

Différences entre vSphere 5.x et vSphere 6

Le nom « vSphere » est apparu vers la mi-2009, date de disponibilité de la version majeure succédant à Virtual Infrastructure version 3.5 (en référence à la version des hyperviseurs ESX). Selon VMware, vSphere est le système d'exploitation du datacenter et la base des environnements de cloud computing. Énormément de produits fonctionnent dans l'écosystème vSphere sous forme de modules additionnels connectés à vCenter (fonctionnalités supplémentaires ou produits complets). Depuis le 12 mars 2015 est sortie la nouvelle version de vSphere : VMware vSphere 6. Contrairement aux précédentes versions, la sortie du produit a été précédée d'une longue période de tests bêta, divisée en deux phases.

La première était une bêta privée ouverte aux internes VMware, à certains clients et aux instructeurs (VCI - *VMware Certified Instructors*). Elle a commencé au deuxième trimestre de l'année 2014.

La deuxième phase bêta avait une particularité : elle était ouverte au public. Une phase bêta ouverte au public, mais non publique. La subtilité est en fait assez simple à comprendre : il était possible pour n'importe qui de s'inscrire mais les informations échangées n'étaient pas publiques. En cas de sélection, VMware envoyait un accès aux téléchargements, forum et « labs en ligne ». Les discussions concernant les produits pouvaient avoir lieu entre bêta-testeurs mais devaient rester privées.

Il nous était interdit de révéler quoi que ce soit sur ce que nous apprenions sur les produits avant la date de GA (*General Availability* - disponibilité au public). La version 6.5 de vSphere a été rendu publique le 15 novembre 2016.

1. Les changements

Les principaux composants que sont vCenter, Update Manager et l'hyperviseur ESXi sont maintenant en version 6 et 6.5.

ESX : depuis vSphere 5.0, il n'y a en fait plus de version ESX mais uniquement ESXi. À ce propos, il sera fait allusion à ESXi à chaque fois que le terme ESX sera cité. Le fait de ne pas utiliser de service console apporte un avantage en termes d'*overhead* mais présente un inconvénient majeur : toutes les commandes sont exécutées directement sur l'hyperviseur, c'est pourquoi la sécurité a été renforcée notamment via le mode de verrouillage (*lockdown* et *strict lockdown*).



La quantité de ressources utilisée par le système et donc non disponible pour les machines virtuelles est appelée *overhead*. L'*overhead* représente le « coût » de la virtualisation.

Dans le cas de connexions à distance, les modes *technical support* ainsi que la connexion SSH sont toujours disponibles mais les commandes sont limitées. Il convient d'utiliser le vMA (*vSphere Management Appliance*) ainsi que la PowerCLI qui permettent respectivement de passer des commandes VMware et des commandes PowerShell de manière centralisée vers les serveurs hôtes. Ces modes de connexions sont pleinement supportés par VMware et peuvent être utilisés pour des actions courantes contrairement au bien nommé *technical support mode* (support technique). Les modes sus-cités présentent quelques changements dans leur fonctionnement :

- Il est désormais possible de gérer les comptes locaux d'un hyperviseur ESXi en ligne de commande (à partir de la vMA) via des nouvelles commandes `esxcli`.
- Le blocage des comptes est permis au-delà d'un certain nombre de tentatives de connexion. Le nombre d'essais avant blocage ainsi que la durée de blocage sont configurables et concernent les connexions SSH et vSphere Web Services. On peut rapprocher ceci du logiciel fail2ban des systèmes Linux, à ceci près que fail2ban bloque des adresses IP, et ESXi bloque des comptes.

Pour plus de renseignements sur le fonctionnement de fail2ban, consultez le lien suivant : http://www.fail2ban.org/wiki/index.php/FAQ_french

Le DCUI (*Direct Console User Interface*) permet de redémarrer les services de gestion, et récupérer les logs en plus d'actions de configuration basiques (nom, interface de gestion, etc.).

L'accès au DCUI peut être bloqué via le mode de verrouillage (*lockdown mode*) selon deux modes :

- Le mode normal (*normal lockdown mode*) : DCUI fonctionne mais seuls certains comptes peuvent y accéder. Ces comptes doivent être entrés dans la liste DCUI.access.
- Le mode strict (*strict lockdown mode*) : DCUI est arrêté.

vCenter Server : il existe depuis vSphere 5 une version Linux sous forme d'appliance virtuelle. La distribution utilisée est SUSE Linux Enterprise Server (SLES) 11. Le serveur vCenter peut gérer des serveurs ESX et ESXi des versions 4 à 6. Certaines fonctionnalités ne sont par contre pas supportées, comme la connexion à une base de données Microsoft SQL Server, Microsoft ne fournissant pas de client SQL pour Linux.

Le cas du vCSA 6.5 est quelque peu différent car le système d'exploitation est Photon OS, qui permet d'exploiter le vCenter 6.5 sous forme de container.

La mise à jour de vCenter ne passe pas obligatoirement par une nouvelle installation comme ce fut le cas pour le passage de v4.0 à v4.1 ; vCenter passait de 32 bits à 64 bits. Ce qu'on appelle « on-place upgrade », c'est-à-dire une mise à jour à même le système, est possible et supporté à partir de vCenter 5.5. La version 6.0 de vCenter introduisant des changements internes, les processus de mise à jour doivent être validés avec VMware (via la base de connaissance, guides de mise à jour, ou le support).

Ne perdons pas de vue que vCenter a la charge des calculs d'équilibrage de charge via DRS (*Distributed Resource Scheduler*). Pendant l'indisponibilité de vCenter, aucune migration à chaud (vMotion) ne sera déclenchée. Dans le cas où la mise à jour de vCenter doit intervenir en production, veillez à l'effectuer pendant des heures creuses et de ne commencer qu'à partir du moment où le cluster DRS est équilibré (balanced cluster).

- Le format de fichier propriétaire VMFS en version 6 permet d'utiliser des volumes de 64 téraoctets. Le formatage se fait uniquement sur une taille de bloc de 1 Mo, comme VMFS 5 et contrairement à VMFS v3 qui pouvait utiliser des tailles de 1, 2, 4 et 8 Mo. Cela conditionnait la taille maximale d'un fichier qu'il était possible de stocker sur le volume. La taille de bloc est héritée dans le cas d'une mise à jour à partir de VMFS v3.x. La mise à jour des partitions VMFS peut se faire simplement en déplaçant les machines virtuelles (à froid ou à chaud) et en reformatant la partition en VMFS. Il est aussi possible de faire la mise à jour du système de fichier à chaud, sans reformatage. À ce moment-là, il ne faut pas oublier que nous conservons les caractéristiques du VMFS 3.x à savoir la taille de bloc (1, 2, 4 ou 8 Mo) et la gestion dite « legacy » en MBR (*Master Boot Record*). Le passage en GPT se fait quand on dépasse 2 To. vSphere 6 utilise VMFS en version 5.61. La situation est ainsi similaire au passage de Virtual Infrastructure à vSphere (4) : le système de fichier VMFS a subi une mise à jour mineure.
- Le client vSphere 6 permet de gérer l'infrastructure virtualisée si les produits vSphere 6 sont utilisés. Si le client est plus récent que les serveurs gérés, le client proposera un téléchargement des binaires correspondants aux anciennes versions.
- Il y a maintenant deux clients d'administration en plus du vSphere Web Client : vSphere Client et vSphere Host Client. Le vSphere Client correspond à l'ancien client (développé en C#) pour Windows, qui pouvait être utilisé pour se connecter à un hyperviseur ou vCenter. Le Host Client reprend l'ergonomie du vSphere Web Client mais permet la connexion directe à un hyperviseur ESXi. En fait, on peut considérer qu'il y a un client supplémentaire pour la gestion d'un hyperviseur ESXi : le client web embarqué en HTML5. Ce client provient des VMware flings, qui représentent des projets d'ingénieurs et développeurs VMware. Ils ne sont pas officiellement supportés pour des environnements de production mais préfigurent des fonctionnalités des prochaines versions. Pour plus de renseignements sur les VMware flings, vous pouvez consulter le site suivant : <https://labs.vmware.com>. En ce qui concerne le client HTML 5 en particulier, ce post de William Lam indique clairement comment le mettre en place : <http://www.virtuallyghetto.com/2015/08/new-html5-embedded-host-client-for-esxi.html>
- Lors de la phase bêta, une version dite RC (pour *Release Candidate*, assez proche de la version finale) proposait le « vSphere Host Client for Mac ». Ce client est l'équivalent du client vSphere pour les systèmes Macintosh (OSX). Lors de la GA (*General Availability* ou sortie officielle), ce composant n'était plus disponible au téléchargement.

- Les clusters de haute disponibilité (HA ou *High Availability*) et d'équilibrage de charge (DRS pour *Distributed Resource Scheduler*) supportent maintenant jusqu'à 64 nœuds (ESXi) contre 32 précédemment.

2. Les nouveautés

vSphere 6 et 6.5, en plus d'induire de nombreux changements au niveau des composants déjà connus, apportent leurs lots de nouveautés :

- Format de machine virtuelle

Le format de machine virtuelle en version 11 (uniquement compatible avec vSphere 6) permet le support de 128 HEC et 4 téraoctets de mémoire vive, une meilleure accélération graphique et des améliorations concernant le nombre de ports série : une machine virtuelle peut comporter jusqu'à 32 ports série virtuels. La version du format de machine virtuelle apportée par vSphere 6.5 est la version 13. Elle permet d'avoir jusqu'à 6 téraoctets de mémoire vive et donne l'accès à 4 contrôleurs NVMe.



On parle de HEC plutôt que de vCPU (processeurs virtuels) pour éviter les confusions. En fait, un HEC (Hardware Execution Context) correspond à la possibilité de gérer une file d'instructions, donc en fait un cœur de processeur. On pourra donc parler de vCPU comportant plusieurs cœurs virtuels.

- Prise en charge d'UEFI (depuis vSphere 5)

L'UEFI (*Unified Extended Firmware Interface*) est le remplaçant du BIOS. Certains systèmes utilisent l'EFI pour démarrer, comme Mac OS X.



Mac OS X utilise EFI dans le cas où il s'agit de versions pour processeurs Intel (x86), donc à partir de la version Leopard 10.5. Les versions précédentes utilisaient Open Firmware (Mac OS X pour processeurs Power PC).

La prise en charge se fait à deux niveaux : un serveur ESXi peut démarrer en utilisant EFI. Ainsi il pourra utiliser un lecteur de disque optique, une clé USB ou un disque dur. Le démarrage par la carte réseau n'est pris en charge qu'en cas d'utilisation du BIOS.



Il n'est pas possible de changer de BIOS à uefi après l'installation d'ESXi, sous peine de démarrer un ESXi qui ne reconnaît pas sa partition principale.

Une machine virtuelle peut aussi utiliser EFI en lieu et place du BIOS. Ce sera utile pour créer des machines virtuelles Mac OS X (OSX Yosemite 10.10 est supporté). Le choix du type de firmware (EFI ou BIOS) se fait dans les propriétés de démarrage la machine virtuelle.

- vSphere Storage DRS

Storage DRS (*Distributed Resource Scheduler*) utilise Storage vMotion pour déplacer les fichiers de machines virtuelles à chaud, afin d'équilibrer l'utilisation des différentes banques de données vSphere. vSphere Storage DRS prend maintenant en charge les caractéristiques des baies de stockage grâce aux API de type VASA (*vSphere API for Storage Awareness*). Les fichiers de machines virtuelles ne sont ainsi pas déplacés sur des datastores n'étant pas dédoublés. L'autotiering des baies de stockage est pris en charge.



Le tiering est une fonction présente dans beaucoup de baies de stockage modernes et permet le classement de différentes classes (tiers) de stockage (SSD, disques SAS 15 000 tours par minute, disques SATA 7200 tours par minute) et surtout la migration dynamique des données entre les différents tiers selon l'utilisation. (On parle souvent de données « chaudes » sur les SSD et de données plus « froides » sur les autres tiers.)

- Profils de stockage

Cette nouvelle fonctionnalité permet de classer le stockage selon le niveau de service fourni. Il devient possible de mettre en place des catégories de machines virtuelles selon la rapidité du stockage associé, et d'y placer les fichiers disques des machines virtuelles selon les classes définies.

- Contrôle de l'entrée/sortie réseau en version 3

De nouveaux contrôles permettent de suivre plus efficacement l'utilisation de l'infrastructure vSphere au niveau des cartes réseau virtuelles (au niveau de la machine virtuelle) et des cartes réseau physiques (les vmnics).

- Contrôle des entrées/sorties stockage amélioré

Le contrôle des entrées/sorties est maintenant étendu aux banques de données NFS (*Network File System*).

- Améliorations des commutateurs virtuels distribués (dvswitches)

Les vSwitches distribués prennent en charge Netflow, SPAN (*Switched Port Analyzer*), RSPAN (*Remote Switched Port Analyzer*), ERSPAN (*Encapsulated Remote Switched Port Analyzer*) et LLDP (*Link Layer Discovery Protocol*). CDP (*Cisco Discovery Protocol*) est toujours pris en charge par les vSwitches standards.

- VMware HA (*High Availability*, haute disponibilité) repensé

La fonctionnalité vSphere HA ne dépend plus de la résolution de nom (DNS). La notion de serveurs primaires et secondaires a été complètement redéveloppée. vSphere HA ne dépend plus de l'agent Legato comme précédemment. Il s'agit maintenant d'un composant, développé par VMware. HA se base aussi sur l'accès aux banques de données via les « heartbeat datastores ». Ceci correspond au fonctionnement depuis la version 5.0. Avec la version vSphere 6.5, HA prend aussi en charge les réservations au niveau réseau. Ainsi, si un hyperviseur ne peut garantir une réservation réseau configurée pour une machine virtuelle, celle-ci devra démarrer sur un autre hyperviseur.

- vSphere vMotion amélioré

vMotion peut désormais être utilisé entre deux sites distants. Les latences de l'ordre de 100 ms sont supportées. Les migrations vMotion sont aussi supportées d'un système vCenter à un autre si les deux vCenter sont enregistrés dans la même base SSO (via le mode lié amélioré).

- Pare-feu intégré à ESXi

Les versions précédentes d'ESXi ne disposaient pas d'un pare-feu, contrairement à ESX. ESXi, depuis la version 5, inclut un pare-feu stateless, auquel on peut ajouter des services.

- Client web vSphere

Le client web, bien que nettement plus rapide que les versions précédentes, est toujours basé sur Adobe Flash. Le

client vSphere (pour Windows) est toujours supporté.

- VMDirectPath I/O version 2

VmDirectPath I/O sur ESXi supporte vMotion depuis vSphere 5.

Depuis vSphere 5.1, un nouveau composant est obligatoire. Il s'agit de la base de données d'authentification unique (vCenter Single Sign On database).

La base de données SSO permet de centraliser l'authentification de tous les composants de la suite vCloud (vCloud Suite).

Précédemment, l'authentification pouvait se faire directement sur l'Active Directory (dans le cas où vCenter était relié au domaine) ou grâce à la base de compte locale, que ce soit vCenter pour Windows ou VCSA (*vCenter Server Appliance*). Aujourd'hui, la base de données SSO permet de créer un domaine de sécurité pouvant être configuré avec plusieurs sources telles que Active Directory ou OpenLDAP.

Chaque authentification donne lieu à une génération de jeton de sécurité délivré par la base de données SSO qui sera utilisé pour s'authentifier sur les différents services : vCenter, vCenter Orchestrator, Site Recovery Manager ou vCloud Director. La base de données SSO est un composant essentiel du nouveau client web (*Web Client*) qui fonctionne sur le même principe que pour les anciennes versions en éliminant leurs limitations : en effet, Web Client offre la possibilité de gérer la totalité de l'infrastructure vSphere à partir d'un simple navigateur web.

- PSC

Cette base SSO est désormais contenue dans ce qu'on appelle le PSC pour *Platform Services Controller*. Le PSC peut être utilisé embarqué sur la même machine que vCenter ou sur une autre machine.

En cas de déploiement de VCSA, chaque appliance peut avoir le rôle de PSC, de vCenter ou des deux.

Le PSC contient les services suivants :

- La base SSO
- Le serveur de licences VMware
- Le service lookup
- Une autorité de certification
- Un magasin de certificats

Les services de certificats sont nouveaux et exclusifs à vSphere 6. La gestion des licences est une version mise à jour des anciens services. Les autres services sont inchangés vis-à-vis de la version précédente.