VMware

Infrastructure 3.5

Perfectionnement - Durée : 2 Jours

FORMATION - REF VIE 006

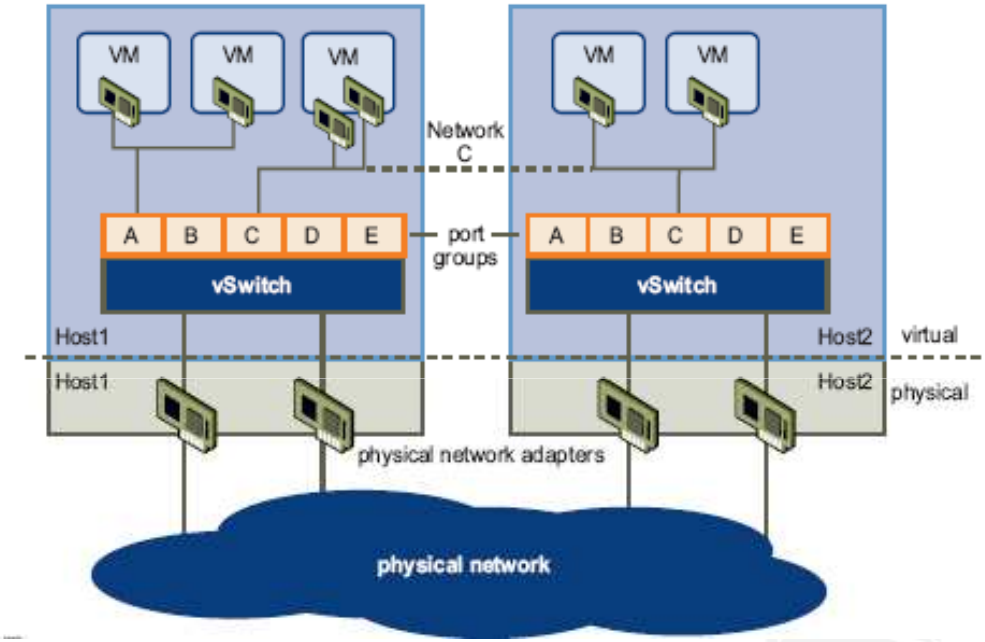
Avolys
Accompagnateur de changement

01. Réseau

- Vue d'ensemble du réseau virtuel
- Le switch virtuel (vSwitch)
- Le portgroup / le VLAN
- Accès au réseau via le VI Client
- Les services réseaux pour le VMkernel
- Création d'un vSwitch pour les services réseaux du VMkernel
- Configuration avancée du vSwitch
- Multiples réseaux sur un serveur ESX

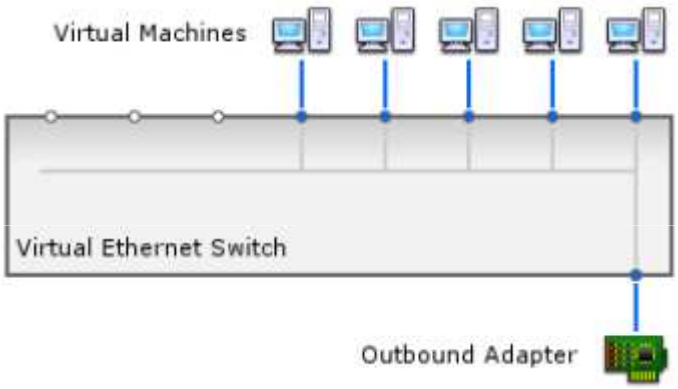
01. Réseau
Vue d'ensemble du réseau virtuel

- Les éléments constituant un réseau virtuel :
  - Les cartes réseaux physiques
  - Les cartes réseaux virtuelles
  - Les switchs réseaux physiques
  - Les switchs réseaux virtuels
  - Les VLANs
  - Les portgroups
  - Les NIC Teaming



01. Réseau
Le switch virtuel (vSwitch)

- Création du vSwitch avec le VI Client
- Constitution d'un réseau interne (privé) entre les VM
- Constitution d'un réseau entre les VM connectées au LAN à travers une ou plusieurs cartes réseaux physiques
- Le vSwitch améliore la bande passante des flux réseaux grâce à la création d'un Nic Teaming
- Le vSwitch intègre le Failover grâce à la création d'un Nic Teaming
- Possibilité de créer jusqu'à 127 vSwitchs sur un serveur ESX
- Par défaut, 56 ports sur le vSwitch (jusqu'à 1016 ports)



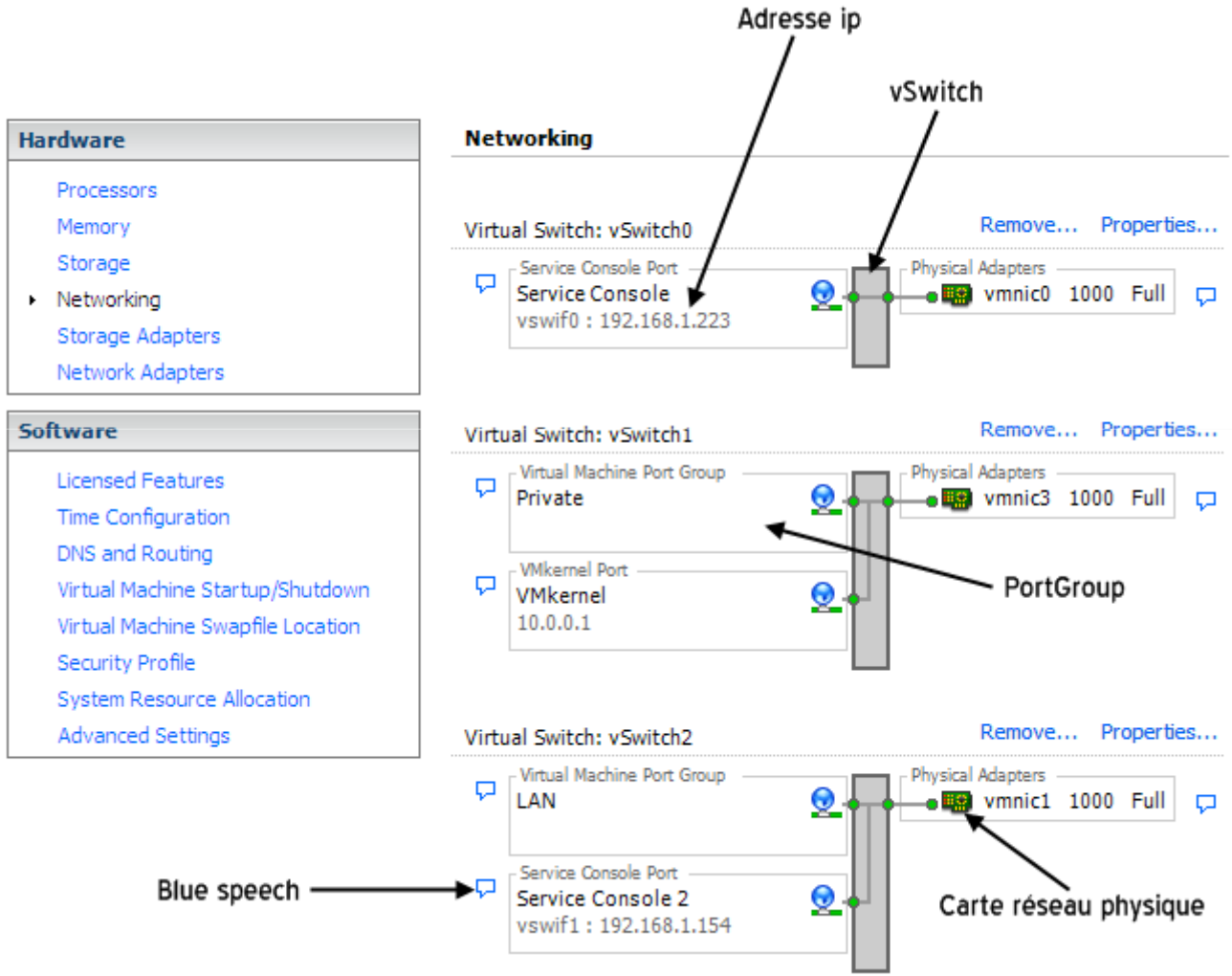
01. Réseau
Le portgroup / le VLAN

- Les portgroups agrègent plusieurs ports d'un vSwitch et fournissent un seul point d'entrée pour les VM connectées
  - Chaque portgroup est identifié par un label réseau unique sur le serveur ESX
  - Plusieurs portgroups possible par switch virtuel
  - Création de VLAN sur le portgroup (optionnel)
  - Jusqu'à 512 portgroups sur un serveur ESX
- Les VLAN permettent la segmentation du réseau physique, ainsi les portgroups sont segmentés et offrent la possibilité d'effectuer de la séparation de flux comme sur les réseaux physiques.
  - Pour améliorer la sécurité (séparation des flux)
  - Pour améliorer la performance (domaine différent de broadcast)
  - Pour le coût (moins de matériel requis)
- Le standard est le 802.1Q

adresse dst.	adresse src.	Len/Etype = 0x8100	**Tag (inséré)**	Data	FCS

01. Réseau

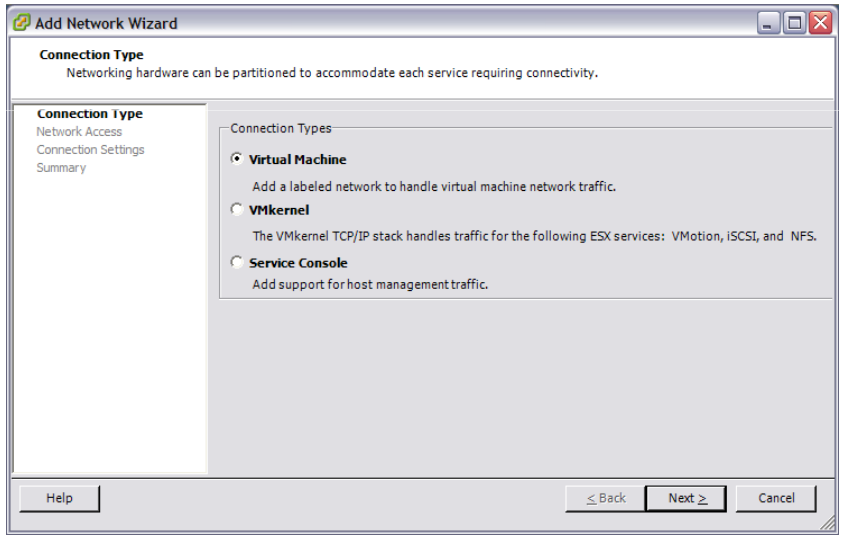
Accès au réseau via le VI Client

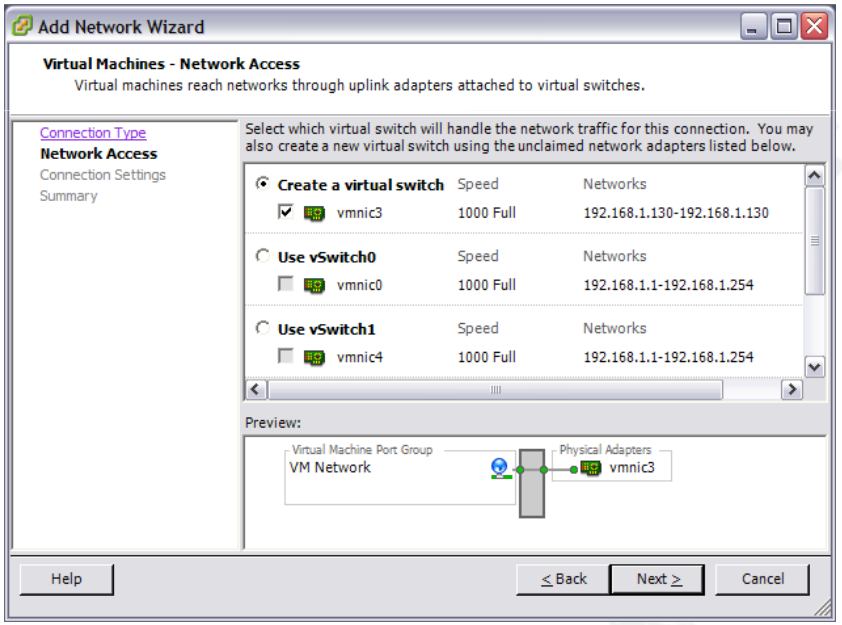


01. Réseau

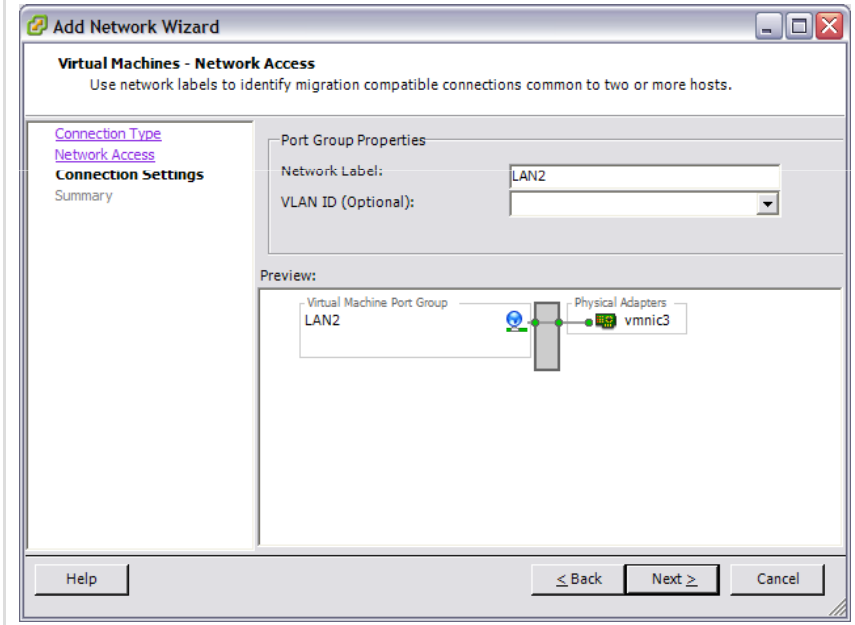
Le vSwitch pour les machines virtuelles (1/2)

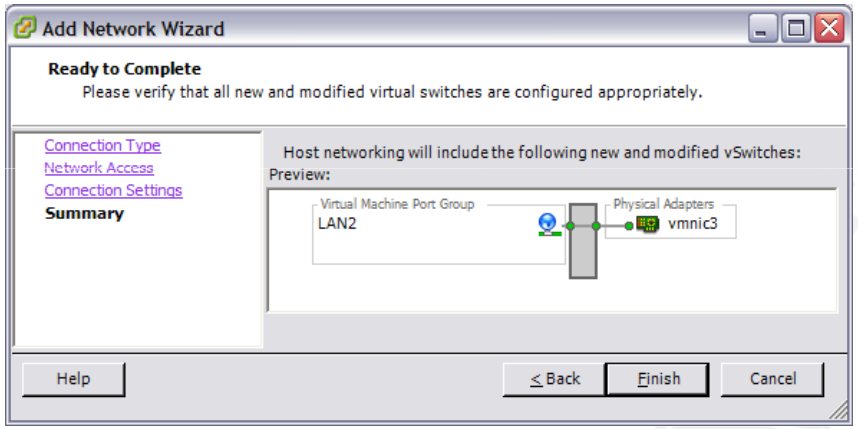
- Onglet « Configuration »
- Page « Networking »
- Cliquer sur « Add Networking… »





01. Réseau
Le vSwitch pour les machines virtuelles (2/2)





01. Réseau

Les services réseau pour le VMkernel

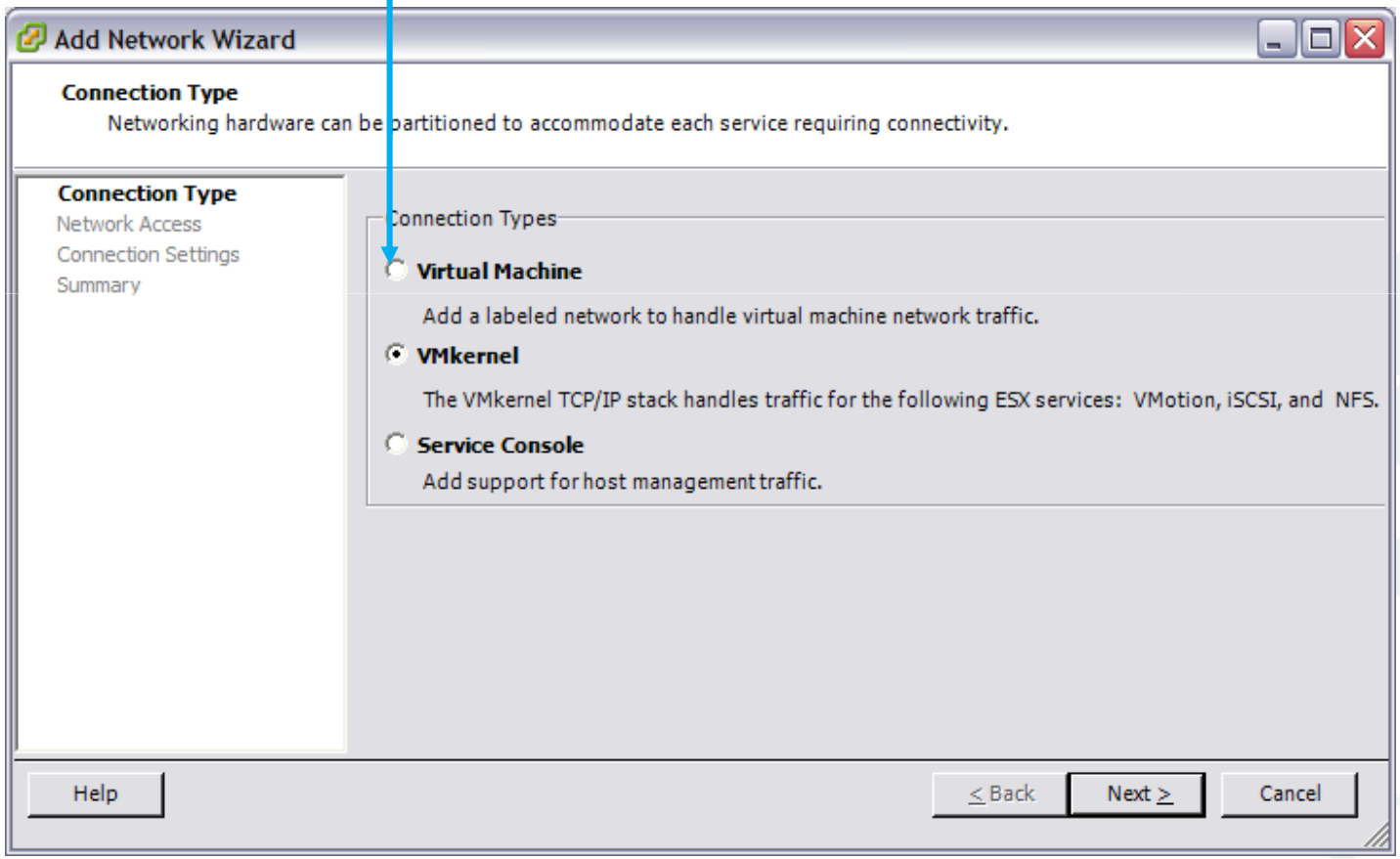
- Configuration d'un service réseau particulier pour le VMkernel :
  - VMotion (déplacement des VM entre serveurs ESX sans coupure de service)
  - iSCSI
  - NAS (NFS)

- Il est recommandé de séparer chaque flux réseau du VMkernel (VMotion, NAS ou iSCSI). Séparé également du réseau du service console.
  - Recommandations :
    - L'adresse IP configurée pour le réseau du VMkernel doit être différente de l'IP du service console
    - Après avoir configuré le logiciel iSCSI, il faut ouvrir le port du firewall pour le service iSCSI
    - A la différence des autres services, le iSCSI a un composant dans le service console, ainsi le réseau qui va servir à atteindre la cible iSCSI doit être identique au service console et au réseau du VMkernel

01. Réseau

Création d'un vSwitch pour les services réseaux du VMkernel (1/2)

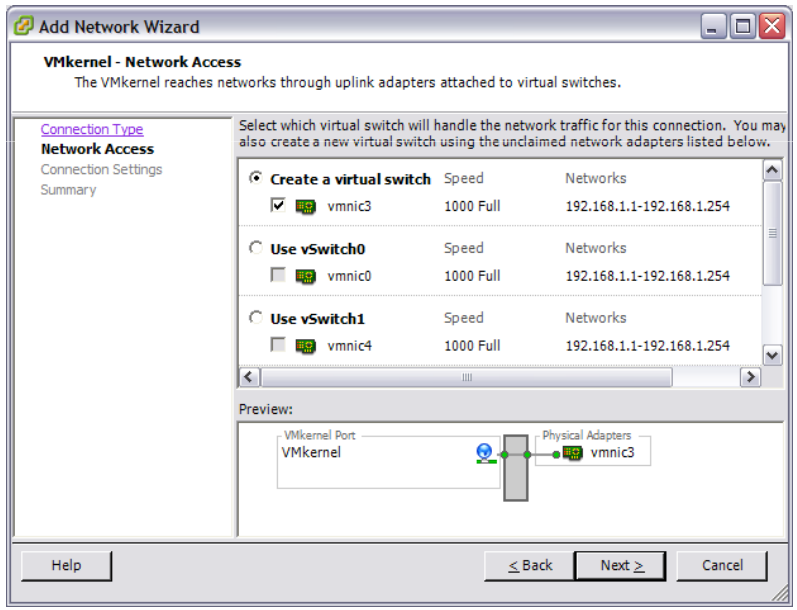
Différents types de connexions pour les vSwitchs

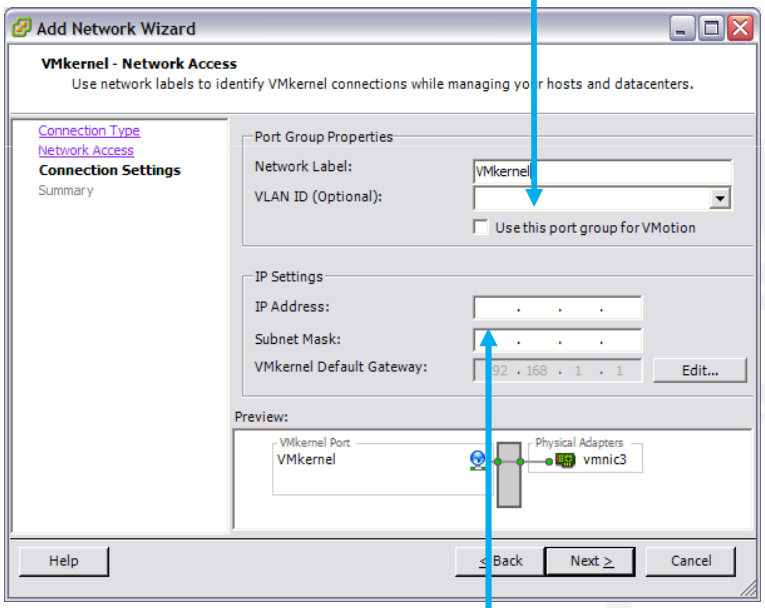


01. Réseau

Création d'un vSwitch pour les services réseaux du VMkernel (2/2)

Si nécessaire, configurer l'id de VLAN
(par exemple sur les serveurs type Blade)

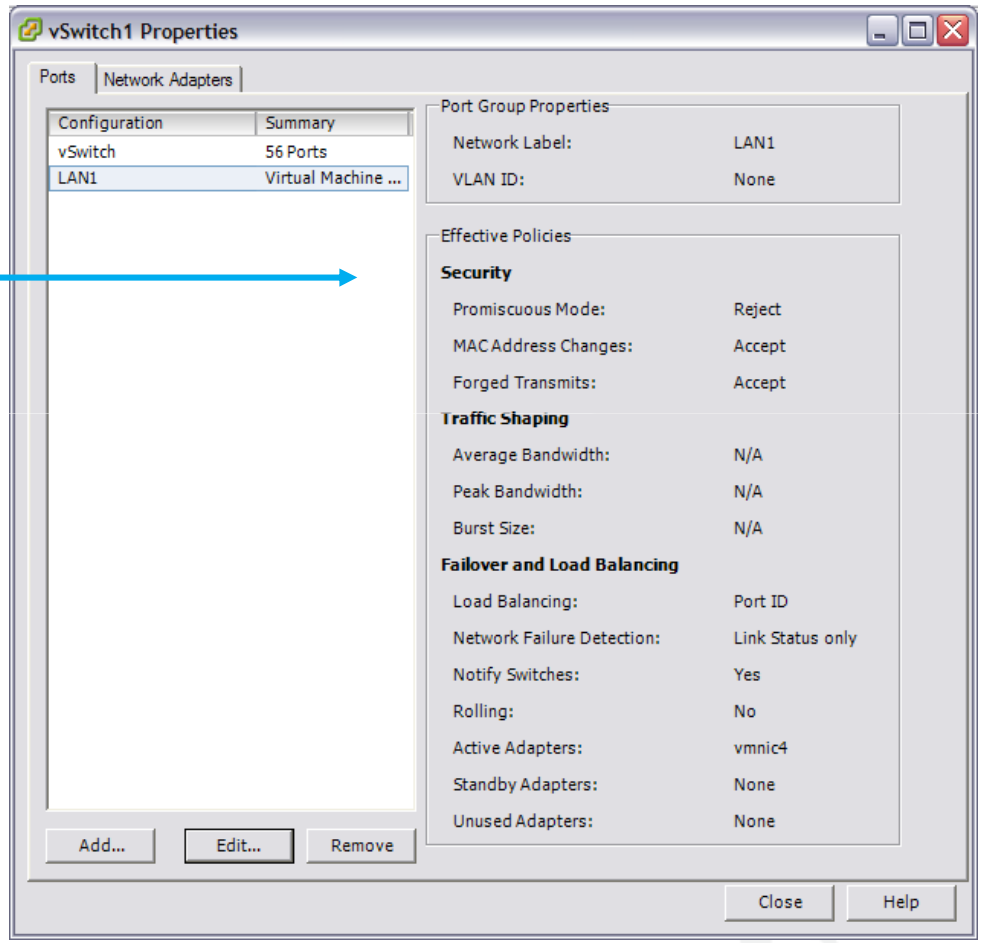




Configuration de l'adresse IP

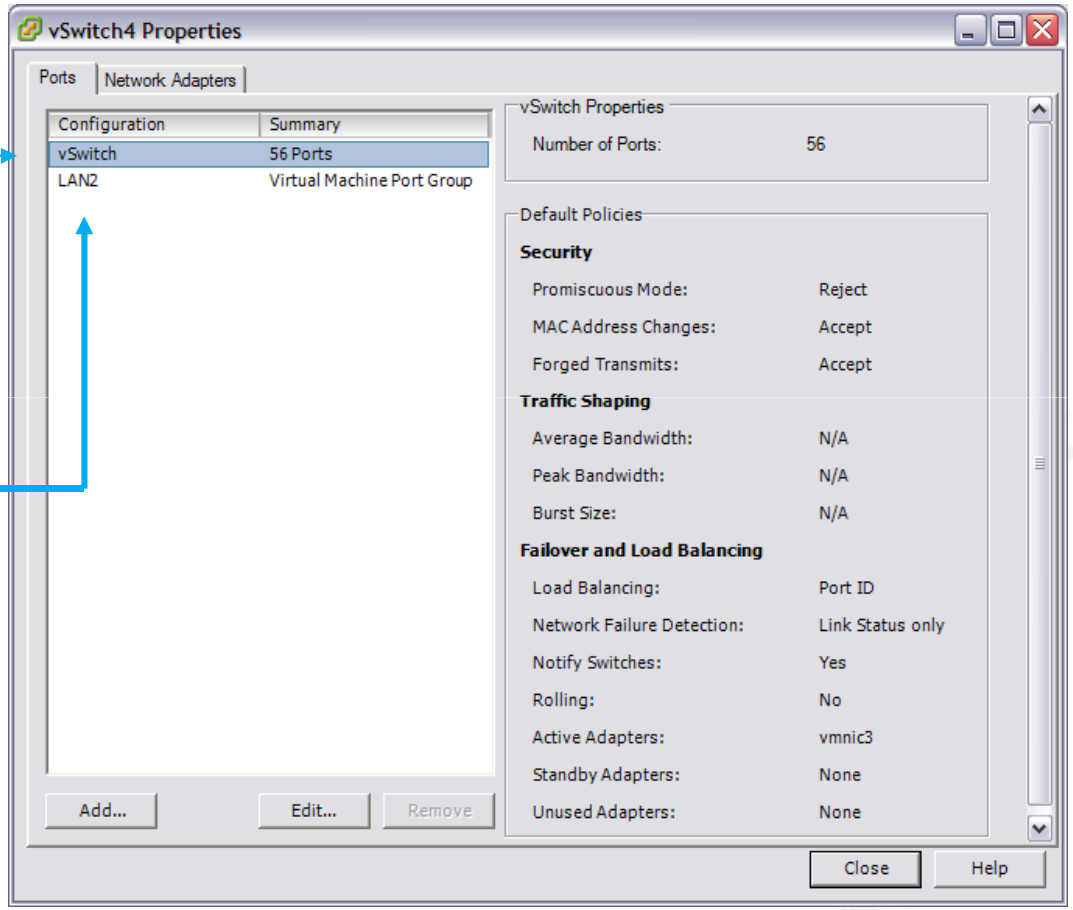
01. Réseau
Configuration avancée du vSwitch (1/7)

- Différentes politiques de sécurité :
  - Security
  - Traffic Shaping
  - Failover
  - Load Balancing



01. Réseau
Configuration avancée du vSwitch (2/7)

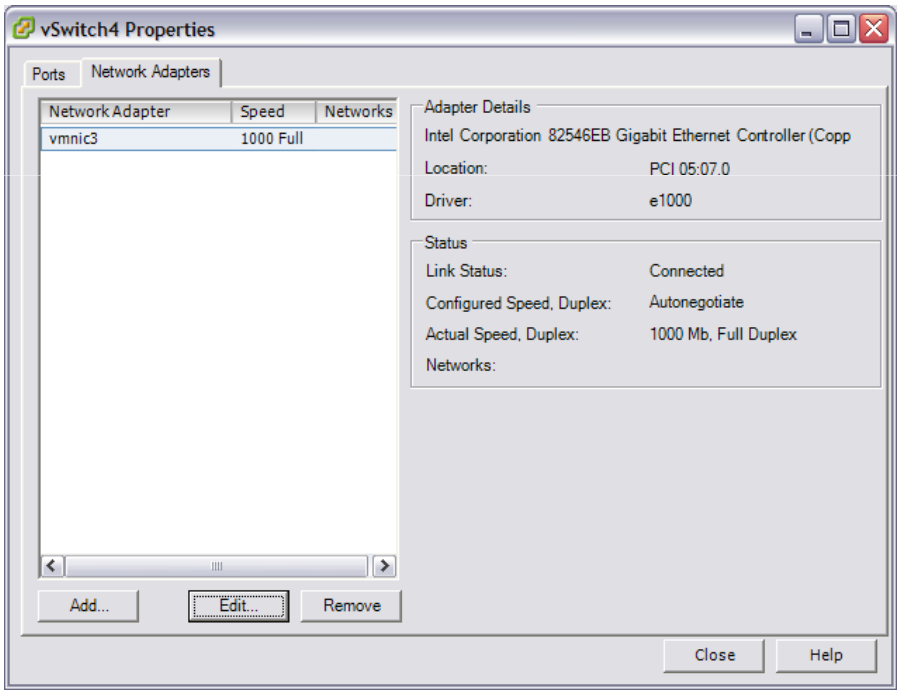
- Permet de configurer le switch virtuel
- Possibilité de modifier les paramètres du switch pour un portgroup en particulier

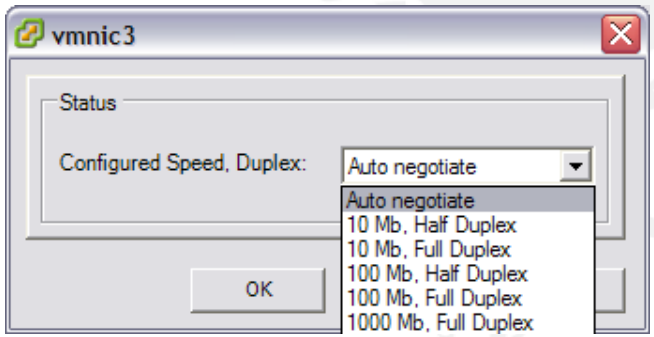


01. Réseau

Configuration avancée du vSwitch (3/7)

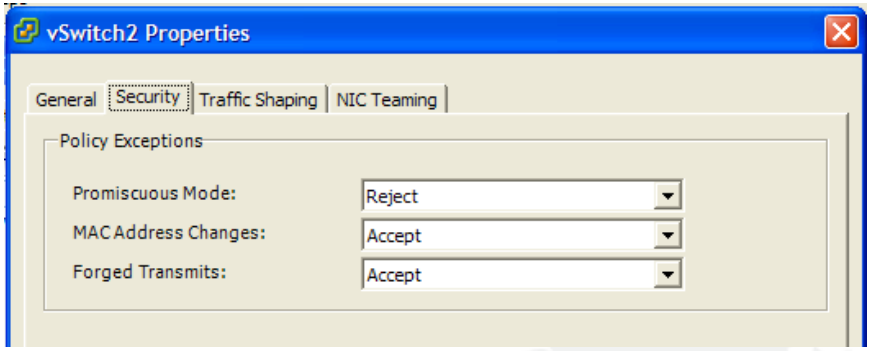
- Modification de la configuration de la carte réseau (vitesse, mode)



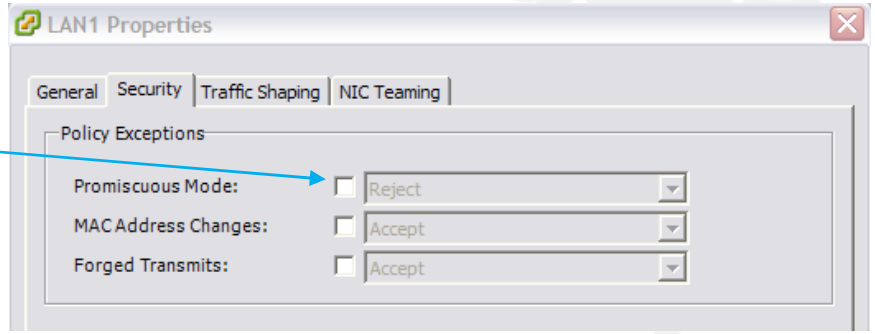


01. Réseau
Configuration avancée du vSwitch (4/7)

- Trois modes de sécurité :
  - Promiscuous Mode
  - MAC Address Changes
  - Forged Transmits

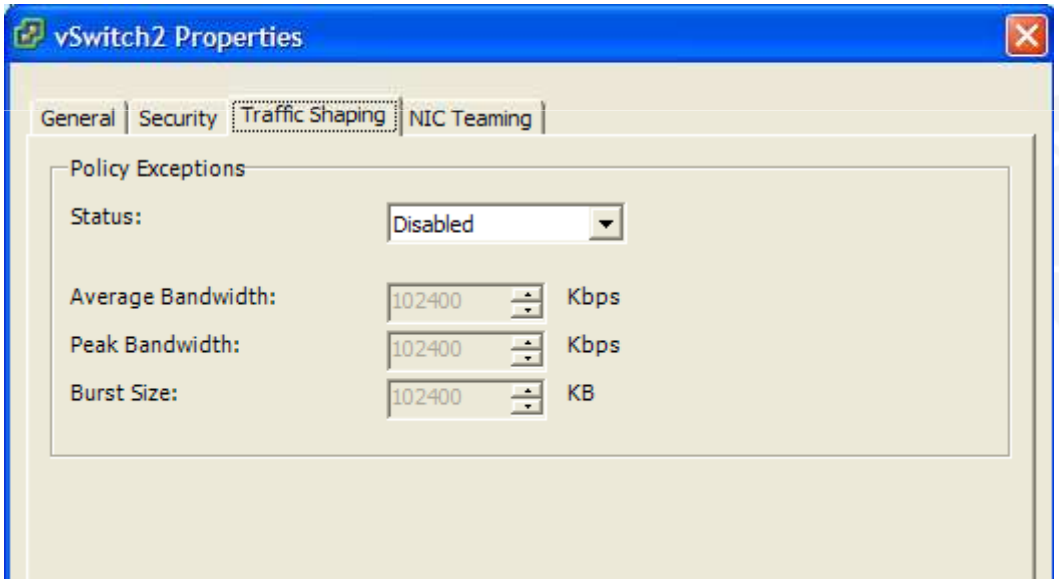


- Si l'édition se fait sur le portgroup, cocher la case pour invalider le paramètre défini au niveau du vSwitch



01. Réseau
Configuration avancée du vSwitch (5/7)

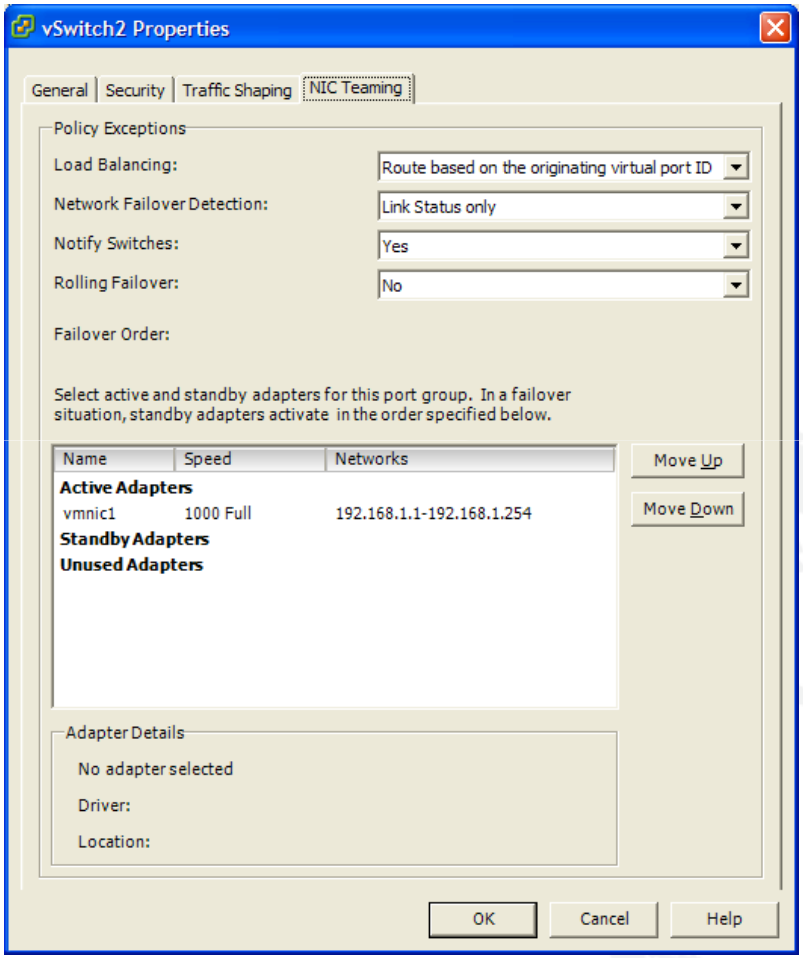
- Comme les autres paramètres avancés, le Traffic Shaping peut se paramétrer sur le switch virtuel ou sur un portgroup en particulier



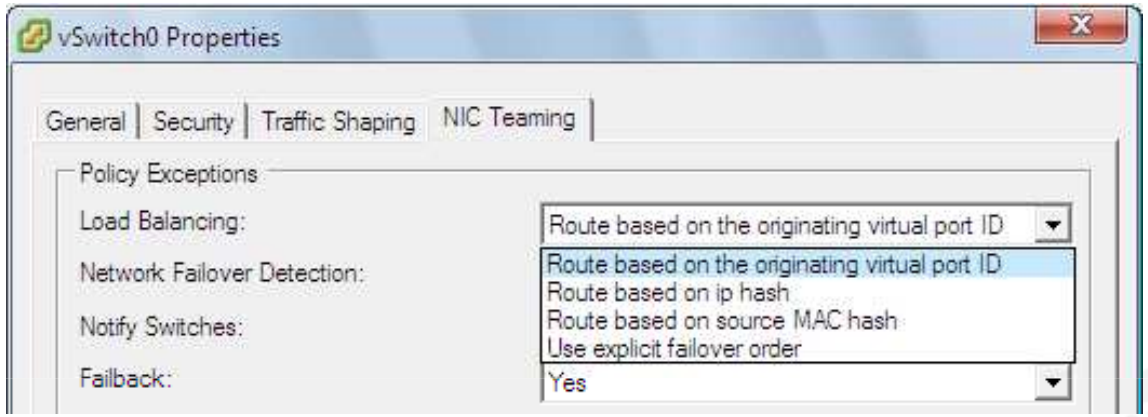
01. Réseau

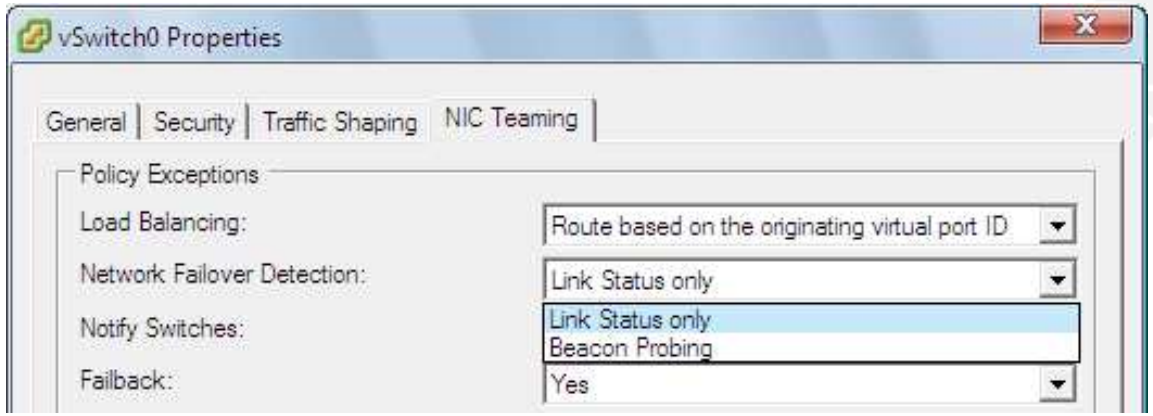
Configuration avancée du vSwitch (6/7)

- Comme les autres paramètres avancés, le NIC Teaming peut se paramétrer sur le switch virtuel ou sur un portgroup en particulier



01. Réseau
Configuration avancée du vSwitch (7/7)

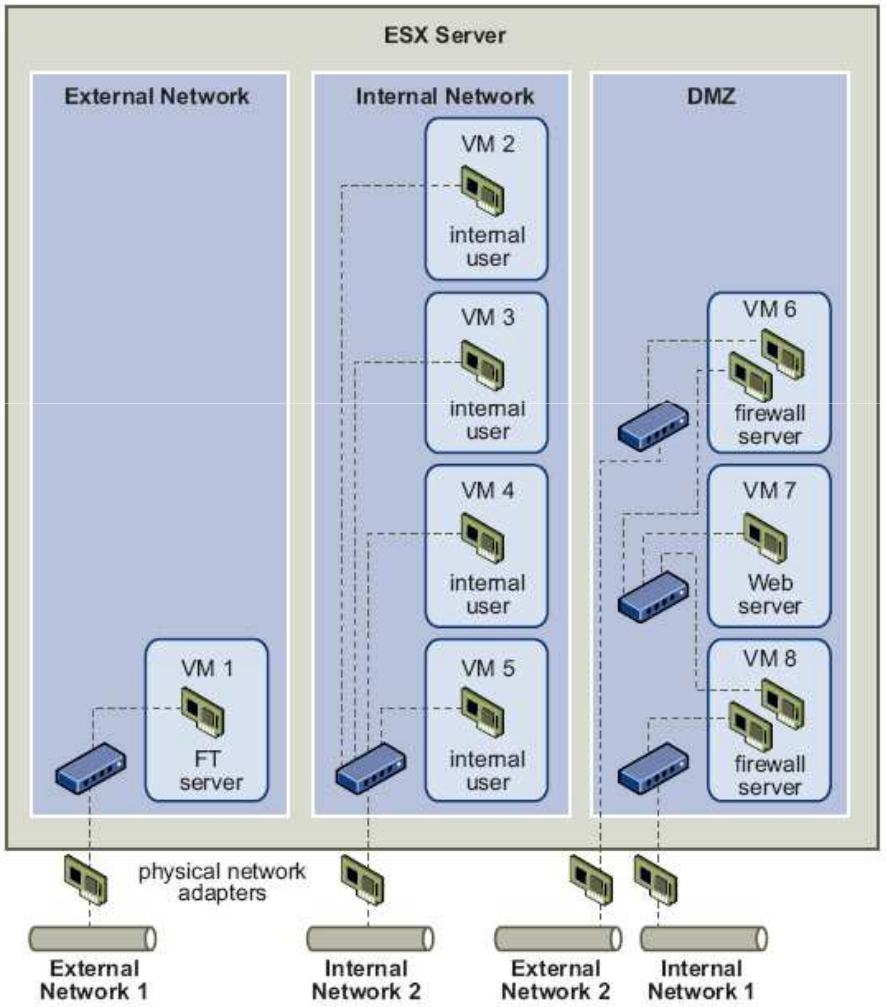


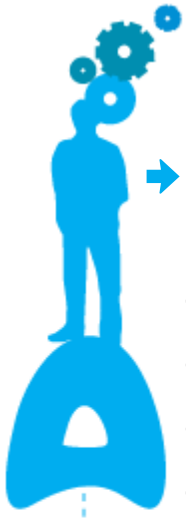


01. Réseau

Multiples réseaux sur un serveur ESX

- Exemple d'utilisation des vSwitchs





Notes

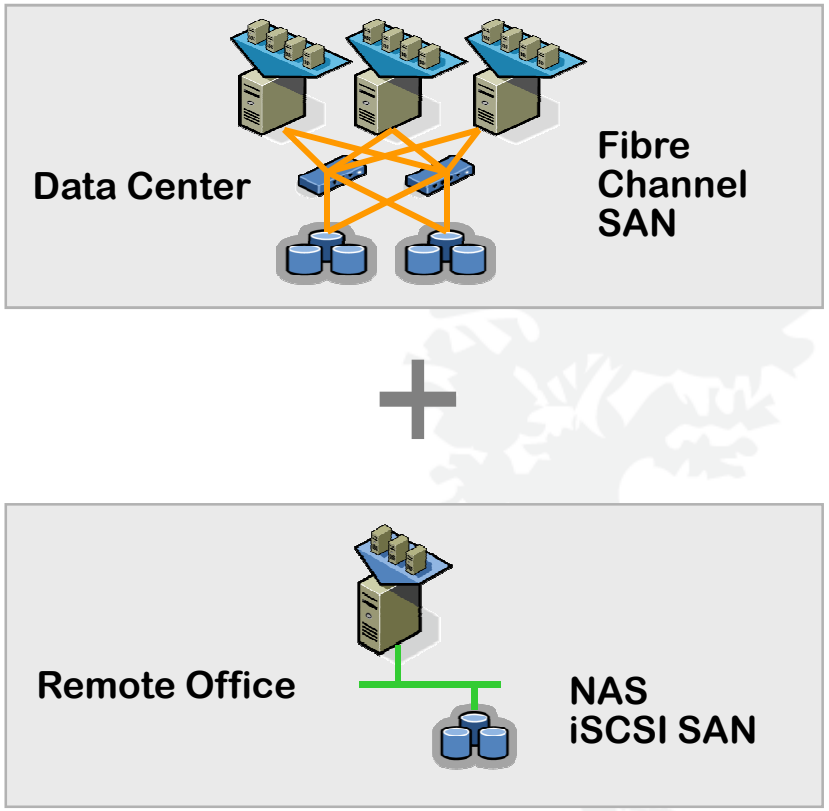
02. Stockage

- Vue d'ensemble du stockage
- Accès au stockage via le VI Client
- Partage des volumes VMFS
- Vue d'ensemble du SAN
- Configuration du stockage SCSI et SAN
- Configuration du stockage iSCSI
- Configuration du stockage NAS
- Raw Device Mapping (RDM)
- Virtual Fibre Channel
- Le « Multipathing »
- Résumé des différents stockages

02. Le stockage
Vue d'ensemble du stockage (1/4)

➔ Terminologie utilisée pour l'environnement de stockage :

- Datastore
- VMFS (Virtual Machine File System)
- Extend
- Fibre Channel (FC)
- iSCSI (Internet SCSI)
- LUN (Logical Unit Number)
- Multipathing
- Failover path
- NAS (Network Attached Storage)
- NFS (Network File System)
- RDM (Raw Device Mapping)



02. Le stockage
Vue d'ensemble du stockage (2/4)

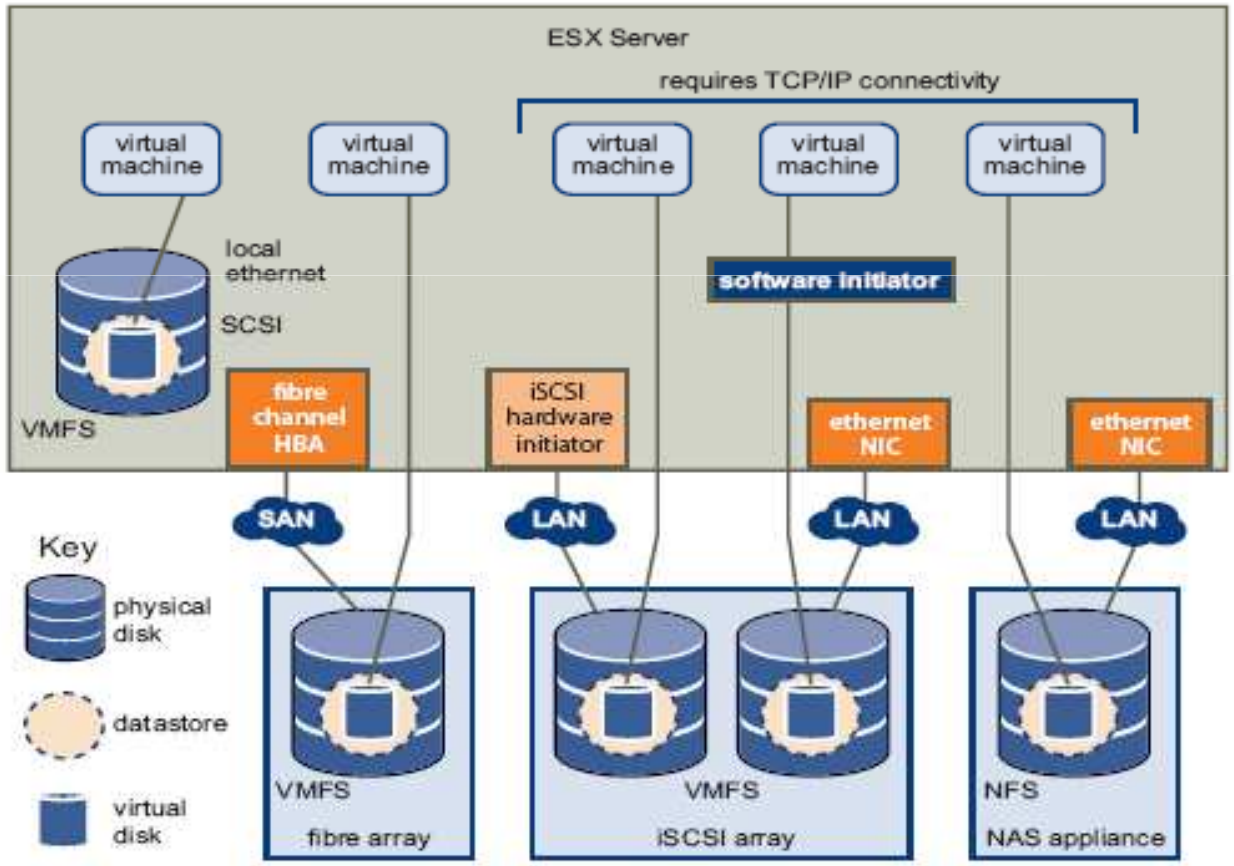
Format du système de fichier

- **Le Datastore que vous utilisez peut être « formaté » avec deux systèmes de fichiers :**
  - VMFS, sur des disques SCSI, LUN iSCSI ou LUN FC
  - Partage NFS sur un serveur NFS, le formatage dépend du NAS

- **Types de stockage**
  - Local, disque SCSI interne ou externe
  - SAN, nécessite au moins une carte HBA (Host Bus Adapter)
  - iSCSI (Hardware Initiated)
  - iSCSI (Software Initiated)
  - NFS

02. Le stockage
Vue d'ensemble du stockage (3/4)

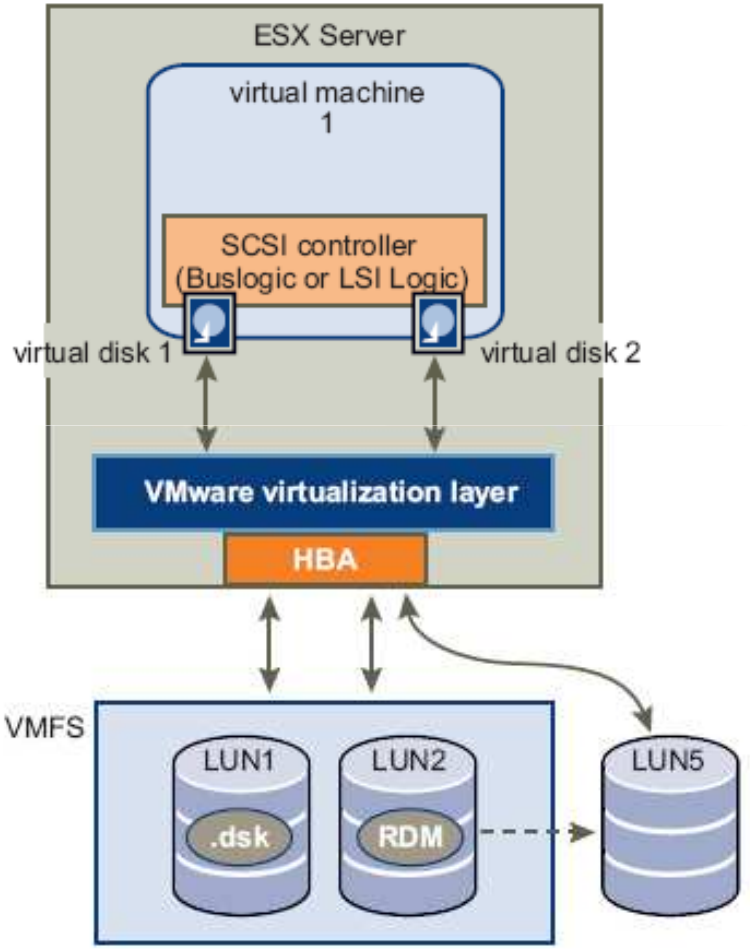
- Les différentes solutions pour qu'une VM accède à son système de stockage



02. Le stockage
Vue d'ensemble du stockage (4/4)

Comprendre le SCSI virtuel

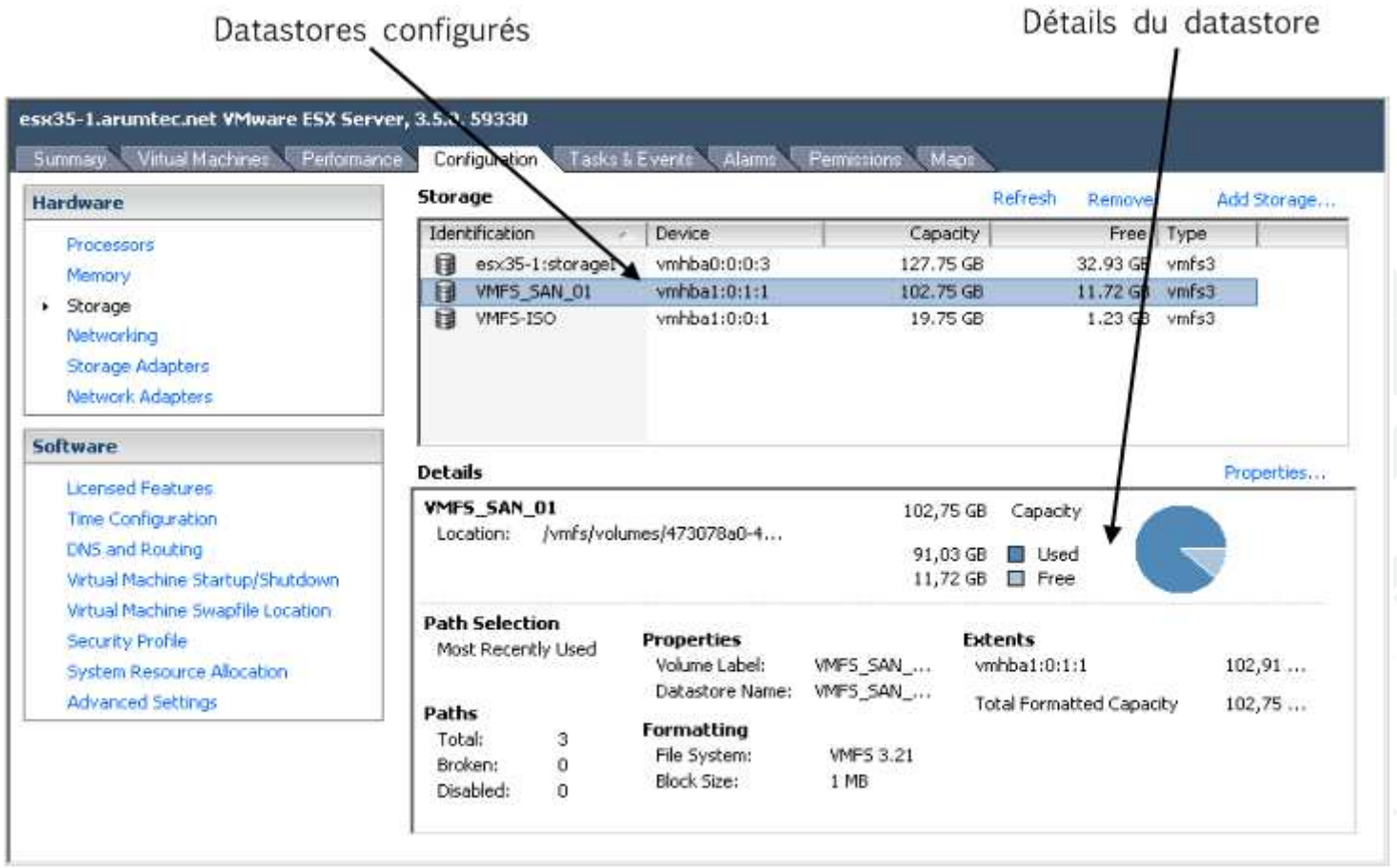
- Dans chaque machine virtuelle il est possible de configurer de 1 à 4 cartes SCSI virtuelles (LSI Logic ou BusLogic)



02. Le stockage

Accès au stockage via le VI Client (1/3)

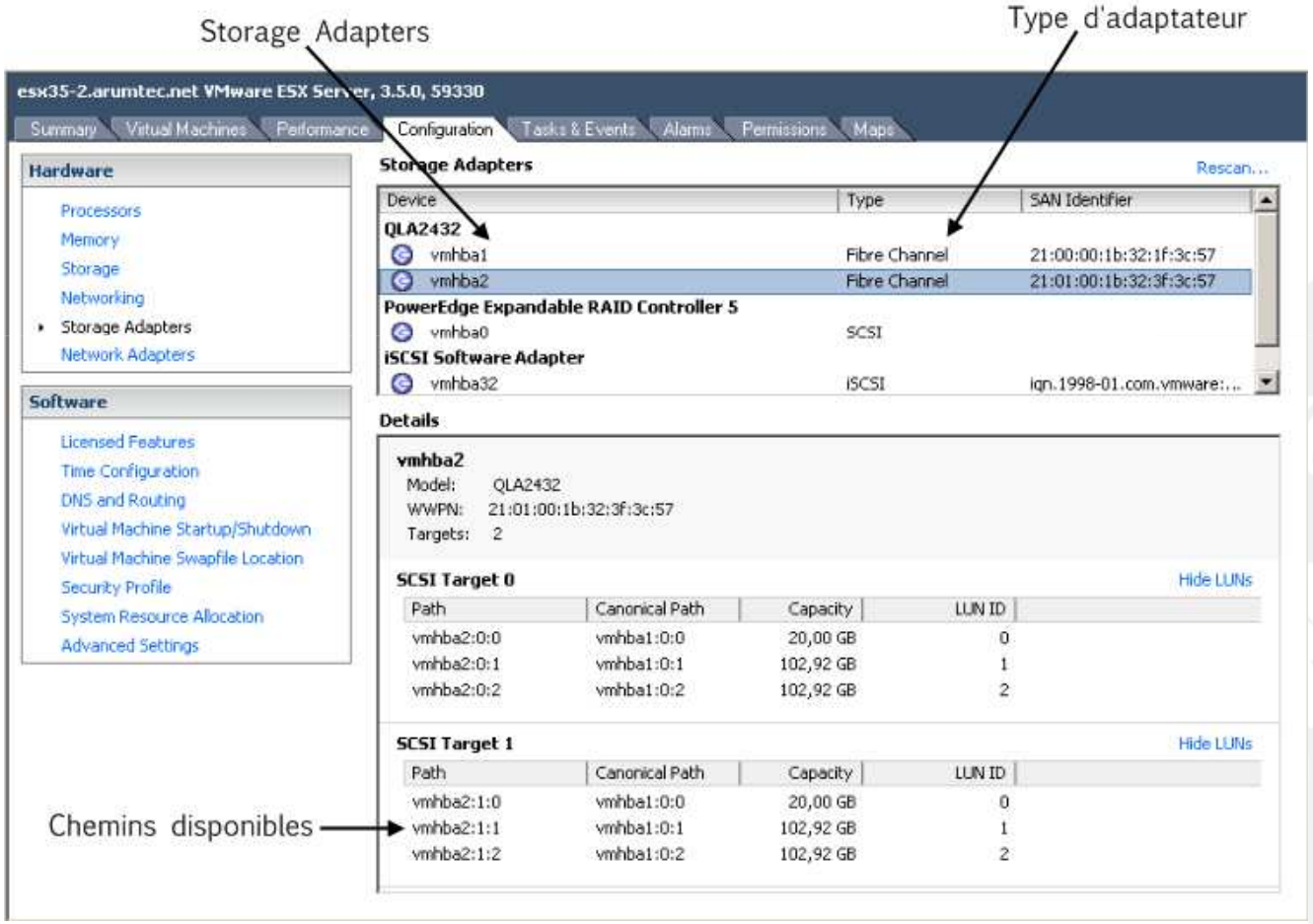
➔ Détail des datastores



02. Le stockage

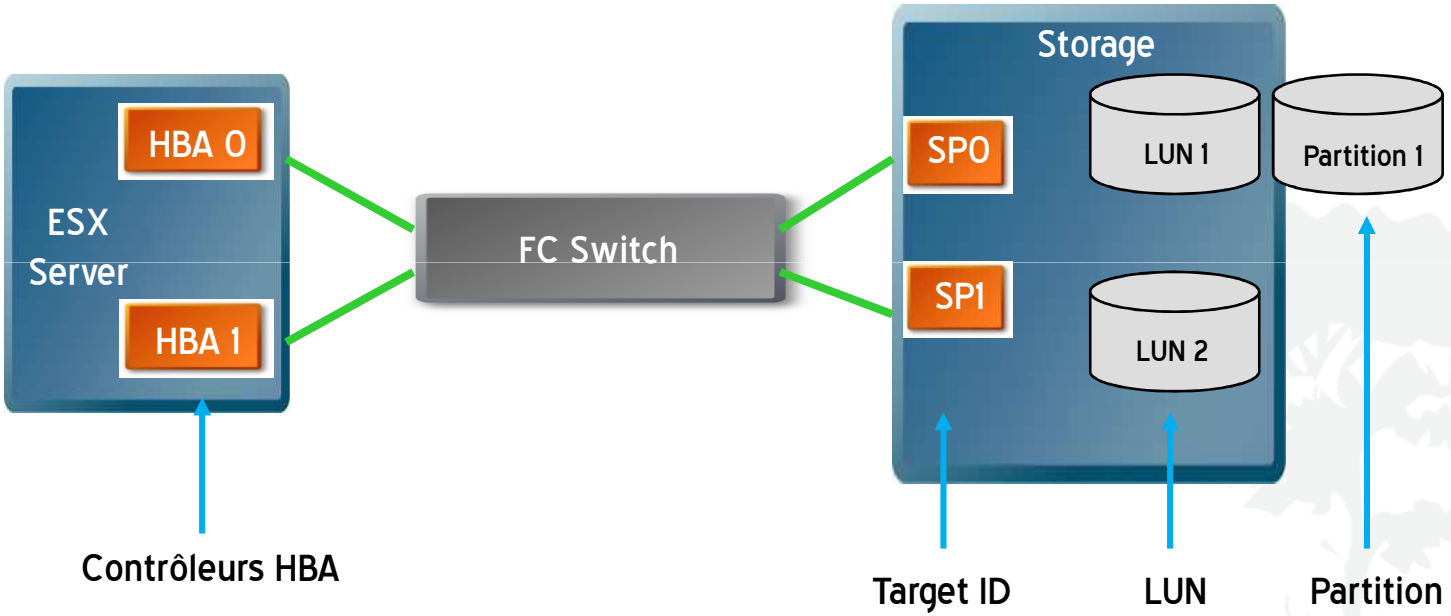
Accès au stockage via le VI Client (2/3)

➔ Détail des cartes d'accès au stockage



02. Le stockage
Accès au stockage via le VI Client (3/3)

- Le VMkernel adresse les partitions selon la configuration suivante :
  - VMHBA C:T:L:P



- Exemple :
  - LUN1 = vmhba0:0:1
  - Partition1 = vmhba1:1:1:1

02. Le stockage

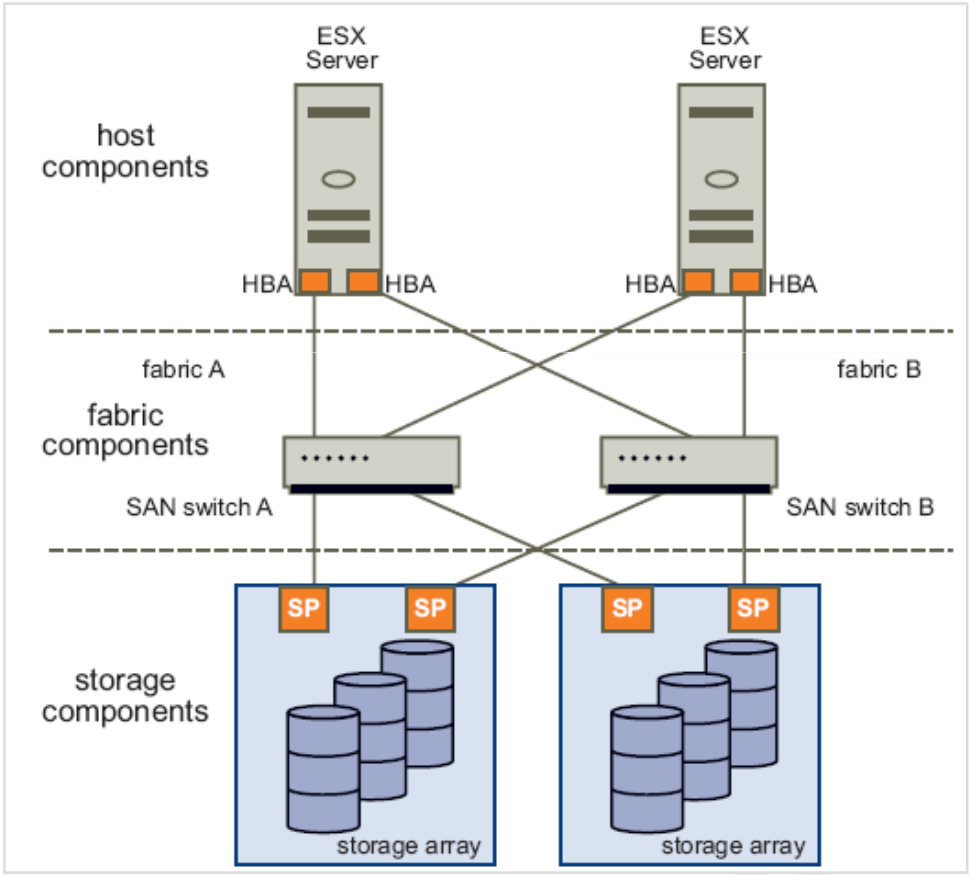
Partage des volumes VMFS sous ESX 3

- Sous VMware ESX 3 , le partage de disques entre machines virtuelles ou entre machines virtuelles et machines physiques passe forcément par le mappage RDM.

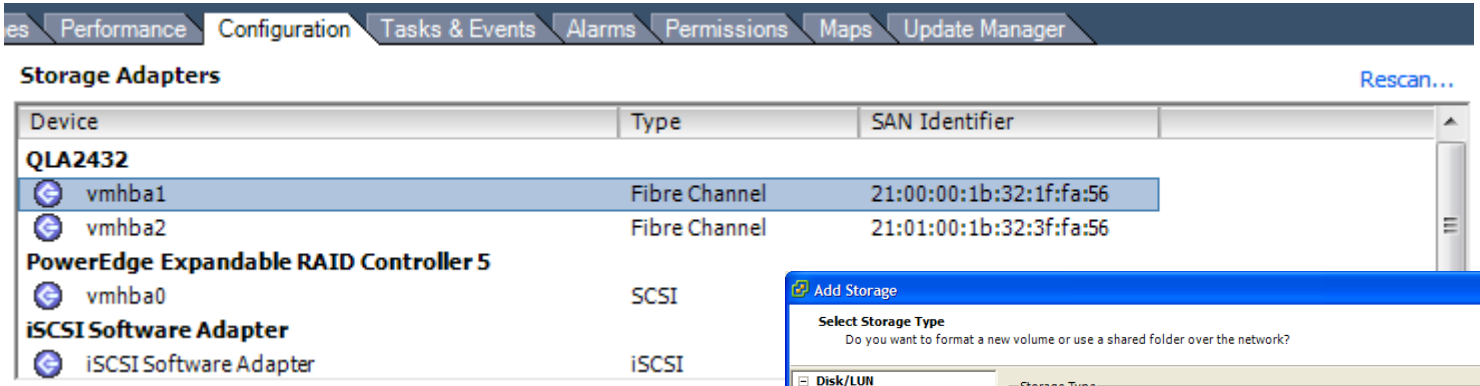
Disque partagé	Rôle	Utilisation
VMFS Public	Verrous par fichier	Mode par défaut, utilisé pour les cluster-in-a-box
RDM Virtuel	Verrous sur les fichiers de mapping RDM	Mode à utiliser dans le cluster accross boxes
RDM Physique	Verrous sur le Raw Device	Mode à utiliser pour le physical to virtual cluster

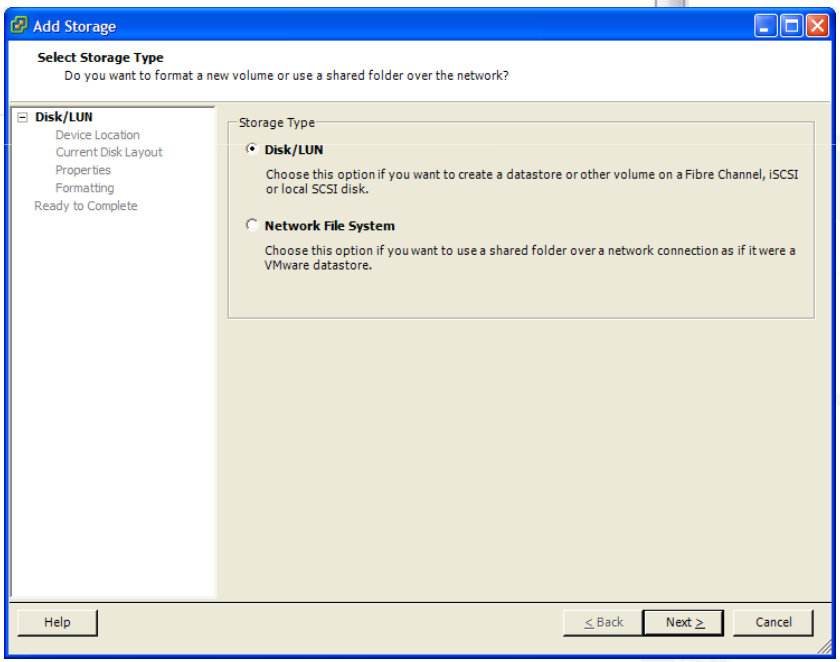
02. Le stockage
Vue d'ensemble du SAN

- Les composants du SAN (Storage Area Network)
  - Chaque nœud d'un SAN est identifié par un port le WWPN
  - Multipathing et Path FailOver
  - Zoning et LUN Masking
  - Active/Active et Active/Passive Storage Array



02. Le stockage
Configuration du stockage SCSI et SAN (1/2)



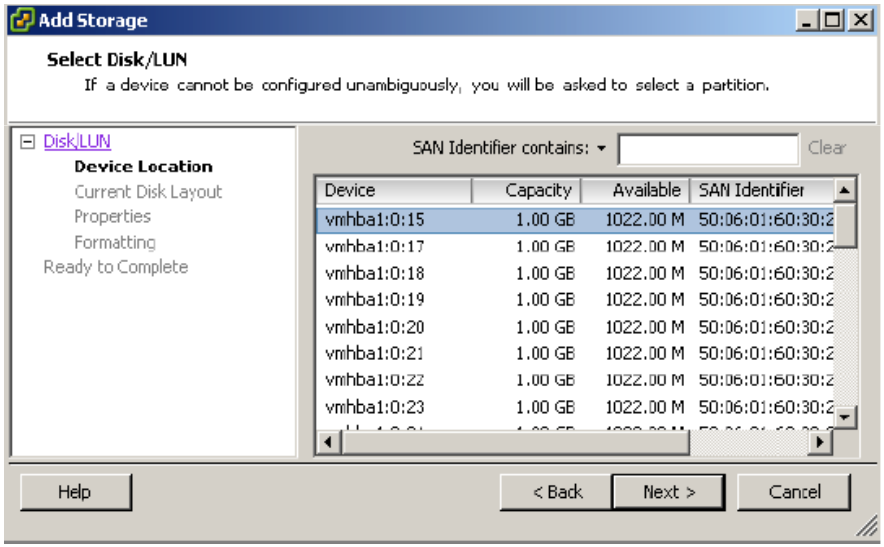


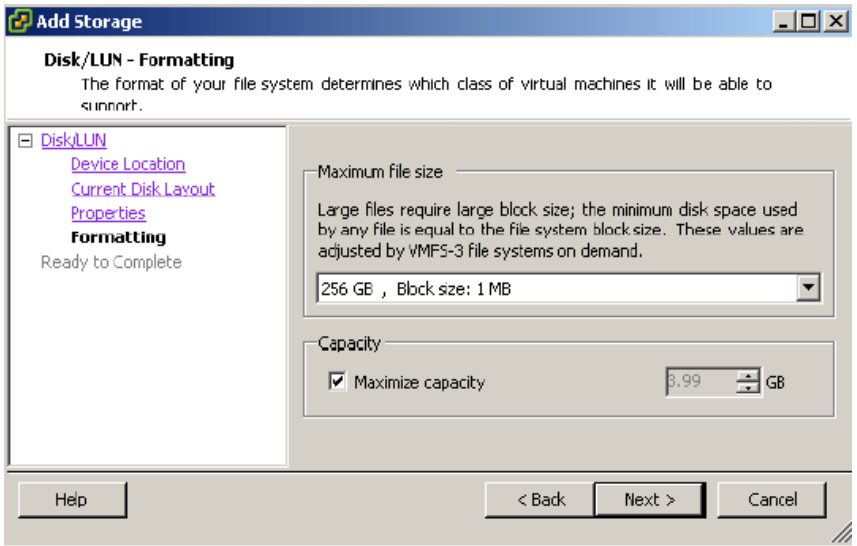
- Sous l'onglet « Configuration », page « Storage Adapters», cliquer sur « Rescan… »
- Sous l'onglet « Configuration », page « Storage », cliquer sur « Add storage »
- Sélectionner Disk/LUN

02. Le stockage

Configuration du stockage SCSI et SAN (2/2)

- Sélectionner la LUN à formater
- Définir un label et formater le volume sélectionné





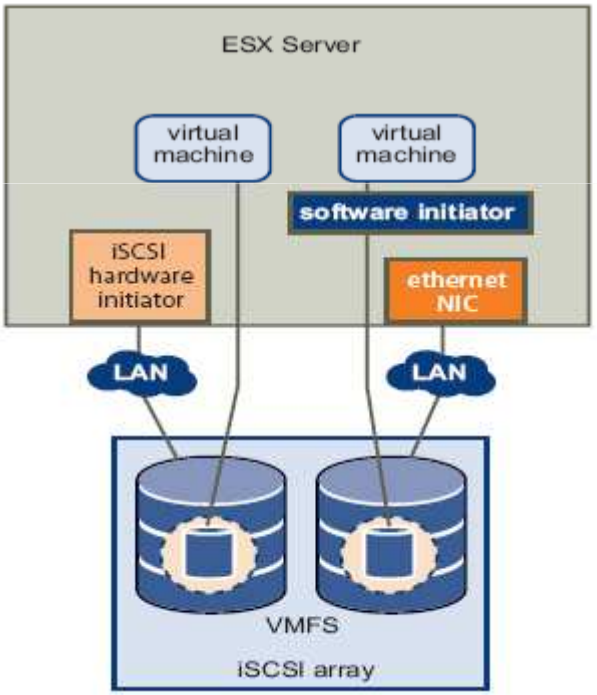
02. Le stockage

Configuration du stockage iSCSI (Hardware et Software Initiator)

Vue d'ensemble de l'iSCSI

- Le iSCSI va permettre au serveur ESX d'accéder à des LUNs via le réseau IP. Les commandes SCSI de la machine virtuelle sont encapsulées dans des paquets IP et transmises à la cible iSCSI.

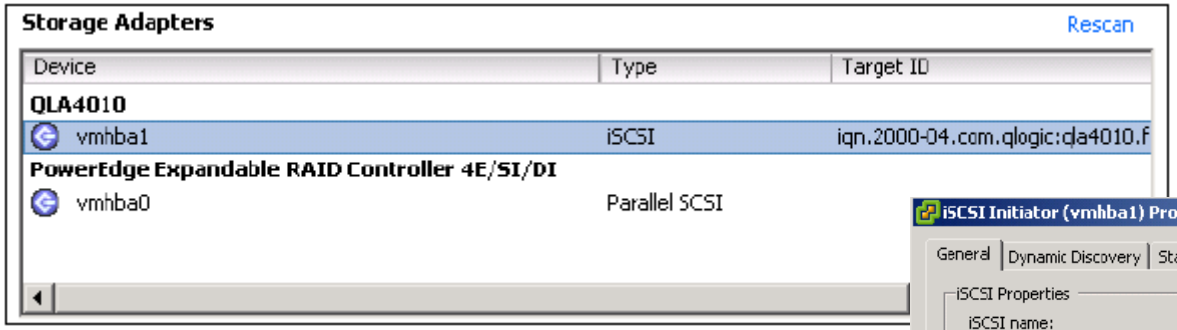
- Types d'initiateurs iSCSI:
  - Hardware iSCSI Initiator, une carte spécifique iSCSI est nécessaire pour la communication avec la cible iSCSI
  - Software iSCSI Initiator, le VMkernel se charge de convertir les commandes SCSI en paquets IP
- Sécurité iSCSI :
  - Utilisation du protocole d'authentification CHAP (Challenge Handshake Authentification Protocol)
  - Périodiquement, l'authentification de la cible iSCSI est vérifiée



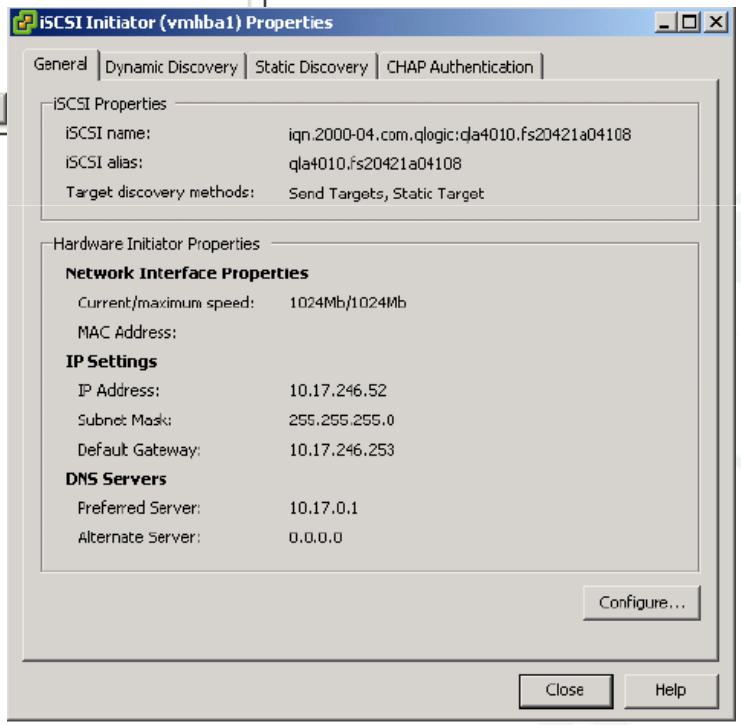
02. Le stockage

Configuration du stockage iSCSI (Hardware et Software Initiator)

➔ iSCSI Hardware Initiator (1/4)



Détail des cartes HBA iSCSI (Hardware Initiator)



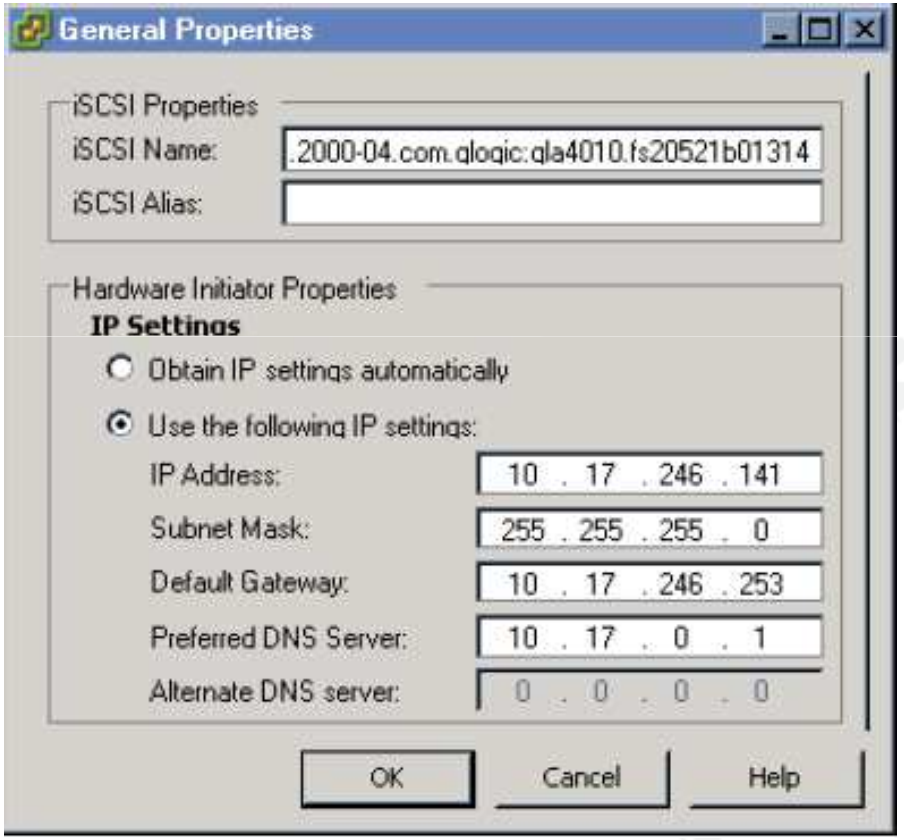
Sélectionner le périphérique iSCSI pour afficher ses propriétés

02. Le stockage

Configuration du stockage iSCSI (Hardware et Software Initiator)

➔ iSCSI Hardware Initiator (2/4)

- Configuration du iSCSI (Hardware Initiator)
  - Modification du nom par défaut et de l'alias
  - Modification des paramètres IP



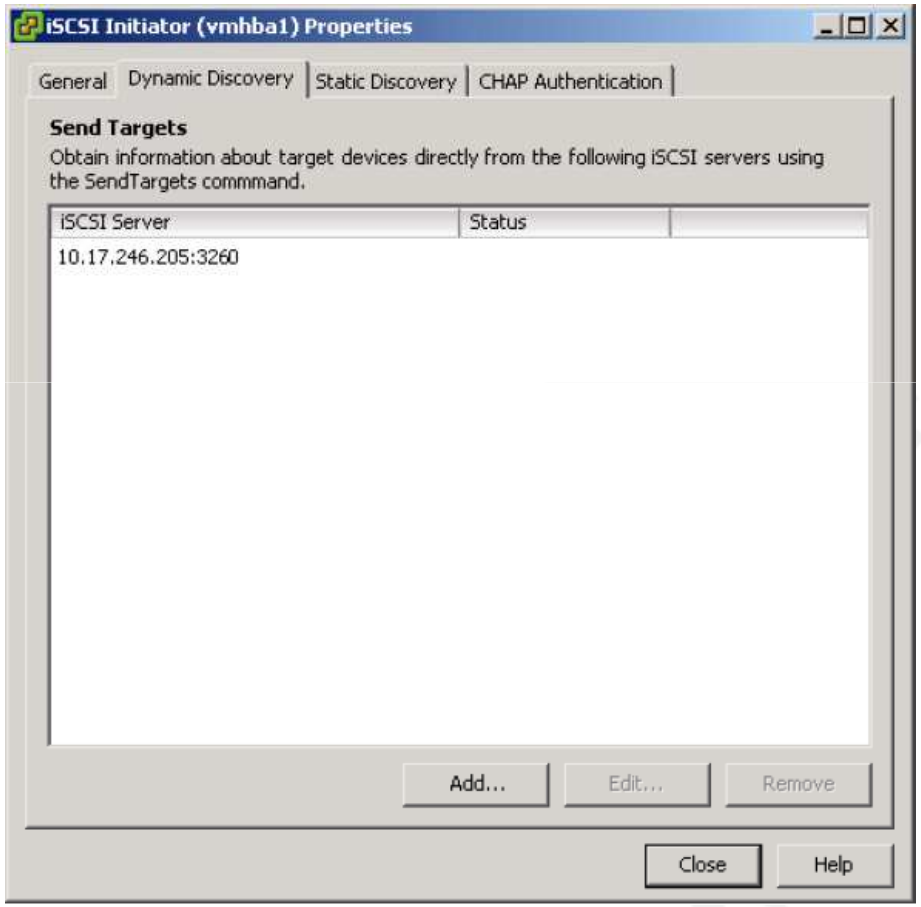
02. Le stockage

Configuration du stockage iSCSI (Hardware et Software Initiator)

➔ iSCSI Hardware Initiator (3/4)

➔ Méthode de découverte des cibles iSCSI

- **Méthode de découverte dynamique**
  - Envoi des paquets « sendtargets » a une cible iSCSI, dont l'adresse a été renseignée au préalable. La réponse est retournée a « l'initiator » avec une liste de cibles autorisées à être accédées par « l'initiator »
- **Méthode de découverte statique**
  - Après l'utilisation du « sendtargets », la liste des cibles additionnelles est affichée dans l'onglet « Static Discovery ». Cette liste peut être modifiée (rajouter / supprimer des cibles)



02. Le stockage

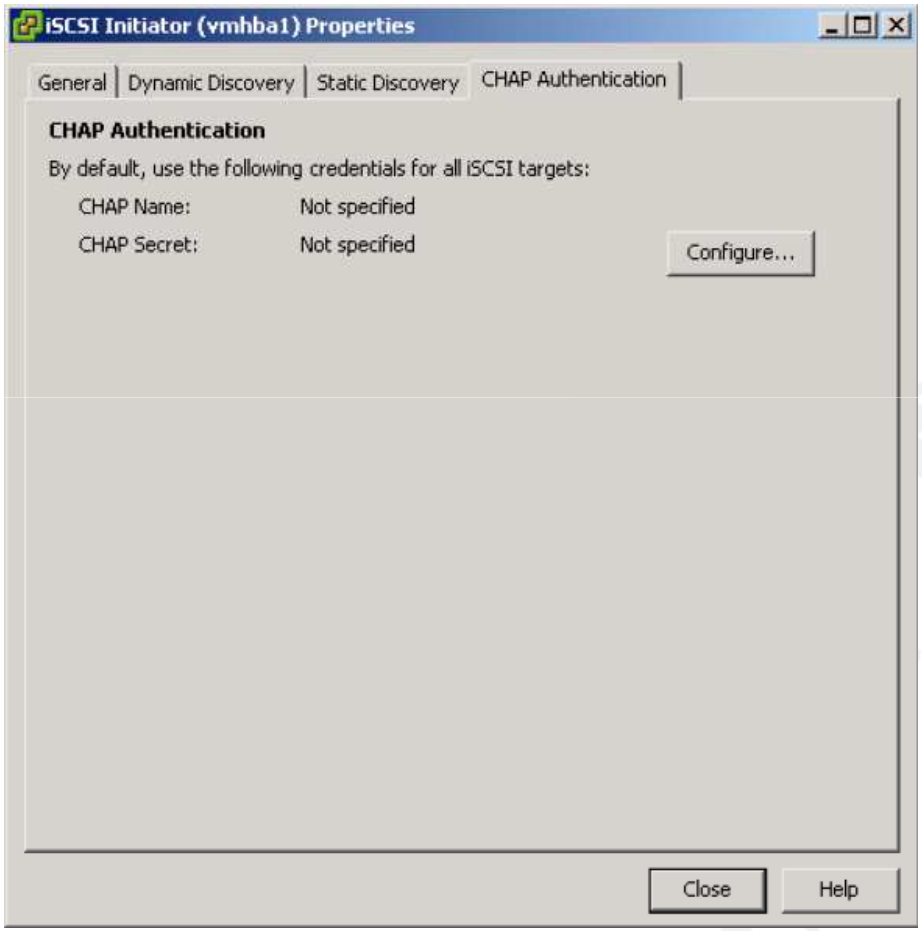
Configuration du stockage iSCSI (Hardware et Software Initiator)

➔ iSCSI Hardware Initiator (4/4)

➔ Sécurité iSCSI

- **Authentification CHAP**
  - L'envoi de données sur le réseau IP nécessite une sécurité supplémentaire, CHAP permet de vérifier la fiabilité de la cible connectée, un code secret doit être renseigné

- **Utilisation du « Fast Retransmit and Recovery »**
  - Certaines baies iSCSI supportent le FRR ; cela consiste à réduire le temps de retransmission des paquets perdus



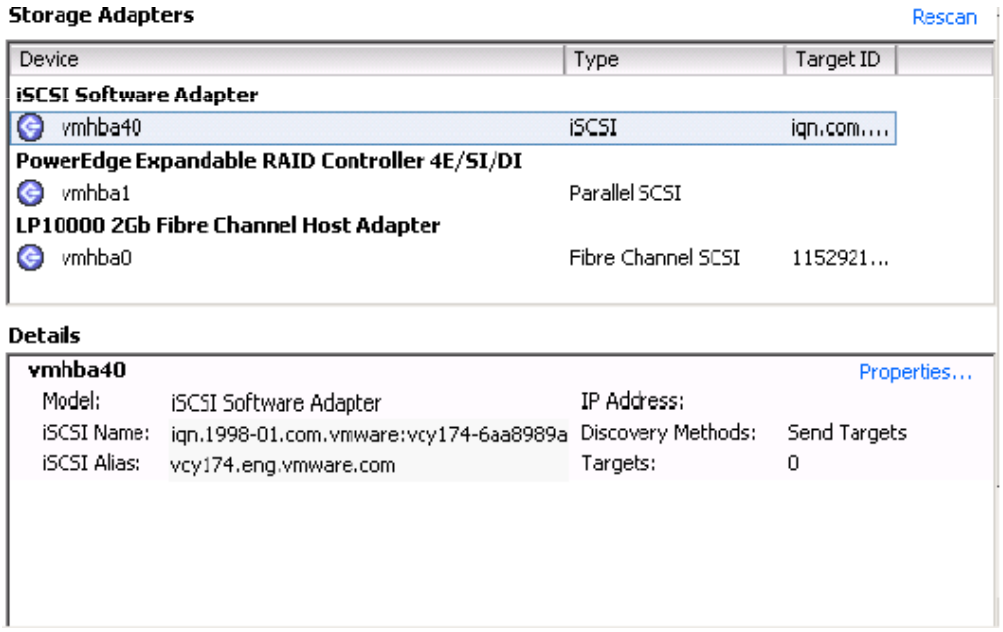
02. Le stockage

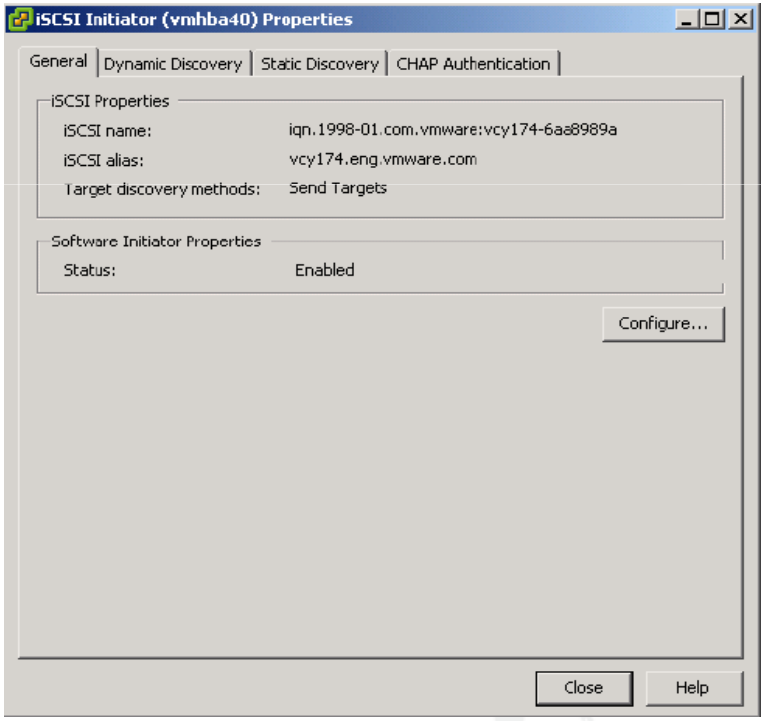
Configuration du stockage iSCSI (Hardware et Software Initiator)

iSCSI Software Initiator (1/2)

Détail des cartes HBA iSCSI (Software Initiator)

- Sélectionner le périphérique iSCSI pour afficher ses propriétés



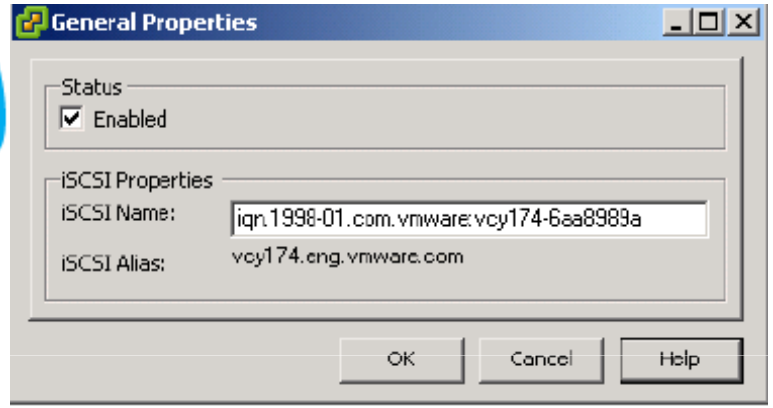


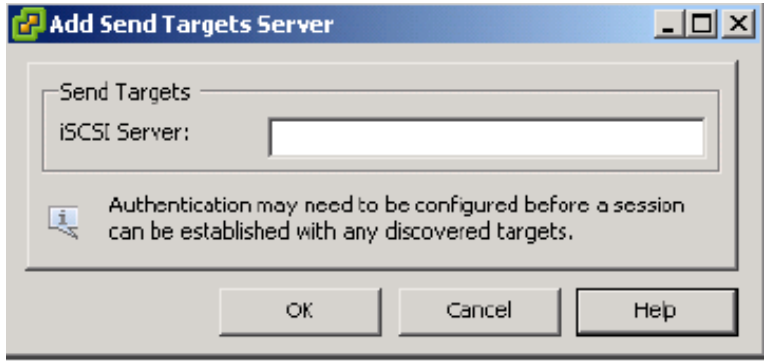
02. Le stockage

Configuration du stockage iSCSI (Hardware et Software Initiator)

➔ iSCSI Software Initiator (2/2)

- Modification du nom par défaut et de l'alias
- Utilisation du « sendtargets » pour ajouter une nouvelle cible iSCSI
- Configuration de la sécurité CHAP
- Ouvrir le port «Software iSCSI client»

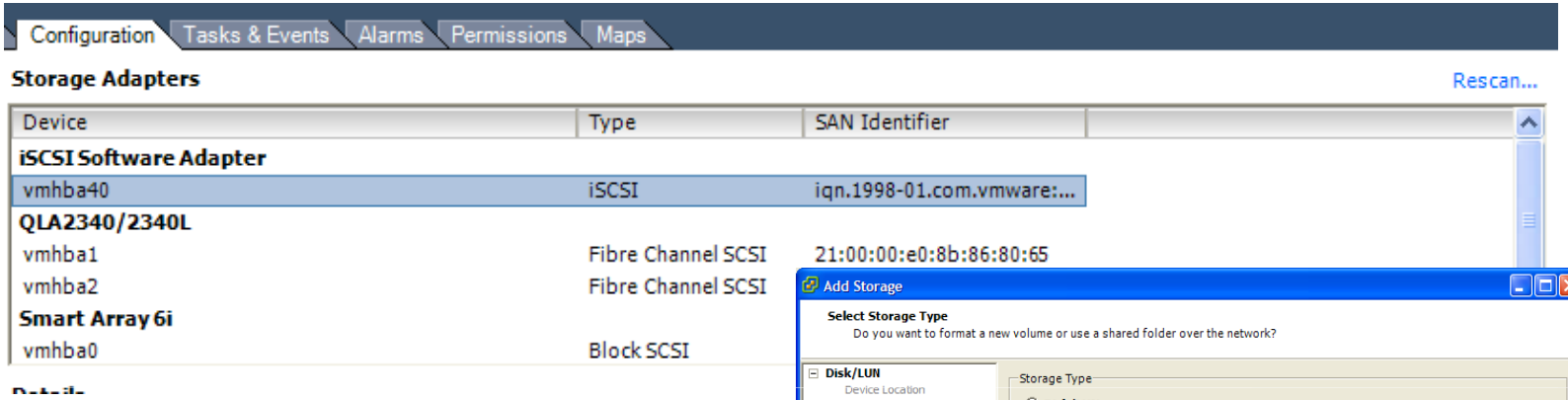


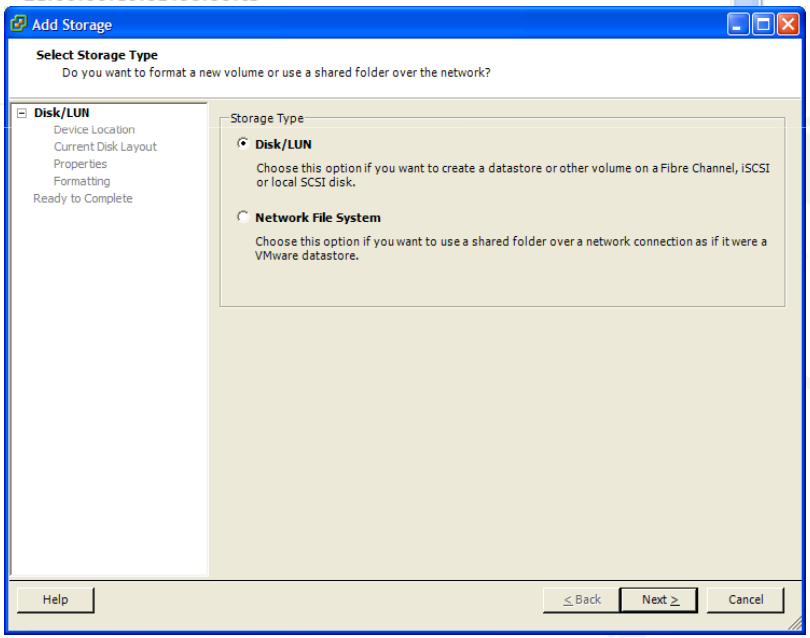


02. Le stockage

Configuration du stockage iSCSI (Hardware et Software Initiator)

➔ Rajouter un volume iSCSI (1/2)



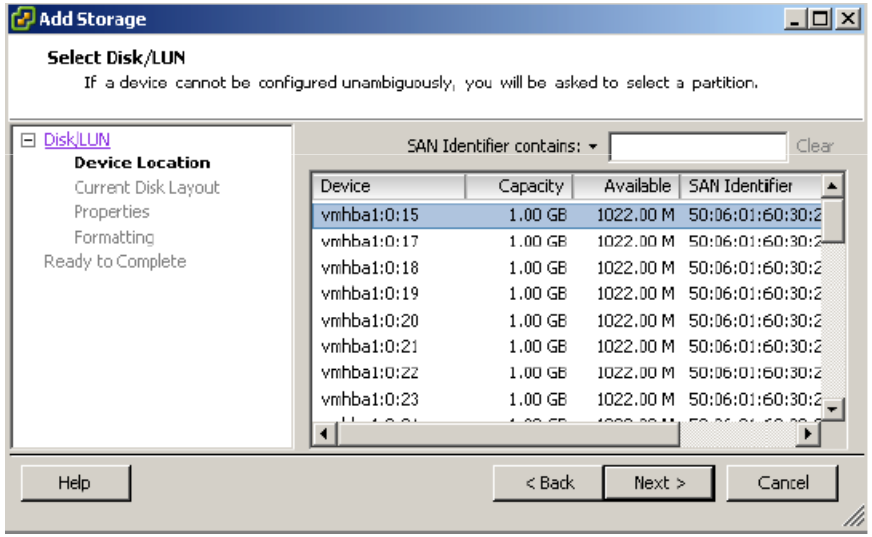


- Sous l'onglet « Configuration », page « Storage Adapters», cliquer sur « Rescan… »
- Sous l'onglet « Configuration », page « Storage », cliquer sur « Add storage »
- Sélectionner Disk/LUN

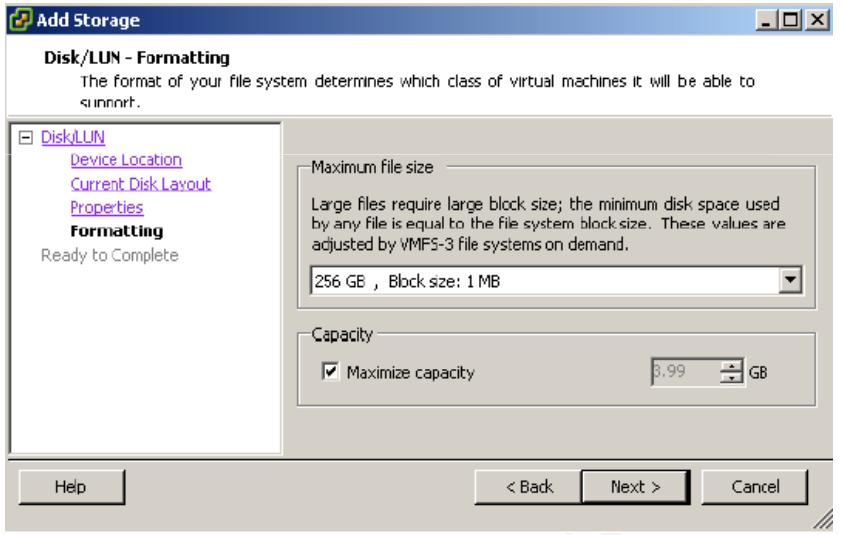
02. Le stockage

Configuration du stockage iSCSI (Hardware et Software Initiator)

➔ Rajouter un volume iSCSI (2/2)



Sélectionner la LUN à utiliser



Définir un label et formater le volume sélectionné

02. Le stockage

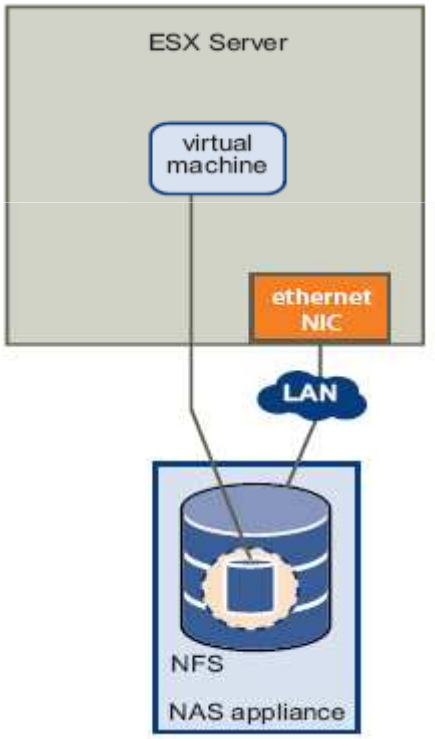
Configuration du stockage NAS (1/3)

Vue d'ensemble du NAS

- Support de VMware ESX connecté sur du NAS (Network Attached Storage) à travers le protocole NFS (Network File System). Support seulement en NFS version 3 via TCP.

- Compatibilité NAS avec VMware ESX :
  - Utilisation de VMotion
  - Création des machines virtuelles dans un volume NAS
  - Boot des machines virtuelles sur un volume NAS
  - Fonctionnalité Snapshot des machines virtuelles supportée sur un volume NAS

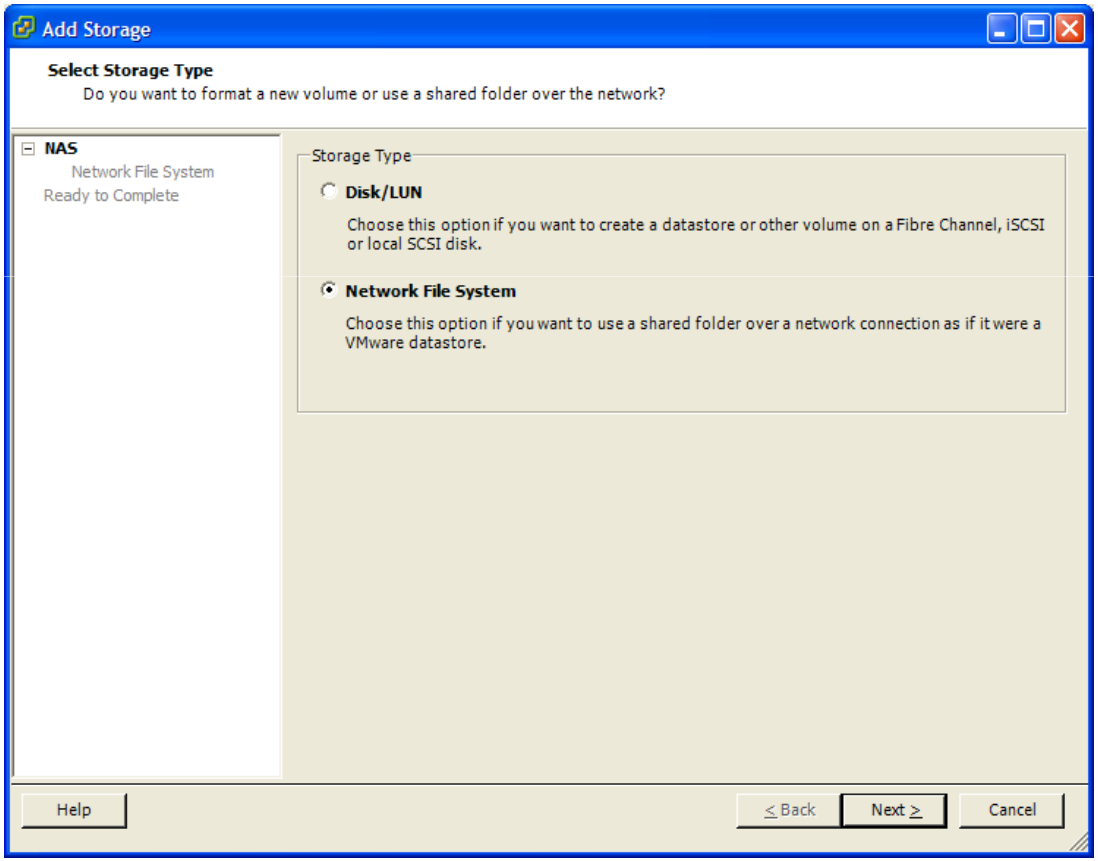
- Utilisation du VI Client :
  - Configuration des volumes NFS comme Datastore
  - Configurer le service réseau du VMkernel pour des accès à un NAS
  - Gestion des volumes NFS



02. Le stockage

Configuration du stockage NAS (2/3)

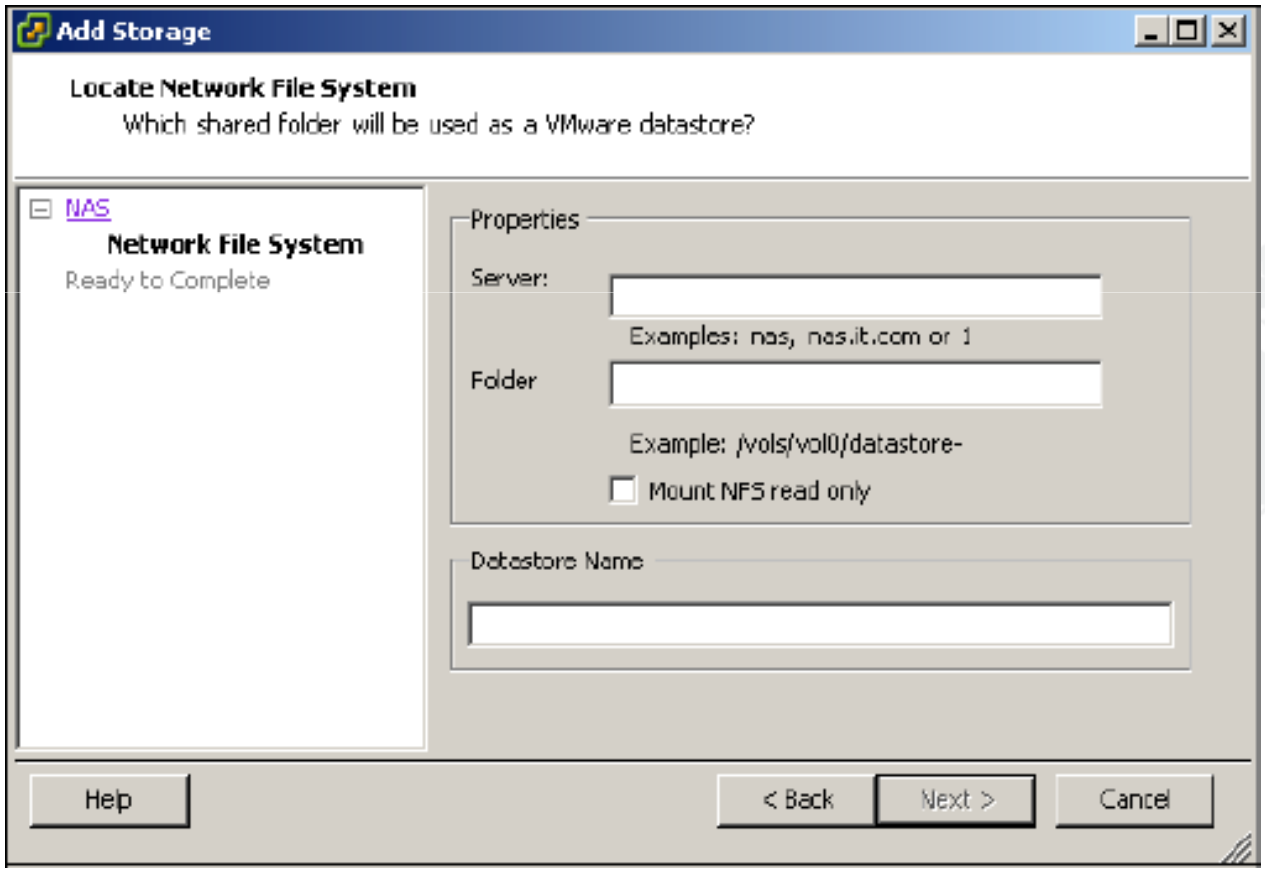
- Sous l'onglet « Configuration », page « Storage », cliquer sur « Add storage »
- Sélectionner Network File System



02. Le stockage

Configuration du stockage NAS (3/3)

- Renseigner le nom du serveur NFS
- Renseigner le répertoire partagé NFS



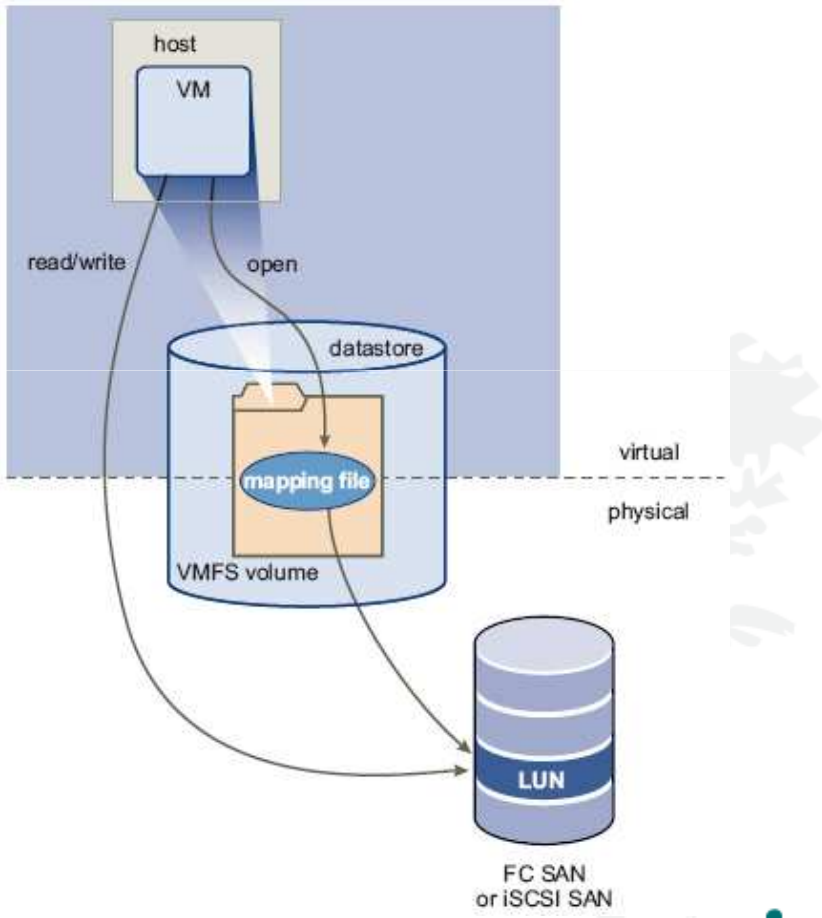
02. Le stockage

Raw Device Mapping (RDM)

➔ Vue d'ensemble du volume RDM

➔ **Le RDM utilise un fichier de mapping qui permet de contenir les informations « metadata » et de rediriger les I/Os vers le « Raw device ». Cela permet de bénéficier de tous les avantages d'une VM stockée dans un volume VMFS**

- **Utilisation des volumes RDM :**
  - Fonctionnalité SAN (Snapshots, mirroring etc.)
  - Cluster logiciel entre une machine virtuelle et un serveur physique
- **Bénéfices des volumes RDM :**
  - Utilisation du VMotion supporté
  - Gestion avec le VI Client
  - Utilisation des Snapshots des VM
  - Overhead moins important qu'avec des disques virtuels
  - N-Port ID Virtualization (NPIV)
- **Inconvénients des volumes RDM :**
  - Pas de snapshots VMware
  - Pas de partition possible dans la LUN

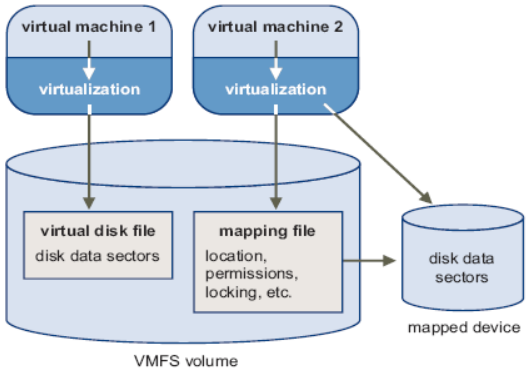


02. Le stockage

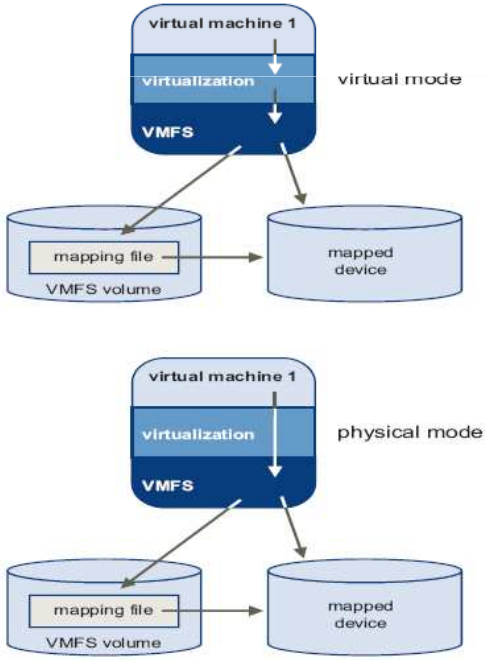
Raw Device Mapping (RDM)

➔ Caractéristiques du RDM

- Le fichier RDM est un fichier stocké dans un datastore, il permet de gérer le « Raw device » comme un fichier disque virtuel, transparent pour la machine virtuelle.



- **Deux modes pour l'utilisation du RDM :**
  - Virtual mode, les caractéristiques matérielles du volume sont cachées à la VM
  - Physical mode, toutes les commandes SCSI sont passées directement au volume sans passer par la couche de virtualisation

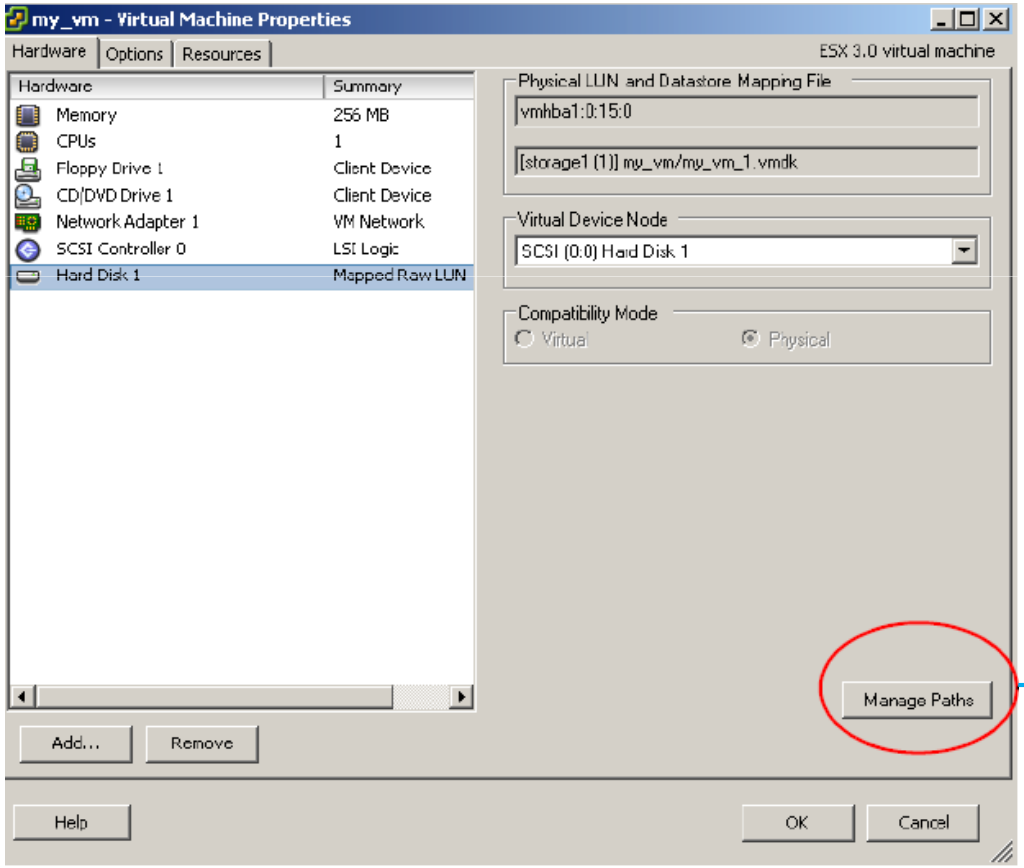


02. Le stockage

Raw Device Mapping (RDM)

Gestion des volumes RDMs

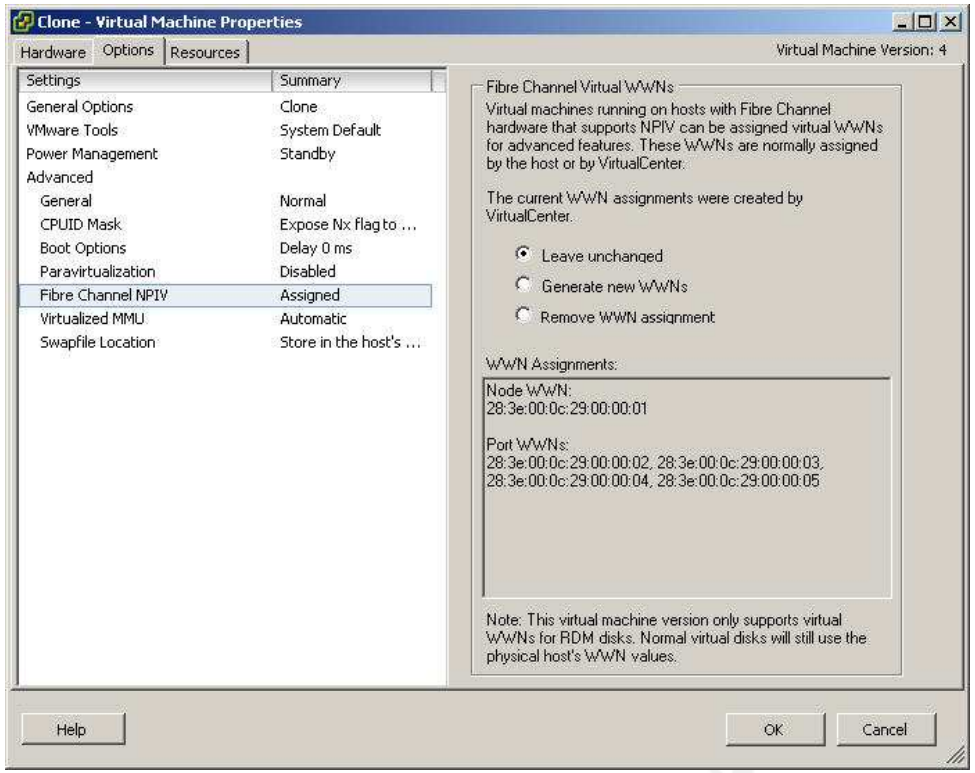
- Les volumes RDM se gèrent avec le VI Client, l'outil vmkfstools en ligne de commande, ainsi que les outils du système de fichier du service console.



Gérer les différents chemins au volume RDM, les politiques d'accès et les chemins préférés

02. Le stockage
Virtual Fibre Channel

- ESX Server 3.5 introduit le support du N-Port ID Virtualization (NPIV) pour les SAN en Fibre Channel
- Permet à chaque machine virtuelle d'avoir son propre World Wide Port Name (WWPN)
- Cette fonctionnalité permet a l'aide d'un outils tiers, la surveillance du trafic généré par une machine virtuelle et d'effectuer le zoning entre la VM et un SP
- Emulex et Qlogic supporte le NPIV avec les drivers par défaut.
- Cette fonctionnalité n'est supportée que pour les RDM uniquement.

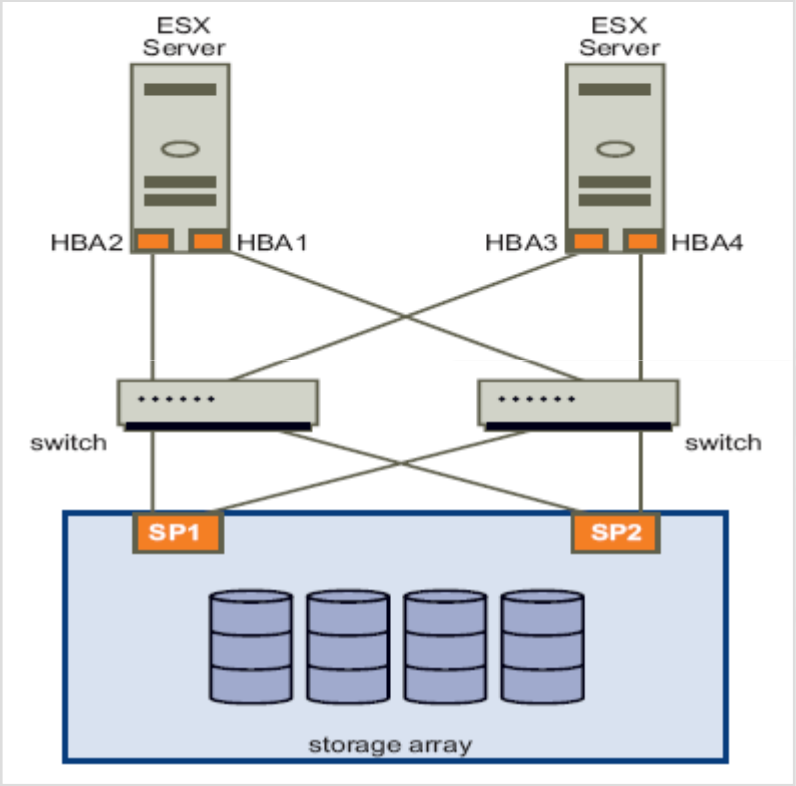


02. Le stockage

Le « Multipathing »

➔ Vue d'ensemble

- Le serveur ESX supporte le « multipathing » afin d'assurer un accès continu à des volumes partagés (SAN, iSCSI et NAS) dans le cas où une carte HBA, un switch, un SP (storage processor) ou un câble ne fonctionne plus.



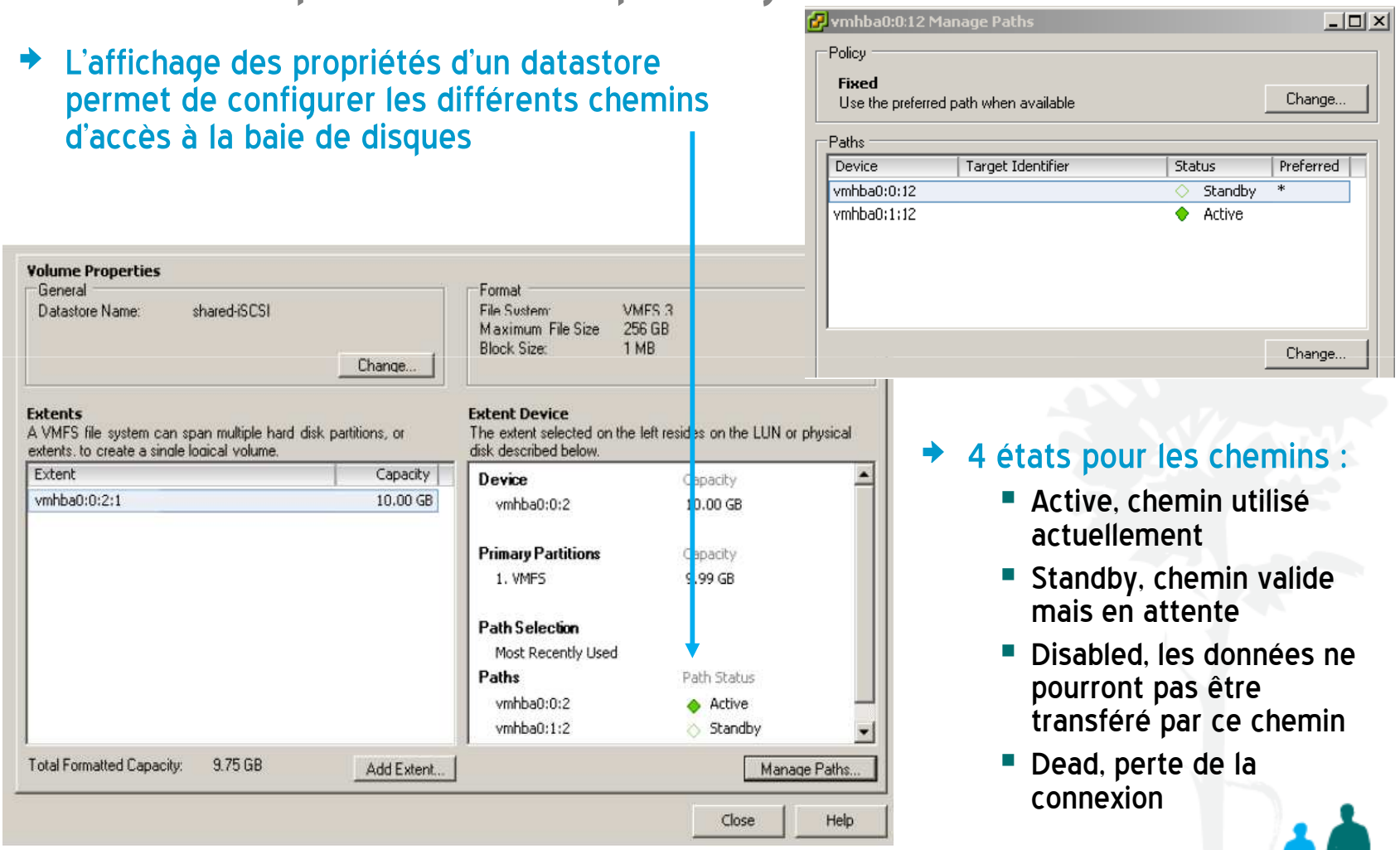
- Dans l'exemple, 2 cartes HBA par serveur, deux switchs fibre et deux ports par SP
  - 4 chemins possibles pour accéder à un volume sur la baie de disque
  - Un seul chemin est utilisé à la fois pour un volume

02. Le stockage

Le « Multipathing »

➔ Caractéristiques du « Multipathing »

➔ L'affichage des propriétés d'un datastore permet de configurer les différents chemins d'accès à la baie de disques



➔ 4 états pour les chemins :

- Active, chemin utilisé actuellement
- Standby, chemin valide mais en attente
- Disabled, les données ne pourront pas être transféré par ce chemin
- Dead, perte de la connexion

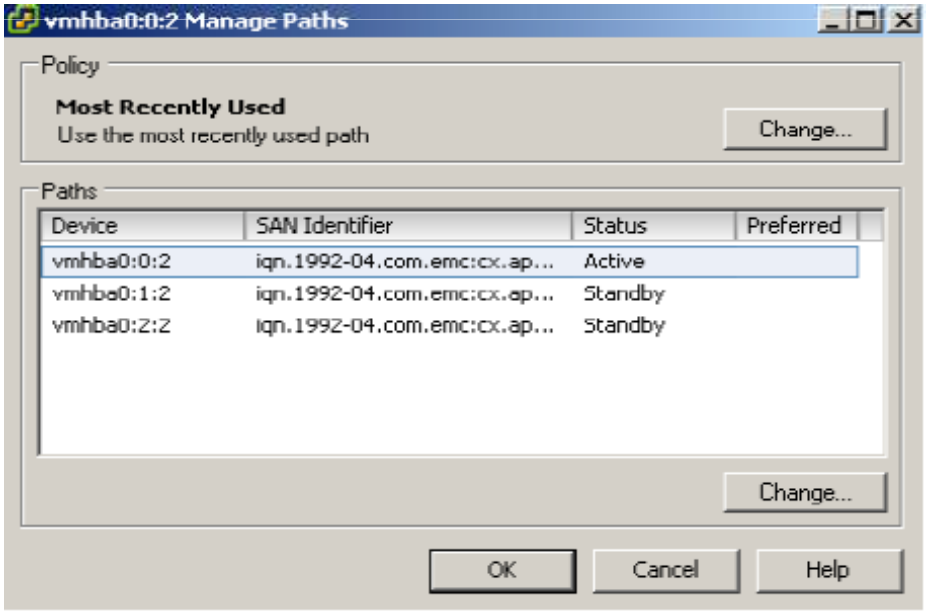
02. Le stockage

Le « Multipathing »

Gestion du « Multipathing »

Les politiques « multipathing » :

- Fixe, le serveur ESX utilise le chemin désigné comme préféré tant qu'il est fonctionnel, si le chemin passe en Dead, il utilise un chemin en Standby et reviendra sur son chemin préféré dès que celui-ci sera à nouveau disponible (Auto Fail Back). Utilisé pour des baies de disques avec des contrôleurs Actif/Actif
- MRU (Most Recently Used), le serveur ESX utilise le chemin qui fonctionne, pas d'Auto Fail Back. Utilisé pour des baies de disques avec des contrôleurs Actif/Passif



02. Le stockage
Résumé des différents stockages

Comparaison des stockages : NAS, iSCSI et Fibre Channel

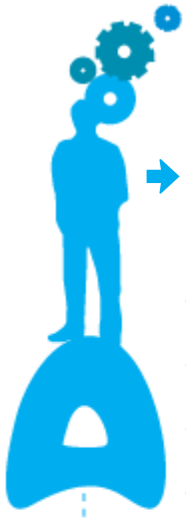
Technologie	Protocoles	Transfert	Interface	Performance
Fibre Channel	FC/SCSI	Accès par block de données / LUN	FC HBA	Haut (réseau dédié)
iSCSI	IP/SCSI	Accès par bloc de données / LUN	iSCSI HBA or NIC	Moyen (dépendant de l'état du réseau)
NAS	IP/NFS	Fichier (pas d'accès direct à la LUN)	NIC and IP switches	Moyen (dépendant de l'état du réseau)

02. Le stockage
Résumé des différents stockages

Résumé des stockages sous VMware ESX

Type	Boot VM	Boot ESX	VMotion	Datastore	RDM	VM Cluster	VMware HA & DRS	VCB
SCSI	Oui	Oui	Non	VMFS	Non	Non	Non	Oui
Fibre Channel	Oui	Oui	Oui	VMFS	Oui	Oui	Oui	Oui
iSCSI	Oui	Oui *	Oui	VMFS	Oui	Non	Oui	Oui
NAS over NFS	Oui	Non	Oui	NFS	Non	Non	Oui	Oui

* Nécessite un initiateur matériel



Notes

02. Le stockage
Questions réponses

Question

Where is LUN masking configured?

A. on the firewall
B. on the Fibre Switch
C. on the storage processor
D. on the Ethernet switch

02. Le stockage
Questions réponses

Question

Which statement is true about running an ESX Server virtual machine on a CIFS share?

A. ESX Server must be granted as a trusted member of the CIFS server.
B. ESX Server does not support datastore on CIFS
C. ESX Server requires gigabit Ethernet adapter in order for CIFS to be used as datastore.
D. ESX Server must be on the same LAN as the CIFS server.

02. Le stockage
Questions réponses

Question

Which three statements are true about sharing storage capabilites on NFS volumes supported by ESX server? Select three.

A. You can use VMotion
B. You can create VMFS datastore on NFS mounted volumes.
C. You can create virtual machines on NFS mounted volumes.
D. You can boot virtual machines stored on NFS mounted volumes.
E. You can configure ESX Server to boot from NFS mounted volumes.

02. Le stockage
Questions réponses

Question

What are two possible storage multipathing policies that you can set on an ESX Server 3 ? Select two.

A. Most Recently used (MRU)
B. Open Shortest Path First (OSPF)
C. Persistent Binding
D. Fixed
E. Dynamic Load Balancing

02. Le stockage
Questions réponses

Question

Which security technology does VMware iSCSI use?

A. CHAP
B. AES
C. RIP
D. IPSec
E. PAP
F. MSCHAPv2

03. Gestion de la sécurité et des permissions

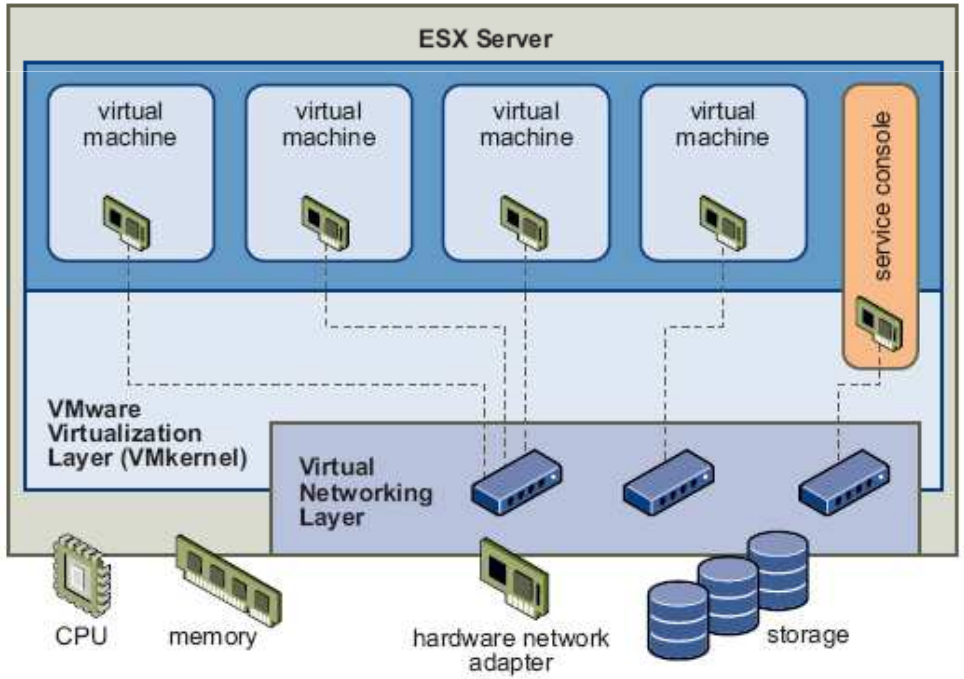
- Vue d'ensemble de le sécurité de l'architecture ESX
- Configuration de la sécurité sur l'architecture ESX
- Authentification et gestion des utilisateurs
- Gestion des permissions

03. Gestion de la sécurité et des permissions

Vue d'ensemble de la sécurité de l'architecture ESX

La sécurité et la couche de virtualisation

- La couche de virtualisation ou VMkernel a été créée par VMware pour faire fonctionner les machines virtuelles. Il contrôle le matériel utilisé par le serveur ESX et distribue les ressources matérielles aux machines virtuelles.
- L'interface du VMkernel a été strictement limitée aux APIs gérant les machines virtuelles.



- **Lockdown Mode**
  - Désactive l'accès distant à l'ESX si celui-ci est managé par un serveur VirtualCenter

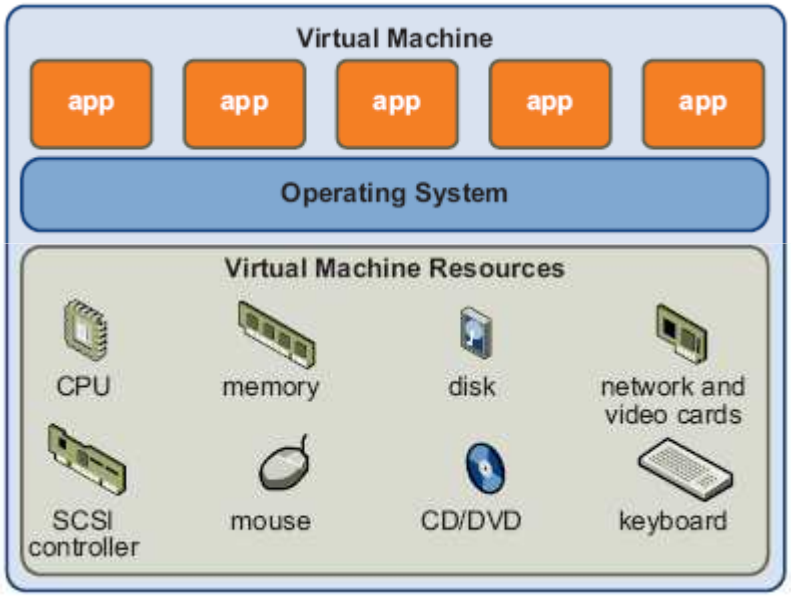
03. Gestion de la sécurité et des permissions

Vue d'ensemble de la sécurité de l'architecture ESX

La sécurité et les machines virtuelles

Les machines virtuelles sont isolées les unes des autres, si un système d'exploitation crash à l'intérieur d'une VM cela n'impacte pas les autres VM.

- Une machine virtuelle ne peut pas accéder à la mémoire d'une autre machine virtuelle
- L'isolation réseau est gérée par le VMkernel à travers les vSwitchs
- L'isolation au niveau de la performance du serveur ESX se fera à travers les limitations et les priorités des ressources par VM



03. Gestion de la sécurité et des permissions

Vue d'ensemble de la sécurité de l'architecture ESX

La sécurité et le service console (1/2)

- Le service console est l'interface de management du serveur ESX, c'est un système d'exploitation basé sur une distribution limitée de l'OS RedHat Enterprise Linux 3 update 6
  - Sécurité maximum par défaut (ports minimums ouverst nécessaire à la gestion de l'ESX)
  - Communication cryptée en SSL 256-bit AES
  - Les services réseaux (FTP, Telnet etc.) ne sont pas activés par défaut

- Recommandation :
  - Limiter l'accès des utilisateurs
  - L'accès root ne doit être utilisé qu'en dernier recours
  - Utiliser le VI Client pour administrer le serveur ESX
  - Utiliser seulement des sources VMware pour installer ou mettre à jour des composants dans le service console
  - Vérifier le niveau de sécurité (esxcfg –firewall –q incoming & outgoing)

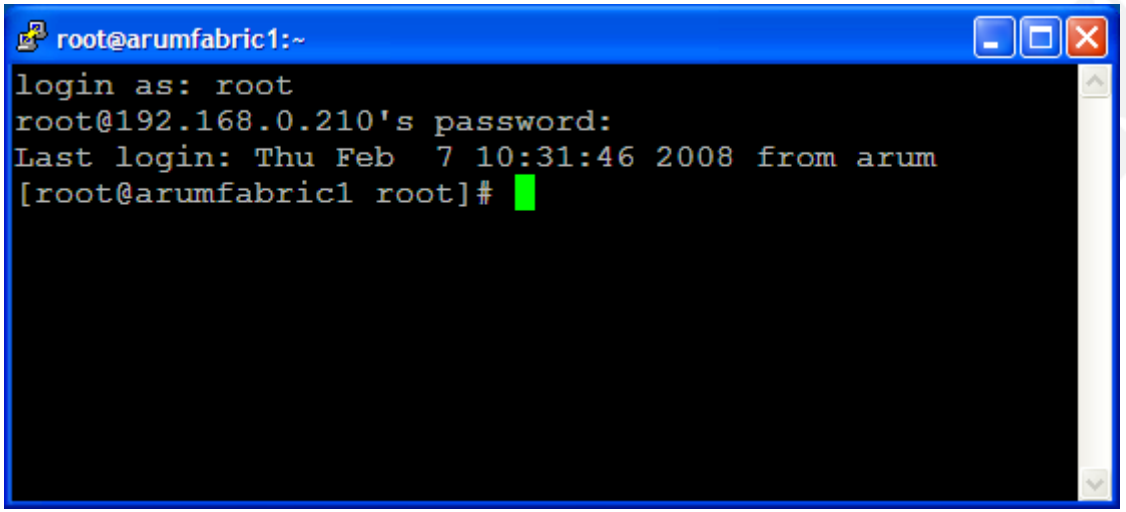
03. Gestion de la sécurité et des permissions

Vue d'ensemble de la sécurité de l'architecture ESX

La sécurité et le service console (2/2)

Autoriser le compte root à se connecter en ssh

- Ouvrir une session console sur l'ESX
- Editer le fichier /etc/ssh/sshd_config
- Changer la ligne *PermitRootLogin* no par *PermitRootLogin yes*
- Sauvegarder le fichier
- Relancer le service serveur ssh en tapant : *service sshd restart*



03. Gestion de la sécurité et des permissions

Configuration de la sécurité sur l'architecture ESX

Sécuriser le réseau avec des Firewalls (1/3)

- Les Firewalls permettent de cloisonner la communication entre des périphériques réseaux, seul l'administrateur peut autoriser l'accès à certains périphériques en ouvrant des ports.

- Le Firewall peut être utilisé :
  - Entre les serveurs physiques, VirtualCenter server et les serveurs ESX
  - Entre les machines virtuelles, constitution de DMZ
  - Entre un serveur physique et une VM

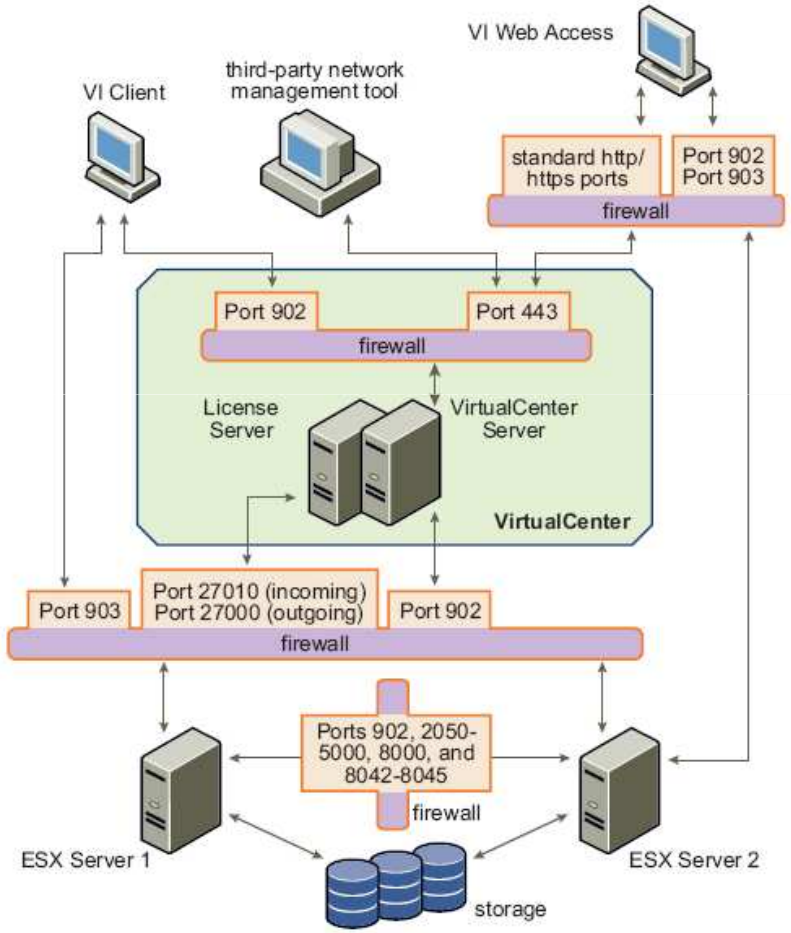
- En fonction de la configuration de l'infrastructure virtuelle (Serveur de licence, serveur VirtualCenter, VI Client, serveur de supervision etc.) les Firewalls seront placés différemment.

03. Gestion de la sécurité et des permissions

Configuration de la sécurité sur l'architecture ESX

Sécuriser le réseau avec des Firewalls (2/3)

- **Configuration des Firewalls avec le serveur VirtualCenter**
  - Configurer vos Firewalls depuis VirtualCenter de façon à bloquer les ports inutiles à la gestion de votre infrastructure virtuelle

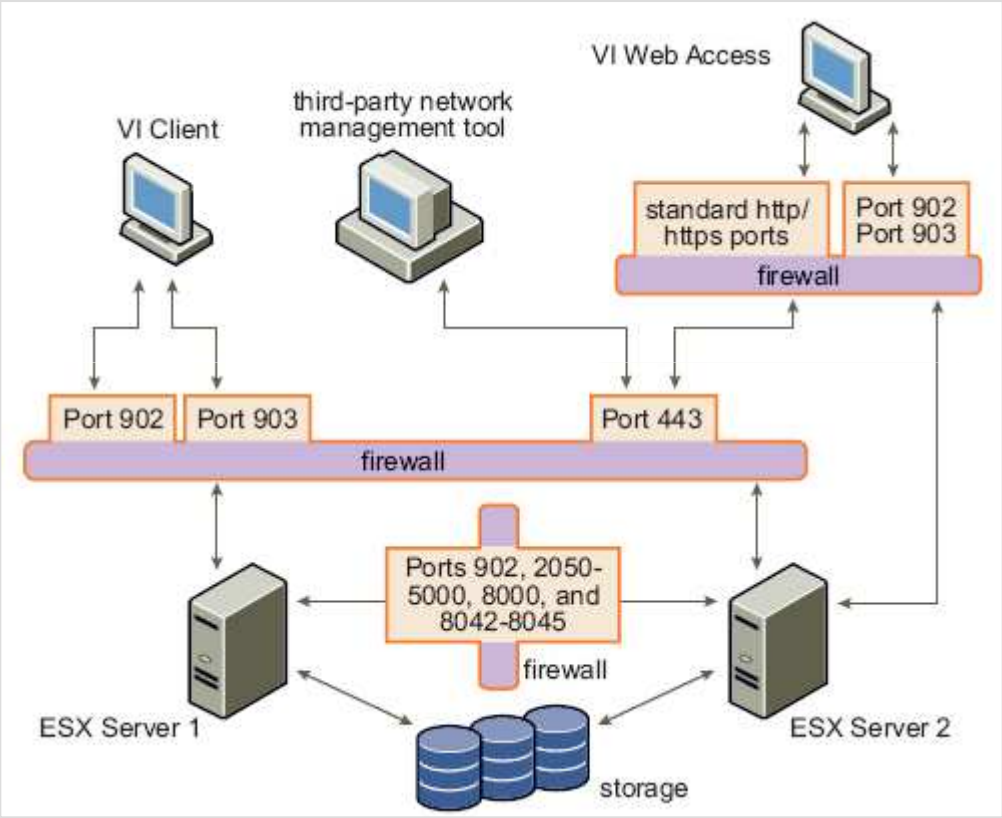


03. Gestion de la sécurité et des permissions

Configuration de la sécurité sur l'architecture ESX

Sécuriser le réseau avec des Firewalls (3/3)

- **Configuration des Firewalls sans le serveur VirtualCenter**
  - Configurer vos Firewalls sur chaque ESX de façon à bloquer les ports inutiles pour la gestion de votre infrastructure virtuelle



03. Gestion de la sécurité et des permissions

Configuration de la sécurité sur l'architecture ESX

➔ Liste des ports pour la gestion de votre infrastructure

Port	Type de traffic	Description
80	Incoming TCP	HTTP Port TCP web, utilisé avec le port 443 (https)
443	Incoming TCP	HTTPS Port Web SSL, utilisé par le VI Web Access
902	Incoming TCP, outgoing UDP	Port d'authentification du trafic pour management des serveurs ESX et des VM, utilisé par le serveur VC, le VI Client et par des serveurs ESX
903	Incoming TCP	TTrafic généré par la remote console
2049	Incoming and outgoing TCP	Utilisé par le VMkernel pour le stockage NFS
2050-5000	Outgoing TCP, incoming and outgoing UDP	Trafic entre des serveurs ESX pour VMware HA et EMC AutoStart Manager
3260	Outgoing TCP	Utilisé par le VMkernel et le service console pour le stockage iSCSI
8000	Incoming and outgoing TCP	Utilisé par le VMkernel pour les requêtes VMotion
8042-8045	Outgoing TCP, incoming and outgoing UDP	Trafic entre des serveurs ESX pour VMwareHA et EMC AutoStart Manager
27000, 27010	27000: outgoing TCP, 27010: incoming TCP	Requête entre le serveur de licence et les serveurs ESX
5988	Incoming and outgoing TCP	CIM XML transactions over HTTPS
5989	Incoming and outgoing TCP	CIM XML transactions over HTTP

03. Gestion de la sécurité et des permissions

Configuration de la sécurité sur l'architecture ESX

Sécuriser les machines virtuelles avec des VLANs (1/2)

- Entre les VM, c'est à travers le réseau que les attaques virales ou autres sont possibles.

- Il est primordial d'ajouter une sécurité au niveau réseau en appliquant ces quelques règles :
  - Ajouter des Firewalls sur votre réseau
  - Ajouter des segmentations réseaux (évite les attaques de type « spoofing »)
  - Ajouter des VLANs, VMware ESX utilise le standard IEEE 802.1q

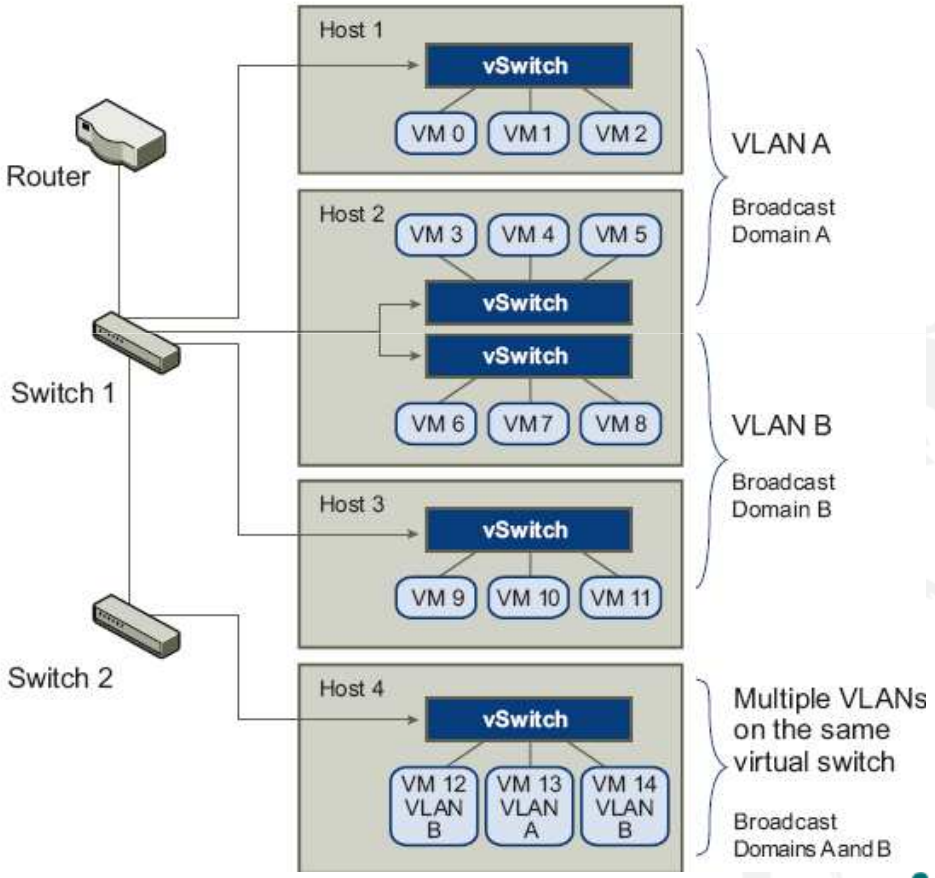
03. Gestion de la sécurité et des permissions

Configuration de la sécurité sur l'architecture ESX

➔ Sécuriser les machines virtuelles avec des VLANs (2/2)

➔ Exemple d'utilisation de VLANs entre les machines virtuelles

- Le routeur transfère les paquets « taggués » d'un VLAN à un autre, la séparation des flux réseaux évite ainsi les infections virales et autres attaques



03. Gestion de la sécurité et des permissions

Configuration de la sécurité sur l'architecture ESX

Sécuriser le stockage iSCSI (1/2)

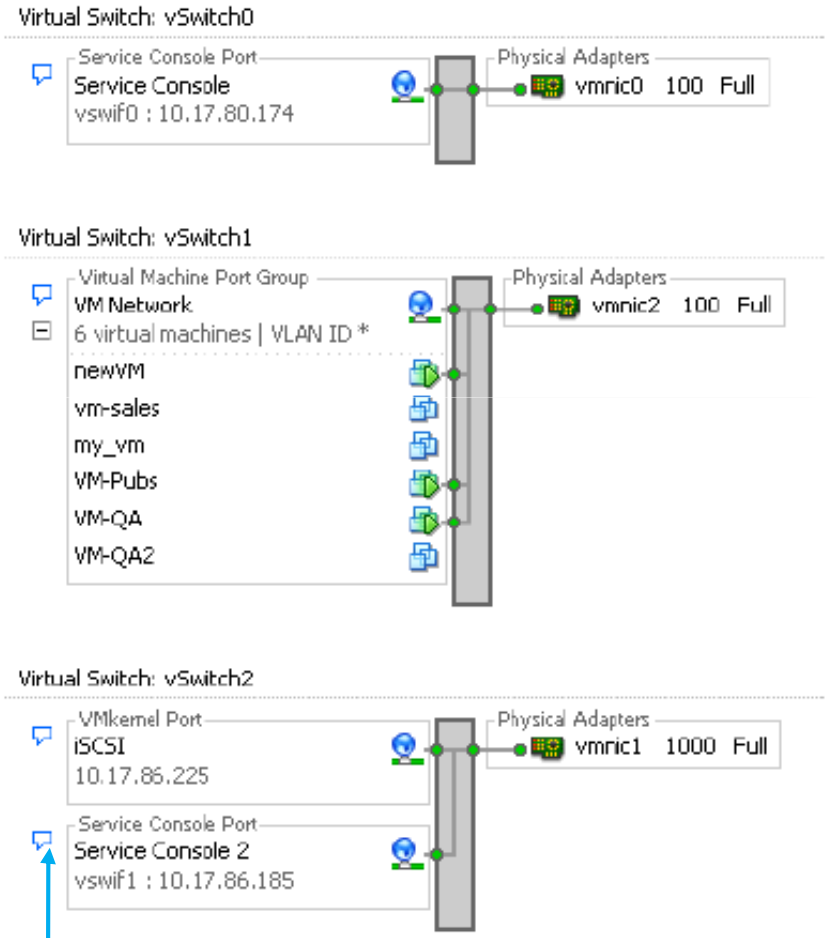
- Le serveur ESX utilise le iSCSI afin d'accéder à un stockage SAN iSCSI. Toutes les commandes SCSI sont encapsulées avec le protocole TCP/IP.
- La sécurité est primordiale, elle commence par l'authentification et la séparation des flux réseaux :
  - S'assurer que la cible iSCSI possède l'autorisation de se connecter au serveur ESX ou « Initiator »
  - Utilisation de l'authentification CHAP
  - Si l'authentification est désactivée, créer un réseau dédié à la communication entre l'Initiator et la cible iSCSI ou un VLAN
  - Créer un vSwitch séparé pour le service réseau du VMkernel ISCSI, ainsi que la communication du service console pour le iSCSI
  - L'authentification est unidirectionnelle : C'est la cible qui authentifie l'initiateur.

03. Gestion de la sécurité et des permissions

Configuration de la sécurité sur l'architecture ESX

Sécuriser le stockage iSCSI (2/2)

- Exemple d'une configuration d'un stockage ISCSI avec des vSwitch séparé (Software Initiator)



- Rappel :
  - Le iSCSI nécessite une communication également avec le service console

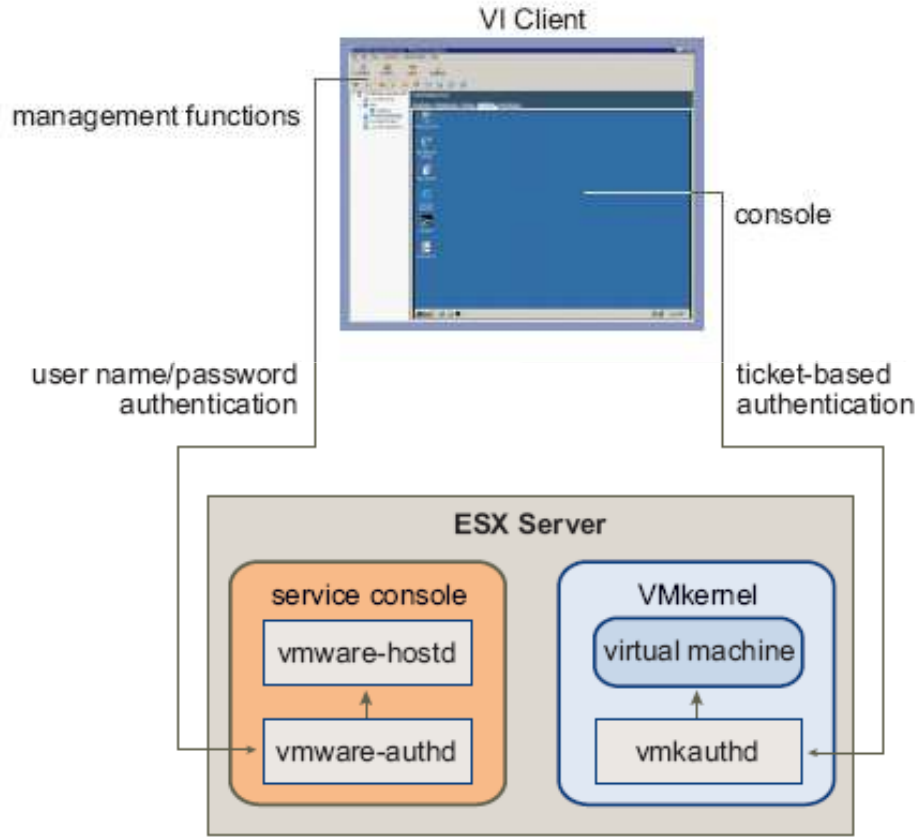
- Configuration pour l'utilisation du ISCSI Software
  - Un service réseau pour le VMkernel
  - Un service réseau pour le service console

03. Gestion de la sécurité et des permissions

L'authentification et la gestion des utilisateurs

Authentification sur le serveur ESX (1/2)

- Le serveur ESX utilise la structure PAM (Pluggable Authentication Modules) quand les utilisateurs accèdent au serveur avec le VI Client, en Web Access ou par le Service Console. Plusieurs process d'authentification permettent d'autoriser où non un utilisateur ou un groupe.



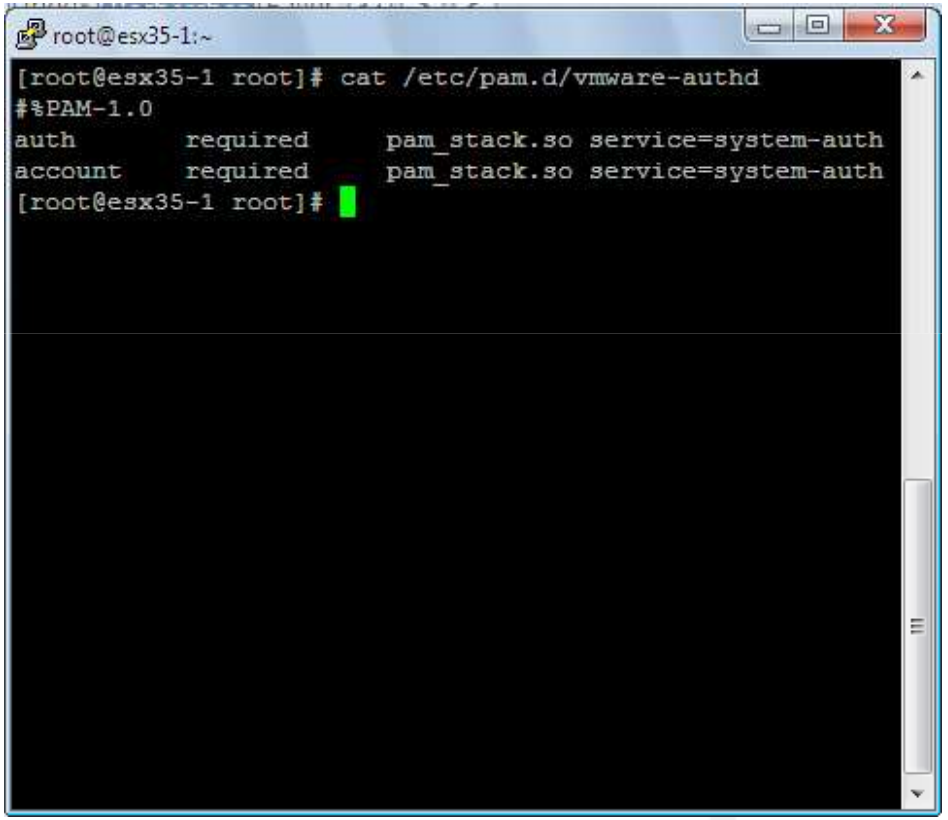
- Utilisateur VirtualCenter, utilisateur ou groupe d'un domaine Windows autorisé à se connecter au datacenter
- Utilisateur en accès direct, utilisateur ou groupe se connectant directement au serveur ESX
- Deux utilisateurs par défaut sur le serveur ESX :
  - root
  - vpxuser (avec un VirtualCenter)

03. Gestion de la sécurité et des permissions

L'authentification et la gestion des utilisateurs

➔ Authentification sur le serveur ESX (2/2)

- Par défaut, ESX Server 3 utilise le fichier */etc/passwd* pour authentifier les utilisateurs
- Le fichier */etc/pam.d/vmware-authd* contient les chemins vers les modules d'authentification actifs
- Les modules PAM (fichiers .so) disponibles sont dans le dossier /lib/security
- A chaque connexion sur le serveur ESX, le processus *vmware-hostd* transfert le nom d'utilisateur et le mot de passe aux modules PAM

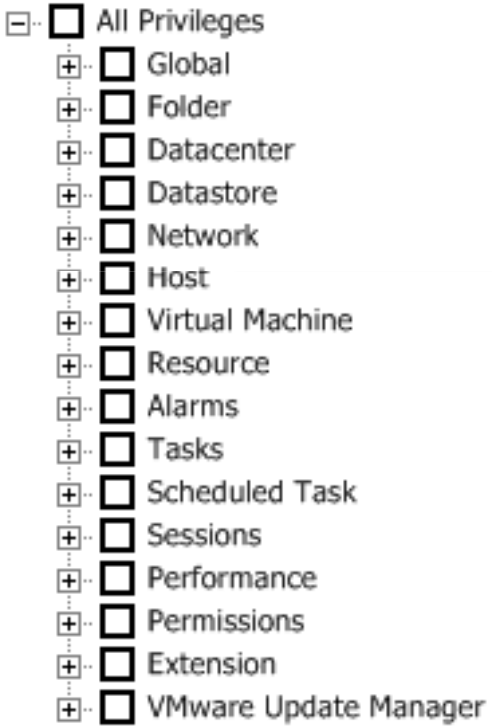


03. Gestion de la sécurité et des permissions

L'authentification et la gestion des utilisateurs

Les rôles et les privilèges

- Les rôles permettent d'autoriser des accès à des objets du datacenter.
  Un rôle est un ensemble de privilèges
  - No Access
  - Read-Only
  - Administrator
  - Virtual Machine User
  - Virtual Machine Power User
  - Resource Pool Administrator
  - Datacenter Administrator
  - Virtual Machine Administrator
  - VMware Consolidated Backup User
- Les rôles créés sous VirtualCenter sont différents des rôles créés sous le serveur ESX

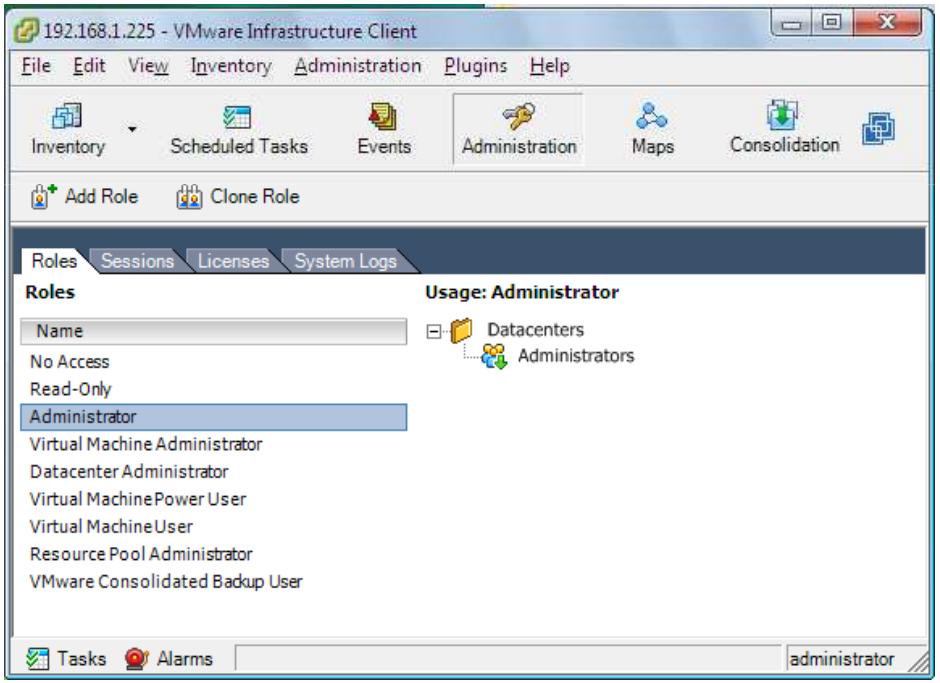


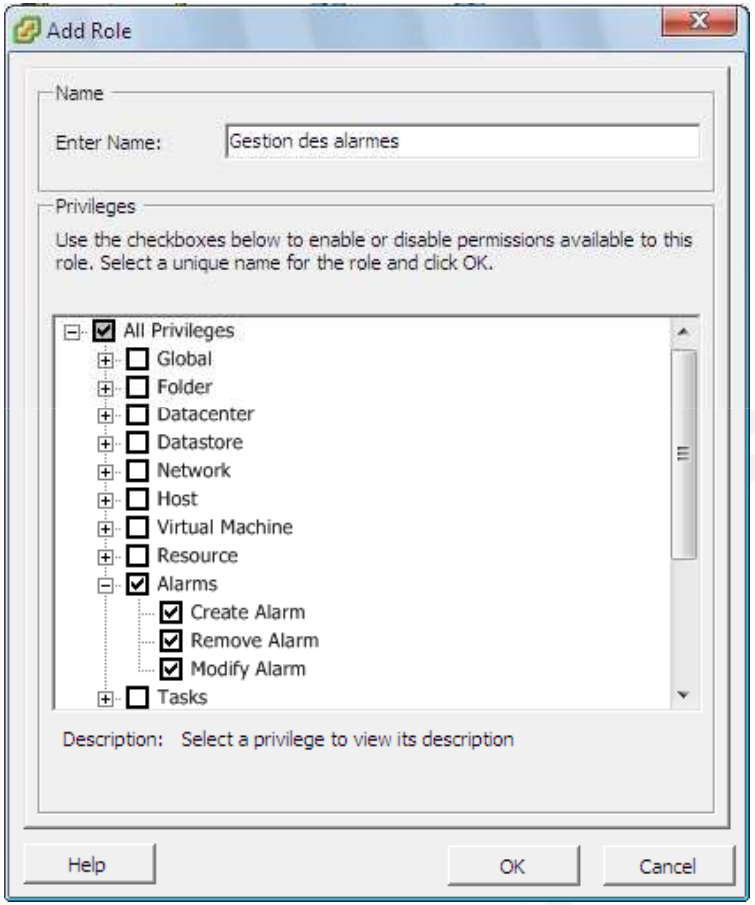
03. Gestion de la sécurité et des permissions

L'authentification et la gestion des utilisateurs

Gestion des rôles

Création des rôles



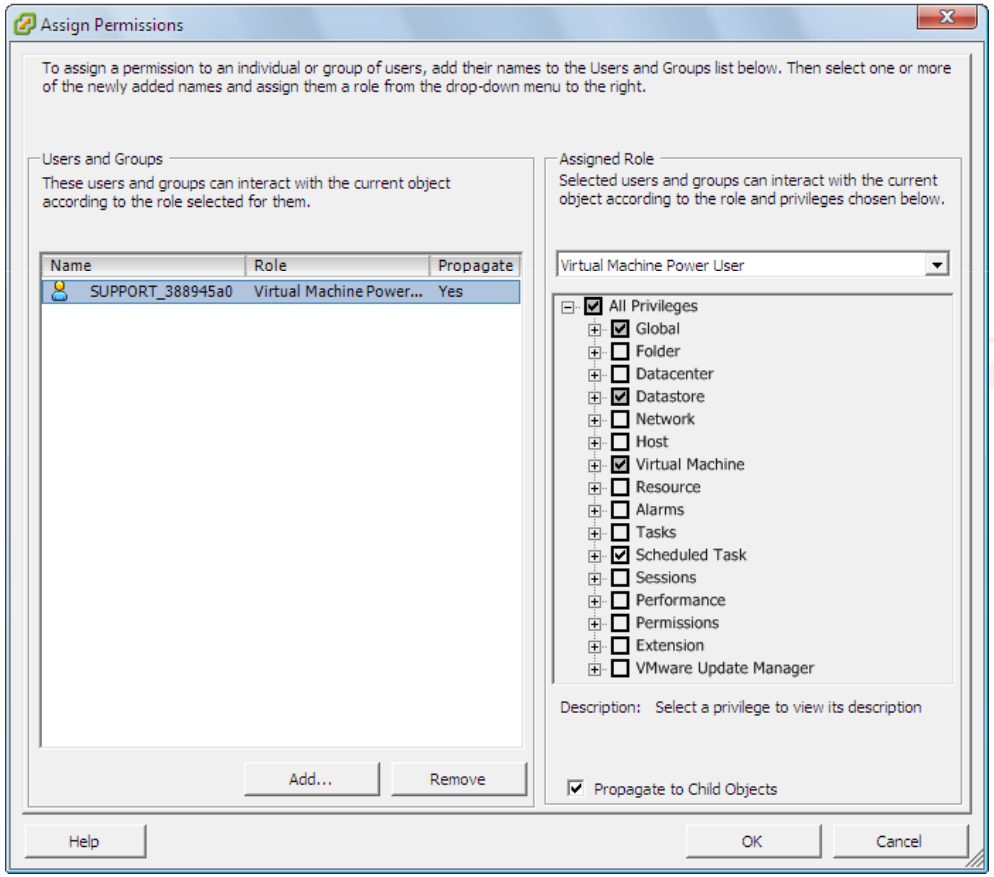


03. Gestion de la sécurité et des permissions

L'authentification et la gestion des utilisateurs

Assignation des rôles

- Sélection de l'utilisateur et assignation du rôle sur un objet du datacenter



04. Protection et disponibilité des données

- Vue d'ensemble
- Les différents types de cluster
- VMware HA
- Snapshots
- Sauvegarde et restauration
- Storage VMotion

04. Protection et disponibilité des données
Vue d'ensemble

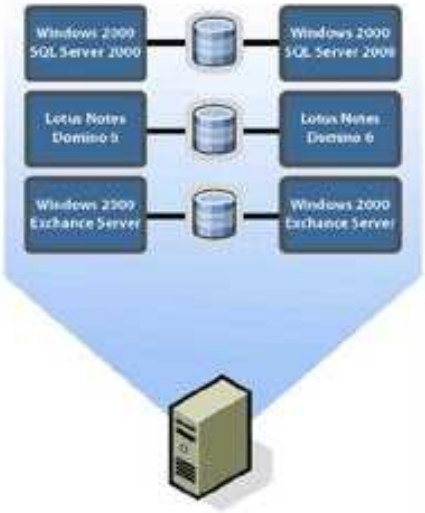
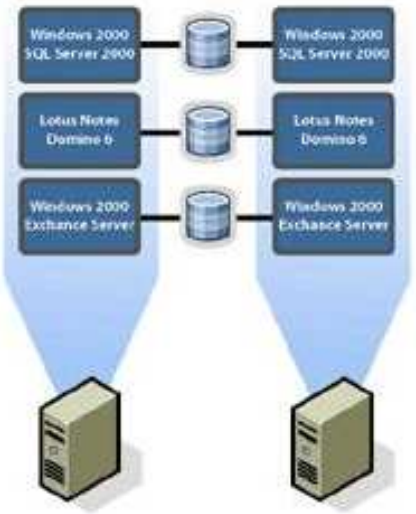
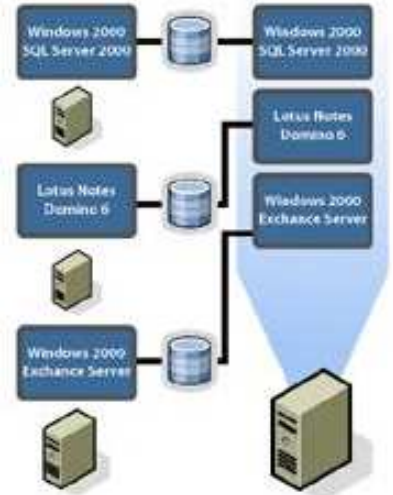
➔ La continuité de service des applications de l'entreprise nécessite la mise en place d'une solution pour protéger les données mais aussi une solution de reprise d'activité.

- **L'infrastructure virtuelle permet de :**
  - Consolider, augmenter le rendement de vos serveurs
  - Améliorer considérablement l'administration
  - Supprimer les coupures de services applicatives lors d'une maintenance
  - Optimiser le niveau de service en effectuant un « load balancing » des ressources
  - Protéger les données grâce à des sauvegardes et des restaurations simplifiées
  - Posséder de la haute disponibilité pour vos applications sans surplus de matériel et coût

04. Protection et disponibilité des données

Les différents types de cluster sous VMware ESX (1/2)

➔ Haut niveau de la disponibilité des applications, intégration du Cluster Logiciel (MSCS, Veritas etc.)

Cluster in a box	Cluster across boxes	Physical to virtual clustering
▪ Plusieurs VM au sein du même ESX Server	▪ Chaque VM possède son jumeau dans un autre ESX Server ▪ Le disque est partagé via SAN FC	
		

04. Protection et disponibilité des données

Les différents types de cluster sous VMware ESX (2/2)

Implémentation des clusters MSCS

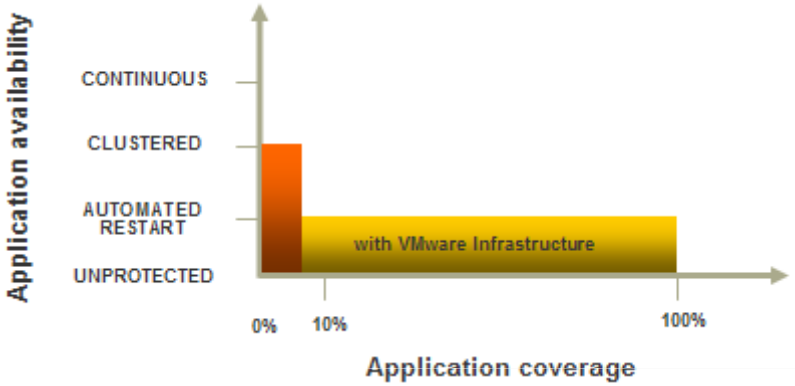
Cluster in a box	Cluster across boxes	Physical to virtual clustering
▪ Disque de démarrage des VM sur une partition VMFS locale ▪ Disques partagés sur une partition locale ou une partition SAN ▪ Controleur virtuel dédié pour les disques partagés, en mode Bus Sharing virtuel ▪ Deux cartes réseaux virtuels ▪ Pas de NIC Teaming ▪ Pas de VMotion, HA ou DRS	▪ Disque de démarrage des VM sur une partition VMFS locale ▪ Disques partagés en attachement RDM virtuel ou physique sur du SAN fibre ▪ Controleur virtuel dédié pour les disques partagés, en mode Bus Sharing physique ▪ Deux cartes réseaux virtuels ▪ Pas de NIC Teaming ▪ Pas de VMotion, HA ou DRS	▪ Disque de démarrage des VM sur une partition VMFS locale ▪ Disques partagés en attachement RDM physique sur du SAN fibre ▪ Controleur virtuel dédié pour les disques partagés, en mode Bus Sharing physique ▪ Deux cartes réseaux virtuelles ▪ Pas de NIC Teaming ▪ Pas de VMotion, HA ou DRS

04. Protection et disponibilité des données

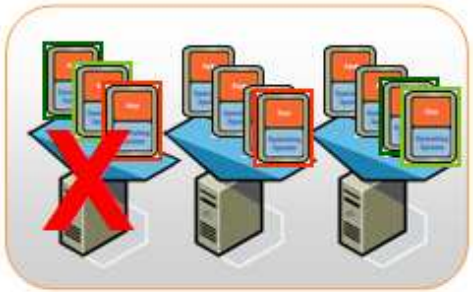
VMware HA (High Availability) (1/3)

- VMware HA consiste à redémarrer une machine virtuelle sur un autre serveur ESX dans le cas où le premier serveur deviendrait indisponible.

- VirtualCenter intègre la fonctionnalité HA dans un cluster constitué au minimum de deux serveurs ESX.

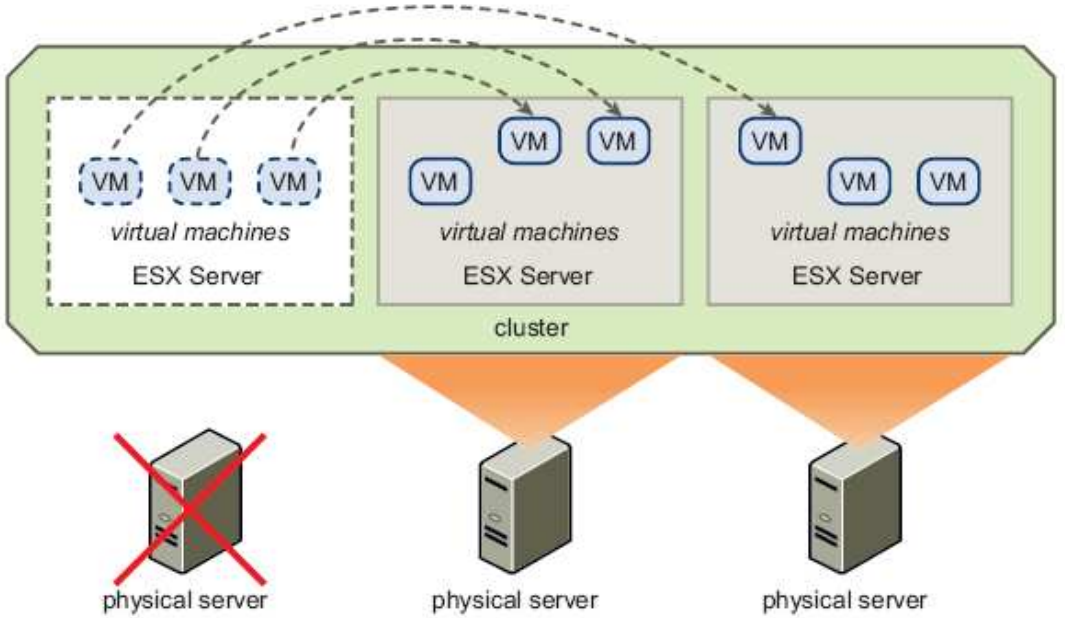


- Avantages :
  - Configuration minimum
  - Cluster à moindre coût
  - Compatibilité de nombreuses applications



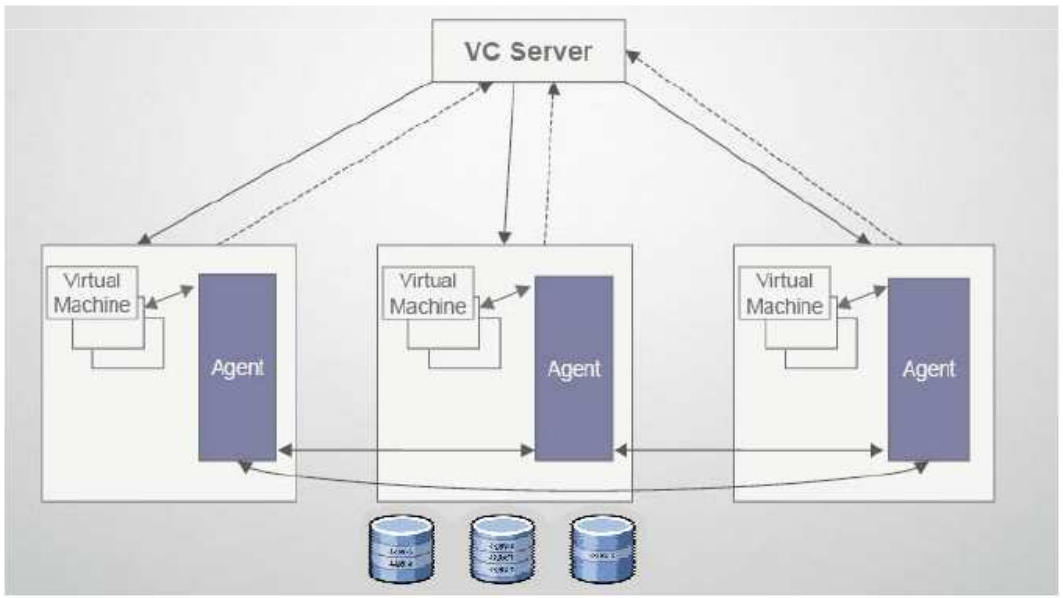
04. Protection et disponibilité des données
VMware HA (High Availability) (2/3)

- Utilisation du VI Client pour gérer HA
- Failover automatique des machines virtuelles si les ressources dans le cluster le permettent
- Attention, lors de l'isolation réseau les VM sont éteintes en « Power Off »
- VirtualCenter monitore continuellement le cluster
- Intégration de VMware DRS dans le cluster
- Gestion de la capacité du failover
- Après installation, HA peut fonctionner sans serveur VirtualCenter



04. Protection et disponibilité des données
VMware HA (High Availability) (3/3)

- VMware HA surveille continuellement les serveurs ESX dans le cluster. Un agent est placé sur chaque serveur et permet de verfier le « Heartbeat » entre tous les serveurs du cluster.
- VMware HA vérifie si les ressources sont suffisantes avant de redémarrer les VM sur les autres serveurs ESX.
- La fonction HA utilise la technique VMware du « File Locking » qui permet à plusieurs serveurs ESX d'accéder aux fichiers des VM sur des stockages partagés.



04. Protection et disponibilité des données

Gestion de VMware HA (1/2)

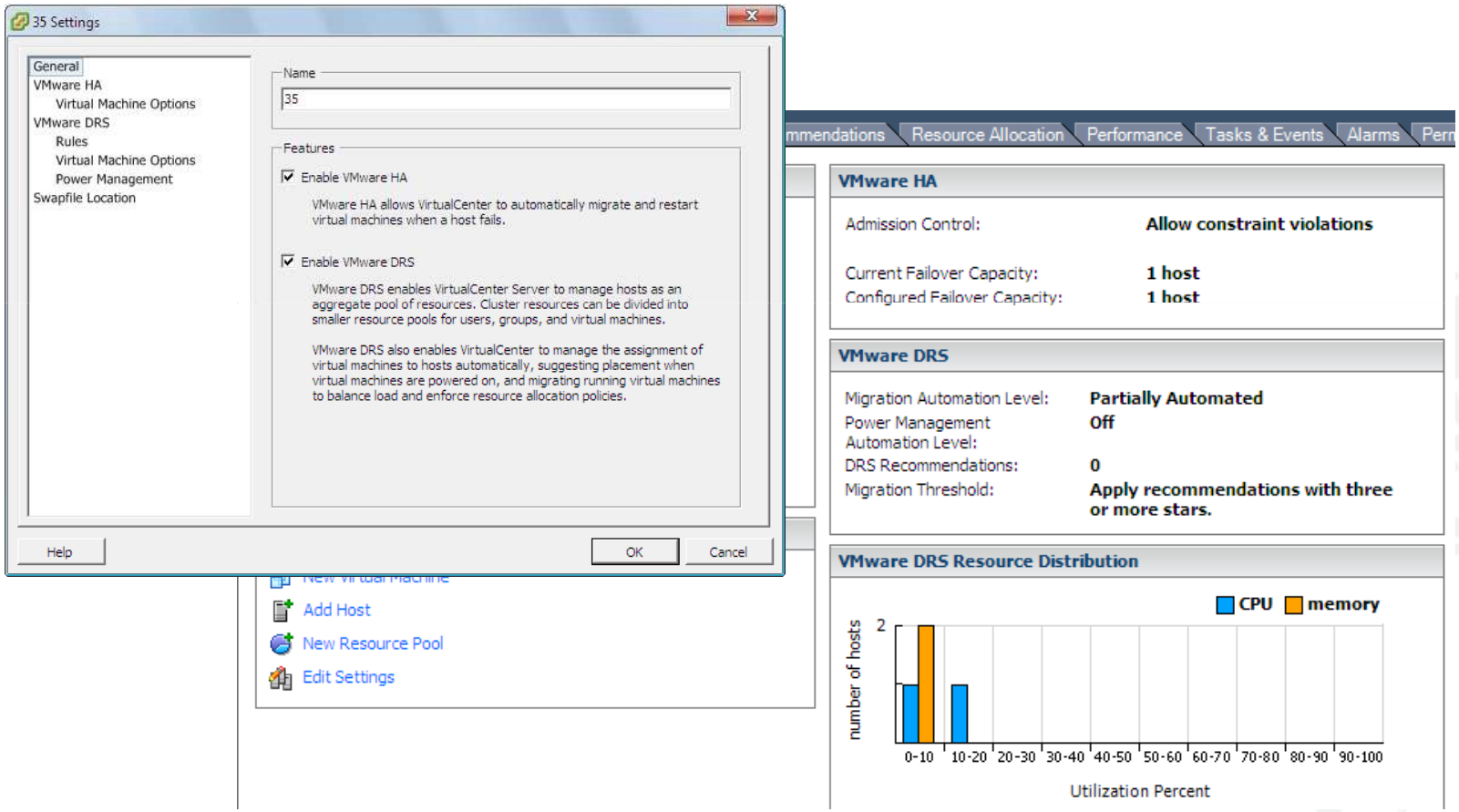
- Choisir le nombre de serveurs pouvant être indisponible
- Ajouter / retirer des serveurs dans le Cluster VMware
- Renseigner les priorités sur les machines virtuelles
- Configurer « Isolation Response » sur les machines virtuelles

- Pré-requis :
  - Les fichiers des machines virtuelles doivent être stockés sur un volume partagé.
  - Les réseaux doivent être identiques entre les serveurs dans le cluster.
  - Chaque serveur dans le cluster doit résoudre les noms et adresses IP des autres serveurs. La résolution DNS et/ou locale doit être configurée sur chaque serveur du cluster.
  - S'assurer de la tolérance de panne réseau pour le Service Console

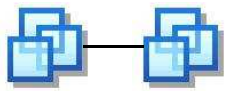
04. Protection et disponibilité des données

Gestion de VMware HA (2/2)

Activation de VMware HA et VMware DRS



04. Protection et disponibilité des données
Comparaison des clusters

"Cluster"	Niveau	Fonctionnement	Restriction
VM Cluster 	VM	Si un noeud du cluster tombe, l'autre noeud prend le relais	▪ Clustering software (MSCS) ▪ Le disque de boot du nœud doit être un SCSI local (pas sur un stockage partagé) ▪ Une VM en cluster ne peut être migrée (VMotion or VMware DRS) ▪ Une VM en cluster ne peut être redémarrée avec VMware HA
VMware DRS Cluster 	Serveur ESX	Load Balancing des VM sur les serveurs ESX intégrés dans le cluster	▪ Les VM résident sur un stockage partagé ▪ VMotion and VMware DRS
VMware HA Cluster 	Serveur ESX	Si un serveur ESX tombe, les VM sont automatiquement redémarrées sur les autres serveurs du cluster	▪ Les VM résident sur un stockage partagé et accessible par plusieurs serveurs ▪ VMware HA

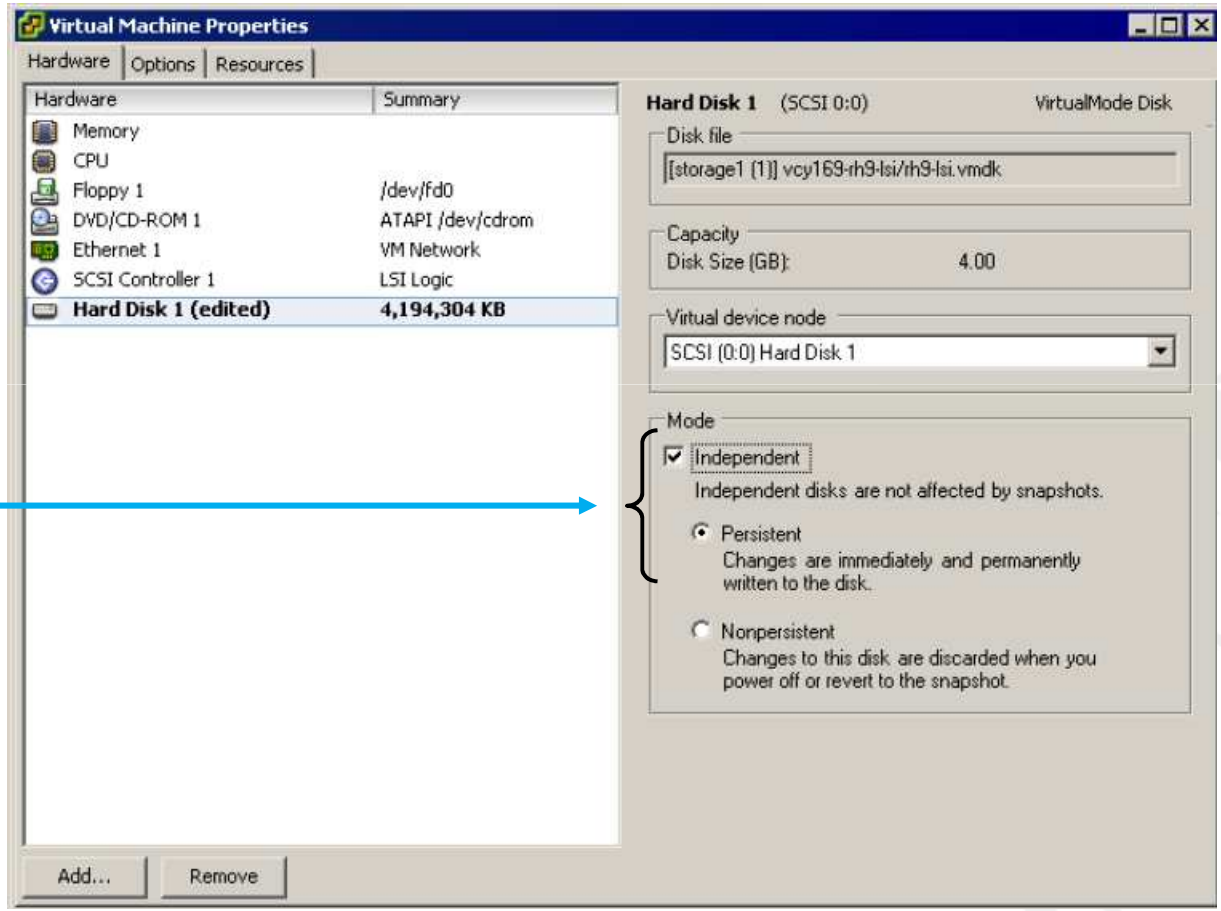
04. Protection et disponibilité des données
Snapshots (1/3)

- La fonction de Snapshot VMware permet d'enregistrer une machine virtuelle à un instant précis et de la restaurer sans perturber le système d'exploitation.
  - **Capture l'état de la machine virtuelle :**
    - L'état de la mémoire
    - Les paramètres de la VM
    - L'état des disques
  - **3 actions possible sur un Snapshot :**
    - « Take a Snapshot », lorsque vous effectuez un Snapshot sur une VM qui possède déjà un Delta, un second Delta est créé
    - « Revert to Snapshot », lorsque vous faites un retour arrière sur un Snapshot, le contenu du fichier Delta n'est pas appliqué au disque virtuel et est réinitialisé.
    - « Delete Snapshot », lorsque vous retirez un Snapshot, les modifications effectuées sur le Delta sont appliquées au fichier de disque virtuel.

04. Protection et disponibilité des données
Snapshots (2/3)

Désactiver la fonction Snapshot

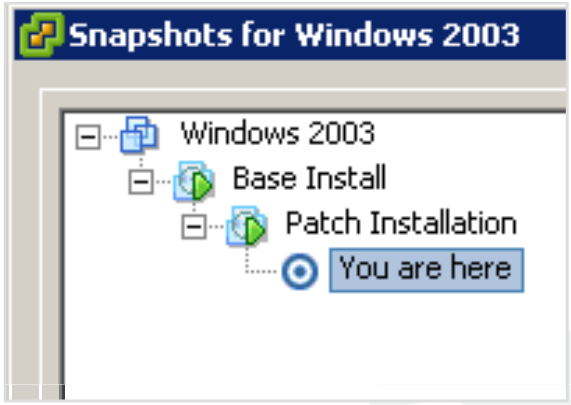
Éditer les propriétés du ou des disques virtuels et passer le disque en mode « Independent », et « Persistent »



04. Protection et disponibilité des données
Snapshots (3/3)

Gestion des Snapshots

« Snapshot Manager » permet de visualiser pour chaque machine virtuelle l'etat des snapshots.



- « Go to » permet de retourner au point de depart du snapshot.
- « Delete » permet d'appliquer les modifications du snapshot aux parents et de supprimer le snapshot sélectionné.
- « Delete All » permet d'appliquer tous les snapshots à la Machine virtuelle et de les supprimer.

04. Protection et disponibilité des données

Sauvegarde et restauration

Vue d'ensemble

La sauvegarde et la restauration sont des processus très importants à mettre en place sur votre infrastructure. L'infrastructure virtuelle VMware propose différentes solutions et plusieurs approches pour sauvegarder et restaurer.

- **Pourquoi sauvegarder ?**
  - Erreur accidentelle de suppression de fichiers…
  - Erreur d'exploitation, suppression d'une VM …
  - Problème matériel, erreurs disque …
- **Deux approches de sauvegarde :**
  - Sauvegarde traditionnelle (niveau fichier et niveau VM)
  - Sauvegarde avec VCB (niveau VM)

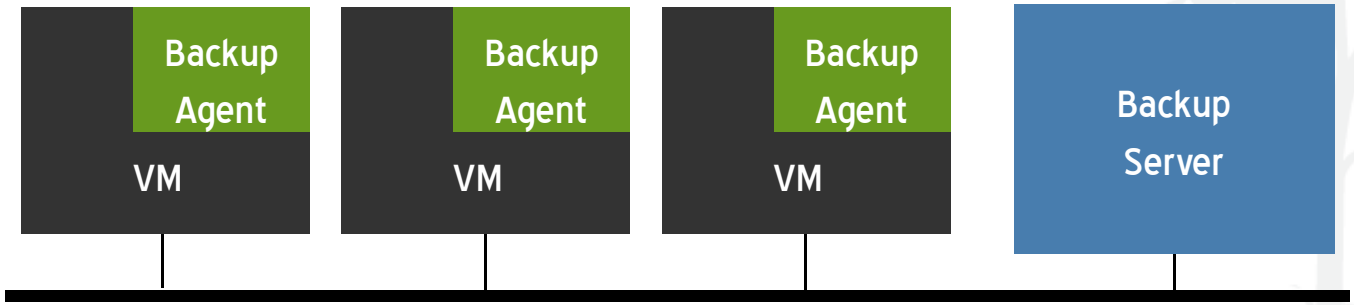
04. Protection et disponibilité des données

Sauvegarde et restauration

La sauvegarde traditionnelle

Possibilités offertes :

- Placer un agent de sauvegarde dans chaque système d'exploitation des VM.
- Placer un agent de sauvegarde dans le service console permet de sauvegarder les fichiers des VM.
- Il est même techniquement possible d'installer le serveur de sauvegarde dans une VM et connecter la librairie de sauvegarde à la machine virtuelle à travers le bus SCSI, mais cela est déconseillé pour des raisons de sécurité.

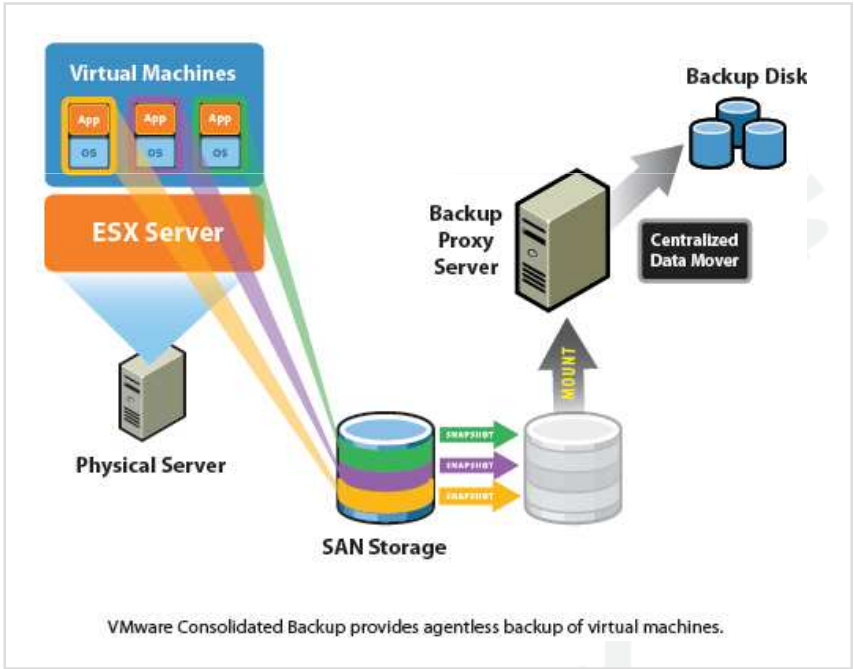


04. Protection et disponibilité des données

Sauvegarde et restauration

VMware Consolidated Backup (VCB) (1/5)

- VMware Consolidated Backup (VCB) est une solution de sauvegarde centralisée et très simple d'utilisation.
  - Un agent est placé sur un serveur de sauvegarde « proxy » séparé du serveur ESX, ainsi aucun agent ne réside sur le serveur ESX
  - Le principe consiste à exécuter des scripts de pré-backup afin de faire un « snapshot » des disques virtuels, ainsi le serveur de sauvegarde « proxy » peut monter les volumes et les sauvegarder. VCB est une solution simple, moins intrusive et générant moins d'overhead.



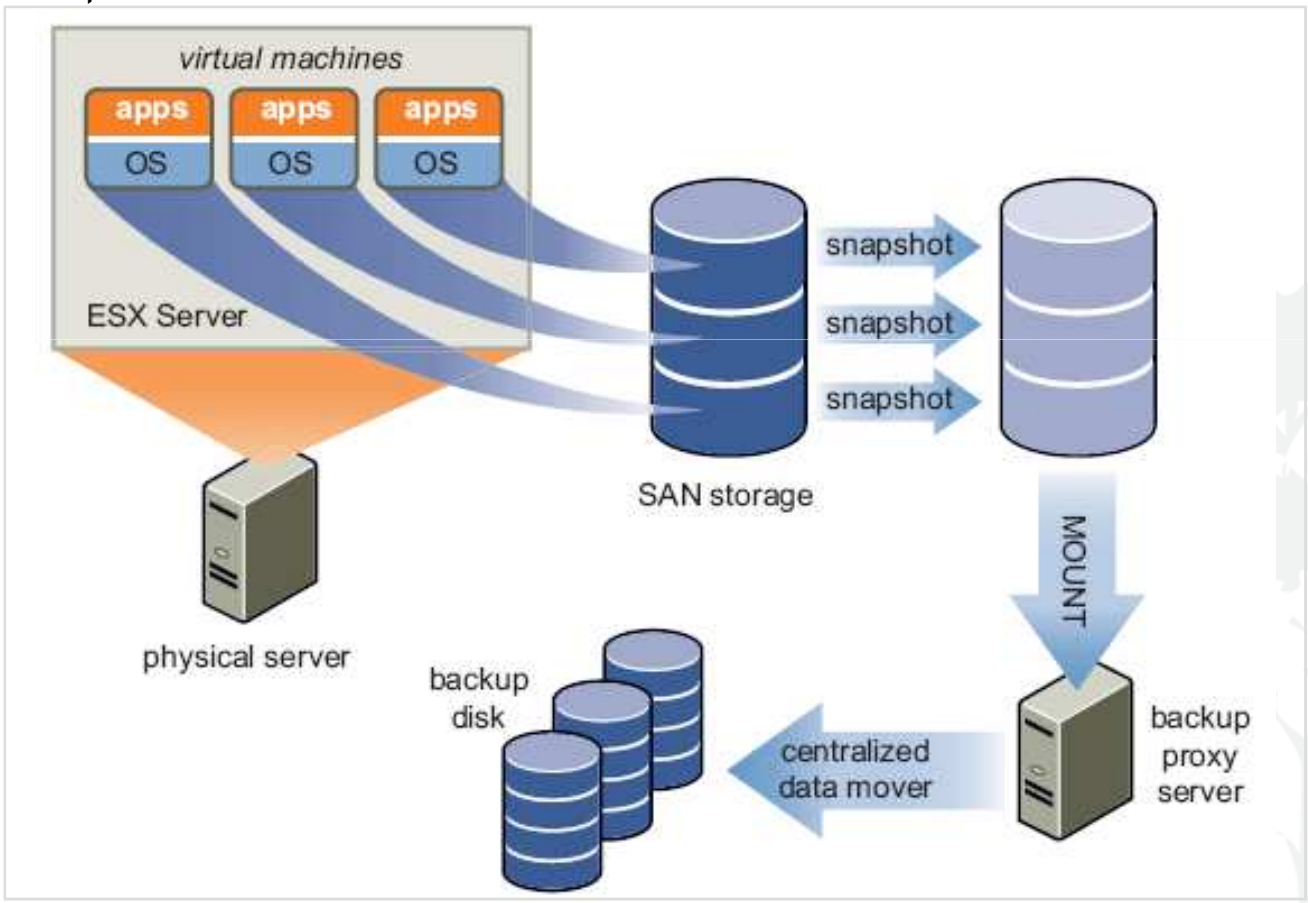
VMware Consolidated Backup provides agentless backup of virtual machines.

04. Protection et disponibilité des données

Sauvegarde et restauration

➔ VMware Consolidated Backup (VCB) (2/5)

Principe de fonctionnement



04. Protection et disponibilité des données

Sauvegarde et restauration

VMware Consolidated Backup (VCB) (3/5)

Utilisation de VCB :

- Sauvegarde « Full » des images virtuelles pour des solutions de « Disaster Recovery »
- Sauvegarde Full et Incrémentale des machines virtuelles pour les systèmes d'exploitation Microsoft pour restaurer des fichiers et des répertoires
- Sauvegarde SAN de type « Lan Free Backup » (connexion du serveur Proxy en Fibre Channel ou en iSCSI sur le SAN)
- Intègre et valide la plupart des solutions de sauvegarde (Veritas, Legato, TSM, etc…)

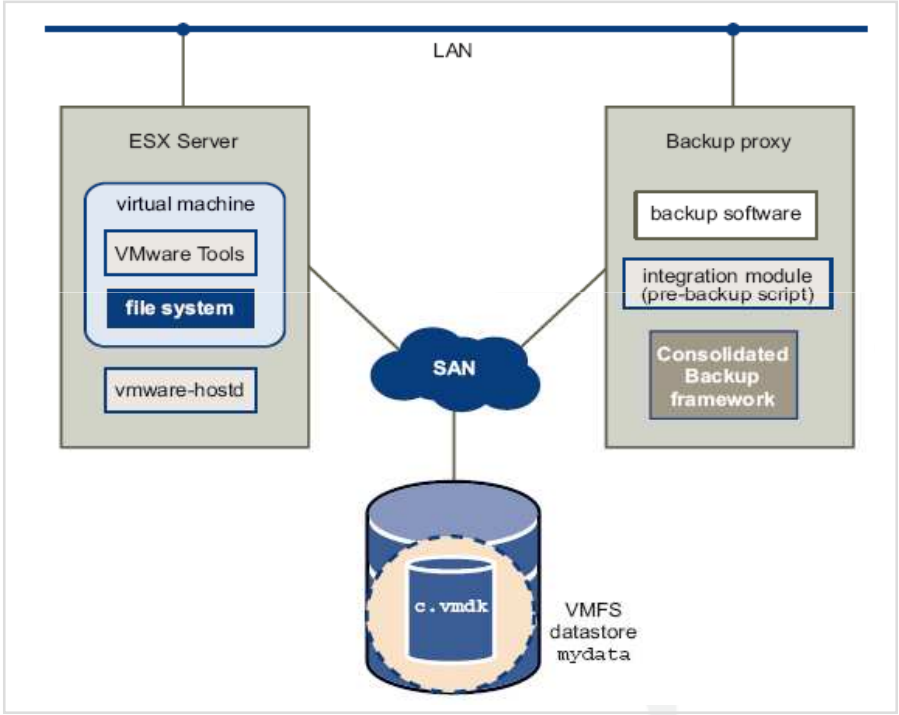
04. Protection et disponibilité des données

Sauvegarde et restauration

VMware Consolidated Backup (VCB) (4/5)

Étapes :

- Exécution du job de sauvegarde
- Lancement des scripts de pré-sauvegarde
- Création du snapshot de la VM
- Montage du disque de la VM sur le proxy de sauvegarde (niveau fichier) ou export du disque sur le proxy VCB (niveau image)
- Sauvegarde des volumes montés (au niveau fichier) pour les OS Windows
- Sauvegarde des disques exportés pour tous les OS (linux et Windows)
- Démontage des disque sur le serveur proxy VCB
- Suppression des snapshots des VM



04. Protection et disponibilité des données

Sauvegarde et restauration

VMware Consolidated Backup (VCB) (5/5)

Scénario VCB type pour la sauvegarde :

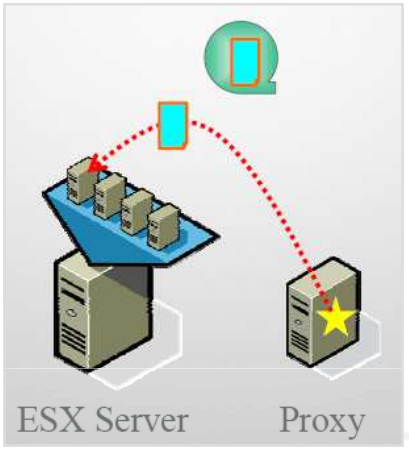
- Sauvegarde avec VCB au niveau fichier (OS Windows) toutes les nuits
- Sauvegarde avec VCB au niveau image périodiquement (hebdomadaire) pour les scénarios de Disaster Recovery
- Sauvegarde avec des agents dans les machines virtuelles (niveau fichier) pour les OS Linux toutes les nuits
- Pour les succursales, le serveur de sauvegarde peut être une machine virtuelle, sauvegarde via les agents installés dans les VM

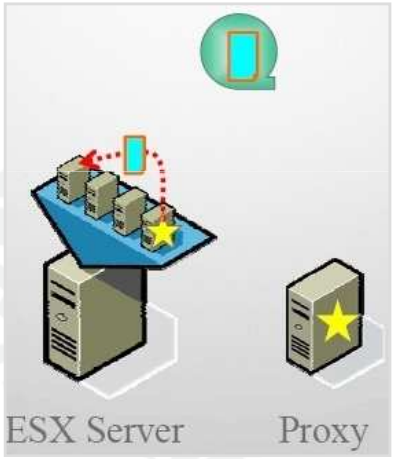
04. Protection et disponibilité des données

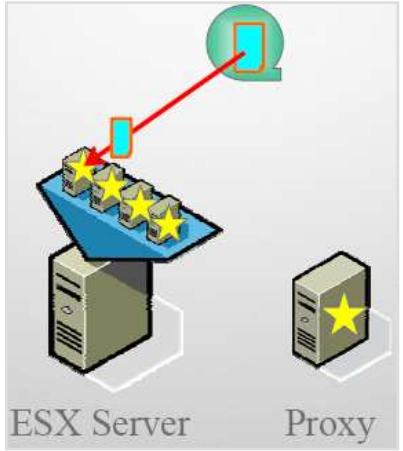
Sauvegarde et restauration

Restauration des fichiers avec VCB

- La restauration au niveau fichier avec VMware Consolidated Backup va pourvoir s'effectuer selon 3 méthodes :
  - **Restauration centralisée**
    - Restauration sur le serveur proxy puis envoi des fichiers pour les VM sur des partages réseaux, évite d'installer des agents de restauration dans les VM
  - **Restauration par groupe**
    - Restauration des fichiers via agent par groupe de VM, bon compromis entre le nombre d'agent installé et la facilité de restauration
  - **Restauration « self-service »**
    - Des agents de restauration sont installés sur chaque VM, restauration traditionnelle via l'agent







04. Protection et disponibilité des données
Storage VMotion

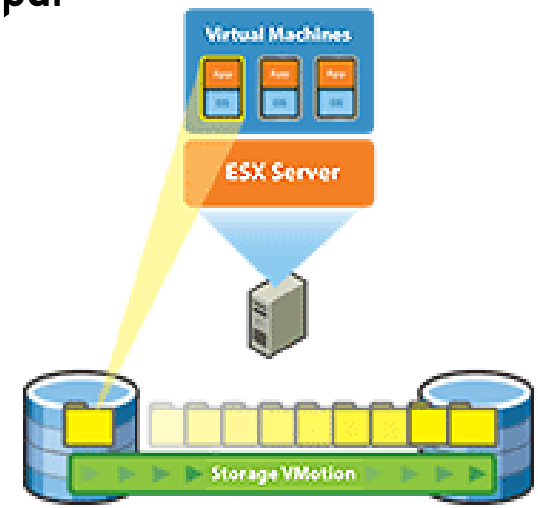
Migration à chaud du stockage virtuel

- Permet la migration des disques virtuels vers un nouveau Datastore
- Aucun arrêt de production à prévoir
- Conserve l'intégralité des transactions en cours
- L'interopérabilité permet la migration vers tous les types de stockage supportés par VMware
- Pré-requis au SVMotion :

Pas de Snapshot sur les VM
Disques en mode persistant ou RDM
Avoir assez de ressources pour supporter 2 instances de la VM
Licence VMotion et VMotion configuré en Gigabit
Le serveur host qui accueille la VM doit avoir accès aux 2 Datastores
Une seule Migration par Datastore à la fois
Une machine avec le R-cli installé (Linux ou Windows)

- Remote Command Line Interface (R-cli) est une série d'outils en Perl mis a disposition par VMware pour gérer des ESX au travers d'une console.

La migration SVMotion est initiée uniquement à partir du R-CLI de VMware.



Notes

04. Protection et disponibilité des données
Questions réponses

Question

On which platform does the VCB proxy run?

A. a Windows physical machine
B. a Windows virtual machine
C. an agent in an ESX Server
D. a Linux physical machine
E. a Linux virtual machine

04. Protection et disponibilité des données
Questions réponses

➔ Question :

What are three requirements for a VMware HA cluster? Select three

A. name resolution between all hosts
B. identical type and quantity of CPUs in each host
C. access to shared storage from all hosts
D. access to the virtual machine networks from all hosts
E. private Gigabit Ethernet network for all hosts.

04. Protection et disponibilité des données
Questions réponses

➔ Question

Which partition is required to store core dumps for debugging and for VMware technical support?

A. vmkcore
B. vmkdump
C. vmfscore
D. vmimages

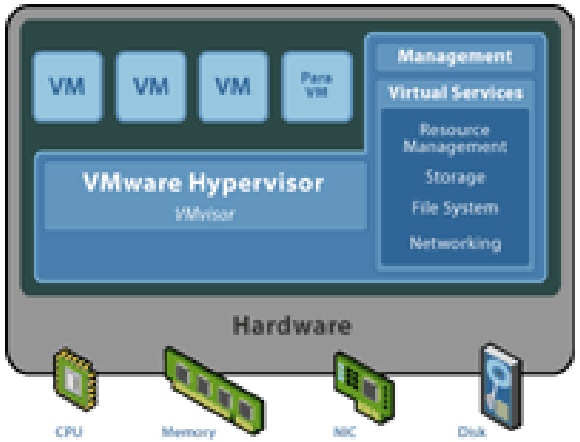
05. Architecture avancée

- Para-virtualisation
- Gestion du fichier Swap
- Virtualisation de CPUs
- Virtualisation de la mémoire
- Gestion de la mémoire
- Architecture de VirtualCenter
- Configuration en ligne de commande

05. Architecture avancée
Para-virtualisation

VMI Paravirtualization

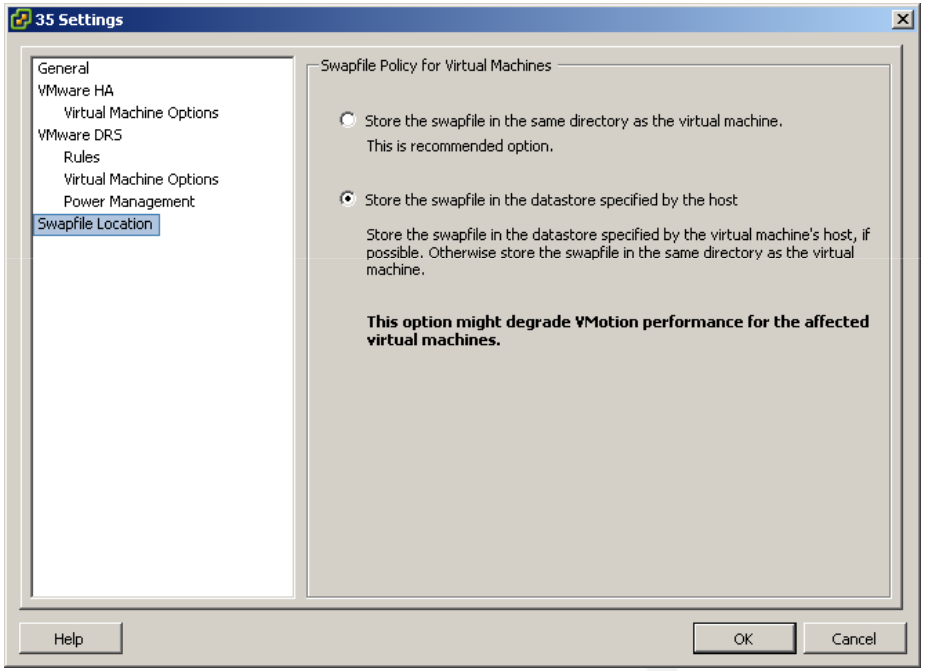
- Permet au Guest OS de communiquer directement avec l'hyperviseur
- Le Guest OS doit être modifié pour utiliser la para-virtualisation
- Actuellement, ne fonctionne que sous Linux
- Amélioration générale des performances de la VM



05. Architecture avancée
Gestion du fichier Swap (1/2)

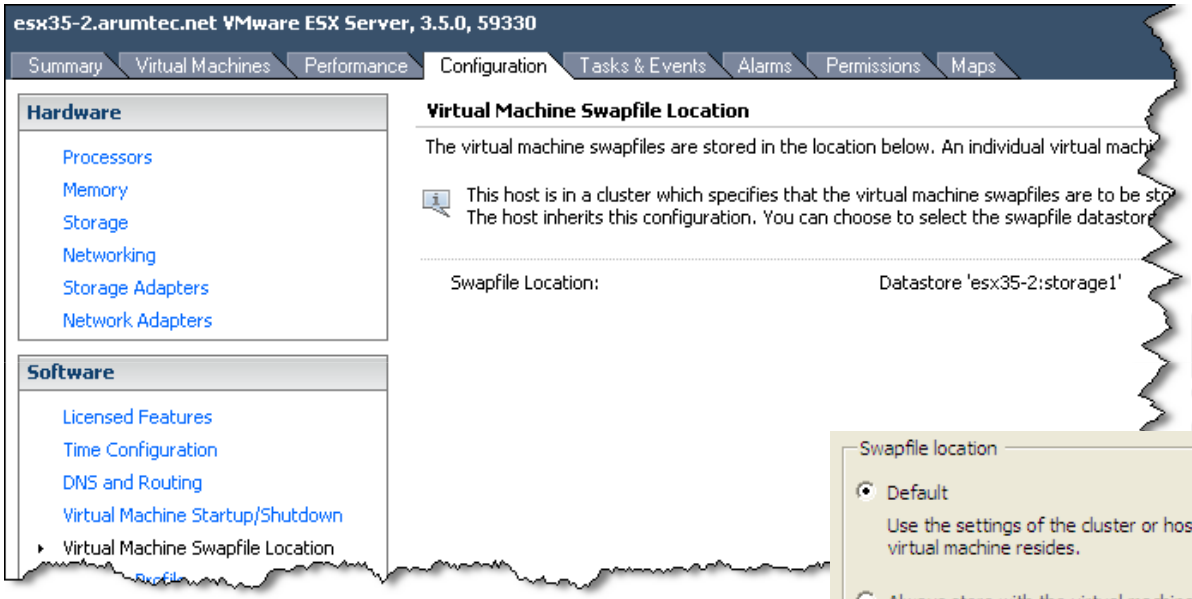
SwapFile Location

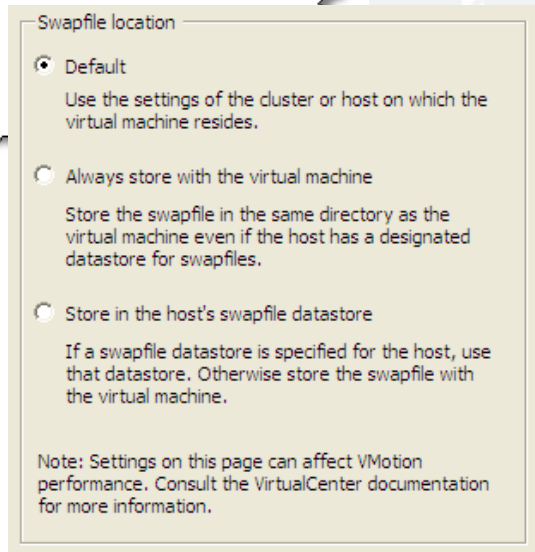
- Par défaut le swap est situé au même endroit que le fichier de configuration de la VM
- Il est possible de configurer l'emplacement du fichier de swap sur l'ESX ou sur la VM directement
- En cas de stockage local du swapfile les performances lors d'une migration VMotion peuvent être dégradées



05. Architecture avancée
Gestion du fichier Swap (2/2)

Gestion de l'emplacement du fichier de Swap par serveurs.



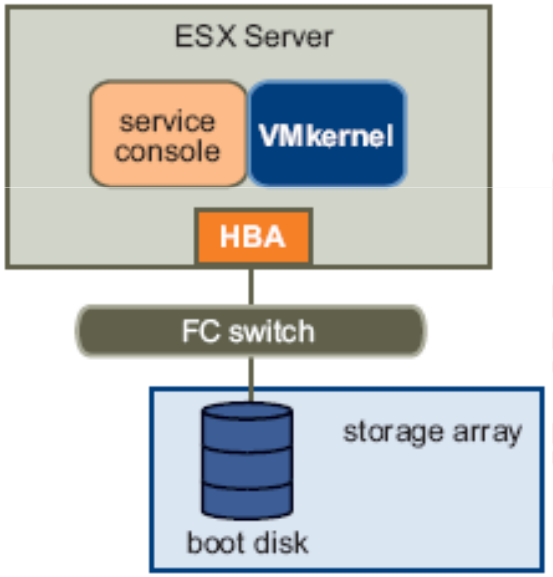


Gestion de l'emplacement du fichier de swap par VM.

05. Architecture avancée
Boot from SAN

Présentation

- Dans un environnement Boot from SAN, les binaires ESX sont installés sur une plusieurs LUN du SAN



Avantages

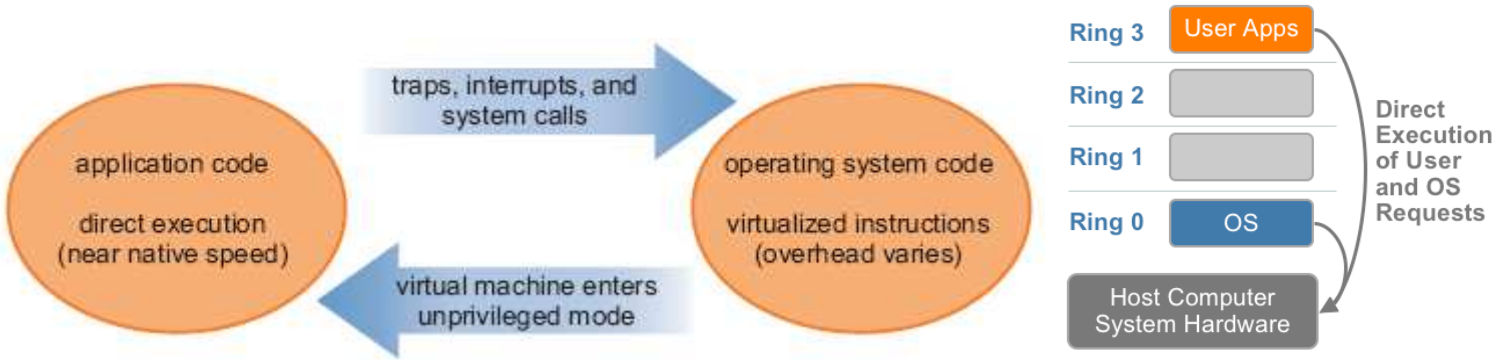
- Serveurs moins coûteux
- Remplacement de serveurs simplifiés
- Processus de backup intégrés au SAN
- Déploiement des ESX améliorés

Inconvénients

- Pas de Cluster Microsoft
- Configuration du bios de la HBA

05. Architecture avancée
Virtualisation du CPU (1/3)

- Émulation versus Virtualisation
  - Dans le mode émulation, toutes les opérations sont exécutées dans un logiciel par un émulateur
  - Dans le mode virtualisation, les ressources physiques sont utilisées si nécessaire, la couche de virtualisation gère les accès aux ressources physiques
- Une machine virtuelle peut fonctionner sur 2 modes :
  - « Direct execution », sous certaines conditions, VMM (Virtual Machine Monitor) peut faire fonctionner la VM directement sur le processeur.
    Cela fournit de meilleures performances dans l'exécution des requêtes CPU
  - « Virtualization mode », si le premier mode n'est pas possible, les instructions CPU seront virtualisées, cela génère de l'overhead



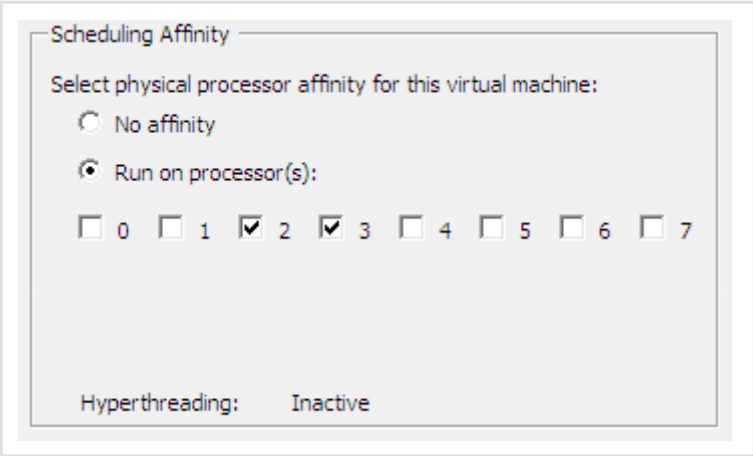
05. Architecture avancée
Virtualisation du CPU (2/3)

- Virtual Machine Monitor (VMM)
  - Composant logiciel qui met en œuvre l'abstraction matérielle de la VM.
  - Responsable du fonctionnement du Guest OS.
- Hyperviseur
  - Composant logiciel responsable de l'hébergement et du management des VM.
  - Fonctionne directement avec le hardware.
  - Ces fonctionnalité varient selon l"architecture et l'implémentation.
- Techniques de virtualisation

Memory virtualization	Partitionnement mémoire et allocation de mémoire physique
Privileged instruction virtualization	Dé-privilégisation ou ring compression (VT-x, Pacifica)
Device and I/O virtualization	Routage des requêtes d'i/o entres périphériques virtuels et matériels

05. Architecture avancée
Virtualisation du CPU (3/3)

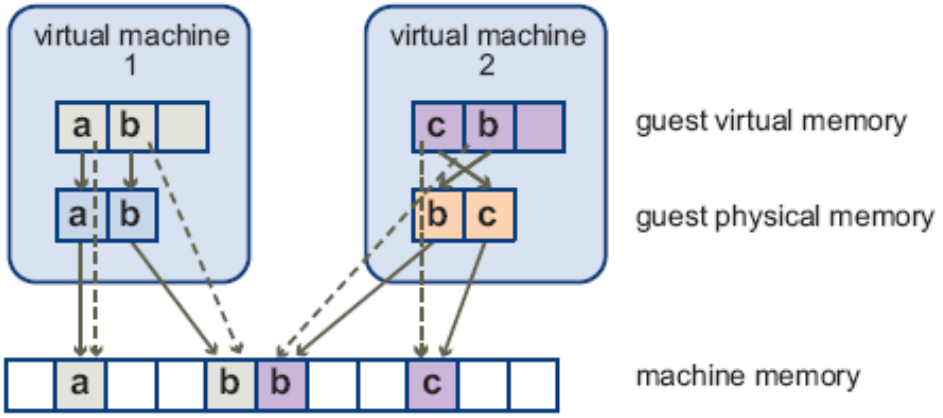
- CPU Affinity : Assignation de Core CPU pour une machine virtuelle sur un système multi processeurs.



- Contraintes :
  - Réduit le load balancing des accès CPU automatiques
  - Peut interférer avec la gestion des ressources (limit et shares)
  - La « CPU affinity » peut être modifiée si une VM est migrée sur un autre serveur ESX
  - Ne fonctionne pas avec DRS en mode « Fully automated »

05. Architecture avancée
Virtualisation de la mémoire (1/2)

- La plupart des systèmes d'exploitation supporte la mémoire virtuelle, principe de dépassement de la mémoire physique. La mémoire virtuelle est divisée en blocs de 4kB, appelés « Pages ». Lorsque que la mémoire physique est saturée, les données des pages virtuelles sont stockées sur le disque.
  - « Mapping » entre la mémoire physique et virtuelle, les tables de page traduisent des adresses de mémoires virtuelles en adresses de mémoires physiques
- Le serveur ESX virtualise la mémoire en ajoutant un niveau supplémentaire, la traduction d'adresses mémoires :
  - Le VMM maintient un mappage entre les pages mémoires du système d'exploitation et les pages mémoires physiques



05. Architecture avancée
Virtualisation de la mémoire (2/2)

- La virtualisation de la mémoire engendre deux « Overhead » mémoire
  - **Temps supplémentaire d'accès à la mémoire (très court)**
    - Erreur de page
  - **Espace mémoire supplémentaire**
    - Service console et VMkernel
    - Machine virtuelle

vCPU	Mémoire (MB)	Overhead VM 32-Bit (MB)	Overhead VM 64-Bit (MB)
1	256	87.56	107.54
1	512	90.82	110.81
1	1,024	97.35	117.35
1	2,048	110.40	130.42
1	4,096	136.50	156.57
1	8,192	188.69	208.85
1	16,384	293.07	313.42
1	32,768	501.84	522.56
1	65,536	919.37	940.84
2	256	108.73	146.41
2	512	114.49	152.20
2	1,024	126.04	163.79
2	2,048	149.11	186.96
2	4,096	195.27	233.30

vCPU	Mémoire (MB)	Overhead VM 32-Bit (MB)	Overhead VM 64-Bit (MB)
2	8,192	287.57	325.98
2	16,384	472.18	511.34
2	32,768	841.40	882.06
2	65,536	1,579.84	1,623.50
4	256	146.75	219.82
4	512	153.52	226.64
4	1,024	167.09	240.30
4	2,048	194.20	267.61
4	4,096	248.45	322.22
4	8,192	356.91	431.44
4	16,384	573.85	649.88
4	32,768	1,007.73	1,086.75
4	65,536	1,875.48	1,960.52

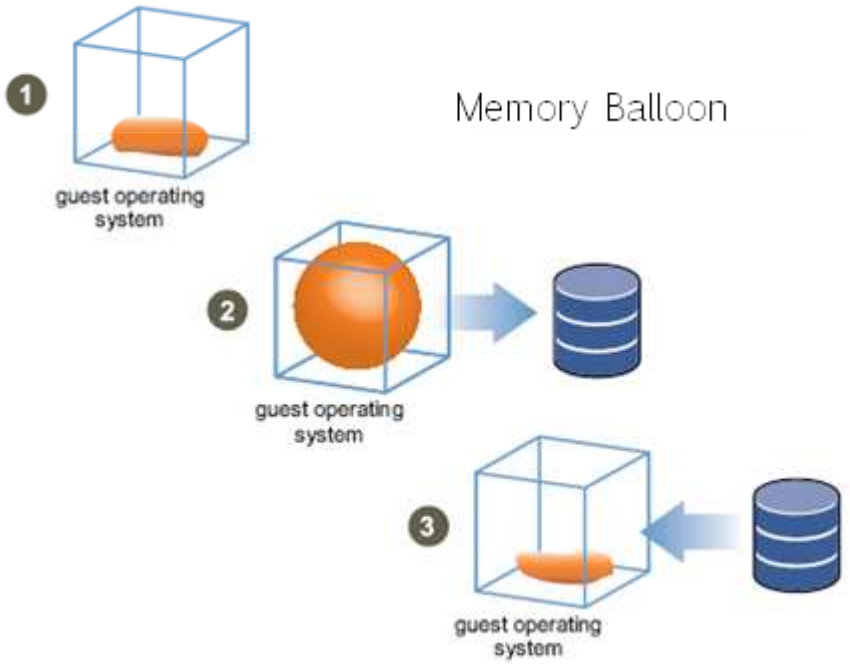
05. Architecture avancée
Gestion de la mémoire

- Lorsque le besoin de mémoire pour les machines virtuelles dépasse la capacité mémoire physique du serveur, on appelle cela « Memory Overcommitment »
- Les machines virtuelles peuvent avoir plus de mémoire configurée que disponible physiquement sur le serveur ESX
- Trois solutions afin de réclamer de la mémoire supplémentaire aux machines virtuelles :

  - « Transparent Page Sharing », page mémoire identique entre plusieurs VM, écrite qu'une seule fois sur la mémoire physique de l'ESX

  - « Memory Balloon », un pilote est installé avec les VMware Tools « vmmemctl », il permet de libérer de la mémoire pour que d'autres VM l'utilisent en cas de contention (schéma ci contre)

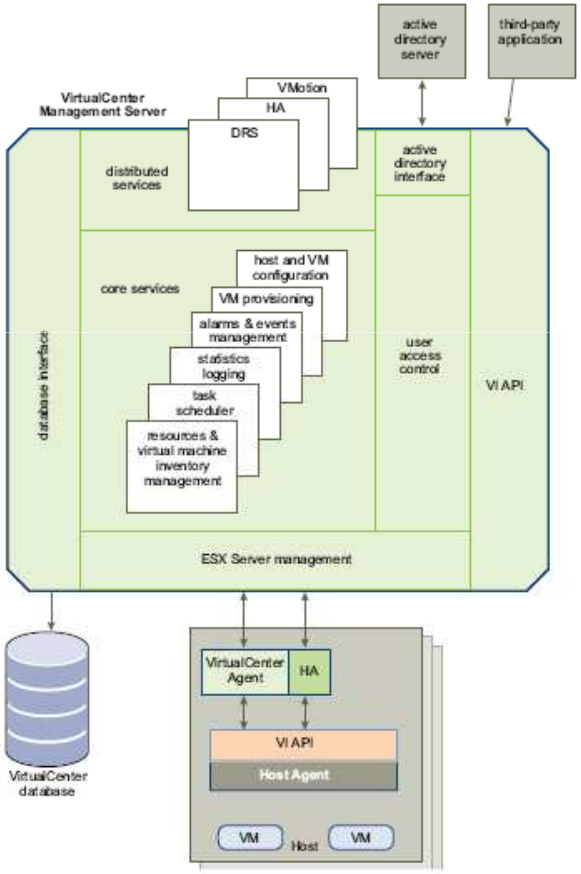
  - « Swap », un fichier de swap sera utilisé en dernier recours

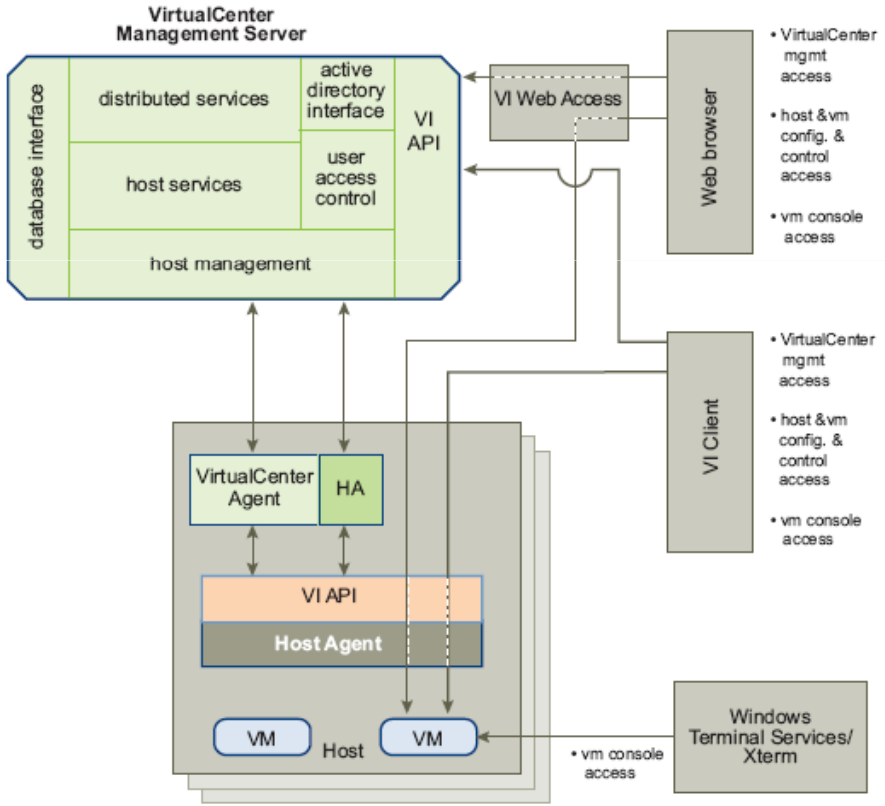


05. Architecture avancée

Architecture VirtualCenter

Composants clés de VirtualCenter Server





05. Architecture avancée
Configuration en ligne de commande (1/2)

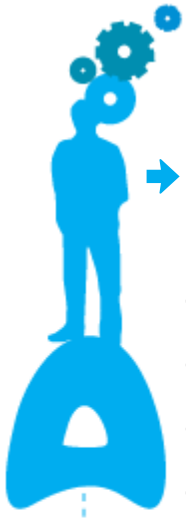
Utilisation des commandes dans le service console

Commande	Description
esxcfg-dumppart	Configuration de la partition de diagnostic
esxcfg-firewall	Configuration des ports Firewalls du service console
esxcfg-info	Fournit un état du service console et du VMkernel
esxcfg-mpath	Configure les paramètres du “multipath” pour le fibre channel ou le iSCSI
esxcfg-nas	Gère les montages NAS (NFS)
esxcfg-nics	Liste des cartes réseaux physiques (Pilote, PCI, vitesse, état)
esxcfg-resgrp	Configuration des pools de ressources
esxcfg-route	Configuration de la passerelle par défaut du VMkernel
esxcfg-swicsi	Configuration du Software Initiator iSCSI
esxcfg-upgrade	Mise a jour du serveur ESX de 2.x a 3.x
esxcfg-vmhbadevs	Liste des mapping du périphérique de stockage dans le /dev du service console
esxcfg-vmknic	Création et mise à jour des paramètres TCP/IP du VMkernel
esxcfg-vswif	Création et mise à jour des paramètres réseau du service console
esxcfg-vswitch	Création et mise à jour des switchs virtuels

05. Architecture avancée
Configuration en ligne de commande (2/2)

Utilisation des commandes dans le service console

Commande	Description
vmkfstools	Création et configuration des disques virtuels et du VMFS
esxupdate	Affiche les updates installés et permet la mise à jour de l'ESX
vmware-cmd	Interaction avec une machine virtuelle
vm-support	Création d'un dump pour débogage
vdf	Rapport sur l'espace disque utilisé
vmkping	Lance un ping en utilisant le VMkernel
reboot	Redémarre le serveur ESX
shutdown now	Arrête le serveur ESX



Notes

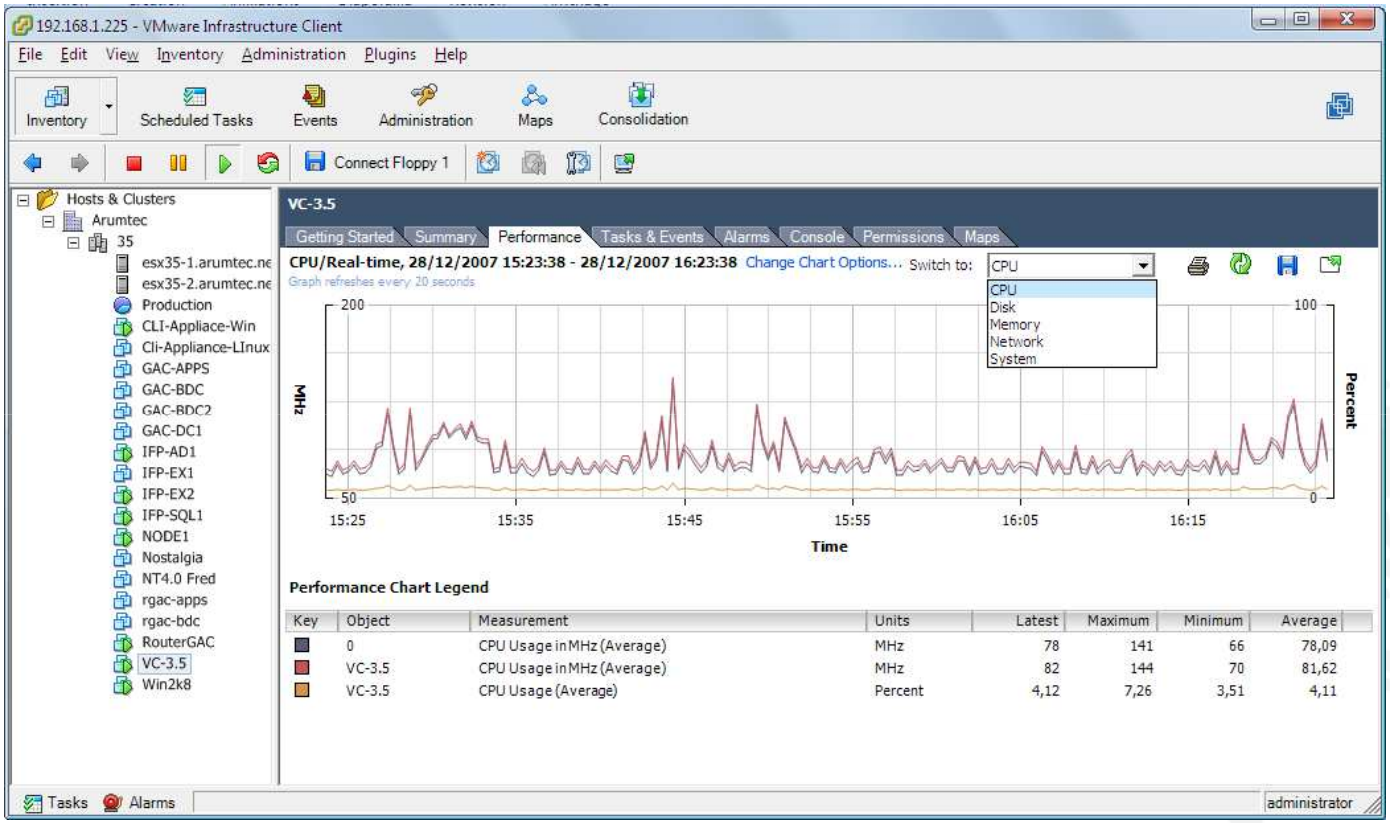
06. Monitoring du datacenter

- Graphique de performance
- Outils de suivi de performance
- Cartographie de datacenter
- Gestion des tâches
- Gestion des alarmes

06. Monitoring du datacenter

Graphique de performance

- CPU
- Mémoire
- Disque
- Réseau
- COS
- Système
- DRS



- Visualisation en temps réel ou sur une plage de temps personnalisée
- Exportation au format Microsoft Excel ou en image (jpg, gif, bmp, png)

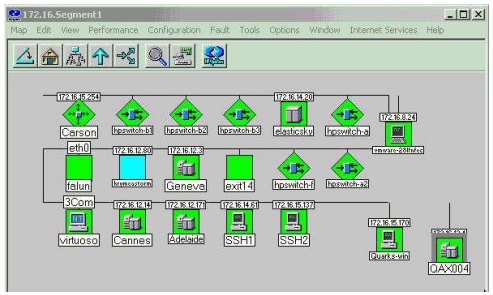
06. Monitoring du datacenter
Outils de suivi de performance (1/3)

SNMP

Configurer et activer l'agent SNMP
- Via les commandes service et chkconfig

Éditer la configuration
- Située dans /etc/snmp/snmpd.conf

État des serveurs ESX



Installer les MIBs VMware dans l'outil de monitoring

MIBs ESX : /usr/lib/vmware/snmp/mibs
MIBS VirtualCenter : C:\Program Files\VMware\Infrastructure\VirtualCenter Server\MIBS

- World IDs

enterprises.vmware.vmwVirtMachines.vmTable.vmEntry.vmVMID

- Quels sont les OS qui tournent ?

enterprises.vmware.vmwVirtMachines.vmTable.vmEntry.vmGuestState

- Écritures sur disques

enterprises.vmware.vmwResources.vmwHBATable.hbaEntry.kbWritten

- Mémoire utilisée

enterprises.vmware.vmwResources.vmwMemory.memTable.memEntry.memUtil

SNMP agent et VMware SNMP subagent avec MUI

```
# snmpwalk –Os -M  /usr/share/snmp/mibs:/usr/lib/vmware/snmp/mibs
–m all localhost public
.enterprises.vmware.vmwVirtMachines.vmTable.vmEntry.vmGuestOS
vmGuestOS.0 = "win2000"
vmGuestOS.1 = "win2000"
vmGuestOS.2 = "linux"
```

06. Monitoring du datacenter
Outils de suivi de performance (2/3)

Monitoring via les outils constructeurs

- **Les outils d'administration système servent à :**
  - Remonter des alertes de dysfonctionnement
  - Inventaire Hardware et Software
  - Session remote
  - Utilisation des ressources systèmes
  - Restauration automatique après détection de pannes
- **Exemples**
  - HP Insight Manager
  - Dell OpenManage
  - IBM Director
- **Remote management**
  - Compaq Remote Insight Lights-Out (RILO)
  - Dell Remote Access Card (DRAC)
  - IBM Remote Supervisor Adapter (RSA)

06. Monitoring du datacenter

Outils de suivi de performance (3/3)

Utilisation de Esxtop

```
 4:01:24pm up 19 days 22:53, 117 worlds; MEM overcommit avg: 0.00, 0.00, 0.00
PMEM  /MB: 32767   total:   272     cos,   400 vmk,    5488 other,  26606 free
VMKMEM/MB: 32060 managed:  1923 minfree,  3032 rsvd,  28861 ursvd,  high state
COSMEM/MB:    11    free:   541  swap_t,   513 swap_f:   0.00 r/s,   0.00 w/s
PSHARE/MB:  8254  shared,   880  common:  7374 saving
SWAP  /MB:     0    curr,     0  target:                0.00 r/s,   0.00 w/s
MEMCTL/MB:     0    curr,     0  target,  7987 max
Display ESX memory on
```

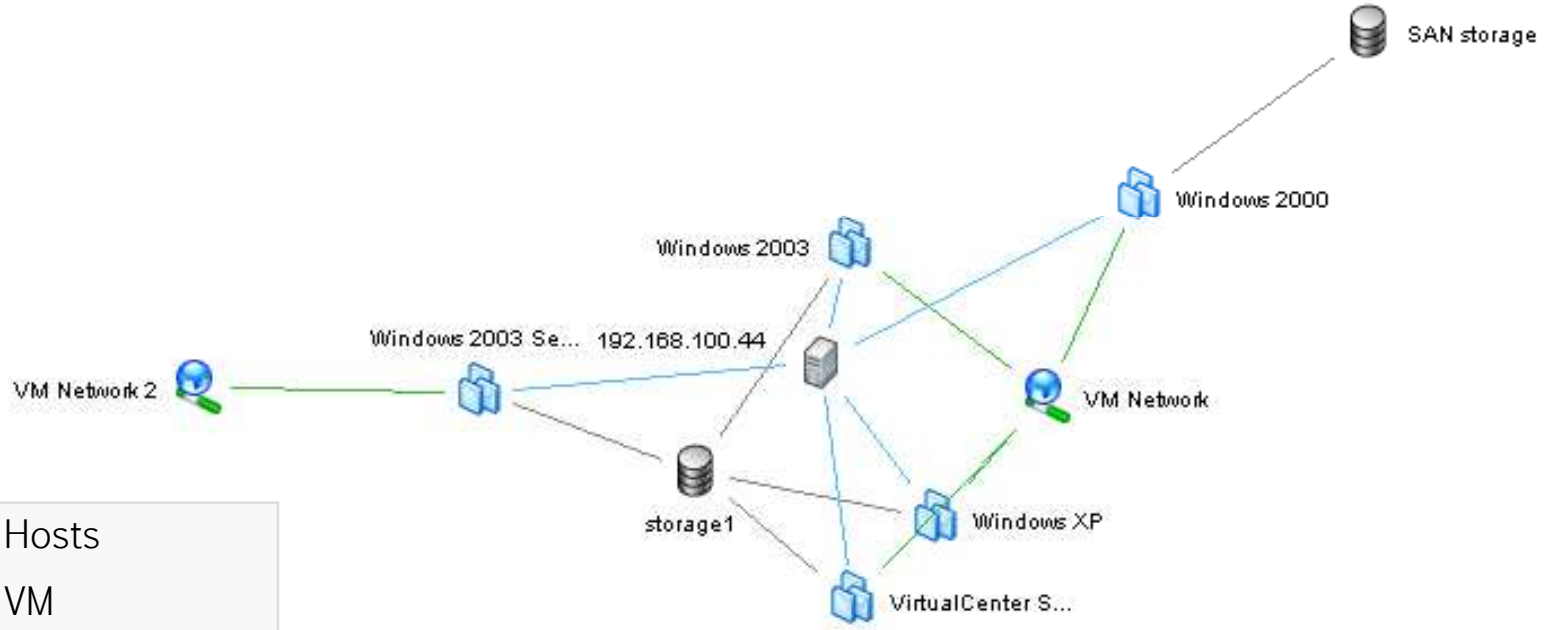
GID	NAME	NWLD	MEMSZ	SZTGT	TCHD	%ACTV	%ACTVS	%ACTVF	%ACTVN	OVHDUW	OVHD	OVHDMAX
17	vmware-vmkauthd	1	5.59	5.59	1.91	0	0	0	0	0.00	0.00	0.00
18	GAC-BDC	6	768.00	529.15	115.20	5	7	7	4	17.64	44.99	88.60
19	GAC-APPS	6	768.00	544.54	176.64	4	8	6	3	17.64	50.55	93.09
20	rgac-apps	6	768.00	431.54	107.52	9	7	8	3	17.64	42.39	85.87
21	GAC-DC1	5	384.00	327.07	107.52	9	12	11	11	14.25	43.10	83.63
22	RouterGAC	6	256.00	285.68	25.60	9	8	9	8	13.12	39.58	79.92
23	GAC-BDC2	5	384.00	338.88	99.84	22	14	18	14	14.25	42.57	83.57
24	rgac-bdc	6	768.00	511.79	99.84	4	6	5	4	17.64	43.99	86.77
26	IFP-EX1	6	2048.00	684.82	61.44	2	1	2	2	28.93	58.02	106.59
27	IFP-EX2	5	2048.00	1060.10	61.44	4	1	3	3	28.93	62.04	111.28
28	IFP-SQL1	6	2048.00	684.93	81.92	5	2	4	4	28.93	62.54	111.48
29	IFP-AD01	5	2048.00	615.00	81.92	4	1	3	4	28.93	53.00	102.30
32	Nagios	5	256.00	321.32	0.00	0	0	0	0	13.12	24.79	70.07

- CPU
- Réseau
- Stockage
- Mode Interactif
- Mémoire
- Mode Batch

06. Monitoring du datacenter

Cartographie du Datcenter

- Représentation des relations entre les composants de l'infrastructure virtuelle

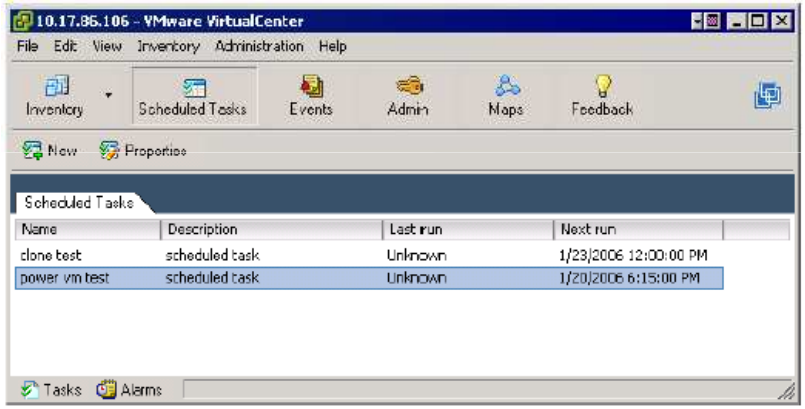


- Hosts
- VM
- Networks
- Datastores

- Export des maps au format BMP, JPEG ou EMF

06. Monitoring du datacenter
Gestion des tâches

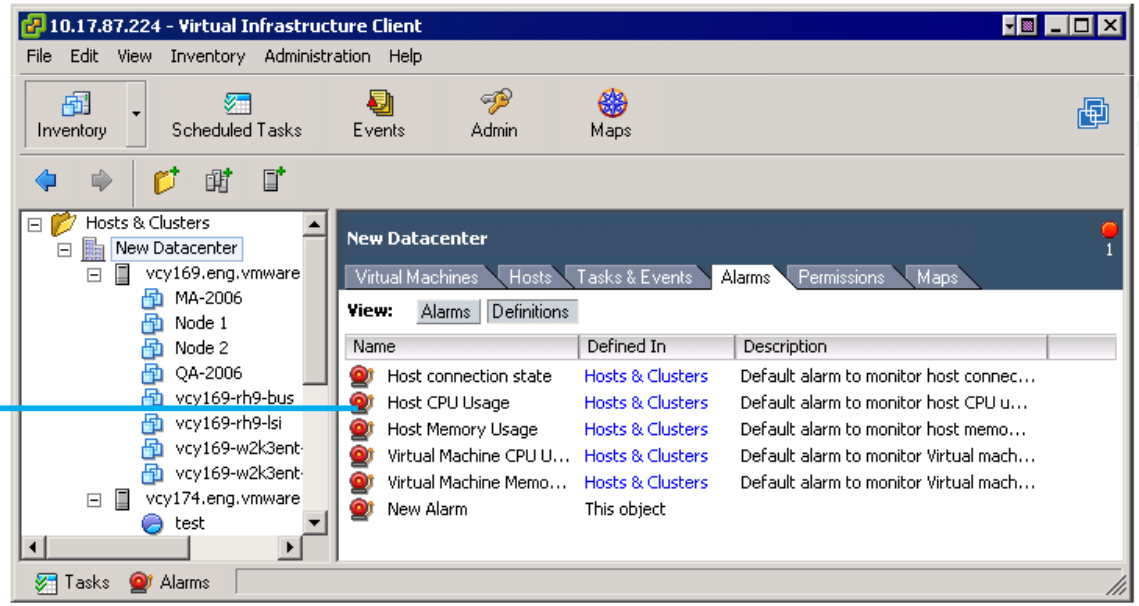
- Lancement d'une tâche immédiatement ou planification des tâches :
  - Changer l'état (on/off) d'une machine virtuelle
  - Cloner une machine virtuelle
  - Déployer une machine virtuelle
  - Déplacer une machine virtuelle avec VMotion
  - Relocate une machine virtuelle
  - Créer une machine virtuelle
  - Créer un snapshot d'une machine virtuelle
  - Custom d'une machine virtuelle
  - Ajouter un serveur ESX
  - Exporter une machine virtuelle
  - Importer une machine virtuelle

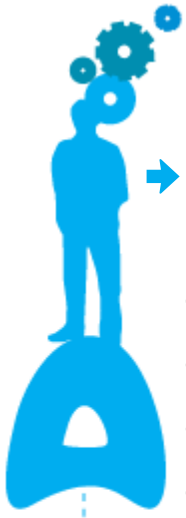


06. Monitoring du datacenter
Gestion des alarmes

- Configuration et gestion des alarmes sur tous les composants du datacenter
  - Serveur, VM : CPU, mémoire, disque et réseau
  - État des serveurs et des VM
- Actions :
  - Envoi d'un email
  - Envoi d'une trap snmp
  - Lancement d'un script
  - Changement d'état (on/off) d'une VM

Host connection state
Host CPU Usage
Host Memory Usage
Virtual Machine CPU Usage
Virtual Machine Memory Usage





Notes

06. Fonctionnalités additionnelles

- Marketplace
- Guided Consolidation
- Capacity Planner
- VMware Converter
- VMware Update Manager

07. Fonctionnalités additionnelles
Marketplace

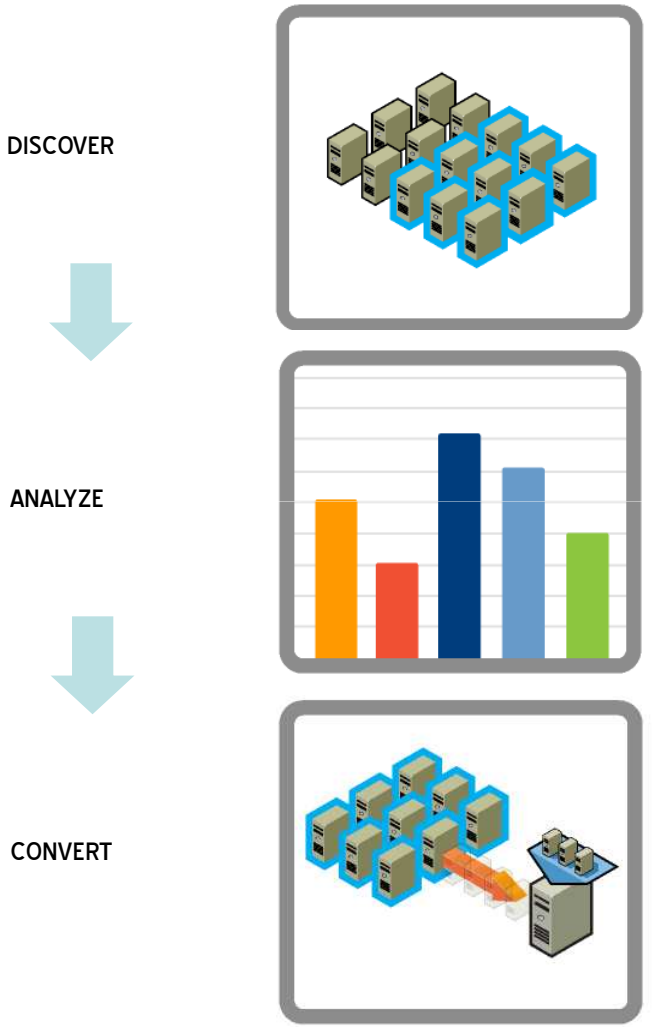
Virtual Appliance Marketplace

- Déploiement de machine virtuelle préconfigurée.
- Import depuis un fichier, Virtual Appliance Marketplace, Intranet.
- Export de VM au format OVF

07. Fonctionnalités additionnelles
Guided Consolidation

Consolidation assistée

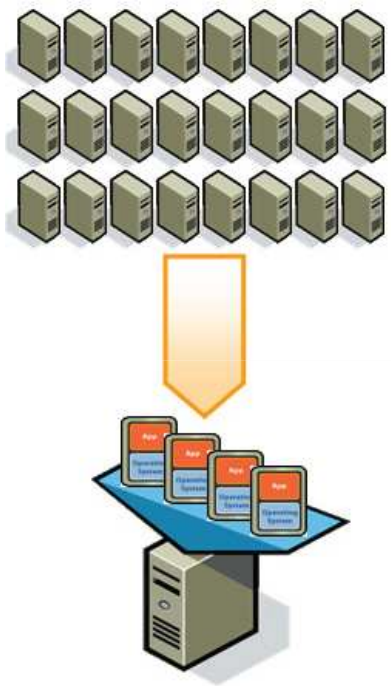
- Découvre automatiquement les serveurs physiques.
- Collecte de données de performance à partir de ces serveurs.
- Converti les serveurs en VM qui sont intelligemment migrés sur l'ESX le plus approprié.



07. Fonctionnalités additionnelles
Capacity Planner

Consolidation de serveurs

- Analyse de la charge et de l'utilisation de votre infrastructure
- Monitoring des ressources
- Décision du scénario de consolidation

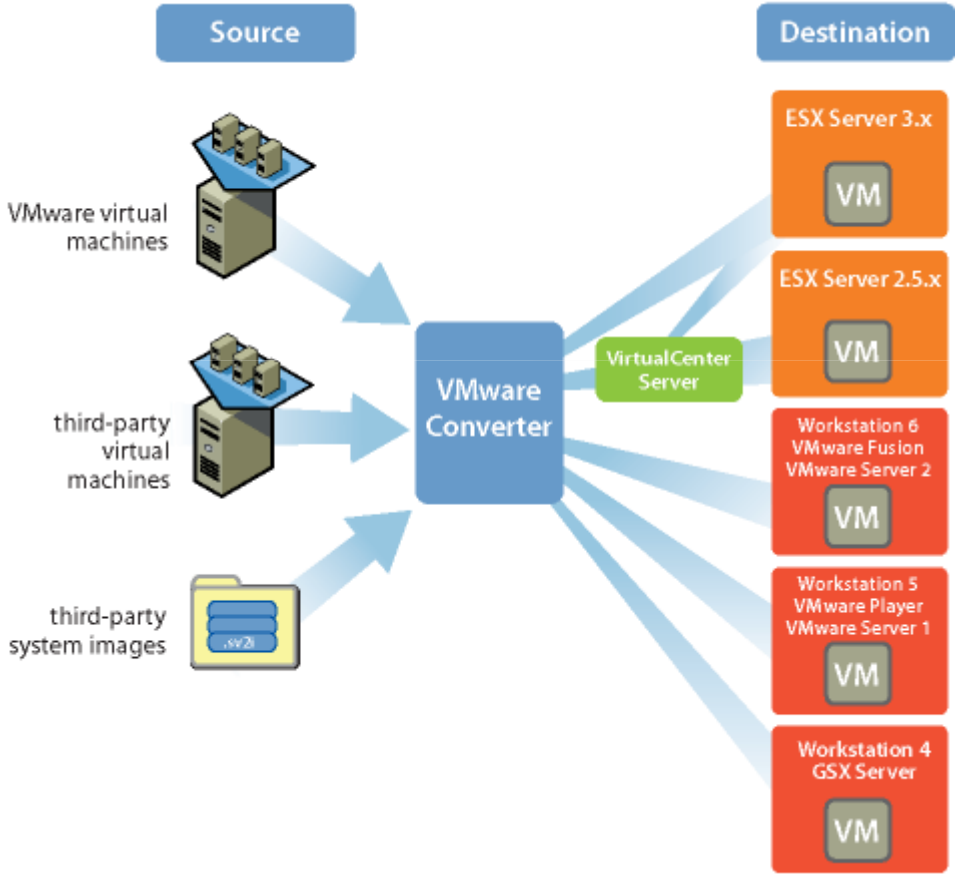


Physical Computer	CPU Info	Memory Info	Status	Confidence	CPU Usage	Memory Usage
VC35	1 x 2,0 GHz	2 GB	Ready for consolidation	High	47 MHz	709 MB

07. Fonctionnalités additionnelles
VMware Converter

Virtualisation/Importation

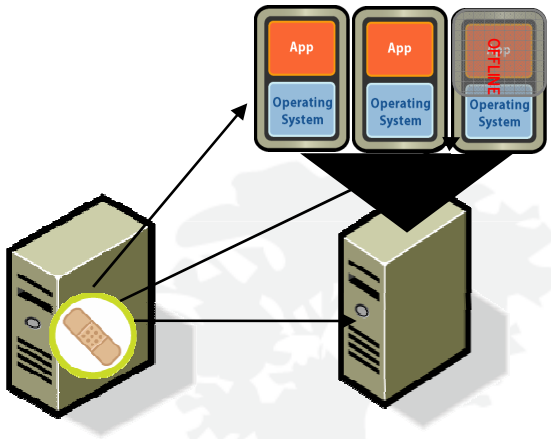
- Conversion de machine Physique en VM (P2V)
- Import de VM vers un ESX (V2V)
- Import de sauvegardes VCB
- Import d'images de logiciels tiers (Virtual Server, Backup Exec System Recovery, Norton Ghost 10)



07. Fonctionnalités additionnelles
VMware Update Manager (1/2)

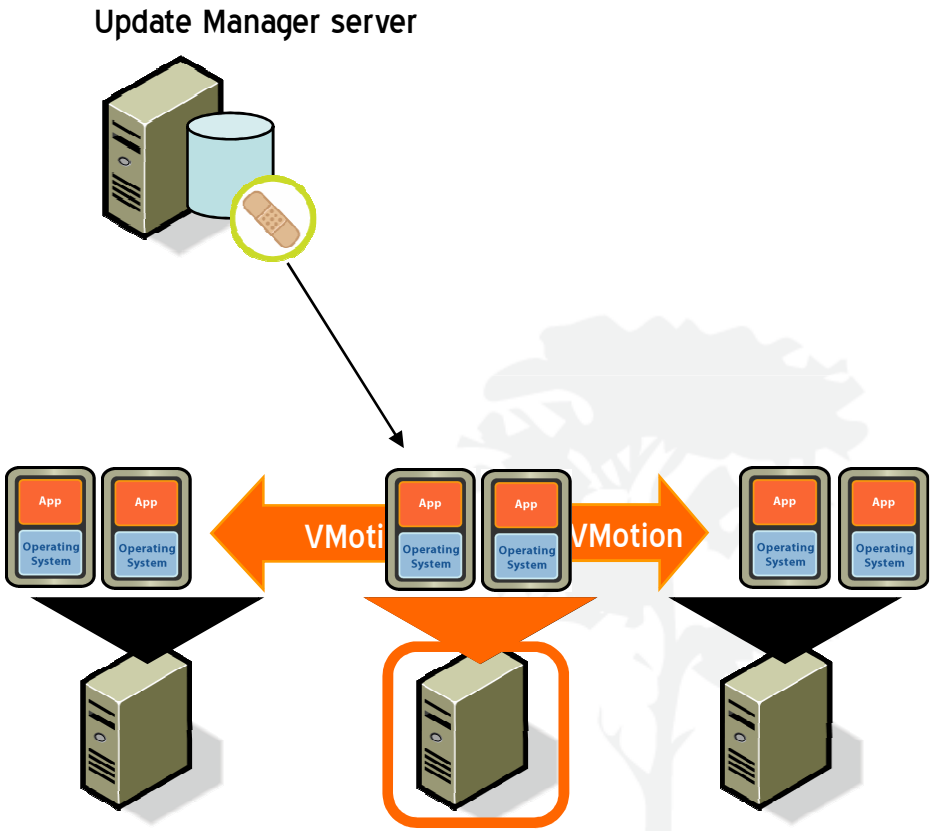
Gestion des patchs de votre infrastructure

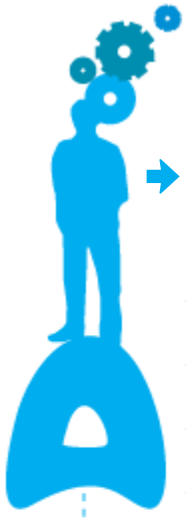
- Update Manager va être capable de gérer les mises à jour pour les ESX, les OS des VM (Windows, RedHat) et les applications tiers (Adobe Macromedia etc.)
- Il est possible de faire un snapshot avant la mise à jour et ainsi l'annuler en cas de problème.
- La gestion des mises à jour s'effectue par groupe (Baseline).



07. Fonctionnalités additionnelles
VMware Update Manager (2/2)

- Chaque ESX du cluster entre successivement en mode maintenance.
- Les VM sont alors migrées sur les autres ESX.
- L'ESX est mis à jour et est redémarré si nécessaire.
- Les VM sont replacées à leur emplacement initial.
- L'ESX suivant est sélectionné.





Notes

Avolys

Accompagnateur de changement