




RSX112

Sécurité des réseaux

Stéphane LARCHER

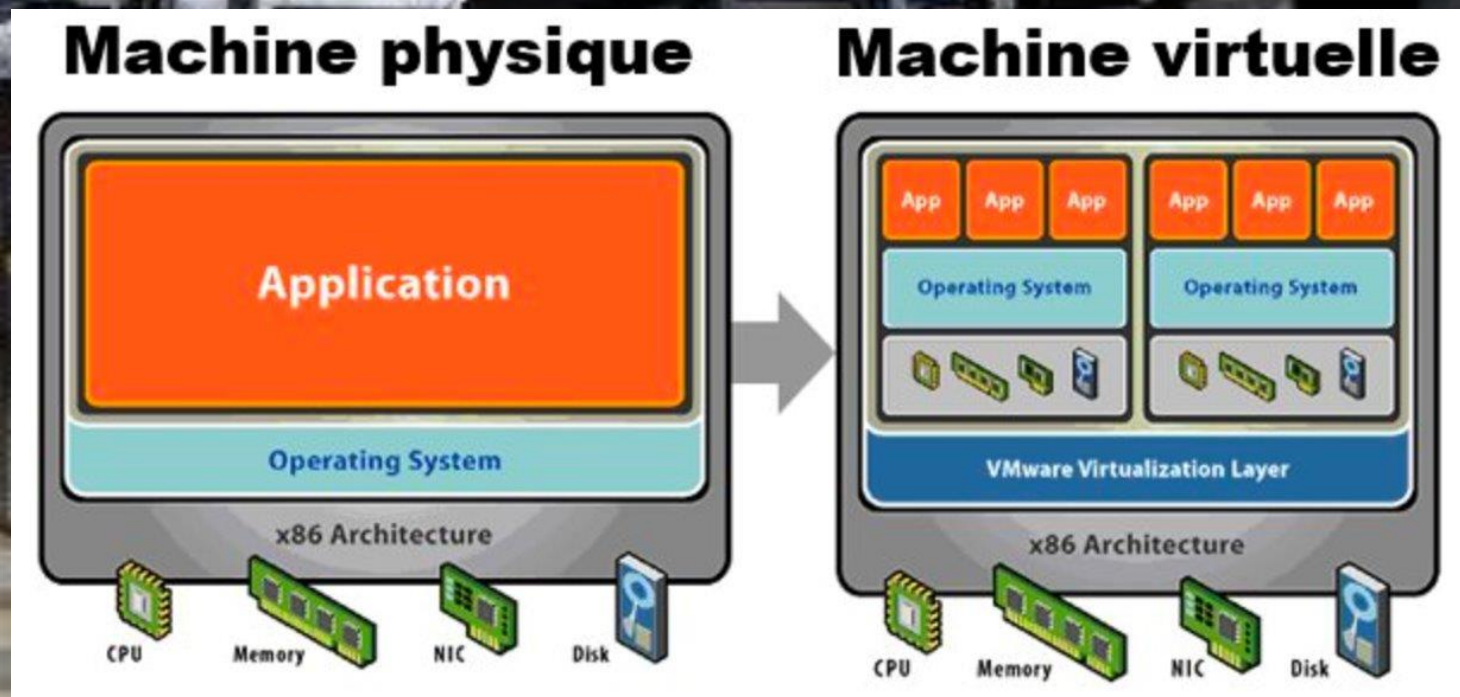


La virtualisation

Le principe technique

Virtualisation des systèmes d'information

Le concept



Virtualisation des systèmes d'information

Le concept

Les composants de la virtualisation

Le serveur physique

Hypervisor

Les machines virtuelles

Le stockage (partagés)

Le réseau

Virtualisation des systèmes d'information

Le concept

L'hyperviseur

Serveur physique assurant le partage des ressources

Monte en mémoire les machines virtuelles allumées

Les nouvelles version d'ESXi

OS minimal

Tout l'OS est en mémoire

Vmtools de la machine virtuelle chargé de l'émulation des drivers

Gestion des machines virtuelles, et de leurs ressources

Virtualisation des systèmes d'information

Le concept

Architecture Générale VMware

ESXi Server

Serveur physique fournissant la mémoire, le réseau, le(s) processeur(s) aux machines virtuelles

Virtual Machine

Environnement Virtualisé d'un serveur x86 dans lequel un système d'exploitation avec les applications associées peut tourner

Virtual Center Server

Point d'entrée pour l'administration de l'infrastructure VMware

VirtualCenter database

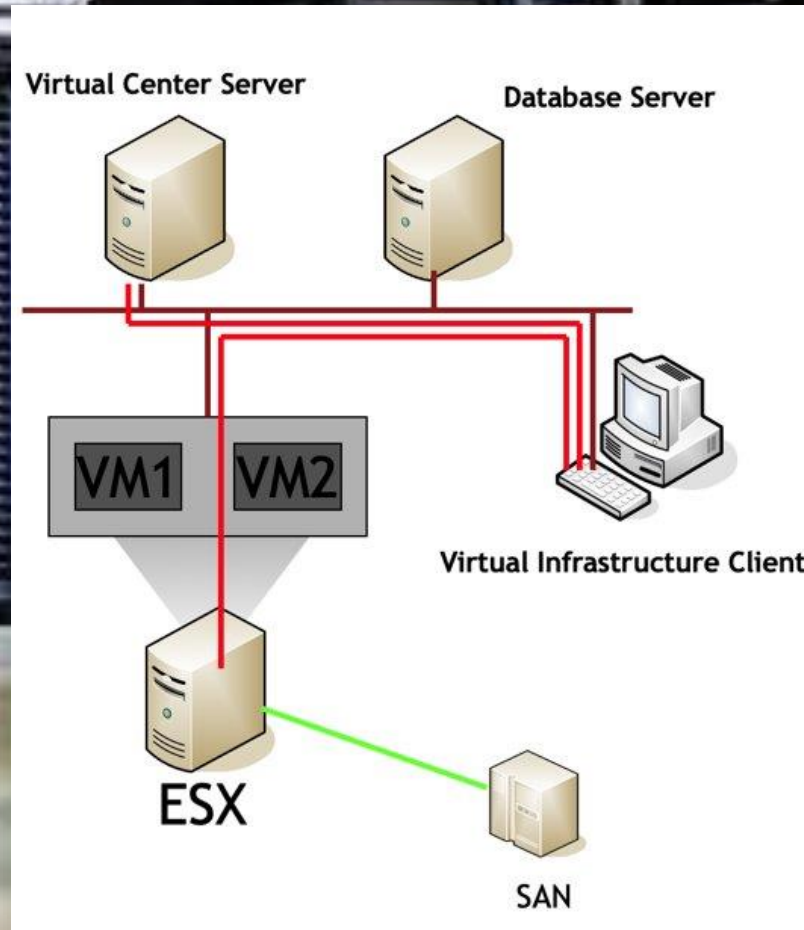
Données chargées de gérer le statut de chaque VM, ESXi, utilisateur du serveur vCenter

Virtual Infrastructure Client

Console d'administration qui permet une connexion direct aux ESXi ou aux vCenter

Virtualisation des systèmes d'information

Le concept



Virtualisation des systèmes d'information

Le concept

Les composants de la virtualisation

L'hyperviseur de type 1

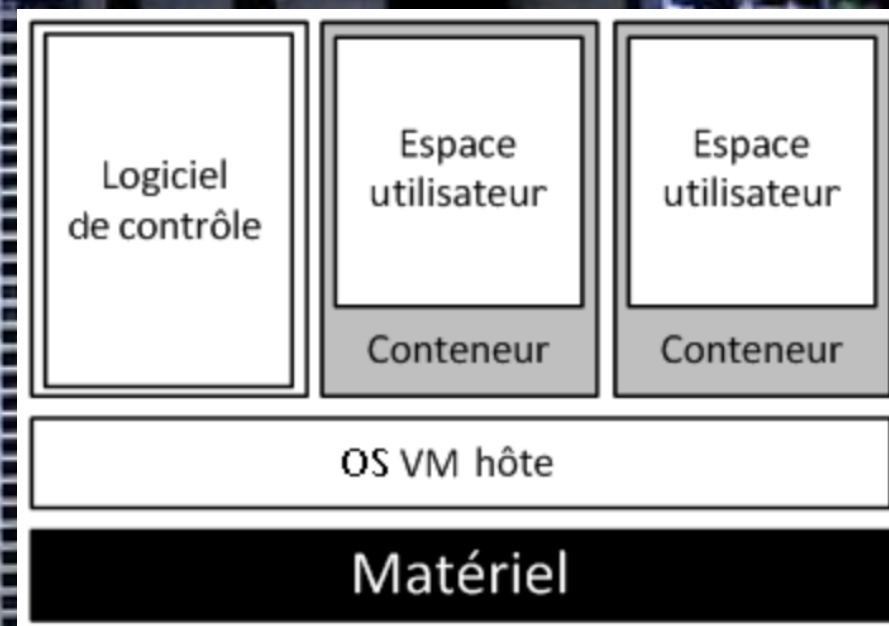
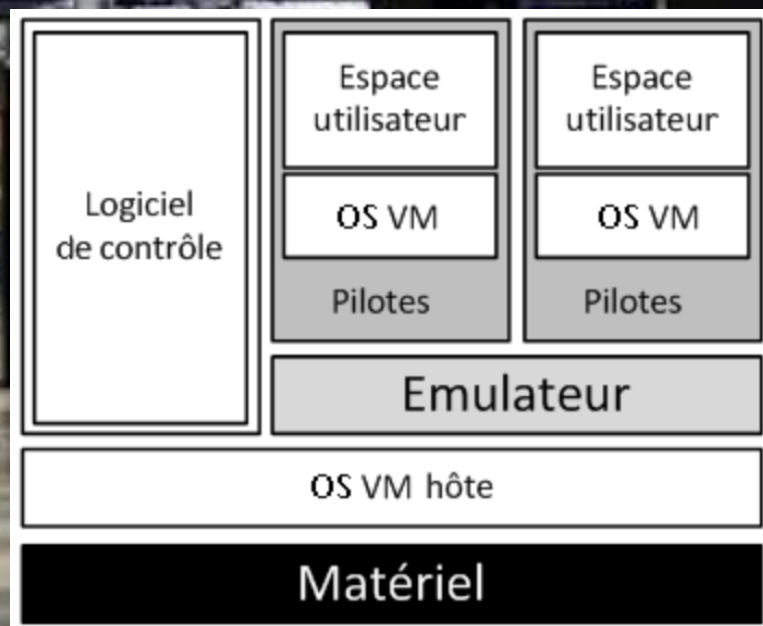
Un hyperviseur fonctionnant directement sur le matériel (Microsoft Hyper-V, VMware vSphere...)

L'hyperviseur de type 2

Un système d'exploitation avant de pouvoir être installé (Microsoft Virtual PC, VMware Workstation...)

Virtualisation des systèmes d'information

Le concept



Virtualisation des systèmes d'information

Le concept

Le grand principe de VMware (de la virtualisation)

Une machine est sous format fichiers

- Les disques

- La mémoire

- Les propriétés de la machine

La configuration de la VM

.VMX

Le disque

.VMDK , **flat.VMDK** : Thin provisioning

Le Bios de la machine

.NVRAM

Virtualisation des systèmes d'information

Le concept

Les snapshot (clichés)

.VMSN

Les métadonnées des snapshot












.VMSD

Les journaux d'activités

.LOG

Virtualisation des systèmes d'information

Le concept

Name	Date modified	Type ^	Size
 caches	03/05/2015 14:01	File folder	
 vmware.log	04/05/2015 13:37	Text Document	350 KB
 Windows 7.vmsd	03/05/2015 13:57	VMware snapshot metadata	2 KB
 Windows 7.vmx	03/05/2015 14:01	VMware Team Member	4 KB
 Windows 7.vmdk	30/04/2015 12:40	VMware virtual disk file	10 705 344...
 Windows 7-000001.vmdk	03/05/2015 13:56	VMware virtual disk file	1 799 872 KB
 Windows 7-000002.vmdk	04/05/2015 13:37	VMware virtual disk file	8 938 368 KB
 Windows 7.nvram	04/05/2015 13:37	VMware virtual machine BIOS	9 KB
 Windows 7.vmx	04/05/2015 13:37	VMware virtual machine configuration	4 KB
 Windows 7-Snapshot1.vmsn	30/04/2015 19:24	VMware virtual machine snapshot	28 KB
 Windows 7-Snapshot2.vmsn	03/05/2015 13:57	VMware virtual machine snapshot	29 KB

Virtualisation des systèmes d'information

Le concept

VMDK

ensemble de fichier composant la machine

Dynamique

Statique

Remise à zéro en différé

Remise à zéro immédiate

Virtualisation des systèmes d'information

Le concept

Le VCenter

Serveur (virtuelle maintenant) en charge de l'infrastructure Virtuelle

Centralise la gestion de l'infrastructure virtuelle

Gestion des hyperviseur

Gestion des machines virtuelles

Gestion du stockage présenté à l'environnement virtuel

Apporte (suivant les licences) plusieurs fonctionnalités de sécurité principalement

Gestion des accès



vcsa.cloud.local

CloudLocal

standalone

standalone2

vsancluster

10.1.149.14

10.1.149.15

10.1.149.16



vsancluster

ACTIONS ▾

Summary

Monitor

Configure

Permissions

Hosts

VMs

Datastores

Networks

Updates



Total Processors: 24
Total vMotion Migrations: 1261
Fault Domains:



CPU Free: 29.58 GHz
Used: 20.79 GHz Capacity: 50.38 GHz
Memory Free: 194.35 GB
Used: 189.35 GB Capacity: 383.7 GB
Storage Free: 1.66 TB
Used: 3.79 TB Capacity: 5.46 TB

Related Objects

Datacenter

CloudLocal

Tags

Assigned Tag	Category	Description
No items to display		

vSphere DRS

Cluster DRS Score ⓘ

VM DRS Score ⓘ



0-20%	0 VMs
20-40%	0 VMs
40-60%	0 VMs
60-80%	14 VMs
80-100%	0 VMs

DRS recommendations: 0

DRS faults: 0

[VIEW DRS SETTINGS](#)[VIEW ALL VMs](#)

Cluster Consumers

[Recent Tasks](#)[Alarms](#)

Virtualisation des systèmes d'information

Le concept

Le VCenter : Le cluster

partage des ressources entre plusieurs
hyperviseur

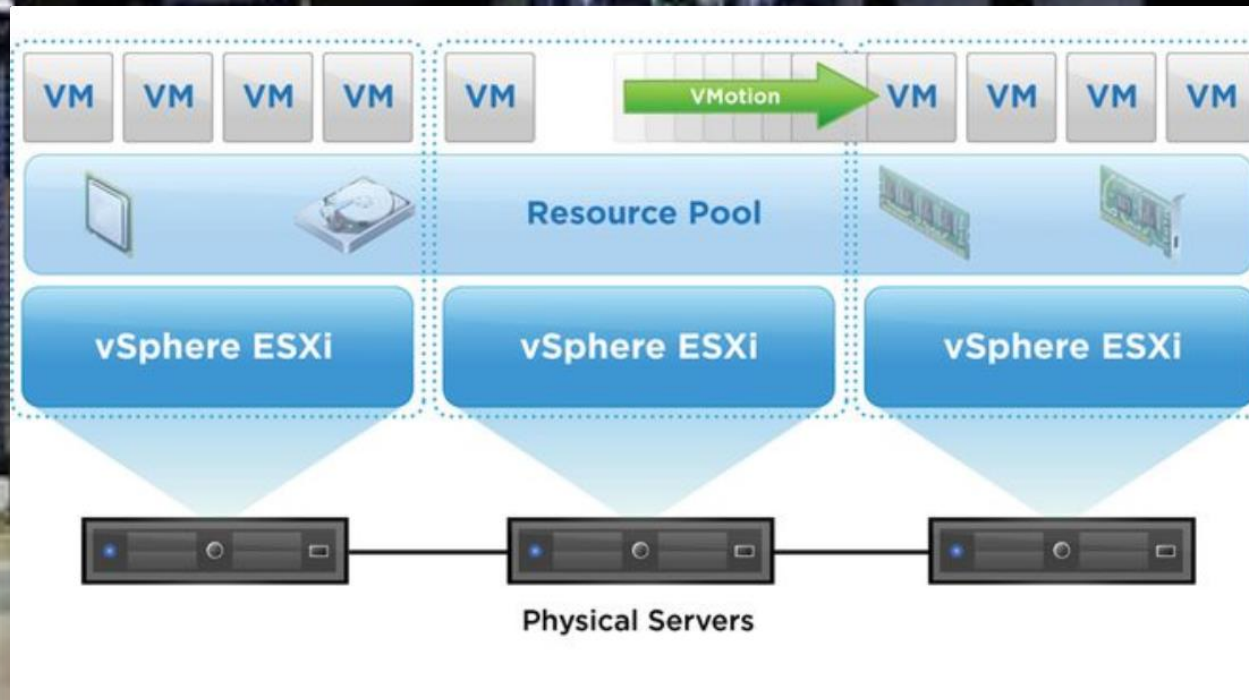
Permet la haute disponibilité

Permet la répartition de charge

Migration de machine

Virtualisation des systèmes d'information

Le concept



Virtualisation des systèmes d'information

Le concept

Hosts:

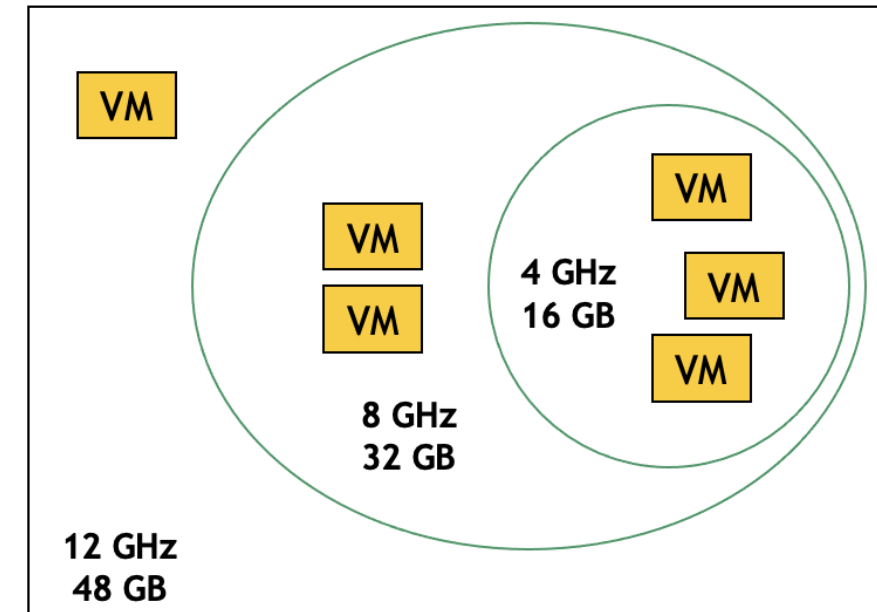
Machine physique ESX

Clusters

Regroupement de machines physiques ESX partageant le même réseau et les mêmes ressources de stockages

Ressources Pools

Réservation de ressources (processeur et mémoire) au sein d'un host ou d'un cluster



Serveur x86 Serveur x86 Serveur x86

Virtualisation des systèmes d'information

Le concept

Le VCenter : Le HA

Fonctionnalité du cluster

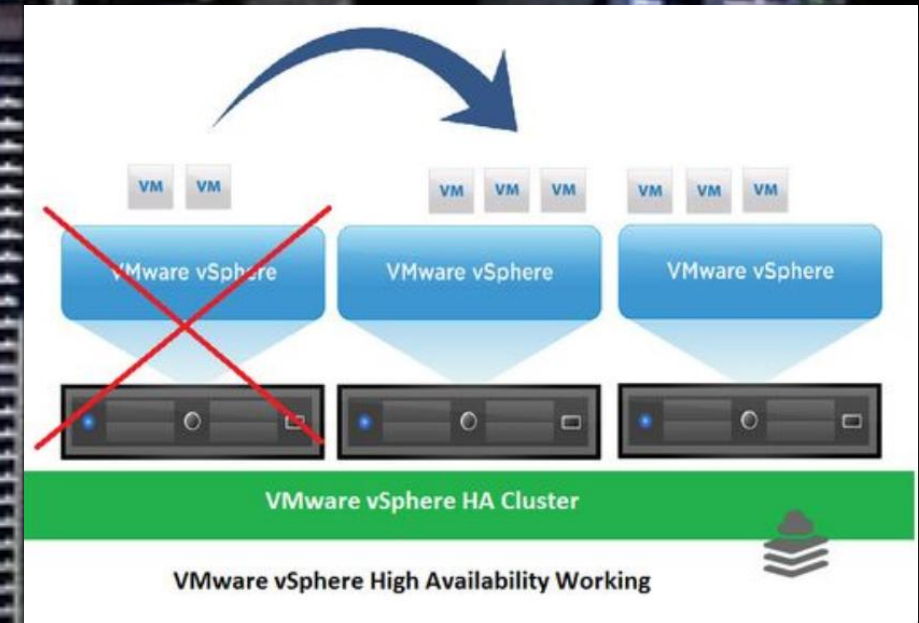
En cas de perte d'un ESXi

Machine redémarre sur un autre ESXi

Arrêt brutale de la machine

Attention à l'isolement d'un ESXi

Deux manières de détecter
la perte d'un ESXi



Virtualisation des systèmes d'information

Le concept

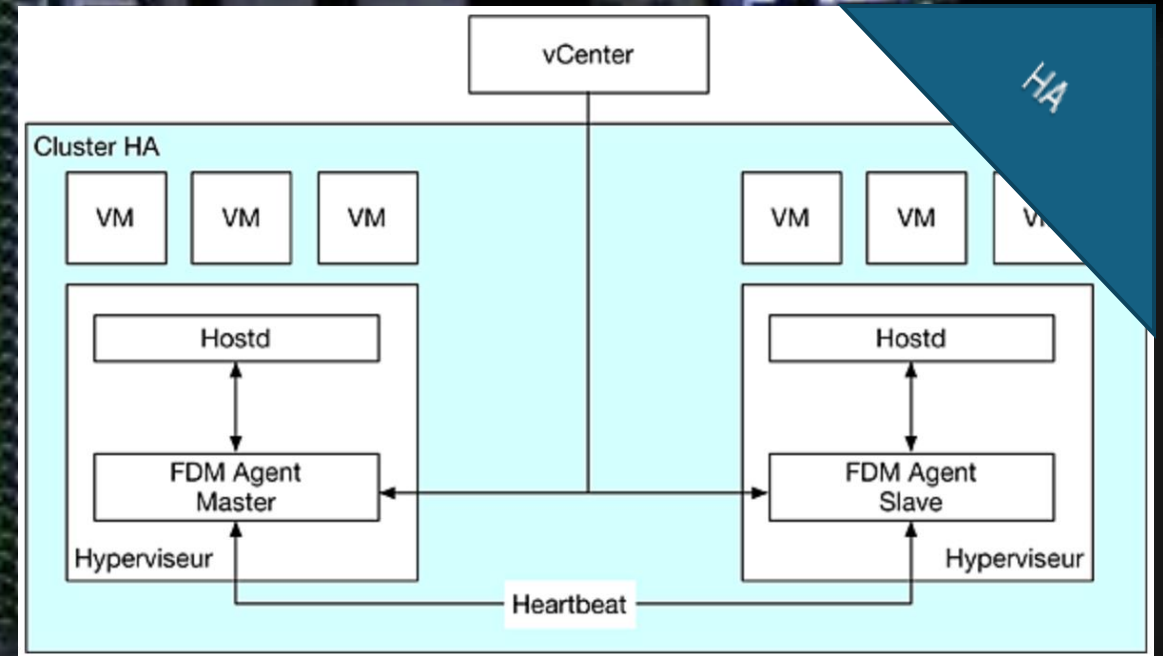
Le VCenter : Le HA

Protection contre la panne d'un serveur en redémarrant les machines virtuelles sur d'autres hôtes

Protection contre la panne système ou applicative en surveillant constamment la machine virtuelle et en la redémarrant en cas de plantage

Protection contre les problèmes d'accès de banque de données (datastore)

Protection contre l'isolement réseau d'un hôte, auquel cas les machines virtuelles peuvent être redémarrées sur d'autres hôtes non isolés



Virtualisation des systèmes d'information

Le concept

Serveur primaire

Supervise l'état des hôtes secondaire

En cas de panne d'un serveur

- Détermine les machines virtuelles à redémarrer

Surveille l'état des machines virtuelles protégées par HA. Si une machine virtuelle venait à être inopérante, le primaire prend la décision de redémarrer celle-ci (et également sur quelle ressource le redémarrage aura lieu)

Maintient une vue complète sur les machines et hôtes protégés

Agit comme interface de gestion de la perspective de vCenter

Signale le statut du cluster HA à vCenter

Virtualisation des systèmes d'information

Le concept

Le VCenter

Les migrations (de machines)

Migration à froid

Machine éteinte

Possibilité de le faire entre
hyperviseurs

datacenters

serveurs vCenter

Déplacement de fichiers

Les phases de migration

Validation d'un hyperviseur compatible

Sélection du choix du datastore cible, et copie des
fichiers sur le datastore de l'hyperviseur cible.
(Optionnel)

Enregistrement de la VM sur le nouvel hyperviseur

Suppression de fichiers du datastore source s'il a
été décidé de déplacer les fichiers. (Optionnel)

Virtualisation des systèmes d'information

Le concept

Rôle du VCenter

Les migrations (de machines)

Migration à chaud

vMotion avec le vCenter

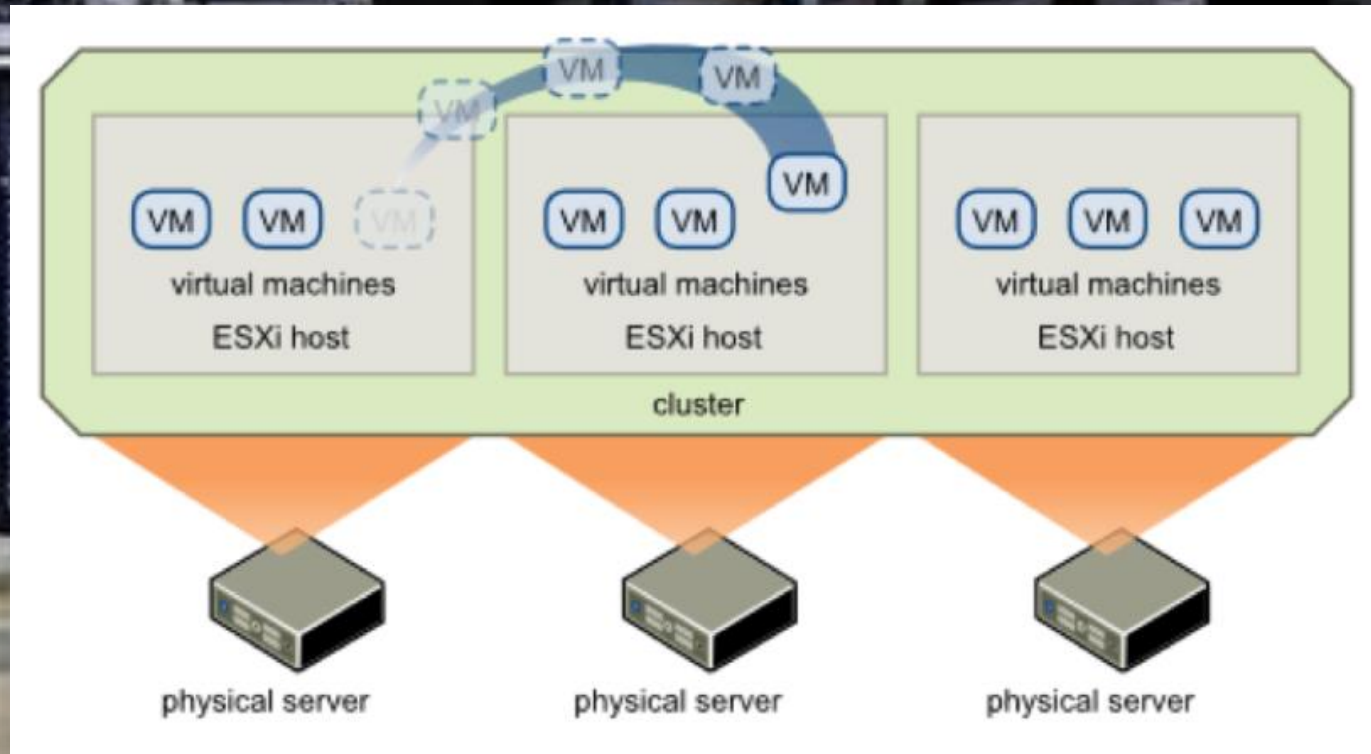
déplacement de l'empreinte mémoire de la machine d'un hyperviseur à un autre

La migration à chaud d'un hyperviseur à l'autre est appelée vMotion

La migration à chaud des fichiers de machines virtuelles d'un datastore à l'autre est appelée Storage vMotion

Virtualisation des systèmes d'information

Le concept



Virtualisation des systèmes d'information

Le concept

Migration à chaud vMotion

Validation d'un hyperviseur compatible

Création d'une copie de la VM sur l'hyperviseur cible

Copie de chaque page mémoire depuis l'hyperviseur source vers l'hyperviseur cible, via le réseau vMotion. Cette étape est nommée précopie et elle s'exécute autant de fois que nécessaire tant qu'il y a des changements dans les pages mémoires

La VM sur l'hyperviseur source est figée et est relancée sur l'hyperviseur cible

Notion d'EVC: lissage des fonctionnalités des CPU d'un cluster.

Virtualisation des systèmes d'information

Le concept

Vmotion

Permet la migration manuel d'une machine virtuelle d'un ESX

Avec le stockage partagé (SAN)

Transfert de la mémoire active + Etat d'exécution de la VM.

VMFS

permet l'accès au fichiers par plusieurs instance ESX

Virtualisation des systèmes d'information

Le concept

Le VCenter

Migration à chaud Storage vMotion

La migration vMotion permet de déplacer les processus de machines virtuelles

Les migrations Storage vMotion concernent les fichiers constitutifs des VM. La migration se fait de datastore(s) vers datastore(s)

- L'agent VPXa copie le répertoire de la machine virtuelle depuis le datastore source vers le datastore cible

La machine virtuelle dite « shadow VM » est démarrée, mais reste en attente de la fin de copie des VMDKs

Le SvMotion demande au Mirror Driver de dupliquer chaque écriture pour chaque bloc déjà copié

En une seule passe la copie des VMDK est faite et complétée au niveau du datastore cible tout en continuant la duplication de chaque I/O

Le SvMotion fait appel aux fonctionnalités Fast Suspend et Resume de la machine virtuelle afin de transférer l'état actif de la machine virtuelle source vers la machine virtuelle dite shadow

Après que le Fast Suspend et Resume ont été complétés, le répertoire et les fichiers (VMX, VMDK) présents dans le datastore source sont supprimés

Virtualisation des systèmes d'information

Le concept

Distributed Ressources Scheduler

Allocation dynamique des VMs suivant la charge des différents serveur ESX

Différents paramétrages possibles

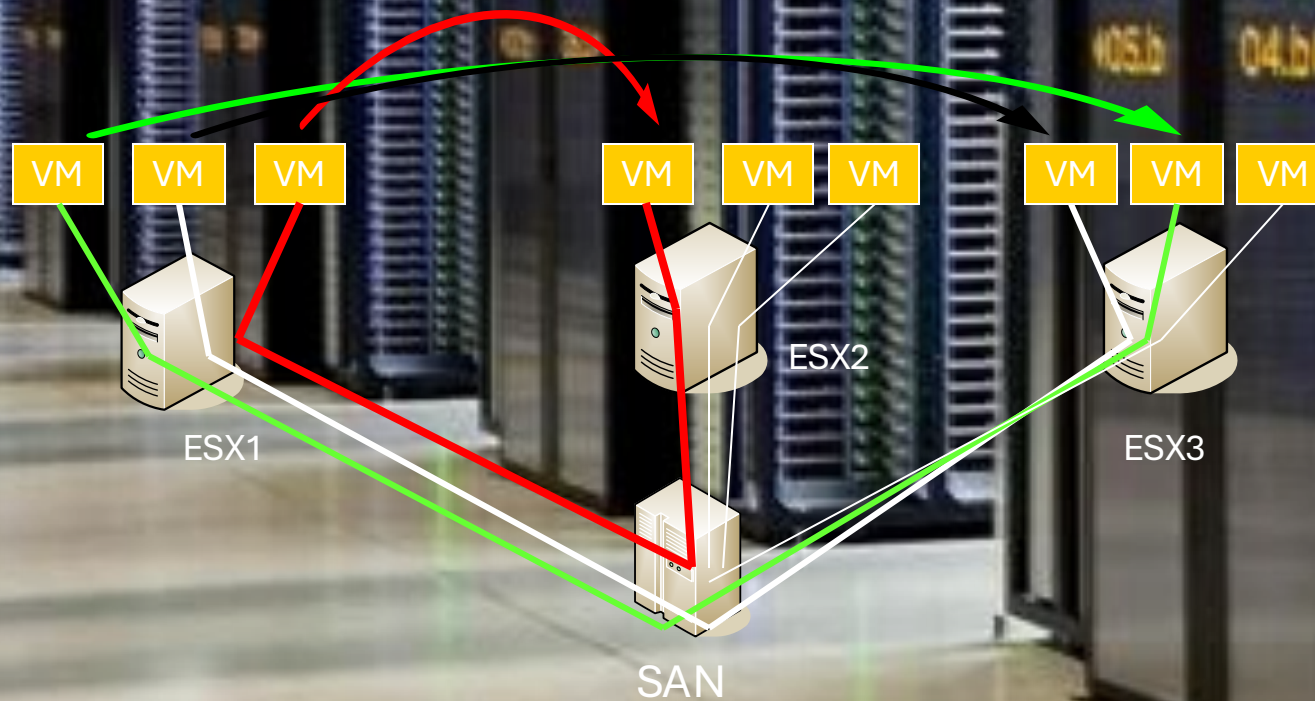
Notion de priorité des VM, etc....

Possibilité de fonctionnement manuel, envoi de recommandations uniquement

Et l'équilibre de charge doit être fait manuellement par Vmotion

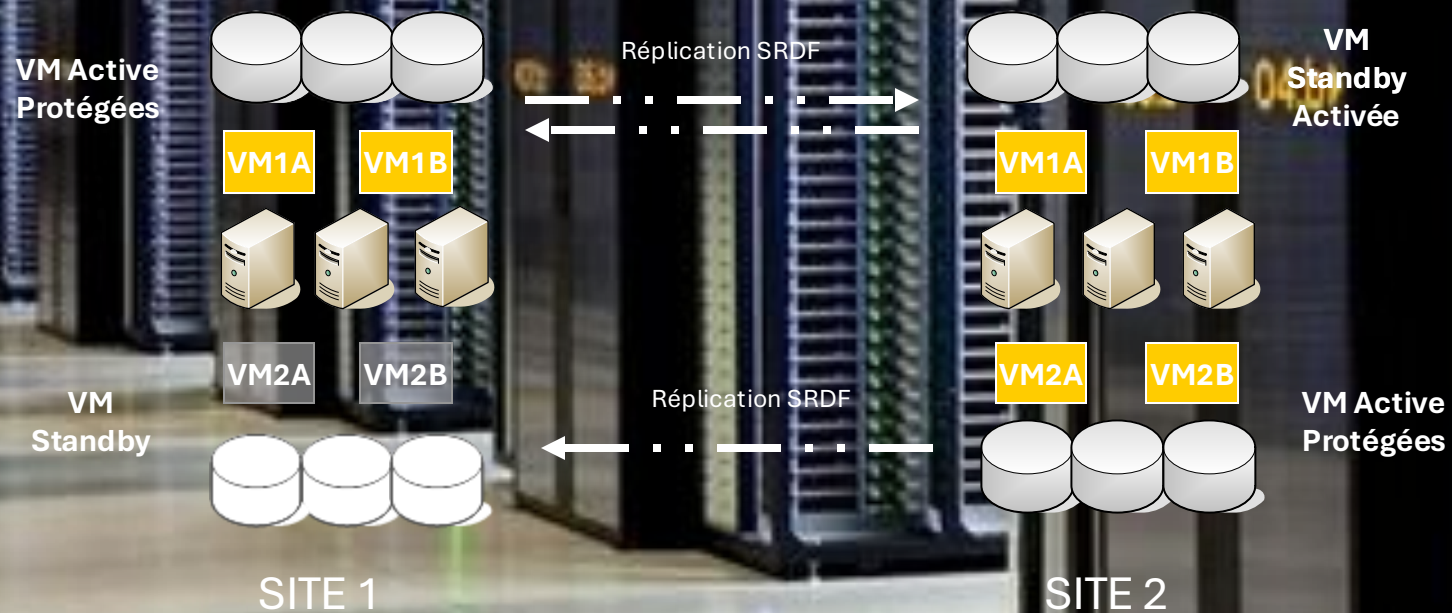
Virtualisation des systèmes d'information

Le concept



Virtualisation des systèmes d'information

Le concept



RTO / RPO

