informatique

Le trio gagnant de l'automatisation dans le Cloud

- **Packer** permet de générer des templates de VM sur un hyperviseur
- **Terraform** permet de déployer des templates et générer des VMs sur un hyperviseur
- **Ansible**, une fois la VM installé permet de faire des post-installations et configurations au travers de SSH sur les VM

Architecture virtuel - Scale out et Hyper-converged



OPEN

THALES
Building a future we can all trust

Merci pour votre attention et bon TP !