h e p i a
Haute école du paysage, d'ingénierie
et d'architecture de Genève

Hes·SO GENÈVE
Haute Ecole Spécialisée
de Suisse occidentale

YOUR VIRTUAL WORKSTATION, ANYWHERE, ANYTIME

Travail de Bachelor réalisé par

Monsieur Karim Korso

pour l'obtention du titre Bachelor of Science HES-SO en
Ingénierie des technologies de l'information avec orientation en

Communications, multimédia et réseaux

Suivi par M. Gérald Litzistorf, professeur HES
et par M. Sylvain Liaudat, directeur adjoint au SIACG

Septembre 2014

Projet de virtualisation du poste de travail dans le cadre de mon travail de Bachelor, afin d'accéder aux ressources communales depuis l'intérieur du réseau intercommunal ainsi que depuis l'Internet.

11.08.2014

Énoncé

INGÉNIERIE DES TECHNOLOGIES DE L'INFORMATION

ORIENTATION - COMMUNICATIONS, MULTIMEDIA ET RESEAUX

YOUR VIRTUAL WORKSTATION, ANYWHERE, ANYTIME

Descriptif :

Ce travail proposé par le Service d'Informatique de l'Association des Communes Genevoises (SIACG), concerne l'accès distant des cadres et membres de l'exécutif au système d'information.

Il doit tenir compte des éléments suivants : mobilité, accès depuis l'extérieur du réseau, variétés des plateformes (Windows, Apple, Android, …) et sécurité

SIACG impose une solution virtualisée basée sur des produits VMware et met à disposition le matériel et les licences logicielles.

Ce travail fait suite au projet de semestre http://www.tdeig.ch/windows/Korso_EPS.pdf

Travail demandé :

Cette étude comprend les étapes suivantes :

1. Spécifier l'interface utilisateur (authentification, applications disponibles, accès aux données)
2. Analyser les risques
3. Définir les principaux tests unitaires
4. Expliquer les fonctionnalités VMware utilisées (pool, template, …) et les choix effectués (clone, …)
5. Installer et configurer Vcenter et Horizon View
6. Expliquer le processus de création depuis le fichier iso de Win7 jusqu'à la VM mise à disposition
7. Effectuer les tests unitaires du §3
8. Spécifier et réaliser une phase pilote puis adapter en fonction du retour utilisateurs
9. Valider l'analyse des risques du §2
10. Définir les données confidentielles qui ne font pas partie du rapport public
11. Analyser la solution VMware Virtual SAN

Sous réserve de modification en cours du travail de Bachelor

Candidat :
M. KORSO KARIM
Filière d'études : ITI

Professeur(s) responsable(s) :
Litzistorf Gérald

En collaboration avec : SIACG
Travail de bachelor soumis à une convention de stage en entreprise : non
Travail de bachelor soumis à un contrat de confidentialité : oui

Timbre de la direction

Remerciements

Je souhaite remercier l'ensemble des personnes qui m'ont accompagné tout au long de ce projet, tout particulièrement les personnes suivantes :

M. Liaudat Sylvain, chef de service adjoint du service informatique des communes genevoises, pour m'avoir donné l'opportunité de réaliser un projet aussi diversifié qu'intéressant. De plus, il a su m'aiguiller et me conseiller autant sur la partie technique que sur la partie documentation.

M. Clarke Samuel, Ingénieur système R&T, pour la partie réseau, notamment la configuration des VLAN, du commutateur distribué ainsi que SAN FC.

M Litzistorf Gérald, professeur responsable du projet de Bachelor, pour le suivi ainsi que les précieux conseils donnés tout au long du projet. Par ailleurs, je souhaite aussi le remercier pour le temps qu'il m'a consacré.

Enfin je souhaite remercier mon employeur pour la confiance et le temps consacré à la réalisation de ce projet.

Table des matières

Table des figures

1 Introduction

Mon projet de Bachelor consiste à mettre en place une solution VDI[1] avec VMware Horizon view[2] 5.3. Elle rendra possible l'accès aux ressources informatiques des communes genevoises depuis l'intérieur et l'extérieur du réseau intercommunal. Cette prestation est exclusivement réservée aux cadres et à l'exécutif des communes genevoises.

À l'occasion de mon travail de semestre, j'ai pu, lors d'une première étude, faire l'analyse de faisabilité du projet. Il s'agissait de dimensionner l'infrastructure pour environ 200 utilisateurs et valider les performances sur notre environnement de test. Les documents s'y rapportant se trouvent aux adresses suivantes :

Énoncé :

http://www.tdeig.ch/windows/Korso_EPS.pdf

Rapport :

http://www.tdeig.ch/windows/Korso_RPS.pdf

Ce travail en amont m'a permis de prendre en compte les paramètres de configuration ainsi que les aspects liés à la virtualisation.

Dans ce document, la première partie décrit mes choix techniques tels que la mise à jour de l'image de base Windows 7, les profils itinérants, la configuration et l'allocation des pools. Une deuxième partie sera consacrée à l'analyse de la solution de virtualisation de SAN (VMware).

En complément, j'ai suivi une formation VMware Horizon View 5.2 « Installe, manage, and configure » de 4 jours et VMware vSphere 5.5: « Install, Configure, Manage » de 5 jours afin de renforcer mes connaissances sur le produit et de pouvoir d'installer le produit et mieux comprendre les différents rôles de chaque composant.

Tout au long du document et afin de faciliter la compréhension, je vous invite à vous référer au schéma du chapitre 2.1 « Schéma fonctionnel global». Les différents rôles de chacun des éléments sont renseignés à l'aide d'une numérotation sous forme de pastilles bleues. (1)

[1]Virtual desktop infrastructure : Infrastructure de postes de travail virtuel.
http://fr.wikipedia.org/wiki/Virtual_Desktop_Infrastructure
[2]VMware Horizon View : Produit de VMware proposant la virtualisation de poste de travail.
http://www.vmware.com/fr/products/horizon-view/

2 Analyse

2.1 Schéma fonctionnel global

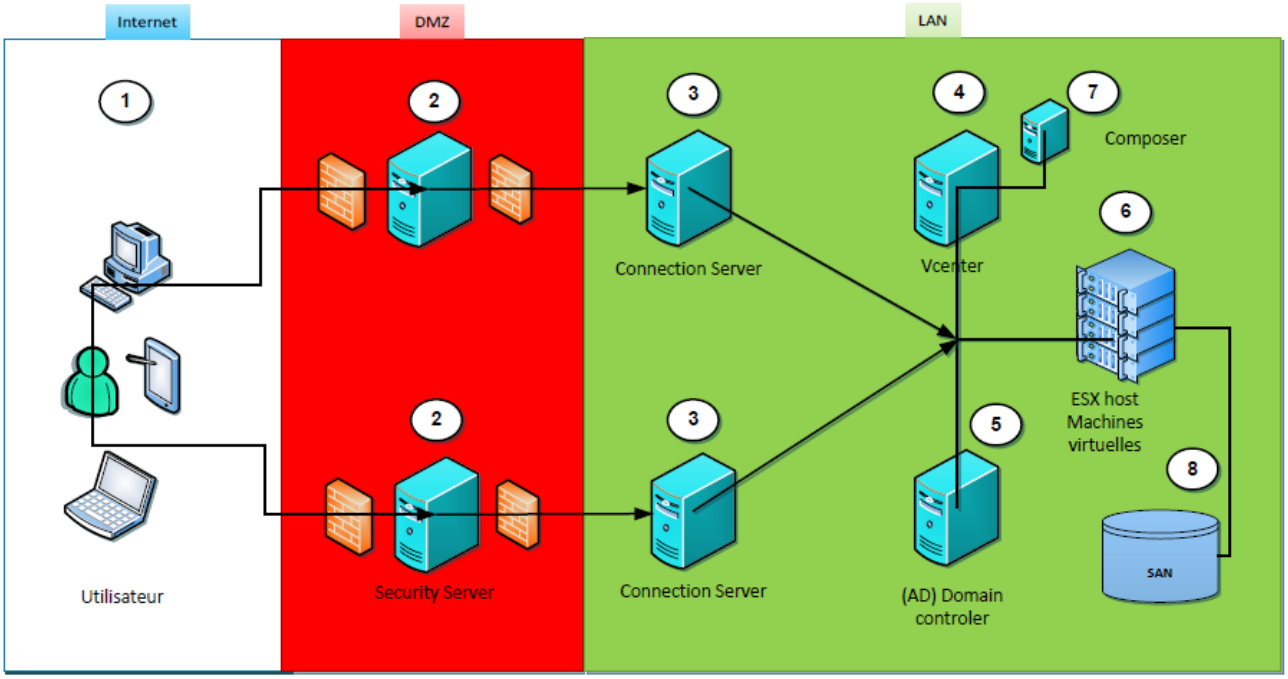


Figure 1 - Schéma fonctionnel global

1. Utilisateur
2. Security Server : serveurs frontaux isolés du LAN entre 2 firewalls (DMZ)
3. Connection Server : ces serveurs gèrent l'authentification des utilisateurs, l'autorisation aux différents pools et d'autres fonctionnalités telle que l'attribution d'application avec ThinApp
4. Vcenter : permet l'administration de la ferme d'ESX
5. Domain controler : annuaire pour l'authentification des utilisateurs, comptes ordinateur des VM, comptes de service pour VMware, stratégie de groupe pour persona management
6. ESX host : cluster de serveur matériel accueillant les machines virtuelles
7. Composer : permet l'utilisation des clones liés
8. Stockage SAN : Espace de stockage sur SAN pour les ESX

2.2 Schéma fonctionnel stockage 8

Ci-dessous une vue du stockage des différents éléments du clone lié :

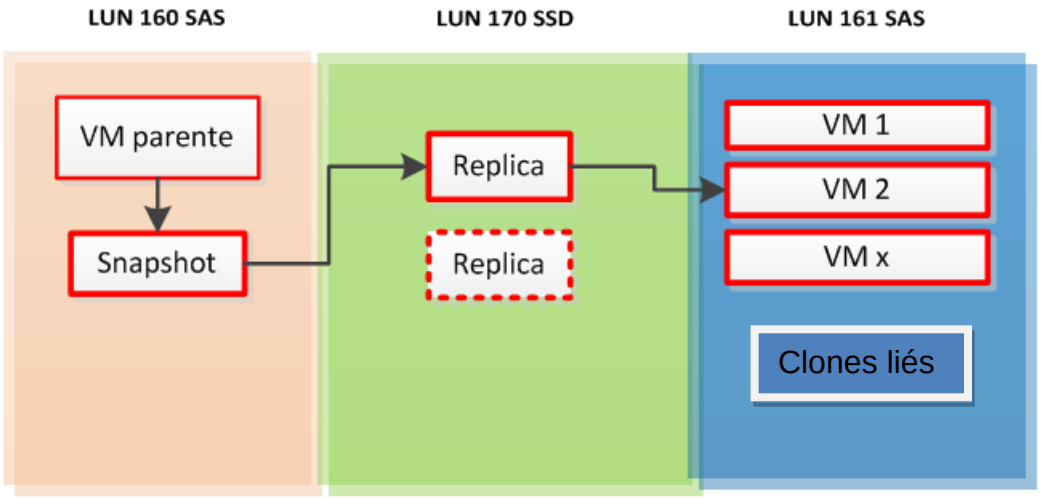


Figure 2 - Schéma fonctionnel stockage

La VM parente[3] ainsi que les clones liés[4] sont stockés sur des disques de type SAS, mais sur 2 LUN séparés. Quant au(x) replica[5](s), ils seront stockés sur SSD.

[3] VM parente : Ceci est la VM de référence. Un snapshot est réalisé puis cloné pour le replica.
[4] Clones liés : VM's générées à partir du replica.
[5] Replica : Copie de la VM parente qui va être utilisée comme image de base pour les clones liés.

2.3 Schéma fonctionnel Pool VMware

Le schéma vous présente les différentes possibilités d'affectation et de création de VM lors de la définition d'un pool. Le chemin en rouge vous montre la solution que j'ai choisie, étant à mon sens la plus adaptée à nos besoins. Cette configuration a en effet l'avantage d'économiser de l'espace disque et du temps en maintenance des VM.

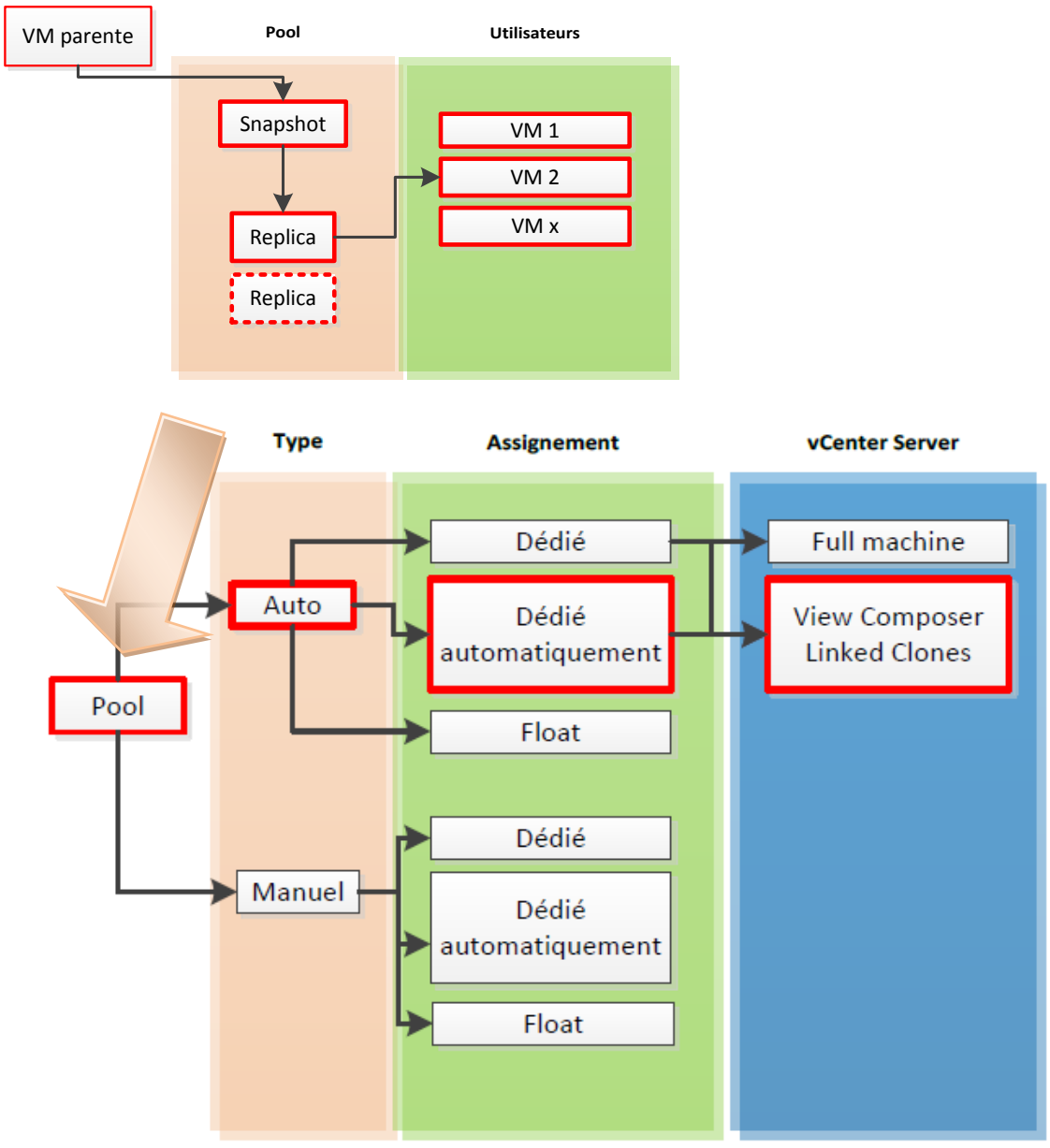


Figure 3 - Schéma fonctionnel pool

2.4 Choix technique

2.4.1 Type de VM

Les VM seront de type clone lié. Elles se basent sur une VM parente, mais en étant toujours liées à celle-ci, contrairement aux machines dites « Full machine virtual » qui ont chacune leur image (Nombres de VM x la taille du template) et qui ensuite sont indépendantes.

Afin de bénéficier de cette technologie, le rôle VMware View Composer[6] 7 sera installé sur le même serveur que VCenter. La contrainte principale du clone lié est de devoir acquérir des disques performants type SSD, donc coûteux. Toutes les vm's du pool[7] peuvent accéder à l'image replica qui génère un nombre élevé d'accès disque, appelé aussi I/O[8]. La partie delta peut être stockée sur des disques plus lents type NL-SAS ou SAS.

2.4.2 Processus de mises à jour

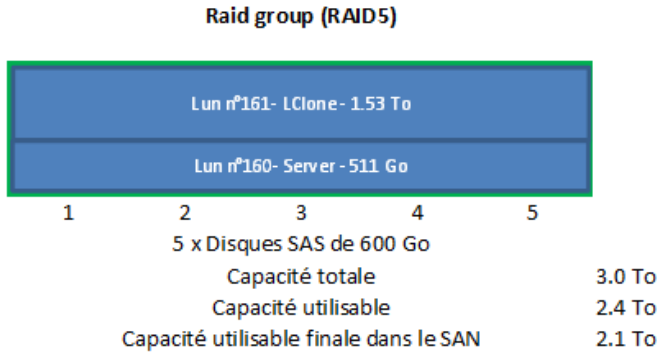
Le gain de temps de maintenance des versions du template se révèle proportionnel au nombre de VM dans le pool. Plus il y a de VM et plus le gain est important. Par exemple, une mise à jour consiste à régénérer un snapshot (recompose) et de le mettre à disposition du pool. Lorsque les prochains utilisateurs se connecteront sur leur poste 1, ils auront ainsi la dernière version de l'image. Comme préconisé par la norme ITIL[9], je vais installer trois environnements sous forme de trois pool :

- Pool de test
  - Utilisé par l'administrateur VMware, 1ers tests techniques.
- Pool validation
  - Utilisé par un groupe « pilote » représentant des utilisateurs.
- Pool production
  - Une fois approuvé sur le pool validation, les utilisateurs sont avertis d'une maintenance et le template est appliqué à la production.

[6] VMware View Composer : utilisé pour le clone lié
[7] Pool : groupe de VM. Des stratégies y sont appliquées (Nombre de VM provisionnées, etc.)
[8] I/O : Entrée / Sortie, nombre d'échanges d'informations entre le CPU et les périphériques
[9] ITIL : Normes de bonnes pratiques. Principalement pour le domaine de l'informatique

2.4.3 Stockage 8

Au niveau du « datastore » (espace de stockage présenté à VMware), j'ai créé 2 RAID5 distincts sur le SAN. Le premier RAID est composé de 5 disques SAS et contient 2 LUN. Le LUN n°161 sera utilisé pour stocker les deltas de chaque VM ainsi que leurs fichiers temporaires. À noter que chaque VM se détruit à chaque fermeture de session et donc libère de la place sur le LUN. Le template, la machine de référence et les différents serveurs seront placés dans le LUN n°160.



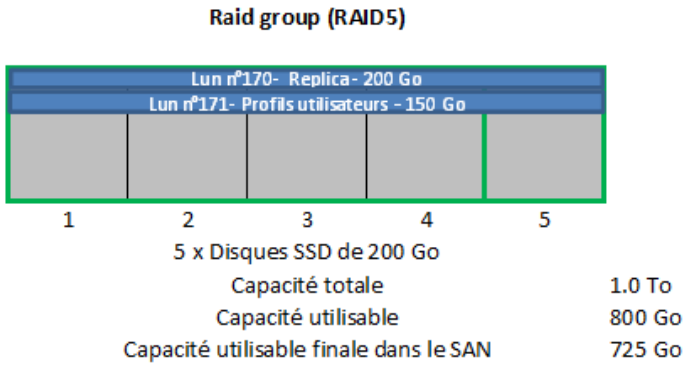
LClone = Linked Clone

Figure 4 - LUN clones, Servers

Vue du pool au niveau SAN :

Pool 10 - s1 - vdi	Ready	RAID5	SAS	2143.178	2138.168	5.010	

Le deuxième RAID est composé de 5 disques SSD. Il sera composé de 2 LUN. Le LUN n°170 est destiné au(x) replica, Le LUN n°171 est destiné aux profils utilisateurs (persona management)



A noter que l'espace disque n'a pas été entièrement alloué car les deux LUN (170, 171) sont déjà surdimensionnés.
L'espace libre pourra être utilisé pour d'autres fonctionnalités futures.

Figure 5 - LUN Replica, profils

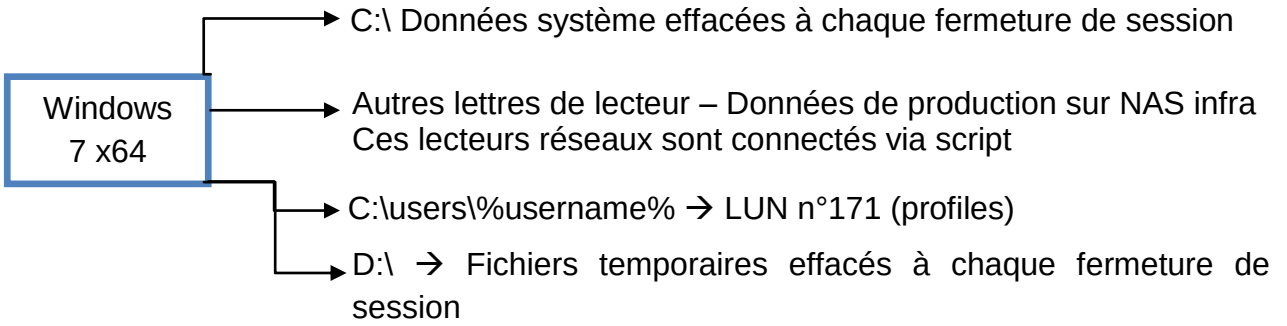
Vue du pool au niveau SAN :

Pool 9 - s1 - vdi	Ready	RAID5	SAS Flash	730.424	725.414	5.010	

La vue des datastores au niveau VMware :

Figure 6 - LUN's

Les quatre datastores sont formatées en VMFS-5. A noter que les données de production sont sur NAS dans notre infrastructure. Aucune donnée ne sera présente sur les VM.



La partition D:\ n'est pas obligatoire mais comporte un réel gain de stockage car à chaque déconnexion ce disque est vidé. Le RAID5 est un bon compromis entre performance et sécurité. Sur les 5 disques, on peut perdre un disque. On garantit ainsi le bon fonctionnement du système. À savoir qu'il y a également un disque de spare en attente sur le SAN. Concernant le débit entre les ESX (6) et le stockage (8), il y a 2 liens FC (Fiber Channel) 8Gbit/s (réseau SAN). Ces 2 liens sont redondants (multipathing[10]) en mode actif /passif.

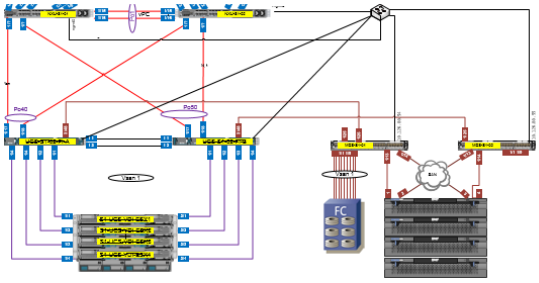


Figure 7 - schéma réseau SAN

À noter que les LUN sont répliqués en mode synchrone dans 2 salles informatiques différentes.

[10] Multipathing : consiste à mettre en place deux liens physiques différents pour accéder à l'infrastructure donnée.

2.4.3.1 Dimensionnement des LUN

Vue virtuelle, vue physique

Il est important de bien dimensionner les LUN; à savoir que l'espace présenté à VMware n'est pas plus élevé que celui des disques physiques. Dans le cas où l'espace physique est dépassé, les VM s'arrêtent. J'ai rencontré ce cas dans le cadre de notre environnement de test. 6 To étaient présentés alors que 1.6 To étaient réellement disponibles sur le LUN.

Pour ne pas avoir de surprise de dépassement d'espace disque, il est nécessaire de présenter la réalité de la capacité disque à VMware, les LUN sont créés en mode « Thick Provisioning ».

Nombre de LUN, risques, avantages et inconvénients

Un seul LUN a été créé afin d'accueillir les VM et de simplifier la configuration. A contrario, le fait de disposer de plusieurs LUN sur le même groupe de disques permet de ne pas perdre l'ensemble des données au cas où le système de fichier se corrompt. Etant donné la fiabilité du système, il n'est pas nécessaire de créer plusieurs LUN. De plus, dans mon cas, les données stockées ne sont pas critiques dans le sens où il s'agit de fichiers temporaires (Windows). En effet, à chaque fermeture de session, la VM est supprimée.

Répartition des I/O

Si l'on veut répartir les I/O, il est nécessaire de disposer de groupes de disques physiques différents. En effet, le découpage logique (LUN) sur des disques physique ne répartit pas les I/O. Derrière ceci, il s'agit des mêmes disques. Et par conséquent, il est indispensable de créer un LUN sur un autre groupe de disques.

Disque VM

Les disques des VM sont de type « Thin Provisioning ». Elles utiliseront uniquement l'espace disque dont elles ont besoin. Cependant, étant donné que les machines virtuelles sont stockées sous forme de fichiers, le système s'arrête s'il ne peut plus écrire. Le point est à surveiller avec le monitoring. Surtout que l'augmentation des VM qui seront hébergées fera fatalement augmenter l'espace de stockage utilisé.

2.4.3.2 Calcul des LUN

Pour le calcul du LUN lclone (n°161), les recommandations VMware indiquent qu'il faut considérer sur le fait qu'il puisse ne plus avoir d'espace mémoire vive de disponible sur les ESX 6. Ce qui engendrerait du swap[11] et donc des dégradations nettes de performances (ratio vitesse RAM et HDD = 10^9)[12]. Le cluster étant surdimensionné au niveau RAM, j'ai décidé de ne pas prendre en compte ceci dans le calcul de dimensionnement.

LUN replica n°170

Nb de replica max / par pool	Nb de Pool	Nb total de replica	Taille replica	Taille total replica	Taille du LUN
2	3	6	25 Go	125 Go	200 Go

Le LUN replica doit pouvoir accueillir 6 replica soit env 6 x 25 Go = 125 Go

Car 3 pools (potentiellement 2 replica / pool) = 6 replica MAX.

Par marge de sécurité, j'ai alloué 200 Go.

LUN lclone n°161

Taille du replica réél	Taille Growth	Taille clone lié	Taille clone lié + growth	Taille total clone lié	Taille du LUN
20.84 Go	2.084 Go	10.42 Go	10.504 Go	2.5 To	1.53 To

Le LUN des clones liés a été calculé de la manière suivante :

Calcul taille une VM :

10.42 Go *(50% de 20.84)* (Linked Clone) + **2.084 Go** *(20% de 10.42) (*Growth%) **= 12.504 Go** *(*espace de stockage par VM)

Calcul taille 200 VM:

Taille de la VM x 200 = 12.504 Go *x 200 = 2.5 To

[11]Swap : fichier d'échange.
[12]Chiffre donné par : http://olbaum.free.fr/old/log/VMw/24-Fonctionnement%20et%20concepts-Gestion%20de%20la%20m%C3%A9moire%20sous%20VMware%20ESX.pdf.

L'espace alloué est de 1.53 To utile. Le LUN sera agrandi au fur et à mesure des besoins.

LUN profils n°171

Nb d'utilisateurs	Taille profil	Taille tot profil
200	20Mo	4 Go

Le LUN des profils a été calculé de la manière suivante :

200 utilisateurs x 20 Mo = 4 Go

Ce LUN ne pourra pas dépasser la valeur ci-dessus, car les profils sont limités avec persona managment (Quota). La taille allouée est de 100Go

2.4.3.3 Calcul IOPS

Les besoins en IOPS

IOPS généré par les 200 VM's : 50 x 200 = **10'000 IOPS**

(Target IOPS x Read I/O%) + ((Target IOPS x Write I/O %) x RAID Penalty) = IOPS

(10'000 x 0.4) + ((10'000 x 0.6) x 4) = 28'000 IOPS

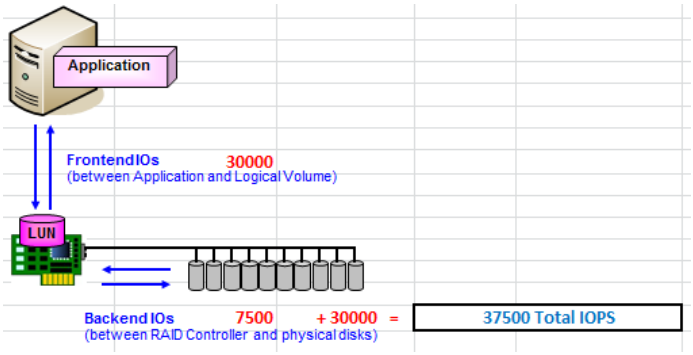
Les IOPS fournits par l'infrastructure en place

Ci-dessous le calculateur d'IOPS sous forme Excel : (voir bibliographie)

RAID SSD IOPS

Calculate IOPS, Usable Space, MB/s based on Number of Disks, Spindle Speed, RAID type and Read/Write Percentages.

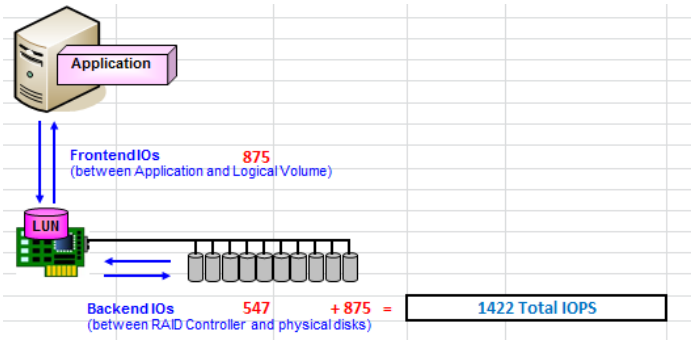
#Disks	Disk Size (GB)	RPM	RAID	RAID Penalty	Read %	Write %	IO Type	Frontend IOPS	Backend IOPS	MB/s	Total Usable Space (MB)
5	200	SSD	RAID5	4	100%	0%	64K	30000	7500	469	800



Replica

RAID SAS IOPS

Calculate IOPS, Usable Space, MB/s based on Number of Disks, Spindle Speed, RAID type and Read/Write Percentages.											
#Disks	Disk Size (GB)	RPM	RAID	RAID Penalty	Read %	Write %	IO Type	Frontend IOPS	Backend IOPS	MB/s	Total Usable Space (MB)
5	600	15,000 RPM	RAID5	4	50%	50%	64K	875	547	34	2400



Clone liés

Soit un total de 38922 IOPS.

Etant donné que les accès se feront sur la partie replica, les IOPS fourni par l'infrastructure sont plus élevés que ce que demande les 200 VM's.

2.4.4 Profil utilisateur

Les profils utilisateurs en virtualisation sont difficiles à gérer, notamment si on travaille en mode clone lié. VMware offre la possibilité d'effacer les VM lors du logoff de l'utilisateur afin de les garder « propres ».

Pour introduire mon choix, je propose ci-dessous un comparatif entre les profils itinérants de Microsoft et la solution « Persona Management » de VMware. Si la méthode VMware est activée, on ne peut plus modifier les profils avec la solution Microsoft. Cependant, on peut utiliser les deux méthodes en gérant par exemple certains fichiers avec l'une ou l'autre solution. VMware recommande fortement d'utiliser une seule méthode pour des raisons évidentes de compréhension. Voir tableau à la page suivante.

Produit	Profils itinérants Microsoft	VMware Persona Management
Synchronisation utilisation	Attend la fermeture de session	Personnalisable (10 minutes par défaut)
Synchronisation Ouverture	Télécharge le profil entier sur le partage défini pour l'utilisateur	Télécharge uniquement les fichiers dont il a besoin pour le lancement de Windows, le reste du profil est téléchargé lors de l'appel des applications. Il est possible de spécifier certains fichiers devant être chargés
Synchronisation Fermeture	Recopie les fichiers sur le partage	Fait le delta uniquement des fichiers modifiés
Profil machine physique VS VM	Ne peut pas fonctionner de façon dissociée entre physique et virtuel	Utilise un référentiel central sans affecter le profil lié à l'Active Directory, ce qui permet de personnaliser le profil persona uniquement pour la VM
Licences	Incluses	Inclus dans les licences View
Partage	CIFS	CIFS[13]
Déploiement	GPO / renseignement du chemin sur chaque user dans l'AD	GPO[14]

Le profil itinérant Microsoft est certes utilisable dans ce contexte, cependant Persona Management est optimisé pour l'infrastructure virtualisée (la raison de sa conception).

Elle offre des fonctionnalités complémentaires telles que l'intervalle de synchronisation et ordre de fichiers à rapatrier dans la session de l'utilisateur. J'ai donc choisi la solution VMware.

[13] CIFS : Common Internet File System.
[14] GPO : Group policy management.

2.5 Rôles VMware Horizon View

Ce chapitre résume les différents rôles des serveurs nécessaires à l'infrastructure VMware Horizon View.

2.5.1 VMware View Connection Server 3

Le serveur « View connection », comme l'indique son nom, est utilisé pour établir la demande de connexion à l'infrastructure View aussi bien du côté client que de celui de l'administration. Il s'occupe également de donner les ordres de création de VM au vCenter. L'administration se fait par le biais de ce serveur en accédant à l'URL : **https://FQDNconnectionserver/admin** . C'est depuis cette URL que l'on va créer nos pools de VM et affecter des droits utilisateurs.

Dans la configuration de ce serveur, il faut préalablement enregistrer la clé de licence.

Il faudra également renseigner le vCenter Server 4 ainsi que le security 2 server auquel il est lié.

Dans notre cas, deux connection server 3 sont installés pour assurer de la haute disponibilité. Si l'un des deux serveurs tombe, l'autre prend le relais.

Un point important à relever est qu'un connection server est relié à un seul security server. C'est pour cela que sur mon schéma, il n'y pas de liens croisés entre les quatre serveurs (2 connection server, 2 security server). Cette variante augmenterait la haute disponibilité, mais n'est pas disponible dans VMware View.

2.5.2 VMware View Security server 2

Pour la partie Security server, j'ai décidé d'installer deux serveurs afin d'obtenir un minimum de redondance.

Les security server ne font pas partie du domaine active directory. Ils sont simplement placés en DMZ. Une configuration dans le firewall est nécessaire à l'ouverture de ports, notamment pour le PCoIP[15] (4172), ssl (443), blas (443, 22443)t[16] (interface web pour accéder à notre VM), RDP (389) (voir page 31).

Sur ces serveurs, il y a le certificat SSL relatif au nom de domaine.

[15] PCoIP : Pc over ip est un protocole d'affichage utilisé par VMware.
[16] Blast : Protocole d'affichage pour Horizon View. Accèder la première fois en SSL (443), puis sur le port 22443.

2.5.3 VMware View Composer 7

Le VMware « view composer » est utilisé pour les clones liés. Il s'installe en principe sur la même VM que le vCenter ou sur une VM différente.

2.6 Maintenance des pools

Les opérations de maintenance doivent pouvoir être réalisées dans la mesure du possible sans perturber les clients. Par exemple, pour gérer le template j'applique la méthode suivante :

- Rallumer la VM parente « dite de référence »
- Effectuer les mises à jour
- Éteindre la VM parente
- Faire un snapshot de la VM
- Affecter le snapshot au pool
- Faire un recompose

Lors du recompose dans VMware View, le pool va créer un nouveau replica et régénérer les VM (refait la partie delta). La mise à jour peut effectivement se faire en pleine journée même si des utilisateurs sont connectés. Si un ou plusieurs utilisateurs sont connectés sur les VM du pool en question, on aura simplement 2 replica pendant un laps de temps. Lorsque tous les utilisateurs du pool se déconnectent, le replica est libéré et supprimé. Concernant les données utilisateurs, elles sont conservées sur le disque persistant ainsi que dans la partie persona management.

2.7 Performances

Les dégradations de performances peuvent survenir dans les cas suivants :

1) Trop grand nombre de VM démarrent en même temps
2) L'antivirus effectue un scan sur les VM
3) Windows ou d'autres applications sont mises à jour

Pour pallier au premier problème, il est important de provisionner[17] suffisamment de VM à l'avance. Dans notre cas, l'utilisation des VM sera probablement répartie dans la journée

[17] Provisionnement du nombre de VM : Il s'agit dans ce cas de prévoir / préparer assez de VM en état de fonctionnement.

ou en soirée. Les entreprises choisissant d'utiliser le VDI à la place de machines physiques sont confrontées à ce problème le matin au moment où le monde se connecte en même temps. Il est alors important de mesurer ce pic et d'adapter le nombre de VM prêtes. Le deuxième problème se résout en désactivant le scan antivirus ou en mettant une solution vShield. L'appliance[18], fournie par les éditeurs, est introduite au niveau de l'hyperviseur et scanne les fichiers en amont sans péjorer les performances. La troisième solution est de désactiver les mises à jour Windows. Ces dernières seront incluses à intervalles réguliers dans la VM parente lors des maintenances.

[18] Appliance : Package fourni par l'éditeur sous forme de VM. Comparable à une boîte noire.

3 Réalisation

3.1 Préparation à l'installation de Vsphere et Vcenter

Avant toute chose, voici quelques points à préparer si possible à l'avance afin d'éviter tout problème :

- Il est important d'effectuer les réservations d'adresses IP nécessaires à l'installation des serveurs. En effet, les IP doivent être statiques.
- Choisir les noms des serveurs
- Renseigner les DNS (forward et reverse zone)
- Créer le LUN accueillant les VM des serveurs

La procédure complète de l'installation de VSphere ainsi que le VCenter est mentionnée dans la bibliographie.

3.2 Création des LUN

Les LUN sont créés sur le SAN (8) afin de les présenter aux ESX comme datastore. L'explication détaillée se situe au § 2.4.4 Stockage

3.3 Pré-installation hyperviseur VSphere (ESX)

Pour rappel, l'hyperviseur est le lien (isolation) entre le matériel physique et la couche virtuelle.

L'installation de l'hyperviseur sur les hôtes se fait par le biais d'un fichier ISO. Dans notre cas, j'ai décidé d'opter pour deux disques SSD locaux en RAID 1. Une fois l'installation terminée, on doit configurer les paramètres IP (Adresse IP, masque de sous réseau, passerelle par défaut, DNS).

3.4 Configuration VCenter

La 1ère étape est de créer un « datacenter ».

Puis j'ai développé un cluster en y ajoutant les hôtes. Une fois que le cluster est opérationnel, il est nécessaire d'affecter les datastore à chaque ESX.

Pour terminer, j'ai activé les licences VMware sur chaque hôte.

3.5 Installation Connection et security server

Dans un premier temps, j'ai installé le 1er connection server. Les informations suivantes sont demandées :

Type de serveur :

View Standard Server : est la 1ère instance du connection server.

View Replica Server : nième instance du connection server. En complément, cette option fonctionne un peu à la manière d'un Active directory entre plusieurs contrôleurs de domaine. Ils s'échangent les informations et sont complètement redondants.

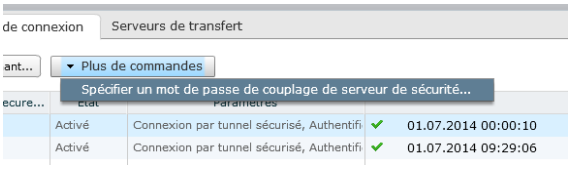
View Security Server : Security server (chaque instance doit être unique).

View Transfert Server : utile pour le mode local (VM déportée en local sur le client).

Ensuite un mot de passe de recovery est demandé. Mon connection server est désormais prêt. Pour contrôler le bon fonctionnement, il suffit de se connecter avec le navigateur à l'adresse suivante : https://FQDNconnectionserver/admin.

J'ai ensuite choisi l'option « Replica Server » pour le deuxième connection server. Le nom du 1er connection server est demandé pour l'association.

Dans un deuxième temps, je me suis occupé des Security server. À savoir qu'un seul security server ne peut être associé à un connection server. Au préalable, il est nécessaire de générer un mot de passe. Ce mot de passe est valide uniquement pendant un laps de temps défini (paramétrable dans l'interface View Administator).



Les informations suivantes sont demandées :

- Adresse IP ou nom du connection server auquels on veut l'associer
- Mot de passe de « couplage »

L'authentification forte se paramètre dans la configuration du connection server, depuis l'interface VMware View Administrator :

Sous l'onglet « Authentification »

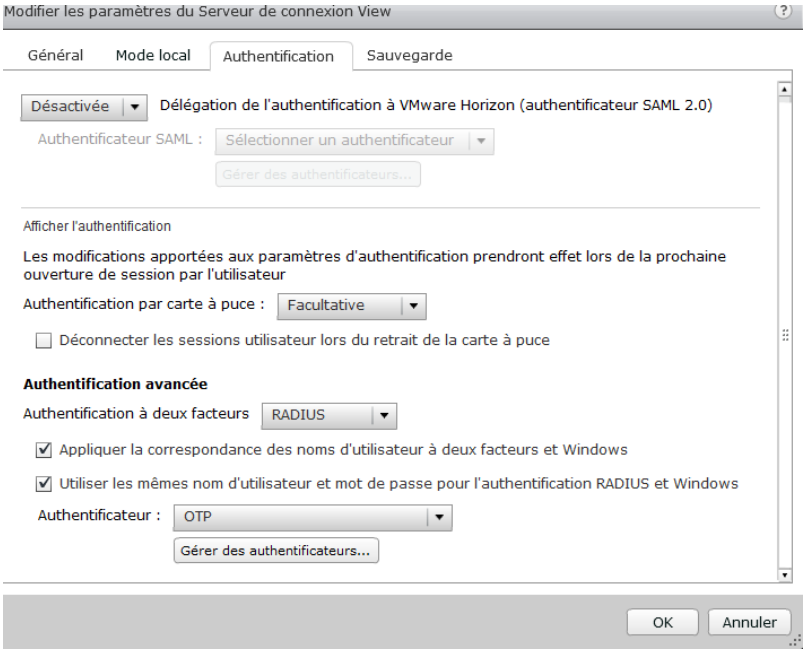


Figure 8 - Authentification RADIUS

J'ai pu ainsi choisir :

- Radius
- Le type d'authentification
- Le secret partagé

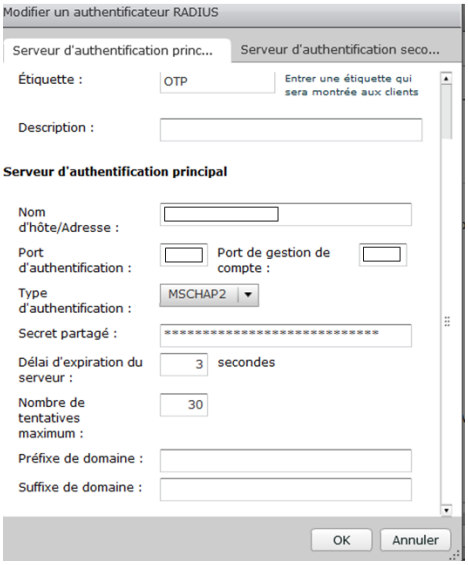


Figure 9 - OTP

3.6 Certificats SSL et authentification forte

3.6.1 Certificats SSL

Une infrastructure fonctionnelle mais non sécurisée n'est pas très pertinente dans une entreprise. Deux fonctionnalités ont été mise en place :

- utilisation de certificats SSL
- système d'authentification forte

Rappel SSL :

Sans entrer dans le détail du fonctionnement du SSL je souhaite rappeler les éléments suivants :

Elément contrôlé lors de la connexion au service :

- nom FQDN du serveur
- validité du certificat + date de péremption
- l'organisation émettrice

Le certificat SSL permet donc de :

- contrôler si l'utilisateur est bien connecté sur le bon seveur
- contrôler la validité du certificat (date d'échéance valide et non révoquée)
- d'authentifier l'organisation

Tableau récapitulatif

Fonction	Explication	
Encryptions et intégrité	Chiffrage des informations transmises qui ne peuvent être interceptées ou modifiées en cours de transit	Encryptions de 1024 à 4096 bits
Authentification	Validation de l'entité par une tierce organisation (émetteur du certificat SSL) dans le processus de délivrance.	Par exemple, TBS à contrôlé la véracité de l'association des communes Genevoises. Puis lors de la demande de certificat SSL pour view.siacg.ch, TBS a contacté le Directeur afin de vérifier si la demande était légitime.
« Certitude » de la destination	Contrôle du nom du serveur sur lequel l'utilisateur est connecté.	Lorsqu'on se connecte à view.siacg.ch, le navigateur vérifie si le nom du certificat correspond bien au nom FQDN view.siacg.ch. Le navigateur contrôle également si le certificat n'est pas révoqué et si la date de péremption est valide.

3.6.1.1 Mise en place des certificats

Dans ce sous-chapitre, j'explique comment j'ai mis en place les certificats. Deux types ont été utilisés. Pour l'externe les certificats sont délivrés par une instance du type TBS ou Verisign. Pour l'interne, ils sont délivrés par notre PKI. L'infrastructure VMware View nécessite au minimum deux certificats SSL, un pour le connection server (interne), un pour le securtiy server (externe). Dans mon cas, j'ai donc 4 certificats à cause de la redondance mise en place.

3.6.1.2 Création d'un modèle de certificat

Avant toute chose, j'ai créé un modèle de certificat spécifique à VMware View en suivant la procédure de VMware qui se trouve dans le lien ci-dessous :

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2062108)

To create a new default template:

1. Connect to the Root CA server or Subordinate CA server via RDP.

   Note: Connect to the CA server in which you are intending to perform your certificate generation.

2. Click **Start** > **Run**, type `certtmpl.msc`, and click **OK**. The Certificate Template Console opens.
3. In the middle pane, under Template Display Name, locate Web Server.
4. Right-click **Web Server** and click **Duplicate Template**.
5. In the Duplicate Template window, select **Windows Server 2003 Enterprise** for backward compatibility.
6. Click the **General** tab.
7. In the Template display name field, enter `VMware Certificate` as the name of the new template.
8. Click the **Extensions** tab.
9. Select **Key Usage** and click **Edit**.
10. Select the **Signature is proof of origin (nonrepudiation)** option.
11. Select the **Allow encryption of user data** option.
12. Click **OK**.
13. Select **Application Policies** and click **Edit**.
14. Click **Add**.
15. Select **Client Authentication**.
16. Click **OK**.
17. Click **OK** again.
18. Click the **Subject Name** tab.
19. Ensure that the **Supply in the request** option is selected.
20. Click **OK** to save the template.

Adding a new template to certificate templates

To add a new template to certificate templates:

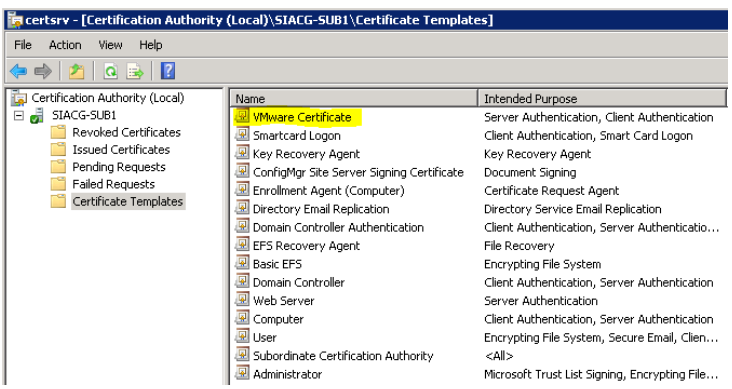
1. Connect to the Root CA server or Subordinate CA server via RDP.

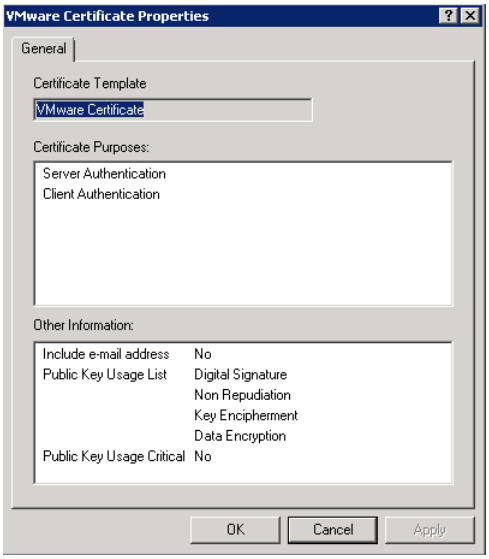
   Note: Connect to the CA server in which you are intending to perform your certificate generation.

2. Click **Start** > **Run**, type `certsrv.msc`, and click **OK**. The Certificate Server console opens.
3. In the left pane, if collapsed, expand the node by clicking the [+] icon.
4. Right-click **Certificate Templates** and click **New** > **Certificate Template to Issue**.
5. Locate `VMware Certificate` under the Name column.
6. Click **OK**.

Un point à relever sur cette procédure, il faut attendre systématiquement 15 minutes pour le que le modèle créé soit visible dans la console.

Résultat du modèle :

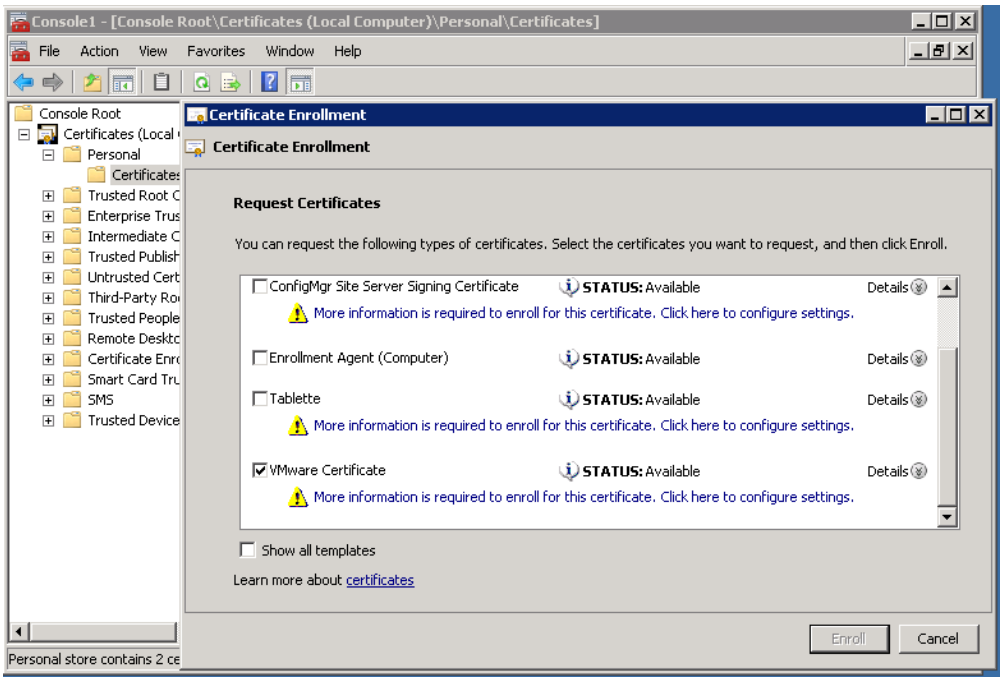




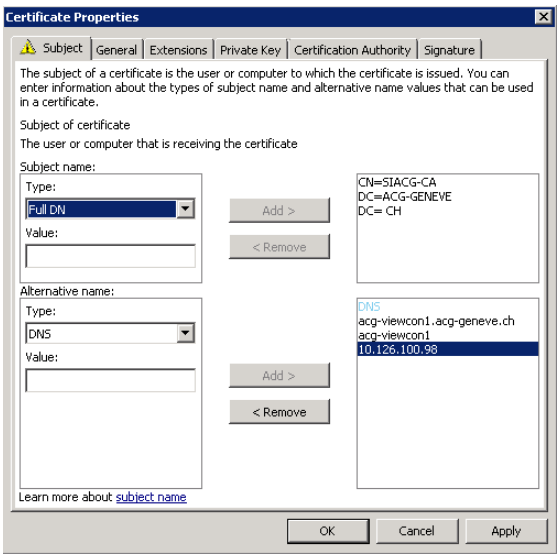
3.6.1.3 Installation des certificats sur les connexions servers

Sur les serveurs de connexion, ouvrir une console MMC « certificates computer ».

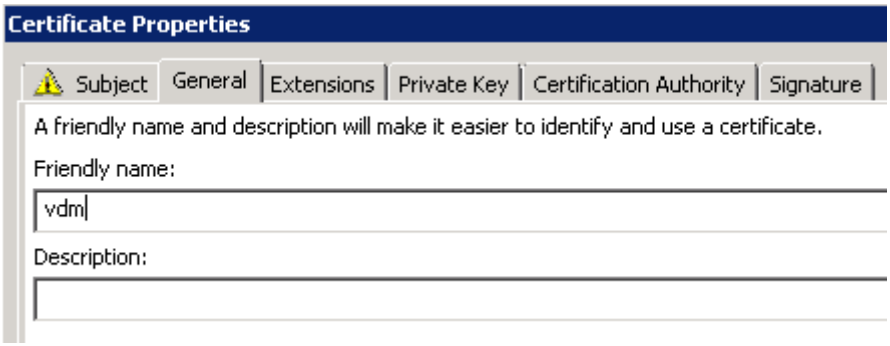
Lancer une demande de nouveau certificat, on voit bien le modèle « VMWare Certificat » créé précédemment. Le sélectionner pour la suite du processus et renseigner les informations requises.



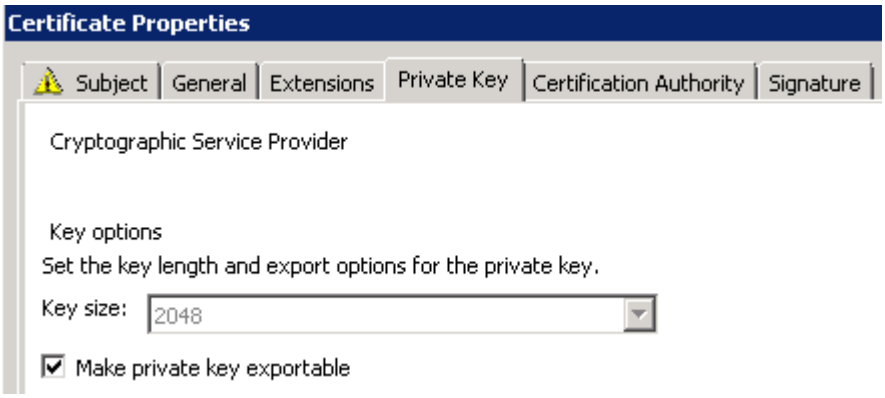
À noter que, comme il s'agit d'un certificat interne, j'ai décidé d'ajouter d'autres noms de serveur non FQDN pour une question de confort lorsqu'on se connecte sur ces serveurs pour administrer la partie View.



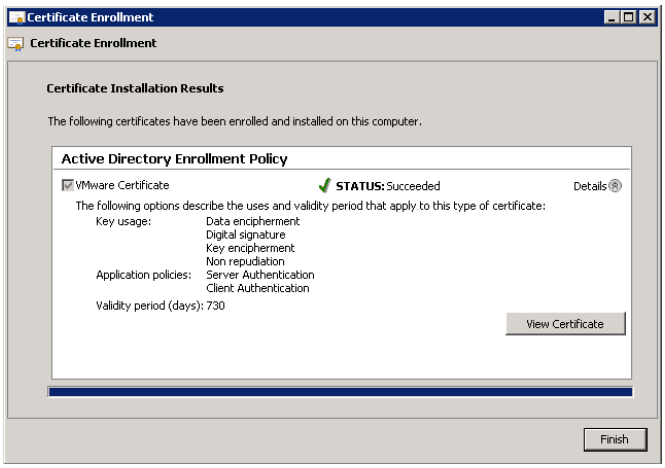
Le nom commun doit être renseigné de la chaîne de caractère « vdm ». Sans cette stricte information, les services systèmes VMware view ne pourront pas utiliser ce certificat. C'est cette information qui est utilisée pour « matcher » automatiquement le certificat avec le service VMware view.



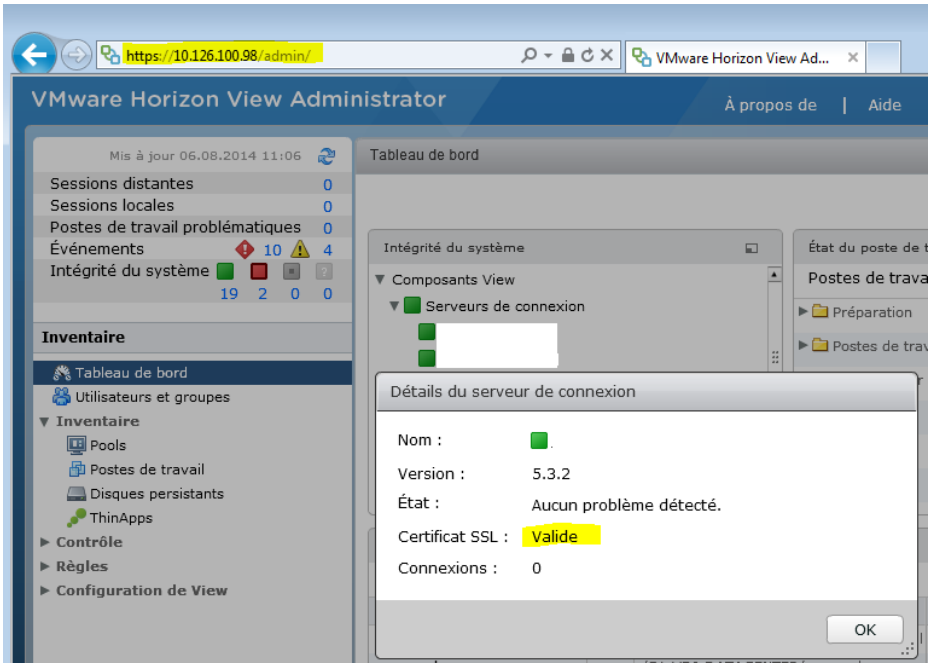
Dans cet onglet, je constate que la clé est bien exportable (déjà coché), configurée précédemment dans mon modèle.



Résultat de la demande



Contrôle du certificat



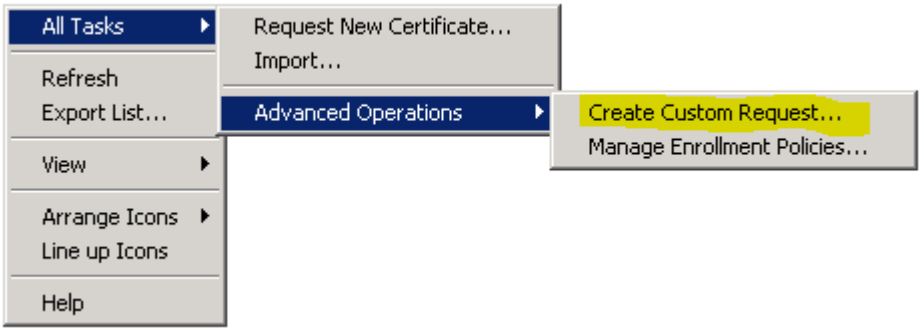
J'ai ensuite répété cette partie sur le deuxième serveur de connexion.

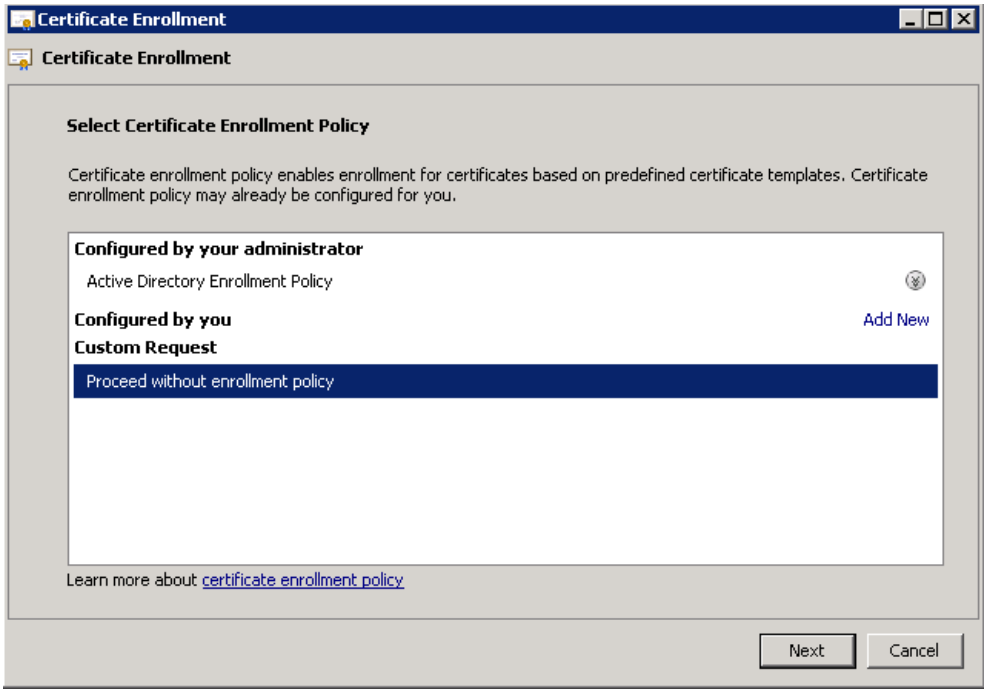
3.6.1.4 Installation des certificats sur les security servers

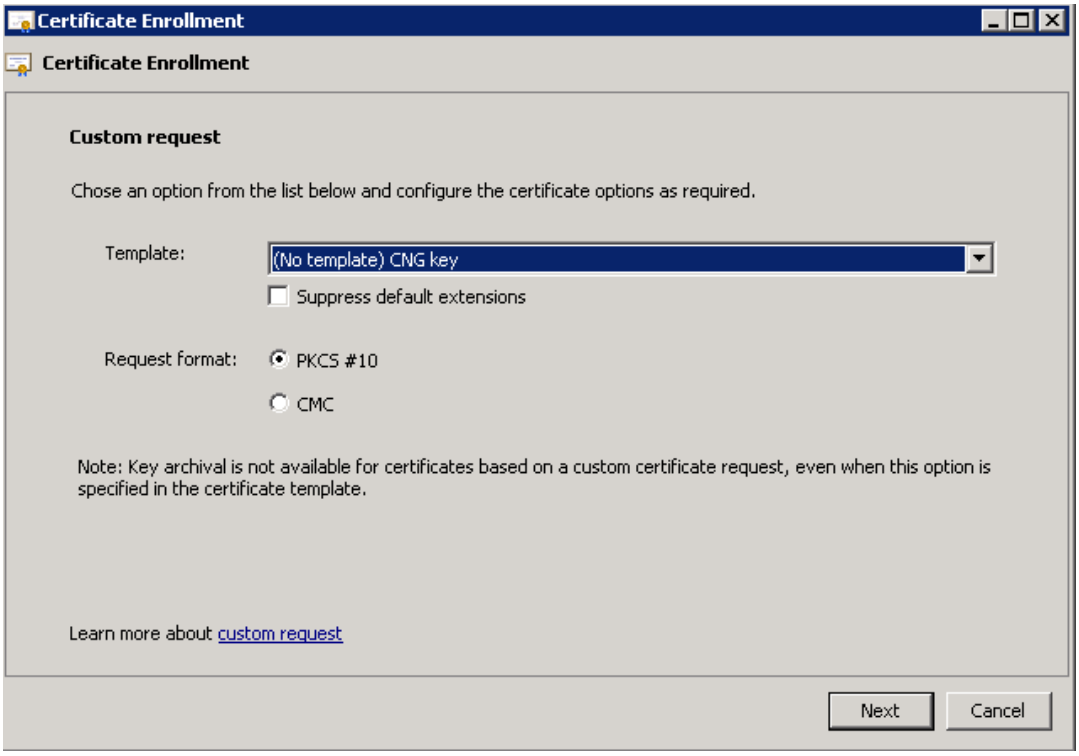
Cette partie a été plus longue à réaliser. La procédure de génération du certificat est en effet gérée par un organisme externe. De plus, les deux security servers sont atteignables par la même URL (nom FQDN). Par ailleurs, l'on m'a demandé un 2ème nom FQDN pour mettre en place la bascule entre les deux serveurs. Cette partie sera réalisée dans un future proche. Pour se faire, il est nécessaire de prendre un certificat de type SAN et installable sur deux serveurs différents. Ce dernier point n'est pas un problème technique Il résulte uniquement du fait de la gestion de droits d'utilisation.

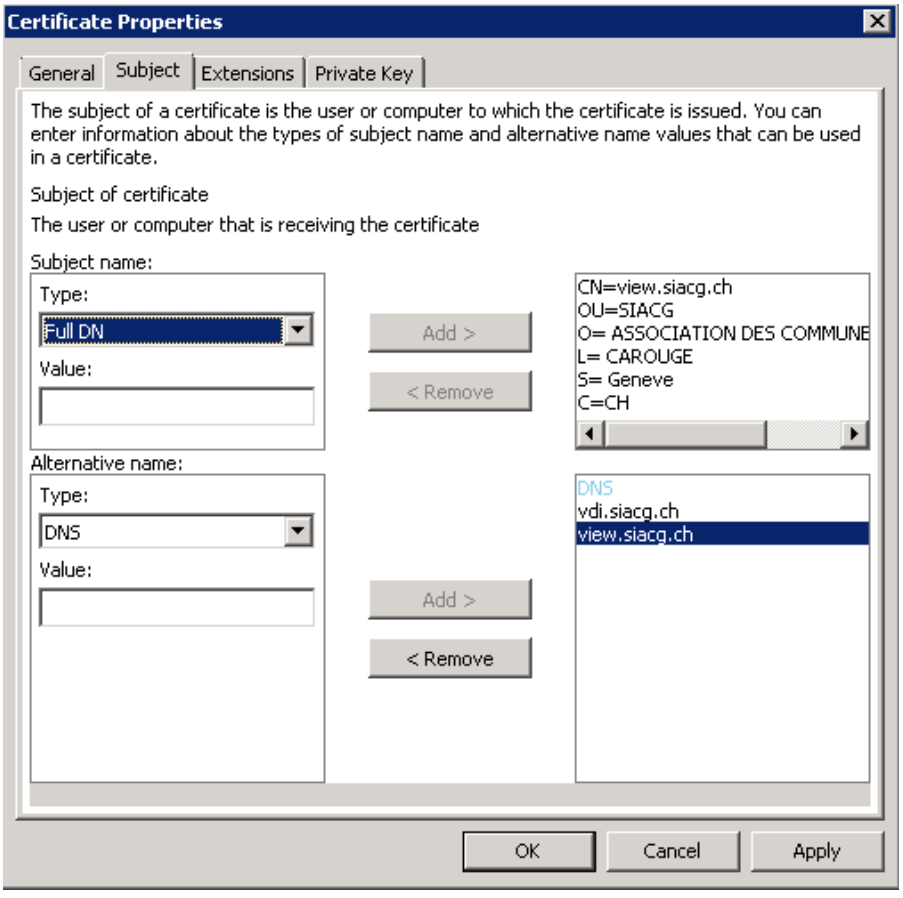
Requête du certificat fichier texte

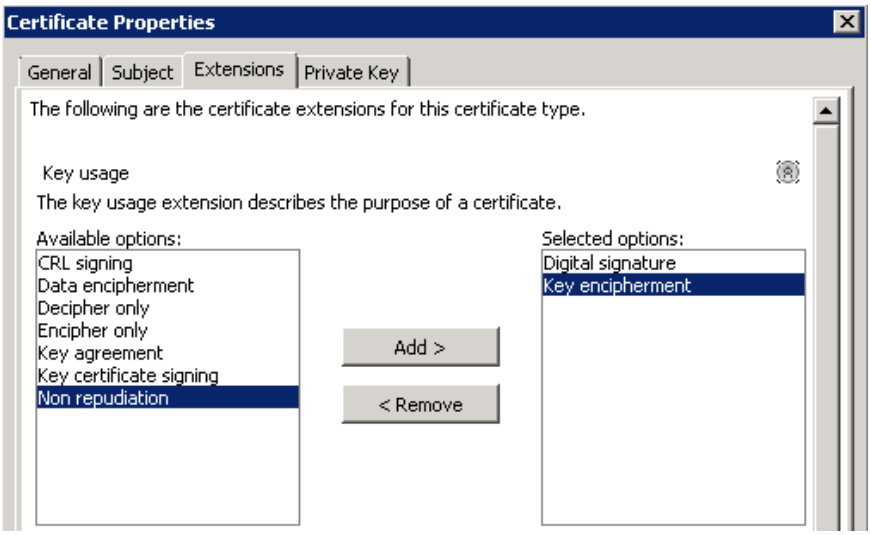
Création de la demande personnalisée depuis la console Microsoft.

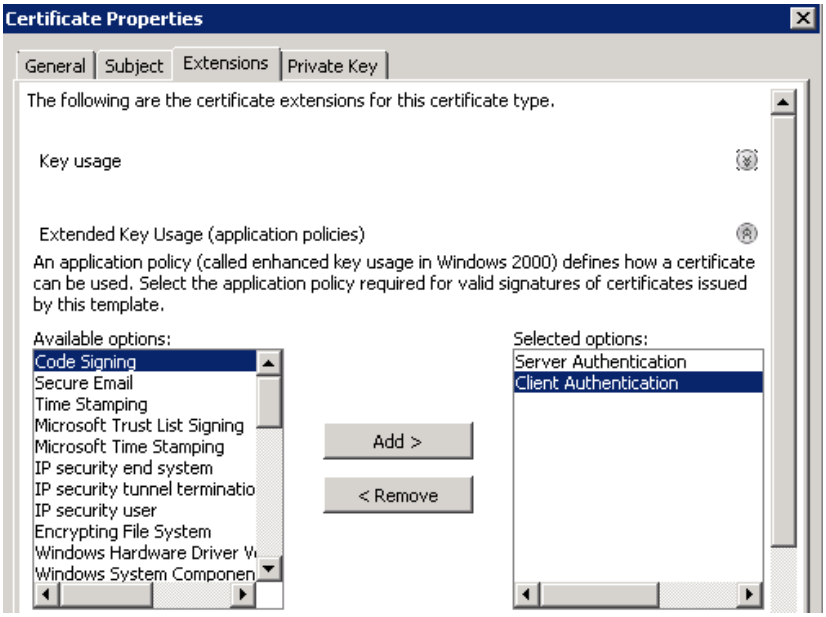


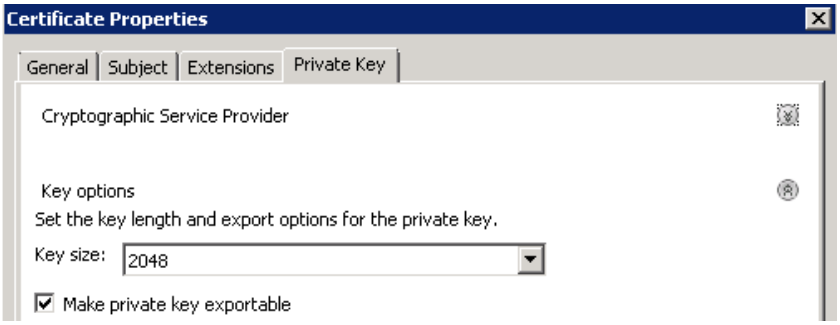



Certificate Enrollment
Certificate Enrollment
Custom request
Chose an option from the list below and configure the certificate options as required.
Template:
(No template) CNG key
Suppress default extensions
Request format:
PKCS #10
CMC
Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template.
Learn more about custom request
Next
Cancel

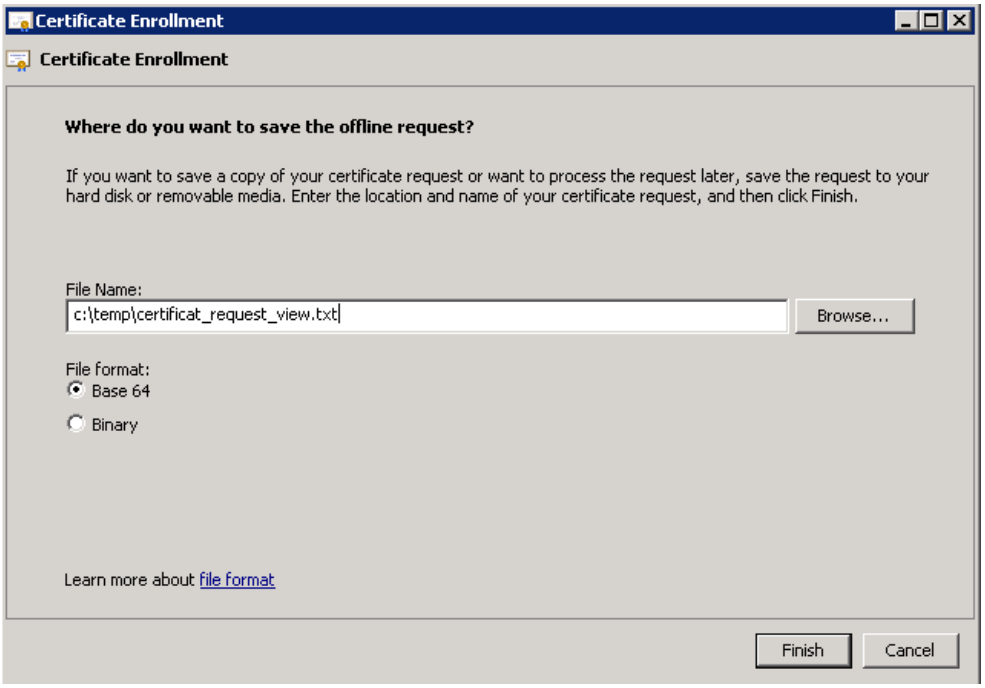

Certificate Properties
General
Subject
Extensions
Private Key
The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.
Subject of certificate
The user or computer that is receiving the certificate
Subject name:
Type:
Full DN
Value:
Add >
< Remove
CN=view.siacg.ch
OU=SIACG
O= ASSOCIATION DES COMMUNE
L= CAROUGE
S= Geneve
C=CH
Alternative name:
Type:
DNS
Value:
Add >
< Remove
DNS
vdi.siacg.ch
view.siacg.ch
OK
Cancel
Apply


Certificate Properties
General
Subject
Extensions
Private Key
The following are the certificate extensions for this certificate type.
Key usage
The key usage extension describes the purpose of a certificate.
Available options:
CRL signing
Data encipherment
Decipher only
Encipher only
Key agreement
Key certificate signing
Non repudiation
Add >
< Remove
Selected options:
Digital signature
Key encipherment

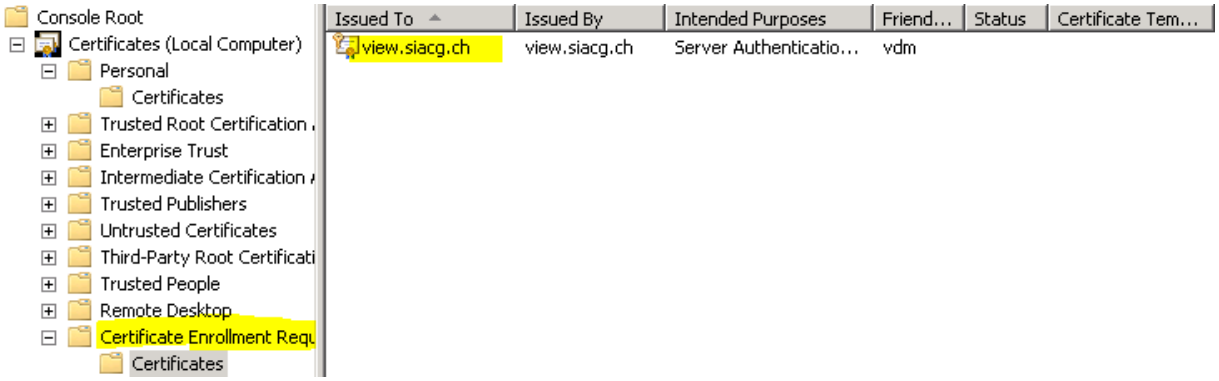

Certificate Properties
General
Subject
Extensions
Private Key
The following are the certificate extensions for this certificate type.
Key usage
Extended Key Usage (application policies)
An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.
Available options:
Code Signing
Secure Email
Time Stamping
Microsoft Trust List Signing
Microsoft Time Stamping
IP security end system
IP security tunnel terminatio
IP security user
Encrypting File System
Windows Hardware Driver W
Windows System Componen
Add >
< Remove
Selected options:
Server Authentication
Client Authentication


Certificate Properties
General
Subject
Extensions
Private Key
Cryptographic Service Provider
Key options
Set the key length and export options for the private key.
Key size:
2048
Make private key exportable

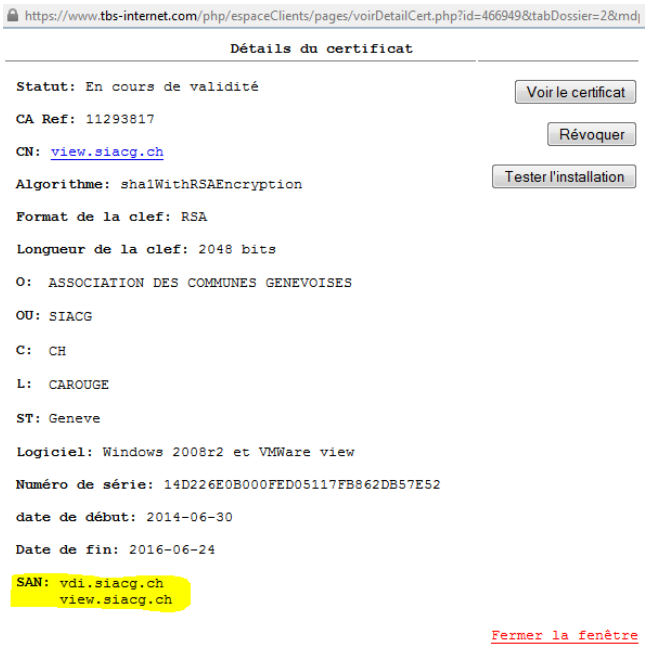
Il faut ensuite enregistrer la demande dans un fichier pour la transmettre à l'autorité émettrice.



La demande de certificat est bien mémorisée dans le serveur.



Je ne peux pas vous montrer ici les informations du processus officiel de demandes chez notre fournisseur pour des questions évidentes de sécurité. Mais je vous délivre le résultat.



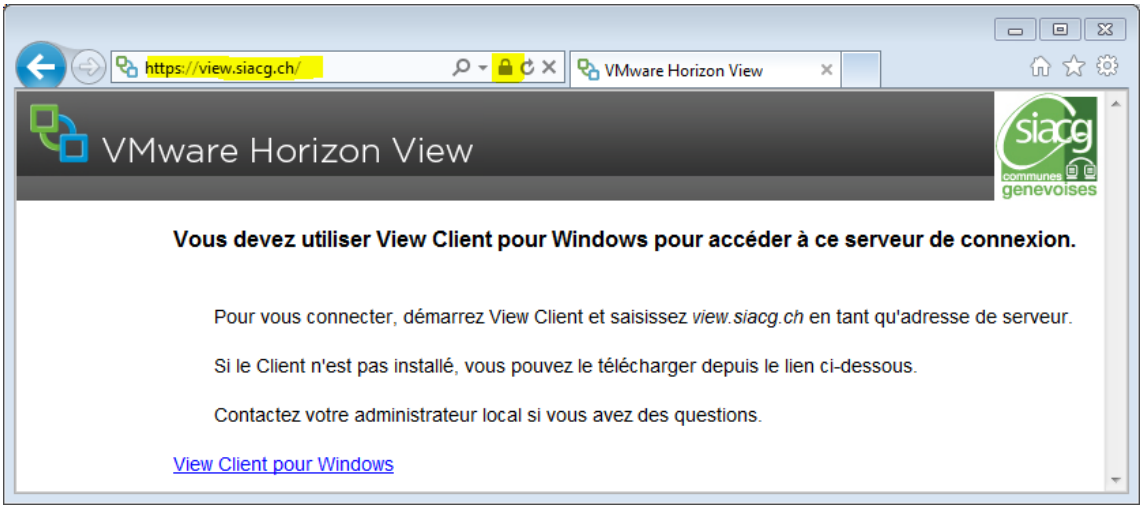
Une fois le certificat généré à partir de notre requête sous forme de fichier CSR, nous pouvons l'intégrer au serveur via la commande ci-dessous :

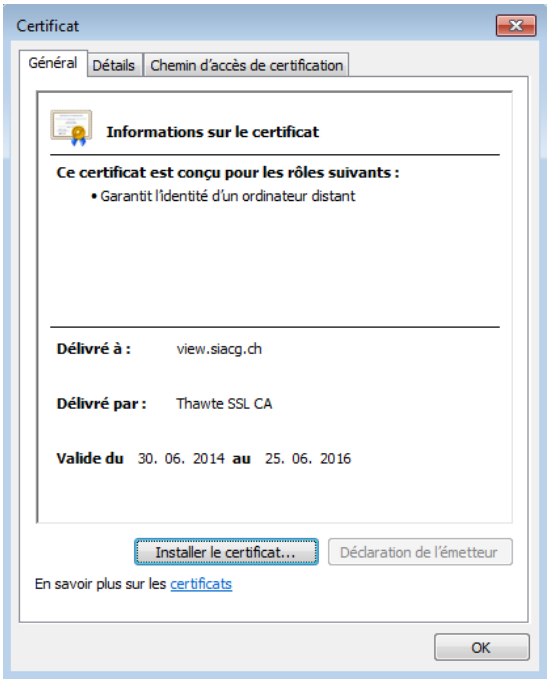
```
certreq -accept cert.cer
```

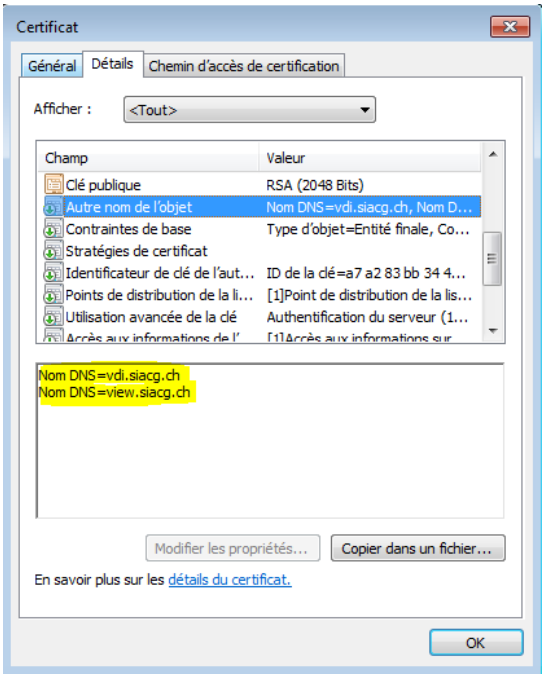
Puis, pour installer le certificat sur le deuxième serveur, il suffit de l'exporter avec sa clé privée et de le réimporter.

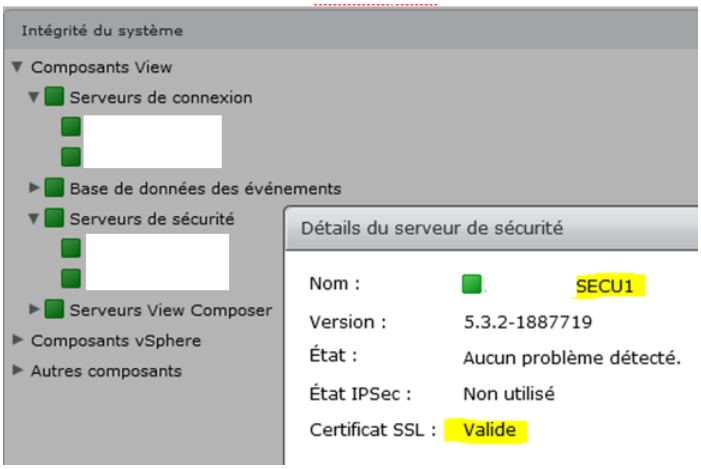
J'ai alors rencontré un problème qui est décrit dans le chapitre « problèmes rencontrés ».

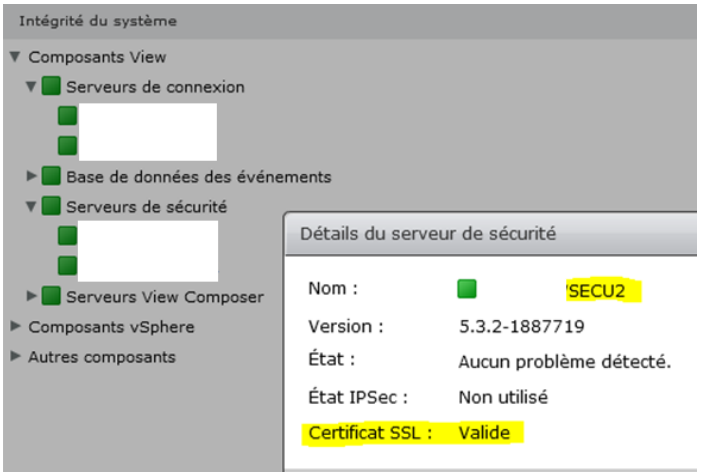
Au final, ce certificat SAN fonctionne.




Certificat
Général
Détails
Chemin d'accès de certification
Informations sur le certificat
Ce certificat est conçu pour les rôles suivants :
• Garantit l'identité d'un ordinateur distant
Délivré à : view.siacg.ch
Délivré par : Thawte SSL CA
Valide du 30. 06. 2014 au 25. 06. 2016
Installer le certificat...
Déclaration de l'émetteur
En savoir plus sur les certificats
OK


Certificat
Général
Détails
Chemin d'accès de certification
Afficher : <Tout>
Champ
Valeur
Clé publique
RSA (2048 Bits)
Autre nom de l'objet
Nom DNS=vdi.siacg.ch, Nom D...
Contraintes de base
Type d'objet=Entité finale, Co...
Stratégies de certificat
Identificateur de clé de l'aut...
ID de la clé=a7 a2 83 bb 34 4...
Points de distribution de la li...
[1]Point de distribution de la lis...
Utilisation avancée de la clé
Authentification du serveur (1...
Nom DNS=vdi.siacg.ch
Nom DNS=view.siacg.ch
Modifier les propriétés...
Copier dans un fichier...
En savoir plus sur les détails du certificat.
OK


Intégrité du système
Composants View
Serveurs de connexion
Base de données des événements
Serveurs de sécurité
Serveurs View Composer
Composants vSphere
Autres composants
Détails du serveur de sécurité
Nom : SECU1
Version : 5.3.2-1887719
État : Aucun problème détecté.
État IPSec : Non utilisé
Certificat SSL : Valide


Intégrité du système
Composants View
Serveurs de connexion
Base de données des événements
Serveurs de sécurité
Serveurs View Composer
Composants vSphere
Autres composants
Détails du serveur de sécurité
Nom : SECU2
Version : 5.3.2-1887719
État : Aucun problème détecté.
État IPSec : Non utilisé
Certificat SSL : Valide

Pour valider la bonne installation, je l'ai contrôlée avec l'outil du fournisseur. Cet outil est à disposition du public **https://www.tbs-internet.com/php/HTML/testssl_verif.php**

Résultat du test

TESTS EFFECTUÉS :

Correspondance des numéros de série	
Période de validité du certificat	
Certificat non révoqué	
Non vulnérable à la faille Debian	
N'est pas un Domain Validated	
Le site testé correspond bien à un CN ou à un SAN du certificat	

Voici le diagnostic de l'installation de votre certificat réalisé par **CO-PiBot** :

```
Site : view.siacg.ch
Port : 443
Adresse(s) ip du fqdn : 91.217.128.43
```

Vérifier un autre site | Vérifier à nouveau ce site

STATUT DU CERTIFICAT

Votre certificat est valide.

DIAGNOSTIC :
• Erreur 0 : OK = Certificat valide. Tous les tests de validité ont été effectués avec succès.

CHAÎNE DE CERTIFICATION :
- **RACINE :** Thawte Primary Root CA — OK
  - **INTERMÉDIAIRE 1 :** Thawte SSL CA — OK
    - **ENTITÉ FINALE :** view.siacg.ch — OK

3.6.2 Authentification forte OTP

L'authentification forte consiste à ajouter un troisième composant d'authentification et valable une seule fois (One Time Password ou On Demande Password), également appelé « mot de passe unique ». Ce troisième facteur d'authentification est généralement matérialisé et doit être possédé.

Facteurs	Mnémotechnique	Explication	Exemple
1er	Ce que je suis	Nom d'utilisateur	Jean
Deuxième	Ce que je connais	Mot de passe	12345_sOleil
Troisième	Ce que je possède	Carte à biffer, Token, téléphone portable pour SMS	187398

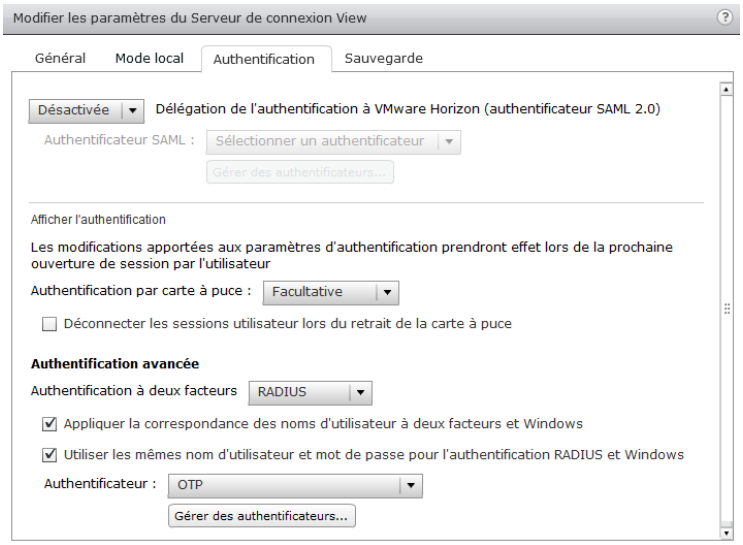
L'utilisation d'un OTP ou ODP permet d'anticiper les menaces comme par exemple le vol de mot du mot de passe ou l'attaque brute force. Dans mon cas, je privilégie l'ODP via SMS. Ne demandant en effet pas de logistique, il sera plus rapide à déployer.

Dans l'entreprise qui m'emploie, j'ai la chance de disposer d'un système d'authentification forte déjà opérationnel. Il est déjà fonctionnel pour l'OTP et l'ODP. Il me reste à interfacer VMWare View à ce système.

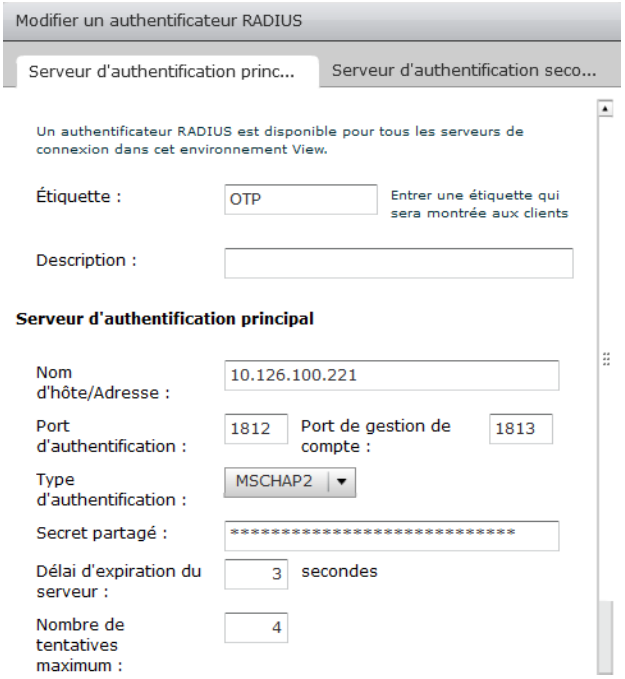
3.6.2.1 Mise en œuvre de l'authentification forte

3.6.2.1.1 Configuration de l'interfaçage OTP sur VMware VIew

VMware View est prévu à la base pour ne s'interfacer qu'à un seul éditeur/constructeur de solution d'authentification forte. Pour s'interfacer avec une autre solution, il faut obligatoirement utiliser un serveur Radius. Heureusement, la solution dont nous disposons offre ce service.



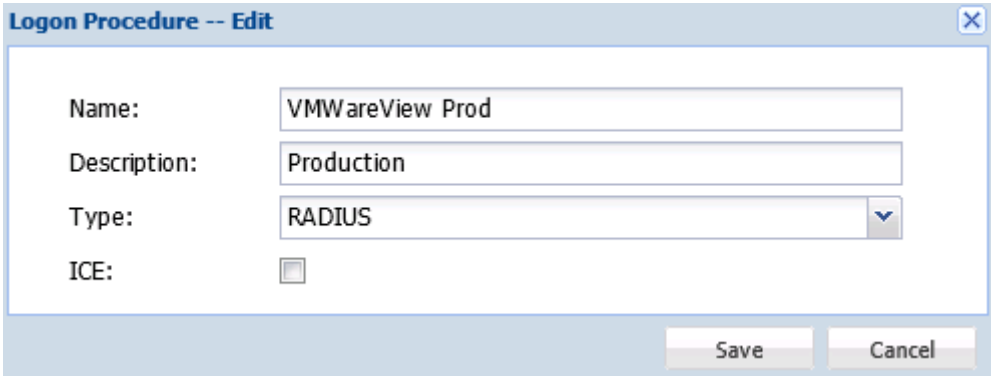
Propriétés de la configuration de l'interfaçage radius.



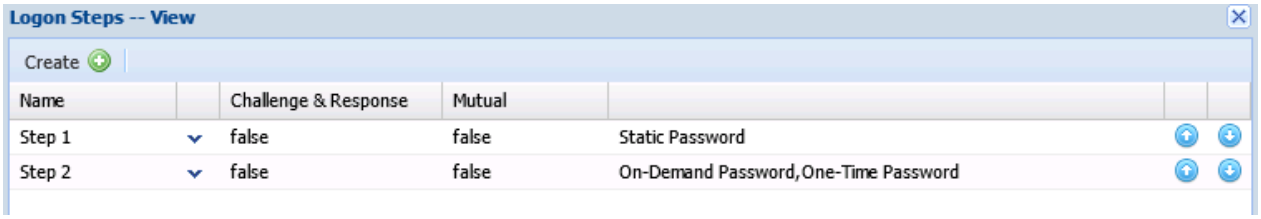
À noter que l'interfaçage sur le deuxième serveur est strictement identique.

3.6.2.1.2 Configuration de l'interfaçage OTP sur notre solution d'authentification forte

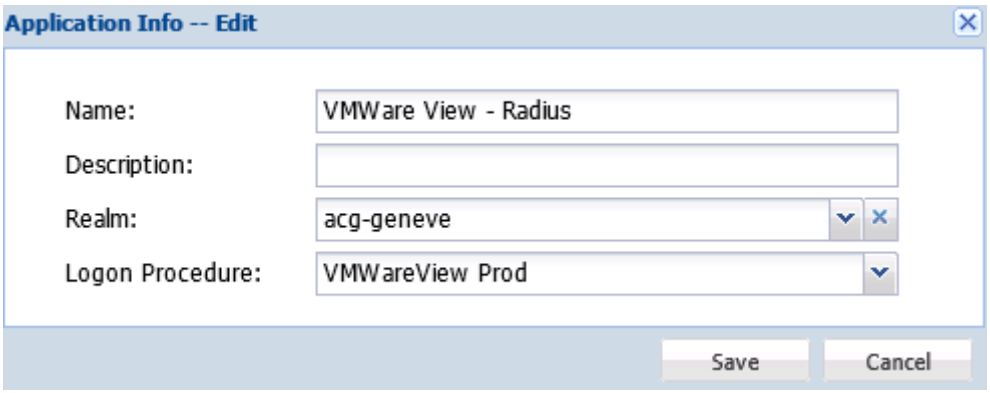
Tout d'abord j'ai créé un composant de départ appelé « Logon Procédure ». Ce composant devra utiliser le serveur Radius.



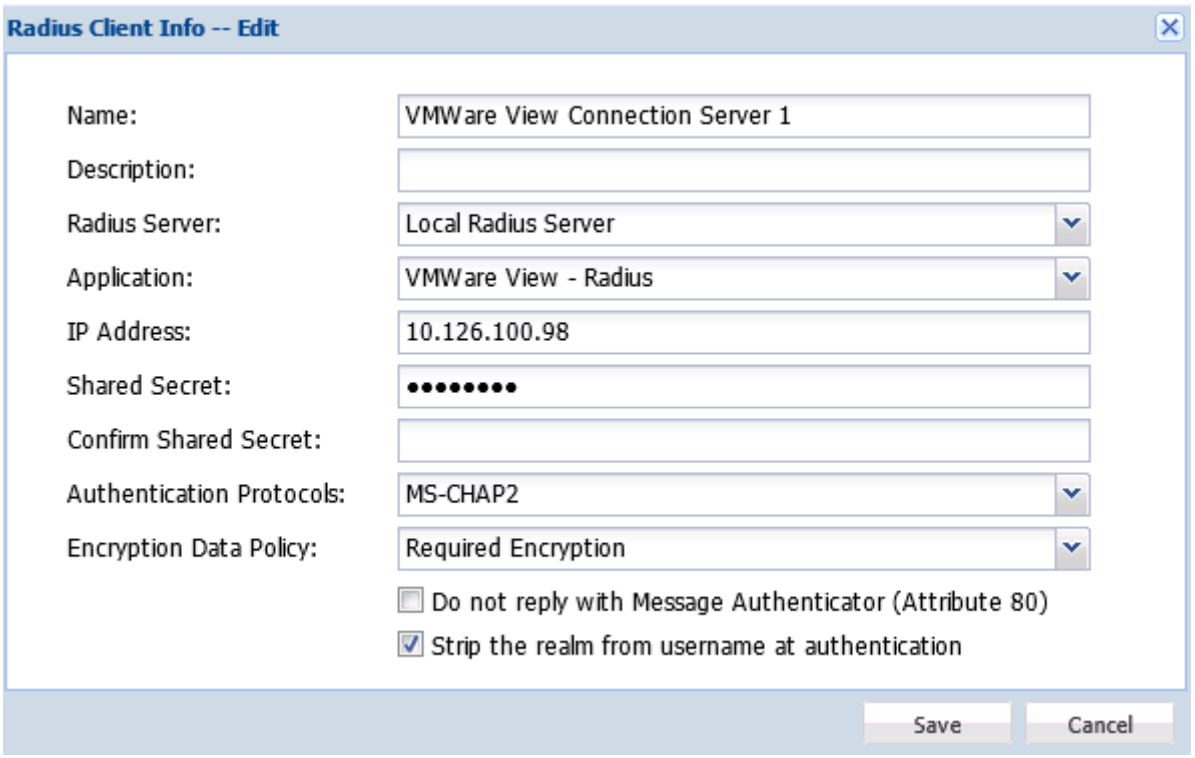
Comme son nom l'indique, ce composant gère la procédure d'authentification. J'ai paramétré cette procédure pour que le système demande un mot de passe et dans un deuxième temps, le mot de passe unique. Comme vous le voyez ici, j'ai configuré le processus pour que l'on puisse s'authentifier aussi bien avec un ODP qu'un OTP. C'est au cas où il serait nécessaire de délivrer à un utilisateur un Token matériel.

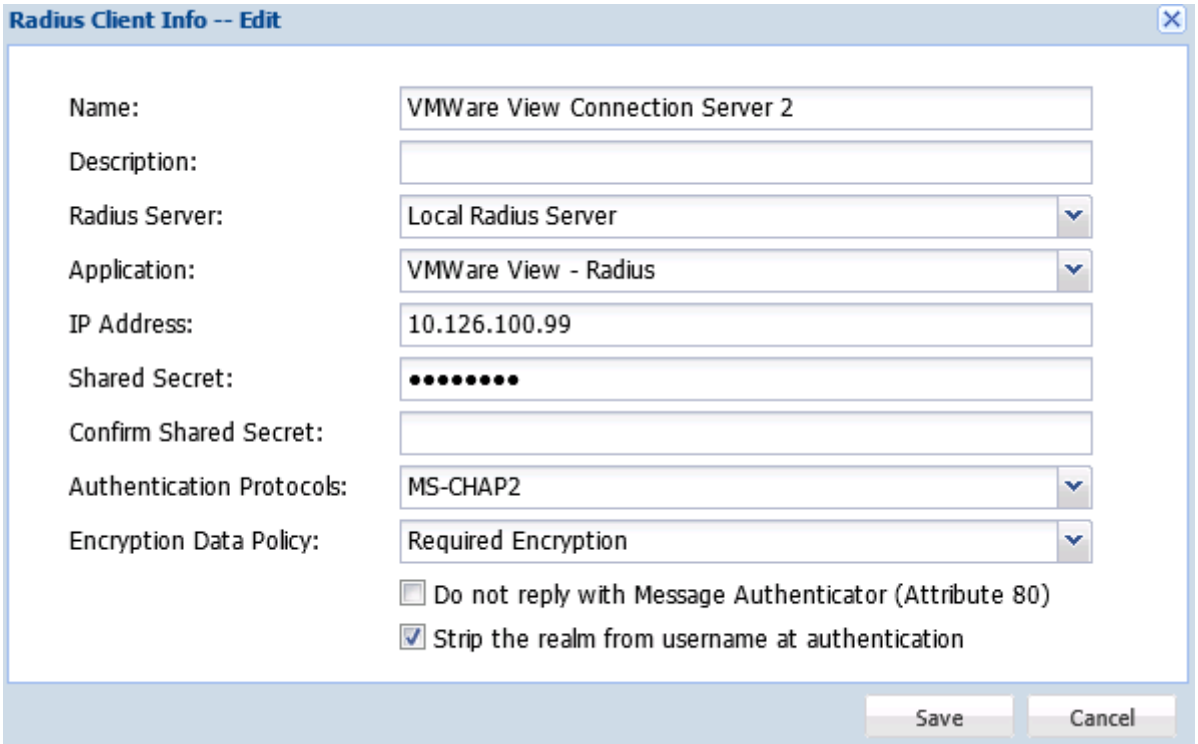


Ensuite, j'ai créé un composant « Application » qui lie la banque de données utilisateur à mon composant précédent.



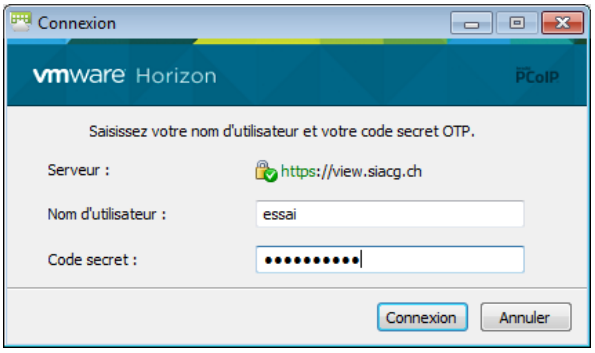
Enfin, j'ai créé les composants clients radius. Ces composants mettent en lien les serveurs VMWare à l'application précédemment créée.


Radius Client Info -- Edit
Name:
VMWare View Connection Server 1
Description:
Radius Server:
Local Radius Server
Application:
VMWare View - Radius
IP Address:
10.126.100.98
Shared Secret:
Confirm Shared Secret:
Authentication Protocols:
MS-CHAP2
Encryption Data Policy:
Required Encryption
Do not reply with Message Authenticator (Attribute 80)
Strip the realm from username at authentication
Save
Cancel


Radius Client Info -- Edit
Name:
VMWare View Connection Server 2
Description:
Radius Server:
Local Radius Server
Application:
VMWare View - Radius
IP Address:
10.126.100.99
Shared Secret:
Confirm Shared Secret:
Authentication Protocols:
MS-CHAP2
Encryption Data Policy:
Required Encryption
Do not reply with Message Authenticator (Attribute 80)
Strip the realm from username at authentication
Save
Cancel

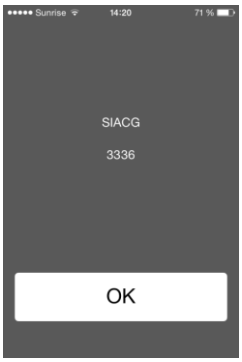
Contrôle du fonctionnement

Lors de la connexion, le client VMWare demande le nom d'utilisateur et le mot de passe. L'OTP n'est pas nécessaire ici, il s'agit là d'un bug d'affichage.

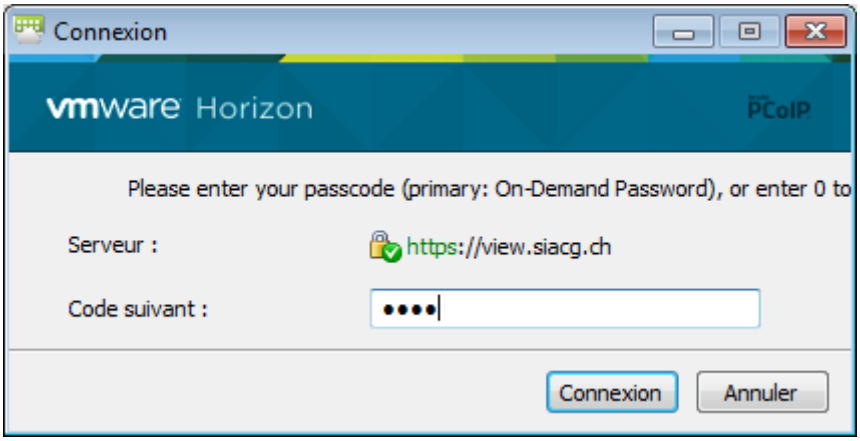


Si le mot de passe de l'utilisateur est correct, le système envoie un SMS contenant le mot de passe unique sur le numéro de portable de l'utilisateur concerné.

Exemple de SMS que nous recevons :



L'utilisateur doit ensuite saisir son code unique et reçu par SMS ou un OTP s'il dispose d'un token matériel, dans la fenêtre suivante qui s'affiche.



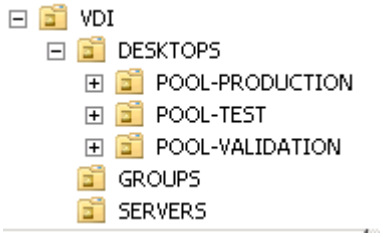
3.7 Installation View Composer

Le rôle View Composer est installé, soit sur un serveur séparé, soit sur le VCenter. J'ai choisi de l'installer sur le VCenter afin de simplifier la configuration. Pour ce serveur le prérequis est d'avoir une base de donnée SQL.

3.8 Préparation Active Directory

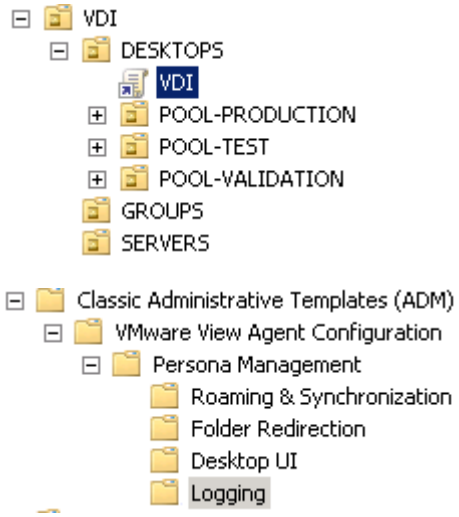
Au niveau de l'active directory, la structure est la suivante :

Vue OU :



En ayant cette structure, chaque pool génère ses VM's dans son OU. Ceci permet d'être flexible si l'on veut appliquer des paramètres différents à chaque pool. L'OU groups sert juste à « ranger » le group VDI-USERS. Ce groupe est dans les remote desktop users des VM's. Le groupe serveur regroupe les 4 ESX.

Vue GPO :



Lorsque j'ai commencé à analyser la façon de mettre en place les profils itinérants, il était nécessaire de trouver une solution afin d'éviter de déplacer les comptes des utilisateurs qui se trouvent dans d'autres OU. La GPO « VDI » ci-dessous s'applique uniquement au « computer » et résout cette contrainte. La 2ème problématique est la suivante : un utilisateur « VDI » se connecte sur un poste physique, son profil itinérant VMware

s'appliquerait-il aussi au niveau de cette machine ? Étant donné que les machines physiques sont également dans d'autres OU, ceci fonctionne donc parfaitement.

Paramètres configurés **:**

Manage user persona : active / désactive les profils

Persona repositroy location : spécifie le chemin des profils (**\\servername\share**)

Remove local personna at log off : Ce paramètre permet de supprimer le profil lors de la fermeture de session. Cette opération nécessite du temps supplémentaire. Étant donné que je supprime le poste à chaque fermeture de session, il n'est pas nécessaire d'effectuer cette opération.

Setting	State
Manage user persona	Enabled
Persona repository location	Enabled
Remove local persona at log off	Disabled
Roam local settings folders	Not configured
Files and folders to preload	Not configured
Files and folders to preload (exceptions)	Not configured
Windows roaming profiles synchronization	Not configured
Windows roaming profiles synchronization (exceptions)	Not configured
Files and folders excluded from roaming	Not configured
Files and folders excluded from roaming (exceptions)	Not configured
Enable background download for laptops	Not configured
Folders to background download	Not configured
Folders to background download (exceptions)	Not configured
Excluded Processes	Not configured
Cleanup CLFS Files	Not configured

Figure 10 - Config personamanagement 1

Add the administrators group to redirected folders : Ce paramètre permet d'ajouter les droits administrateur sur le dossier utilisateur final. Ceci est nécessaire pour que les administrateurs puissent supprimer, par exemple, un utilisateur. Par défaut, seul l'utilisateur a le droit de le faire. Le seul moyen de supprimer le répertoire par la suite est de changer le propriétaire dans les options de sécurités Windows (Take Ownership).

Desktop / Favorites : permet de rediriger le dossier « Bureau » et « Favoris » de l'utilisateur sur un partage.

Setting	State
Add the administrators group to redirected folders	Enabled
Files and folders excluded from Folder Redirection	Not configured
Files and folders excluded from Folder Redirection (exceptions)	Not configured
Application Data (Roaming)	Not configured
Contacts	Not configured
Cookies	Not configured
Desktop	Enabled
Downloads	Not configured
Favorites	Enabled
History	Not configured
Links	Not configured
My Documents	Not configured
My Music	Not configured
My Pictures	Not configured
My Videos	Not configured
Network Neighborhood	Not configured
Printer Neighborhood	Not configured
Recent Items	Not configured
Saved Games	Not configured
Searches	Not configured
Send To	Not configured
Start Menu	Not configured
Startup Items	Not configured
Templates	Not configured
Temporary Internet Files	Not configured

Figure 11 - Config personamanagement 2

Show progress when downloading large files : Ce paramètre permet de configurer une barre de progression si un fichier de grosse taille devait être téléchargé (Taille paramètrable).

Show critical errors to users via tray icon alerts : Ce paramètre rend possible la notification de l'utilisateur s'il y a une erreur avec certains fichiers.

Setting	State
Hide local offline file icon	Not configured
Show progress when downloading large files	Enabled
Show critical errors to users via tray icon alerts	Enabled

Figure 12 - Config personamanagement 3

Logging filename & flags : Redirection des logs concernant persona management

Setting	State
Logging filename	Enabled
Logging destination	Not configured
Logging flags	Enabled
Debug flags	Not configured

Figure 13 - Config personamanagement 4

3.9 Préparation VM parente

3.9.1 Image de base Windows 7 x64

La VM parente est nécessaire lors de l'utilisation du clone lié. Tout paramètre de base (configuration Windows, mise à jour, lecteurs cd virtuel etc) est répercuté sur les clones. Il est donc important d'avoir une image de base propre. Pour ce faire, j'ai utilisé notre image Windows 7 personnalisée qui est au format .WIM.

3.9.2 Convertir image de base .WIM en ISO

Afin de la rendre disponible dans VMware, j'ai dû convertir celle-ci au format ISO. J'utilise l'outil Oscdimg[19] afin d'effectuer cette opération. L'image de base SIACG étant plus grande que 4 Go, le paramètre –u2 est nécessaire. Il permet de dépasser la limite de taille (Format UDF de fichiers).

Commande finale utilisée :

oscdimg.exe –lWIN7SIACG -m -u2 -bC:\WIN7SIACG\boot\etfsboot.com C:\WIN7SIACG C:\WIN7SIACG.ISO

Une fois l'ISO généré, je l'ai déchargé dans le datastore prévu à cet effet :

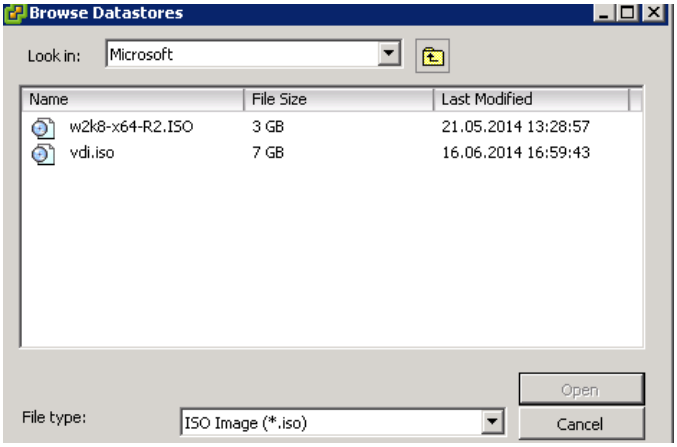


Figure 14 - Datastore ISO Windows 7

[19] Oscdimg.exe http://technet.microsoft.com/fr-fr/library/cc749036%28v=ws.10%29.aspx.

3.9.3 Création VM parente.

Paramètres de la VM parente :

- RAM : 4 GB
- CPU : 1 x vCPU (2 cores)
- HDD : Un disque de 50 Go en Thin provision
- Lecteur CD / DVD : 1

Ne pas oublier de cocher « Connect at power on » et de changer l'ordre de boot dans le BIOS en mettant le DVD en 1er.

J'ai ensuite édité le lecteur de la VM parente en sélectionnant l'ISO précédemment uploadé.

3.9.4 Personnalisation VM parente

Ci-dessous les points essentiels à la personnalisation de la VM parente :

- Installer les VMware Tools
- Mise dans le domaine (même domaine que les futurs clones)
- Activation Windows par KMS
- Activation Office 2010 Standard par KMS
- Script d'optimisation fourni par VMware
    - Désactivation de services inutiles en virtualisation
    - Désactivation thèmes, fonds d'écran etc
    - Optimisations diverses
- Installation de l'agent VMware
- Installation d'Office 2010
- Update Windows
- Update antivirus
- Release ipconfig
- Shutdown de la machine

3.9.5 Snapshot pour pool VMware View

Une fois la VM parente personnalisée et éteinte un snapshot doit être fait. Il sera ensuite affecté à un pool de machines.

3.9.6 Quickprep vs Sysprep

Quickprep est un outil de personnalisation propre à VMware. On peut exécuter un script avant et après le quickprep. Le SID est commun à tous les clones liés.

Customization specifications manager:

Deux possibilités s'offrent à nous via un wizard créé par VMware. Elles se trouvent dans VCenter.

On peut importer un fichier unattend.xml. Cette méthode est fortement déconseillée par VMware. Je l'ai testée et j'ai effectivement rencontré des problèmes.

Le deuxième choix consiste à suivre le wizard en renseignant le domaine, la clé d'activation Windows (KMS), paramètres réseaux, etc. J'ai donc choisi cette méthode.

3.9.7 Optimisation

Afin d'optimiser les performances essentiellement graphiques du poste de travail virtualisé, j'ai personnalisé le profil par défaut. La technique utilisée pour Windows 7 est de charger le fichier NTUSER.DAT (c:\users\default\NTUSER.DAT) dans le registre et d'éditer les clés (attention à activer les fichiers cachés système). Une fois édité, lorsque les utilisateurs se connecteront, les paramètres seront copiés dans leur profil.

Ci-dessous les quelques réglages appliqués dans notre VM parente :

- Désactivation des animations (fenêtres, clique droit)
- Thème Aero désactivé → Windows 7 basic

3.10 Configuration des pools

Au niveau de la configuration des pools, j'ai opté pour les mêmes réglages. En effet, la seule différence entre les pools réside dans la version du snapshot. La configuration des pools est en quelque sorte assimilée au comportement des VM qui s'y trouvent.

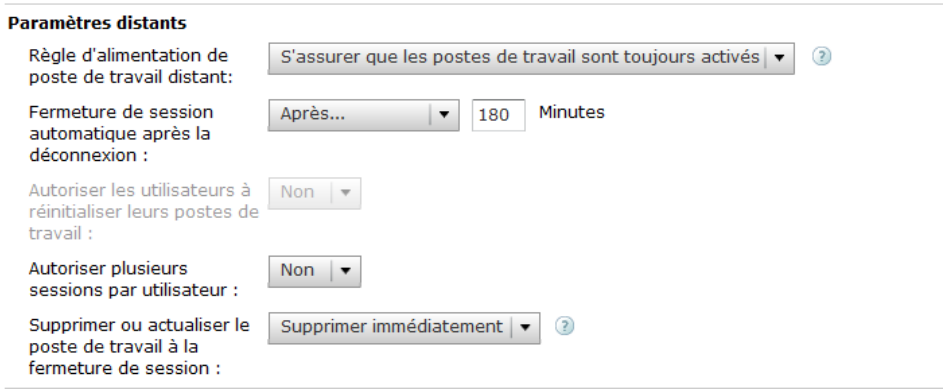
Onglet général

Sur cet écran, deux paramètres sont importants. Le 1er est d'affecter un disque séparé pour chaque VM relative aux fichiers temporaires. En effet, un gain de place se produit lorsque l'on utilise cette option. Il est nécessaire de mettre au minimum la taille de la RAM allouée. Le deuxième paramètre consiste à séparer, au niveau datastore, le disque replica des deltas des VM. Le replica sera accédé par toutes les VM en même temps et aura

besoin d'un grand nombre d'I/O. À contrario du delta disk qui sera accédé uniquement par la VM concernée.

Onglet Paramètres de pool

Dans cet onglet, on retrouve les paramètres ci-dessous :

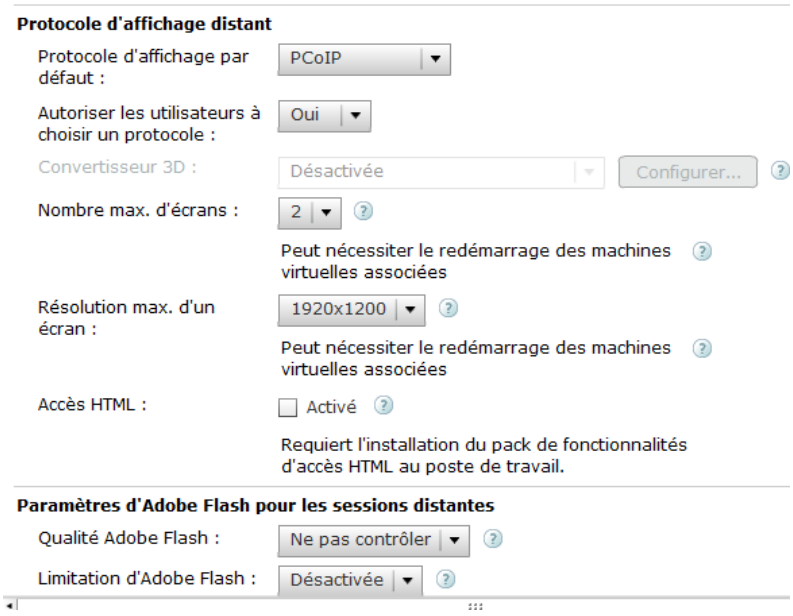


La règle d'alimentation est utile au cas où l'utilisateur ferait un shutdown de sa machine. Je l'ai mise bien que les machines sont supprimées lors d'une fermeture de session.

Le deuxième paramètre est de laisser la session active 3h00 lors d'une déconnexion. Une coupure internet peut arriver à tout moment.

Les sessions multiples sont désactivées, je préfère garder une machine pour un utilisateur. Comme derniers paramètres, je décide de supprimer la VM afin de les garder le plus « propre » possible.

Deuxième partie de cet onglet :



Concernant les protocoles utilisés, il y a le PCoIP de VMware et RDP de Microsoft. Par défaut, j'ai choisi de laisser le PCoIP qui est optimisé pour la virtualisation (légèreté, rapidité, réactivité).

Il est impératif de laisser choisir le protocole de connexion à l'utilisateur. En effet, certaines connexions sans fil (style-hôtel) peuvent avoir des blocages sur certains protocoles, tels MAC et Linux.

Onglet Paramètres d'approvisionnement

Dans cet onglet, l'attribution du nom des VM est configurée. La syntaxe {n :fixed=3} est un incrément automatique pour le nommage des VM. Dans notre cas, j'ai fixé à 3 le nombre de digits utilisés, car nous aurons maximum 200 VM.

Exemple VDI-{n :fixed=3} = VDI-001

Pour la partie dimensionnement, le nombre maximum est de 200VM. Les VM de rechanges sont des machines de spares toujours actives. Si un utilisateur prend une machine provisionnée, VMware View fait en sorte d' en avoir toujours 5 en réserve.

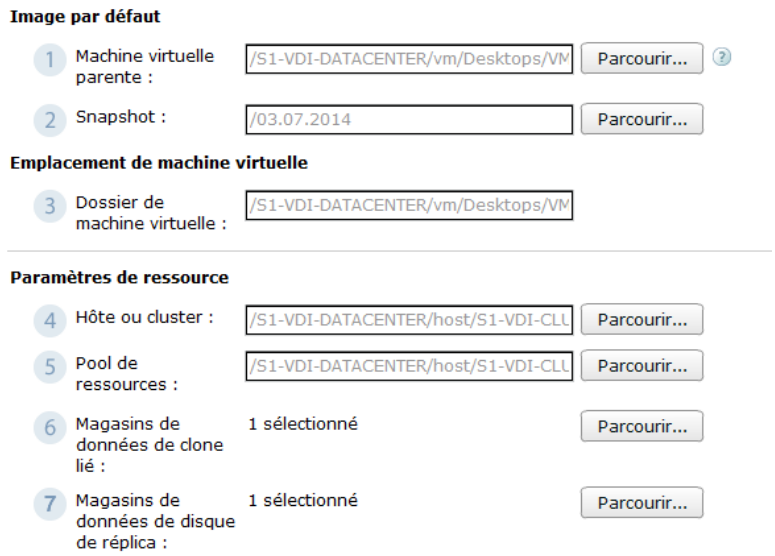
Le dernier paramètre est le nombre de VM provisionnées en cas de maintenance. Pour l'instant ce paramètre reste à 0. Je pars du principe que si je suis en mode maintenance, je ne veux pas de nouvelles VM.

Il y a deux choix pour la durée d'approvisionnement :

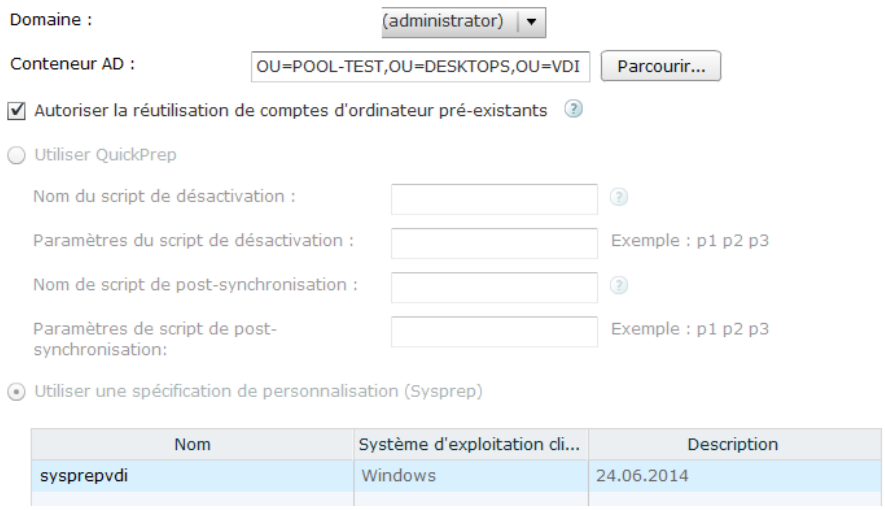
- Provisionner les machines à la demande, avec un minimum de 10 dans mon cas. L'avantage est que les 190 autres VM ne sont pas provisionnées et donc ne prennent pas de ressources. Mais il faut faire attention aux pics de connexion / déconnexion, car s'il n'y a plus de VM provisionnées, l'utilisateur attend.
- Provisionner la valeur maximum, dans notre cas 20 pour commencer lors de la phase pilote et à terme au maximum à 200.

Onglet Paramètres de VCenter

Rien de particulier si ce n'est de choisir la bonne VM parente, le bon snapshot et les datastores :



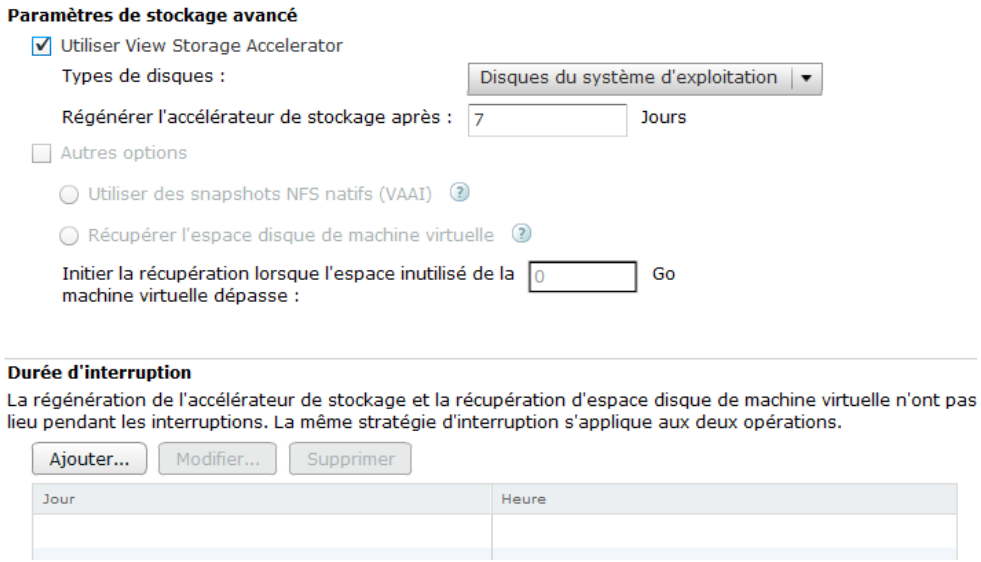
Onglet Personnalisation du client



Sur l'écran ci-dessus, on spécifie le domaine ainsi que l'OU où les VM seront inscrites. Ce qui facilite la maintenance comme expliqué au §3.7 « Préparation Active Directory ».

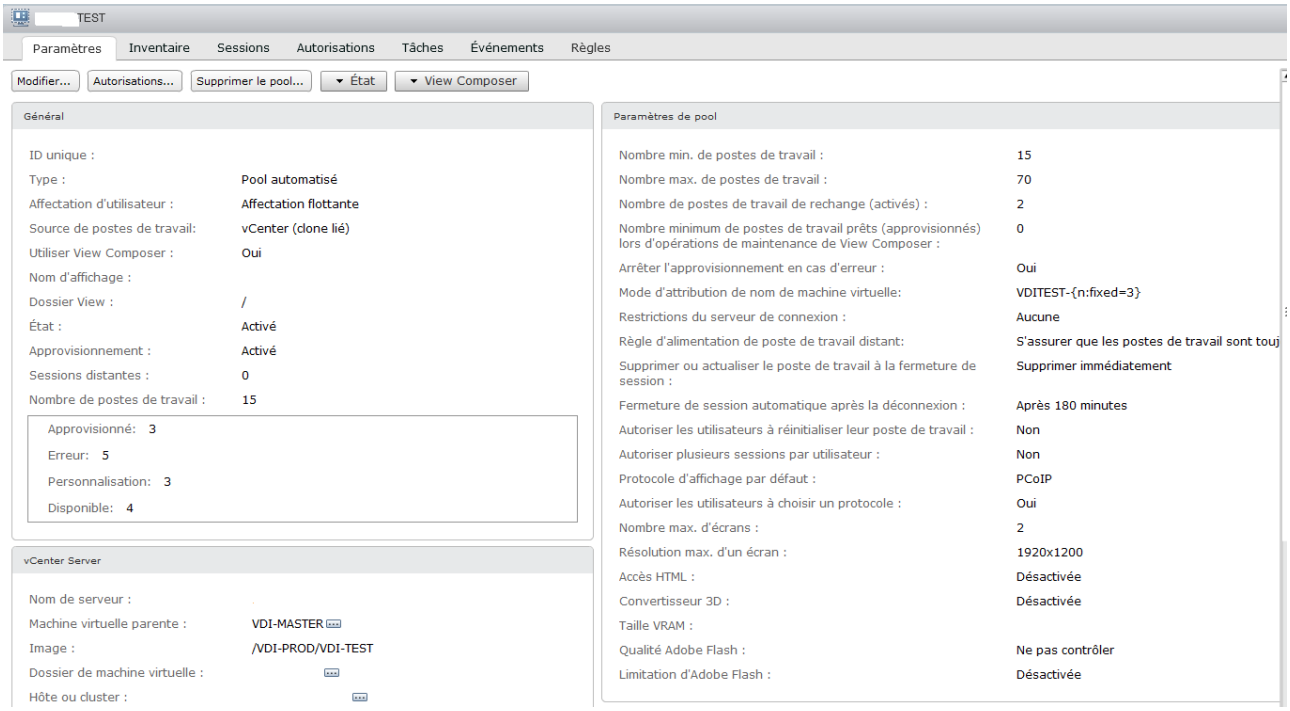
Ensuite, on choisit le sysprep précédemment créé.

Onglet Stockage avancé



Ci-dessus l'utilisation du « View Storage Accelerator » permettant de faire du page sharing.

L'écran principal résumant la configuration mise en place pour les pools de test / prod :



3.11 Configuration de Personamanagement

Les VM étant supprimées à chaque fermeture de session, j'utilise les profils itinérants VMware afin de garder les profils utilisateurs. Ils sont à la fois dans un disque persistent[20] (lié à l'utilisateur) ainsi que sur le datastore SSD (redirect folder).

3.12 Réglages généraux de VMware View

Délai d'expiration de la session :	600 minutes
Authentification unique :	Désactiver après 45 minutes
Mise à jour automatique :	Désactivée
Délai d'expiration de la session de View Administrator :	45 minutes
Message de pré-ouverture de session :	Non
Afficher un avertissement avant la fermeture de session forcée :	Oui

Figure 15- Réglages généraux 1

Sécurité

Modifier... | Modifier le mot de passe de récupération de données

Authentifier à nouveau les connexions par tunnel sécurisé après une interruption de réseau :	Non
Mode de sécurité des messages :	Activé
Activer IPSec pour le couplage du serveur de sécurité :	Oui
Désactiver l'authentification unique pour les opérations en mode local :	Non

Figure 16 - Réglages généraux 2

[20] Disque persistant

3.13 Script personnalisation

Le script de personnalisation consiste à mettre une solution sous forme de batch permettant de copier des icônes et des paramètres spécifiques à l'utilisateur. En effet, en fonction de la commune de l'utilisateur, certaines icônes ne sont pas identiques. De plus, ce script pourra être utilisé pour d'autres besoins.

Structure du script :

- récupère le login name
- regarde le champ « département » du compte AD
- correspondance avec le numéro de commune (tableau n°commune / nom commune)
- copier raccourci dans \\serveurERP\shareERP\programeERP-XX dans c:\users\%username%\desktop

XX = numéro de commune

3.14 Upgrade VMware View 5.3.1 à 5.3.2

Avant la mise en production, nous souhaitons être « up to date » avec notre version de View. De plus, la version 5.3.2 corrige la faille du virus lié au SSL (Heart Bleed). Avant de procéder à la mise à jour, j'ai fait un snapshot de toutes mes VM type « serveur ». Puis j'ai procédé ainsi :

Connections server : Passer l'exécutable de la mise à jour, puis contrôler le changement de version dans la console View

Security server : Passer l'exécutable de la mise à jour, puis nécessite la réassociation avec son connection server ainsi que contrôler le changement de version dans la console View

Parent VM : Passer l'exécutable du nouvel agent VMware, puis contrôler dans la console View le changement de version (régénérer VM du pool nécessaire).

3.15 Backup VM servers (Dataprotection+fichiers)

VMware Dataprotection est une solution de sauvegarde pour VM. Elle repose sur la technologie employée par Avamar[21]. Elle permet de sauver les VMDK des VM. Elle se

[21] Avamar : Solution de sauvegarde professionnelle proposée par EMC.

présente sous forme d'appliance tournant sur une distribution linux. Elle s'interface totalement avec la solution d'administration VCenter (web uniquement). Une fois l'appliance configurée, il suffit de sélectionner les VM's que l'on veut sauvegarder. Nous avons effectué un test de restore d'un connection server. Nous avons éteint le connection server n°2, et restaurer la VM. Elle était opérationnelle en moins de 10 minutes.

QNAP ayant développé un plugin pour VMware, nous avons utilisé notre NAS QNAP pour stocker ces sauvegardes. Depuis ce plugin, il est aisé de créer notre datastore.

Exemple statuts sauvegarde :

Le temps de backup (incrémental) des 2 serveurs + 2 vm parente = 10-15 minutes.

Afin d'avoir une autre méthode de restauration en cas de crash, j'ai configuré notre logiciel de backup pour sauvegarder les fichiers .vmdk des VM's.

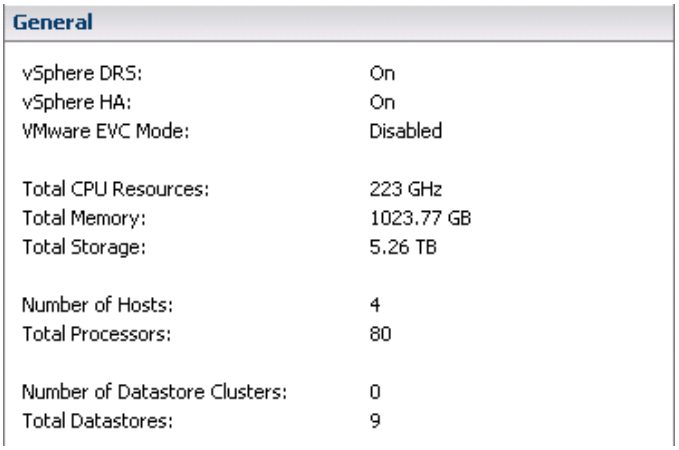
4 Configuration et tests

4.1 Configuration

4.1.1 Matériel

- 4x Blade server UB200M3
  - 8x CPU E5-U2680 v2 (2.80 GHz)
  - 256 Go RAM par lame (DDR3-1866GHz)
  - 2 x SSD 100 Go (RAID 1 pour hyperviseur)

Puissance totale du cluster :



4.1.2 Logiciel

Serveur infrastructure VMware View, recommandations VMware minimums et appliquées :

Rôle	vCPU [Min]	vCPU [App]	vRAM [Min]	vRAM [App]
Vcenter et composer	4	2	3 Go	8 Go
Connection server	2	2	4 Go	8 Go
Security server	2	2	4 Go	8 Go

Système d'exploitation des serveurs :

Système d'exploitation	Version	Édition	Espace disque [Min]	Espace disque [App]
Windows server 2008 R2	64 bits	Enterprise	40 Go	100 Go

4.2 Tests

4.2.1 Tests de disponibilité

4.2.	4.2.1.1.1.1.1 Tests	Résultat	Commentaires
4.3 1 – Hardware			
4.4 1.1 – Alimentation électrique			
A	Sur l'UCS Châssis serveurs: Retirer les alimentations : Couper prise 1, attendre 2 minutes et remettre Couper prise 2, attendre 2 minutes et remettre Couper prise 3, attendre 2 minutes et remettre Couper prise 1 et 4, attendre 2 minutes et remettre Couper prise 1, 2, 4, attendre 2 minutes et remettre Couper prise 1, 2, 4, attendre 2 minutes et remettre Retirer le bloc FAN 2. Résultat attendu : Les VMs doivent rester dans le même status « Powered On ».	OK	
B	Sur les **UCS 6296UP** : Retirer l'alimentation 1, contrôler que chaque UCS 6120 reste allumé. Remettre l'alimentation 1	OK	Perte d'un ping sur vcenter en faisant tomber le Fabric interconnect

	Retirer l'alimentation 2, contrôler que chaque UCS 6120 reste allumé. Remettre l'alimentation 2 Retirer les alimentations 1 et 2 du Fabric interconnect A. Le B doit devenir master. Remettre les 2 alimentations. Retirer les alimentations 1 et 2 du Fabric interconnect B. Le A doit devenir master. Remettre les 2 alimentations.		master (A)

4.5 1.2 – Disque

A	Sur UCS : Retirer le disque 0 de toutes les lames. Vérifier que le serveur continue de fonctionner. Remettre les disques en place.	OK	
B	Sur UCS : Retirer le disque 1 de toutes les lames. Vérifier que le serveur continue de fonctionner. Remettre les disques en place.	OK	

4.6 1.3 – Réseau FCoE

A	Sur UCS 6296UP fabric A: Retirer tous les câbles du fabric A.	OK	

	Vérifier que les cartes apparaissent déconnectées dans VC. Effectuer, à partir d'une machine non virtuelle, un ping d'une ressource active connectée sur le vSwistch et le VDS. Vérifier que la ressource réponde. Rebrancher les câbles. Résultat attendu: Aucun « Request timed out. » n'apparaît dans les réponses. Aucune coupure SAN		
B	Sur UCS 6296UP fabric B: Retirer tous les câbles du fabric B. Vérifier que les cartes apparaissent déconnectées dans VC. Effectuer, à partir d'une machine non virtuelle, un ping d'une ressource active connectée sur le vSwistch et le VDS. Vérifier que la ressource réponde. Rebrancher les câbles. Résultat attendu: Aucun « Request timed out. » n'apparaît dans les réponses. Aucune coupure	OK	

	SAN		

4.7 1.4 – Réseau Ethernet

A	Sur UCS **6296UP A**: Retirer les deux câbles du 6296 A en direction des Nexus. Effectuer, à partir d'une machine non virtuelle, un ping d'une ressource active connectée sur le vSwistch et le VDS. Vérifier que la ressource répond. Rebrancher les câbles. Résultat attendu: Aucun « Request timed out. » n'apparaît dans les réponses. Aucune coupure SAN	OK	
B	Sur UCS **6296UP B**: Retirer les deux câbles du 6296 B en direction des Nexus. Effectuer, à partir d'une machine non virtuelle, un ping d'une ressource active connectée sur le vSwistch et le VDS. Vérifier que la ressource répond. Rebrancher les câbles. Résultat attendu: Aucun « Request timed out. »	OK	

	n'apparaît dans les réponses. Aucune coupure SAN		
B1	Sur UCS 6296UP A et B Couper le lien HA entre les deux 6120 Lancé un VMotion Couper le lien du **6296UP** A sur Nexus 5000 Rebrancher le **6296UP** A sur Nexus 5000 Couper le lien du **6296UP** B sur Nexus 5000 Rebrancher le HA (resynchronisation) Rebrancher le **6296UP** B sur Nexus 5000 Arrêt complet du **6296UP** A. Le B passe en primary. Rallumer le A, attente de la synchronisation et extinction du B. puis rallumer le B. Contrôle du status HA !	OK	Le temps nécessaire à la reconstruction du HA est d'environ 3min

4.8 1.5 –ARRET BRUTAL (Test final)

A	Contrairement au plan initial (arrêt brutal de l'UCS), nous avons décidé de couper l'alimentation électrique générale soit une coupure totale ! --- Contrôler que tous les éléments actifs fonctionnent. Couper l'alimentation électrique générale (retour UPS) Attente d'une minute Rallumer l'alimentation électrique. Simulation d'un crash majeur. Aucune panne matérielle ne doit survenir. Noter ce qui s'est passé au niveau logique.	OK	Vcenter doit être rallumé après coupure si shutdown propre

4.8.1 Tests de performance

Quelques chiffres :

Quoi	
Provisionnement de 1 VM. (Clone VM parente + delta + personnalisation + domaine	7min
Provisionnement de 100 VM. (Clone VM parente + delta + personnalisation + domaine	35min
Espace disque utilisé par 100 VM [Datastore Lclone] [Datastore Replica]	 512 Go 27 Go
Espace disque utilisé par 1 VM [Datastore Lclone] [Datastore Replica]	 5.12 Go 27 Go
1er login sur VM (devant créer le profil sur le share persona) • Commence par le login Windows • Créer le répertoire de profil + répertoire de redirection de dossiers • Synchronise le profil avec la VM (rapatriement en local) • Lancement du script SIACG	32sec
1er login sur VM (en ayant déjà un profil sur le share persona) • Commence par le login Windows • Synchronise le profil avec la VM (rapatriement en local) • Lancement du script SIACG	13sec

	Infra visité	Infra SIACG
Cluster Tot CPU [GHz]	243 GHz	223 GHz
Cluster Tot RAM [Ghz]	1.50 To	1 To
Nombre de CPU	96	80
Espace disque	6.83 To	5.03 To
Nombre de VM	153	200
Nombre d'hôtes	8	4

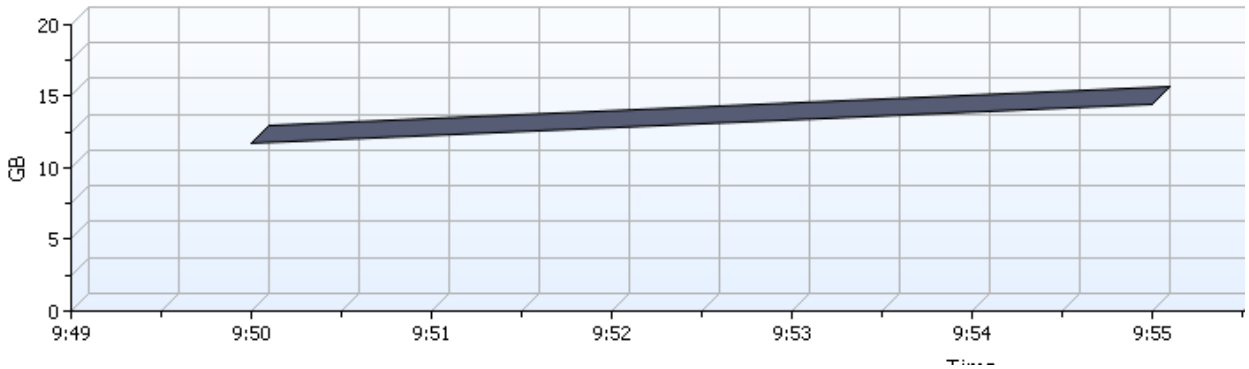
Pour vérifier mes prévisions en terme de performances, j'ai utilisé le logiciel « Veeam One ». Pour disposer de valeur factuelle et large, j'ai procédé à 5 mesures :

Conditions de tests :

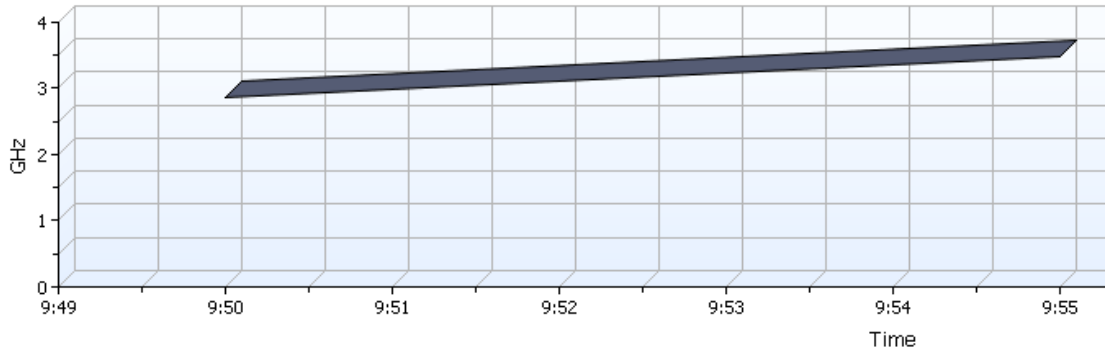
Pool de test activé et prêt à être provisionné.

1er test - Génération d'une VM

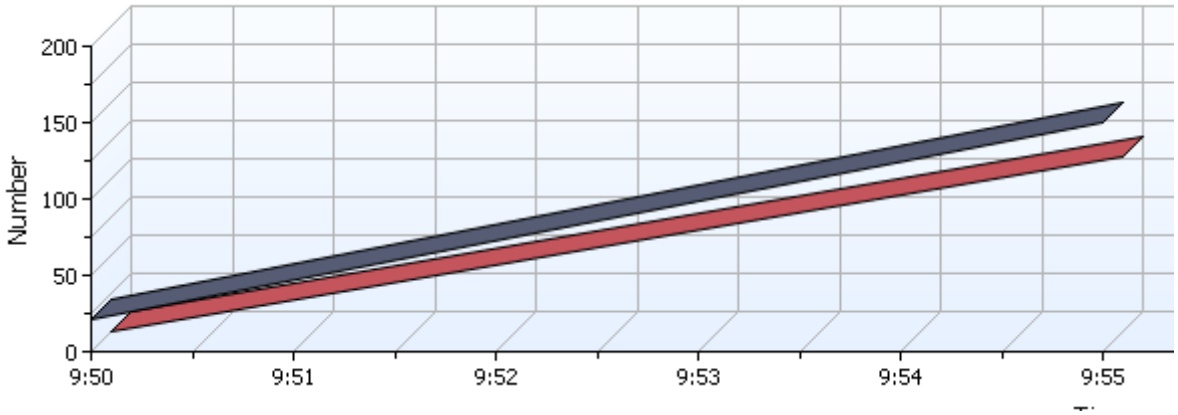
RAM



CPU

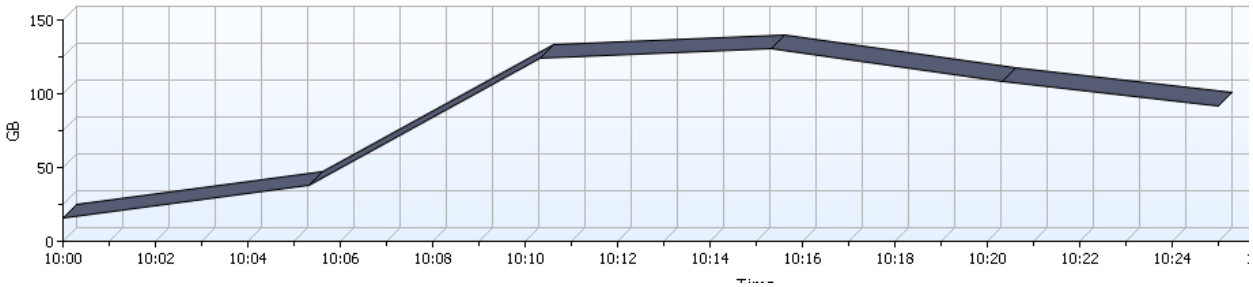


Nombre d'I/O Datastores

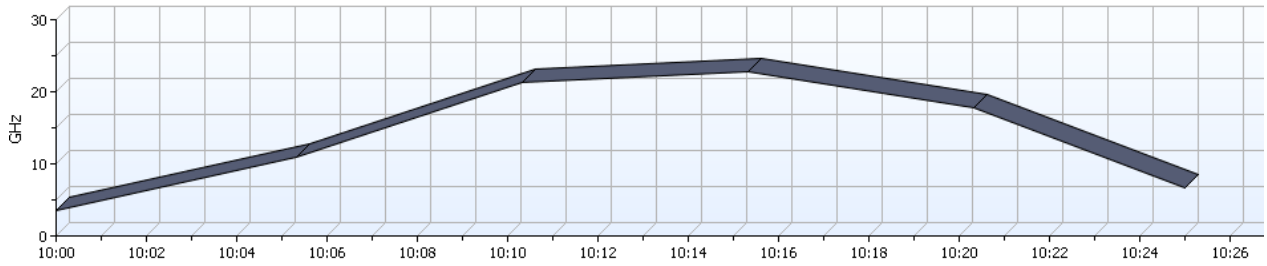


2ème test - Génération de 50 VM's

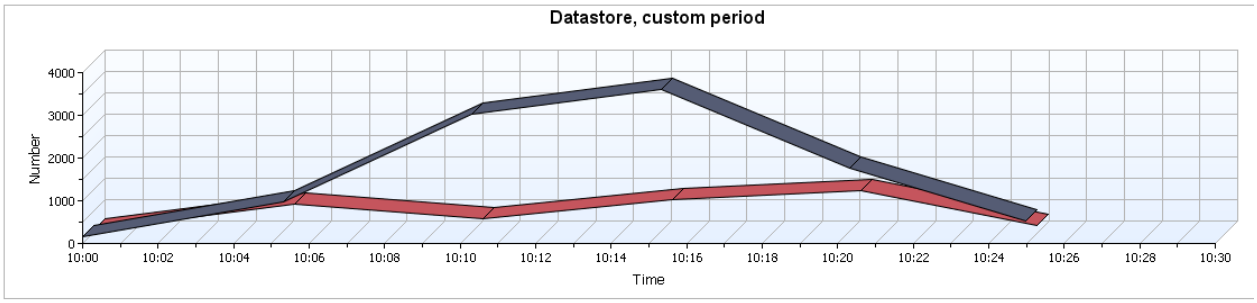
RAM



CPU



Nombre d'I/O Datastores

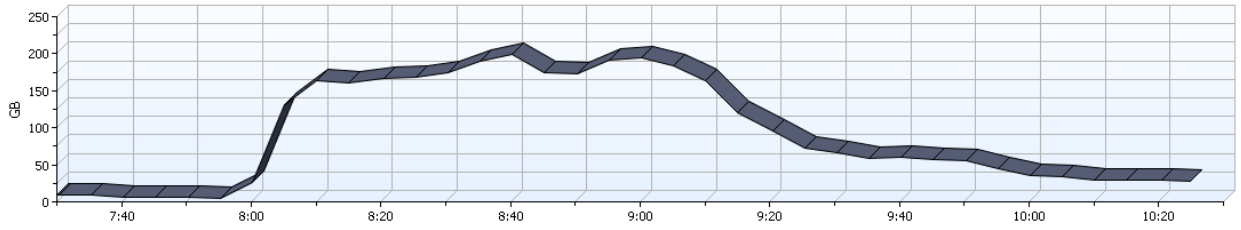


Performance chart legend

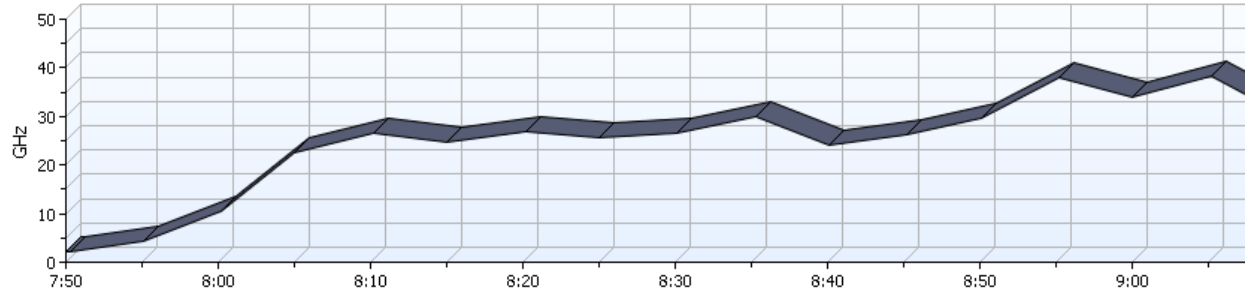
Key	Object	Counter	Units	Latest	Minimum	Average	Maximum
	S1-VDI-CLUSTER/vnx-lun161-Lclone	Datastore I/O	Number	501	139	1658	3588
	S1-VDI-CLUSTER/vnx-lun170-Replica	Datastore I/O	Number	133	36	471	969

3ème test - Génération de 100 VM's

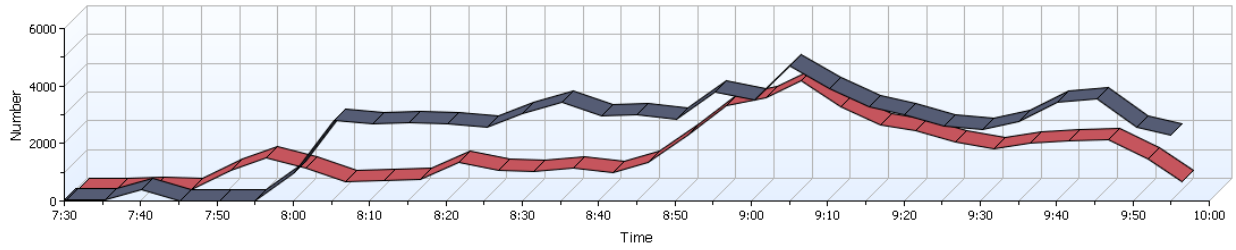
RAM



CPU



I/O Datastores



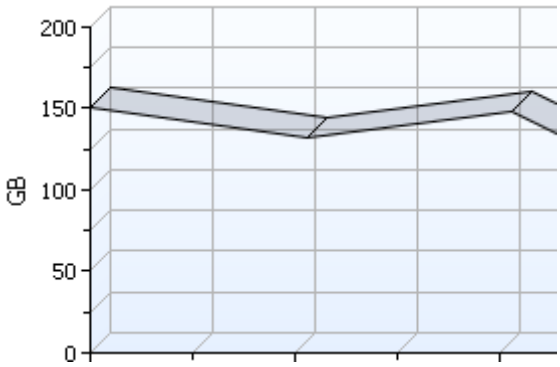
Display known events Advanced... Chart options: Current object Chart views: Custom view... Period:

Performance chart legend

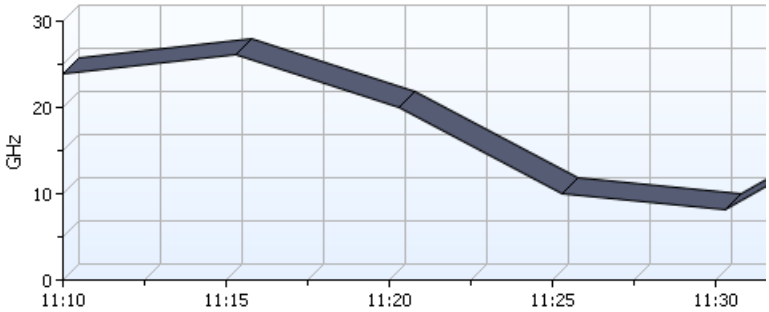
Key	Object	Counter	Units	Latest	Minimum	Average	Maximum
	S1-VDI-CLUSTER/vnx-lun161-Lclone	Datastore I/O	Number	2251	0	2382	4676
	S1-VDI-CLUSTER/vnx-lun170-Replica	Datastore I/O	Number	274	0	1203	3763

4ème test – Test réel avec 8 utilisateurs pendant env 30 minutes

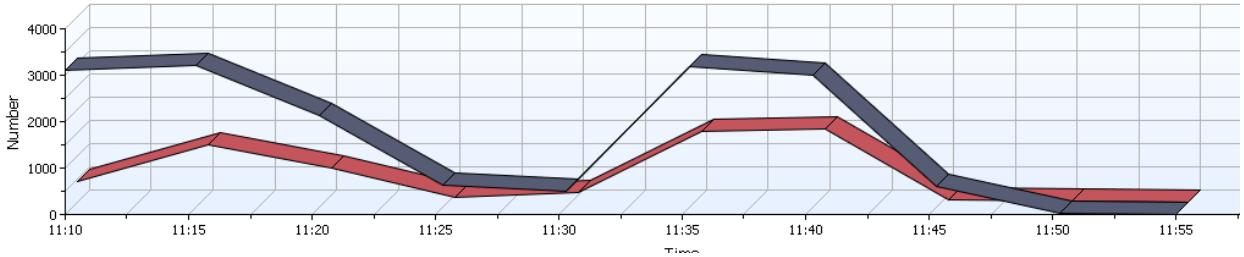
RAM



CPU



I/O Datastores



4.8.2 Tests fonctionnels

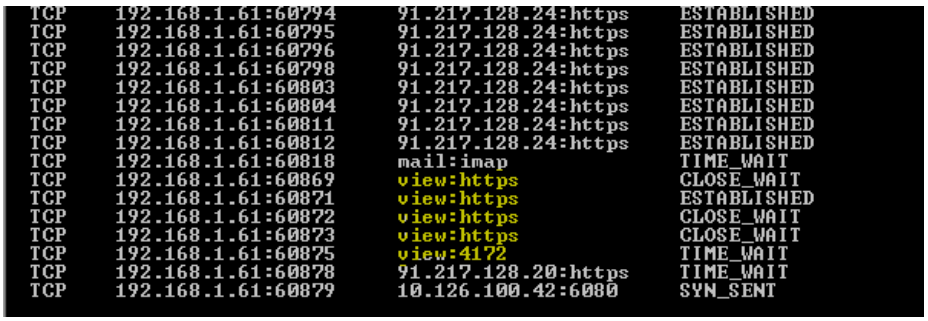
Fonctionnalité testée	Résultat	Remarques
Administrateurs		
Suppression d'un Pool, fichiers VM supprimés datastore ?	OK	
Recompose d'un pool, utilisateurs connectés gardent leur session ?	OK	Replica ancien pool bien détruit ok
Actualisé pool	OK	Efface uniquement partie delta
Désactiver l'approvisionnement, maintenance	OK	
Quota windows pour personamangement	OK	Message d'alerte
Connexion PCoIP, intérieur et extérieur du réseau	OK	Attention ports à ouvrir + agent + vmware tools (driver vidéo)
Connexion RDP, intérieur et extérieur du réseau	OK	
Utilisateurs		
Profil gardé lors de la fermeture de session ? Test en se connectant sur d'autres VM	OK	
Changement de pool, profil itinérant ok ?	OK	
Wizard 1er login outlook disparait lors de reconnexion ?	OK	Prendre roaming profile, sinon NOK
Logiciels ERP	OK	
Windows activé ?	OK	
Office activé ?	OK	
Favoris internet explorer	OK	Pris dans Roaming
Favoris Mozilla Firefox	OK	Pris dans Roaming
Impression sur imprimante réseau	OK	

Connecter un lecteur USB	OK	Attention, toutes les clés ne sont pas compatibles.
Test sur iPad et iPhone	OK	
Test sur MAC	OK	

Test du protocole :

Lors de la connexion à VMware View, une 1ère connexion en https se crée afin de diagloguer avec l'infrastructure. Une fois le poste de travail sélectionné, une 2ème connexion sur le port 4172 (PCoIP) s'ouvre.

Ci-dessous est présenté le résultat avec la commande netstat –b. L'on voit bien que la connexion est en https et qu'il utilise bien le PCoIP



RDP :

Pour le RDP, deux connexions https s'ouvrent.

5 Problèmes rencontrés

5.1 Installation de VCenter

Symptôme

Lors de l'installation du VCenter, le message suivant apparait :

Analyse

Il s'agit là d'un problème d'enregistrement du VCenter. Les certificats SSL n'étant plus ou pas valables ils doivent être supprimés manuellement. Une fois ceux-ci supprimés, il faut relancer l'installation.

Solution

J'ai trouvé la solution sur ce blog :**http://www.petenetlive.com/KB/Article/0000941.htm**

Temps passé sur le problème : 4h00

5.2 Connexion base de données « Évènements »

Symptôme

Lors de la configuration des évènements dans la console VMware View, la connexion à la base de données se termine par un échec. Pour rappel, cette opération est réalisée sur le connection server.

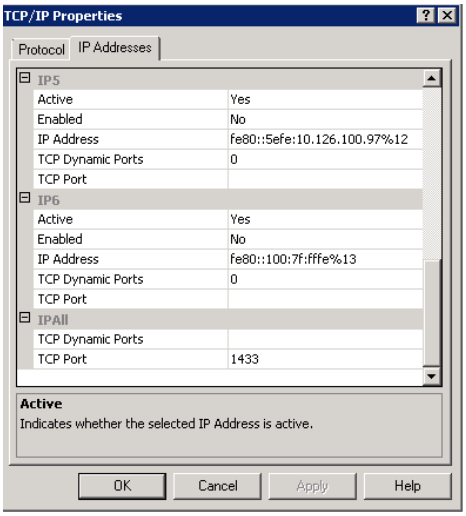
Analyse

Problème n°1 : En faisant un « netstat –a » sur vcenter, je me suis aperçu que le port par défaut (1433) n'était pas ouvert (en mode listening).

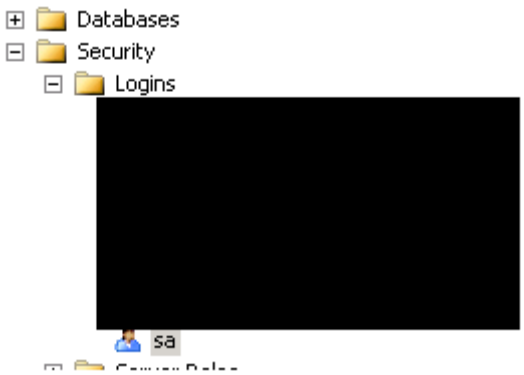
Problème n°2 : Le compte « sa » de la base de données était désactivé pour le login.

Solution

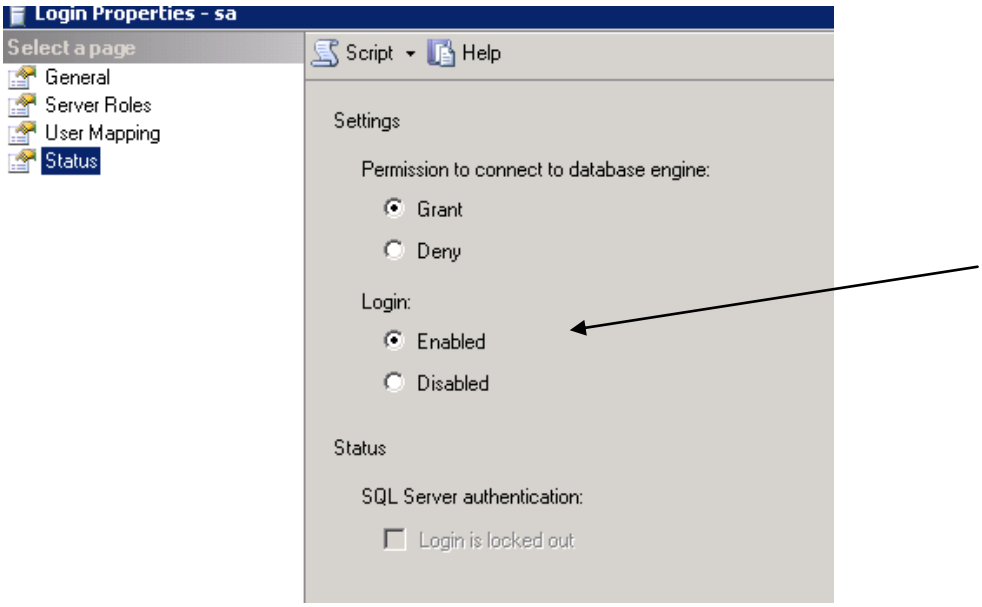
Solution n°1 : Aller dans SQL Server Configuration Manager puis changer la configuration TCP / IP → Port dans Microsoft SQL. Redémarrer le service SQL. Attention, VMware view n'est plus disponible pendant le redémarrage des services (SQL, VMware etc.).



Solution n°2 : Activer le compte « sa » à l'aide de la console de management SQL



Propriétés sur le compte, puis :



Temps passé sur le problème : 3h00

5.3 Personnalisation VM

Symptôme

Lors du provisionnement des VM, les VM avaient le statut « Customizing » et se terminaient en erreur.

Analyse

Solution

VMware agent manquant

Temps passé sur le problème : 24h00

5.4 DHCP Full

Symptôme

L'agent ne pouvait plus communiquer avec le serveur.

Analyse

Je me suis aperçu que les VM à problème n'avaient pas d'adresse IP.

Solution :

En regardant le statut du range IP dans le DHCP, je me suis aperçu qu'il était à 100% d'utilisation suite à la génération de 100 VM's. Le problème est que le bail était de 8 jours

et donc ceci « bloquait » le renouvellement de bail des nouvelles VM's. J'ai abaissé à 2h00 le renouvellement.

Temps passé sur le problème : 1h00

5.5 Activation office 2010

Symptôme

L'activation d'Office 2010 ne s'effectuait pas lors du démarrage de la VM.

Analyse

En tapant la commande cscript //b C:\Program Files\Microsoft Office\Office14\ospp.vbs /dlv, la version d'office était en MAK édition et non en mode KMS.

Solution

Pour résoudre ce problème, j'ai adapté notre .msp (fichier configuration) pour une installation en mode KMS. Puis le script d'activation (run once du sysprep VMware) fait son travail lors de la génération des VM's.

Temps passé sur le problème : 2h00

5.6 Profils personamanagement profile / vs redirect folder

Symptôme

Les répertoires redirigés des utilisateurs ne sont pas repris lorsqu'on se connecte sur une autre VM.

Analyse

En voulant rediriger les dossiers « bureau » et « favoris » dans le même répertoire que les profils gérés par personamanagement, aucun dossier n'est créé. Si je choisis un autre répertoire, la synchronisation fonctionne. J'ai donc fait des recherches à ce sujet et j'ai trouvé ma réponse dans le lien mentionné dans la solution.

Solution

Ci-dessous se trouve le lien qui m'a permis de comprendre l'erreur. Il y a aussi d'autres cas qui permettent un bon 1er debugging des profils.

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2019502

Temps passé sur le problème : 2h00

5.7 Protocole d'affichage non disponible

Symptôme

Lors de la connexion au VDI, il y a le message « Protocole non disponible, veuillez contacter votre administrateur » et / ou lenteur extrême est constatée pour se connecter.

Analyse

Souvent ce phénomène peut arriver lorsque le pilote installé par les VMware tools dans la machine parente pose problème. J'ai donc cherché sur internet et contrôlé la version du pilote. La version était correcte et j'ai trouvé sur ce lien :

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1018158

Solution

Le lien ci-dessus décrit le mode configuration du PCoIP. Les symptômes correspondant à mon problème, j'ai simplement appliqué la procédure qui consiste à désinstaller les VMware tools ainsi que l'agent. Puis, il convient d'installer les VMware tools et l'agent. L'ordre est en effet important sinon cela pose problème. En effet, j'ai fait une mise à jour de l'agent sans prendre en compte ce détail. Ceci en est probablement la cause.

Temps passé sur le problème : 3h00

5.8 CBT (change block tracking) recompose pool

Symptôme

Lorsque j'effectue un « recompose » du pool, le provisionnement s'arrête avec l'erreur suivante : « cannon read or open log tracking ».

Analyse

Ceci est venu lorsque j'ai mis en place dataprotection. Il travaille en mode blocs et a dû changer les paramètres de la VM parente (fait partie des VM sauvegardées)

Solution

J'ai trouvé la solution dans le KB VMware qui indique la procédure soit :

- Eteindre ou supprimer toutes les VM du pool
- Supprimer tous les snapshots

- Editer les paramètres de la VM (option, général, configuration paramètres) et ajouter ctkenable = false
- Supprimer les fichier CTK.vmdk
- Allumer la VM (mise à jour des tables et paramètres)
- Eteindre la VM

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2032214

Complément de procédure trouvée ici :

http://www.symantec.com/business/support/index?page=content&id=TECH197311

Temps passé sur le problème : 3h00

5.9 Certificat SSL, clé privée exportable

Symptôme

Impossible de finir le modèle de certificat.

Analyse

Etant donné que j'ai suivi la procédure à la lettre, j'ai ouvert un ticket chez VMware. La 1ère question du support a été de me demander si ma clé privée était exportable.

Solution

Le support VMware m'a donné le KB suivant à suivre :

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=203240

Resolution

The Microsoft `Certreq` tool is available by default on a Windows Server 2008 R2 system, so a Cer generated quickly.

Note:The tool uses a configuration file to generate a certificate request.

To create the configuration file

1. Save the file `request.inf` (see the *Attachments* section at the end of this article). The file

```
;----------------- request.inf -----------------
[Version]

Signature="$Windows NT$"

[NewRequest]

Subject = "CN=View_Server_FQDN, OU=Organizational_Unit_Name, O=
L=City_Name, S=State_Name, C=Country_Name" ; replace attributes
below
KeySpec = 1
KeyLength = 2048
; Can be 2048, 4096, 8192, or 16384.
; Larger key sizes are more secure, but have
; a greater impact on performance.
Exportable = TRUE
FriendlyName = "vdm"
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0
```

5.10 Certificats SSL, exportation certificat Windows 2008 R2

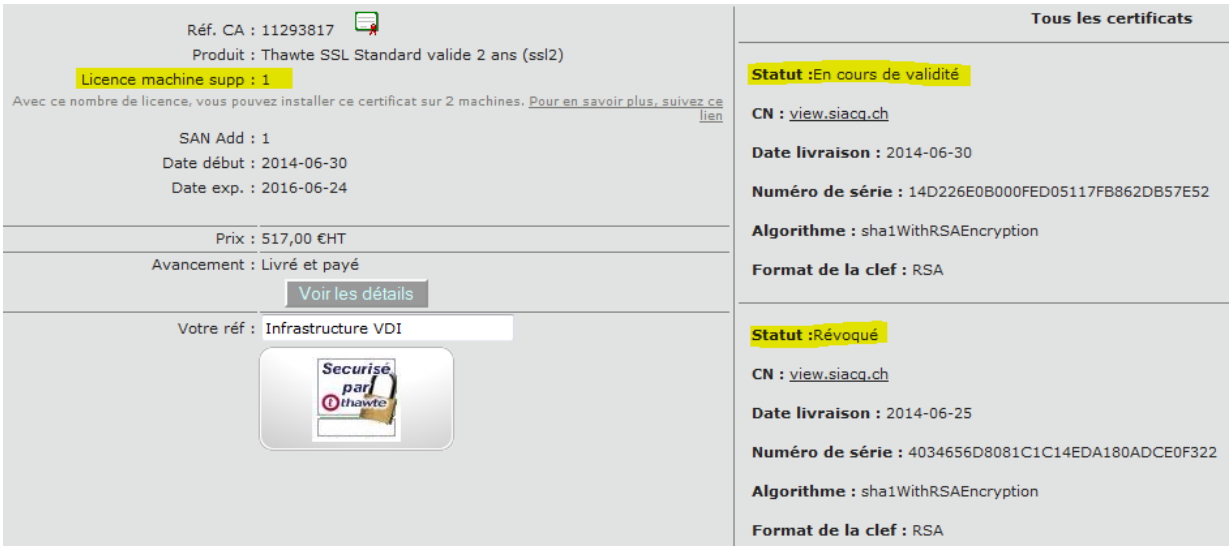
Symptôme

Impossible de le faire fonctionner sur ce deuxième serveur. Le service VMWare refuse d'utiliser ce certificat. L'erreur suivante est remontée dans les journaux d'événements VMWare.

[2014-06-20 12:17:35.175] [ERROR] 1488 [absg-master] - keystoreutil.exe failed to load certificate from ['windows-local-machine', 'MY', 'vdm'] 1 'Key CryptExportKey get size FAILED (error 2148073483)'

Analyse

Après différents essais, j'ai ouvert un ticket chez VMWare. Toutes les astuces données par le support ne m'ont pas aidé. Par soucis d'éventualité, j'ai demandé une re-fabrication du certificat au fournisseur en expliquant la raison. Le support m'a également donné quelques pistes mais sans succès, le certificat a donc été re-fabriqué. La première version a été révoquée comme vous pouvez le voir.



Malheureusement cela n'a pas fonctionné. Ayant demandé de l'aide à mon collègue, il a trouvé la solution. Il s'agit d'un bug non référencé chez Microsoft.

Solution

L'exportation d'un certificat SSL avec clé privée peut dans certain cas ne pas fonctionner. La solution est d'importer le certificat complet émis par l'autorité dans un serveur 2003, l'exporter depuis ce serveur même serveur 2003 et l'importation (toujours avec la clé privée) fonctionne parfaitement dans sur un serveur 2008 r2.

6 Améliorations et besoins futurs

6.1 Infrastructure

Il serait intéressant d'avoir un répartiteur de charges matériel. Ceci permettrait d'une part de répartir au mieux la charge selon l'utilisation des security serveur et des connection serveur. En effet, la répartition de charges actuelle est basée sur celui qui répond le plus vite (ping). Le répartiteur de charge matériel permet en outre de mesurer la charge CPU, RAM, réseau et ainsi donner des indices de charges plus précis.

De plus, un « vrai » répartiteur de charges garde les sessions actives, lors de basculement d'un serveur à un autre. Dans notre situation actuelle, si un des chemins tombe, une interruption de service est constatée car la session utilisateur est perdue. Cependant, lors de la prochaine connexion, l'utilisateur trouvera sa VM allumée au même état lors de la coupure. Certes, on n'est pas à l'abri qu'un des deux chemins tombe. La redondance mise en place (deux chemins) est présente principalement pour avoir deux chemins différents et ainsi de bénéficier de flexibilité pour la maintenance des serveurs.

Le désavantage de cette solution est financier. En effet, le coût s'élève à (~20'000.- Frs)

6.2 Stockage

Concernant le stockage, il sera nécessaire d'augmenter le LUN LClone au fur et à mesure de l'utilisation. Les autres datastores sont surdimensionnés intentionnellement et n'ont pas pour l'instant besoin d'être agrandis.

7 VSAN de VMware

7.1 Introduction au VSAN (Virtual Storage Area Network)

Avant de me lancer dans cette analyse, je me suis documenté pour comprendre ce qu'est, en terme générique, la virtualisation de baie de stockage dans un réseau de stockage ou SAN pour Storage Area Network. Pour poser le sujet, je vous propose cette définition :

« La virtualisation de SAN unifie de façon logique des matériels différents afin de présenter les espaces de stockage, aux serveurs candidats, de manière fédérée en une ou plusieurs ressources de stockage ».

Cette « abstraction » du matériel apporte des avantages évidents au même titre que la virtualisation de serveurs. Ces avantages dépendent des différentes solutions du marché qui offrent plus ou moins de services évolués. Par exemple : réplication entre baies d'origines différentes, extension de volumes à chaud, copies instantanées (snapshots), journalisation des I/O, migration des données toujours à chaud, déplacement automatique des données sur différents matériels suivant certains critères de performances, etc.

Certaines solutions sont même disponibles sous forme de machine virtuelle que l'on intègre dans sa ferme de virtualisation. Le choix entre une solution matériel ou purement logicielle et intégrée à la brique supérieure n'est pas sans conséquence. En effet, ce type de solution est passablement consommatrice de ressources processeur et mémoire dépendant des fonctionnalités additionnelles exploitées. D'autre part, il est important de se poser la question suivante : virtualiser au sein même de l'hyperviseur est-il adéquat du point de vue de la disponibilité ?

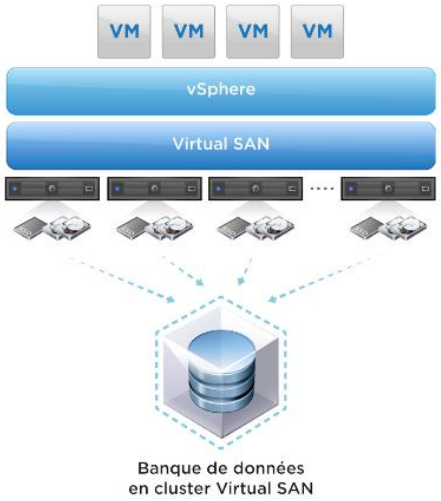
À titre informatif, voici une liste de quelques solutions du marché : DataCore Sansymphonie, Pilar Data, EMC VPLEX Metro, IPStor ou encore et qui fait l'objet de la présente analyse, VMware® Virtual SAN™.

Dans cette analyse, je vous décris :

- ce qu'est VMware® Virtual SAN™ ;
- quelles sont ses spécificités et éventuelles différences avec d'autres solutions ;
- avantages et inconvénients.

7.2 VMware® Virtual SAN™

Cette solution s'intègre dans l'hyperviseur VSphere. Elle crée un niveau de stockage appelé SDS (Software-Defined Storage) pour vSphere. Les disques SSD des hyperviseurs sont utilisés comme cache en lecture/écriture ce qui permet selon VMWare d'augmenter considérablement les performances. J'ose émettre une petite réserve puisque cet argument est peut-être avancé sans tenir compte de la spécificité majeure de cette solution, soit le RAID distribué et détaillé plus loin.



Source VMware

Prérequis matériel :

Pour fonctionner, vous devez disposer au minimum des éléments suivants :

- Cluster hyperviseur de trois hôtes minimum
- Au moins un disque SSD sur chaque hôte
- Carte réseau de 1 Go (10 Go recommandés)
- Adaptateur de bus hôte SATA/SAS ou contrôleur RAID
- Au moins un disque dur standard pour chaque nœud contribuant aux capacités ou une ou plusieurs baies de stockages.

La solution de virtualisation de SAN proposée par VMware s'intègre à vCenter via une appliance. Il s'agit d'un énorme avantage car il est connecté directement à vSphere et donc proche des VM's.

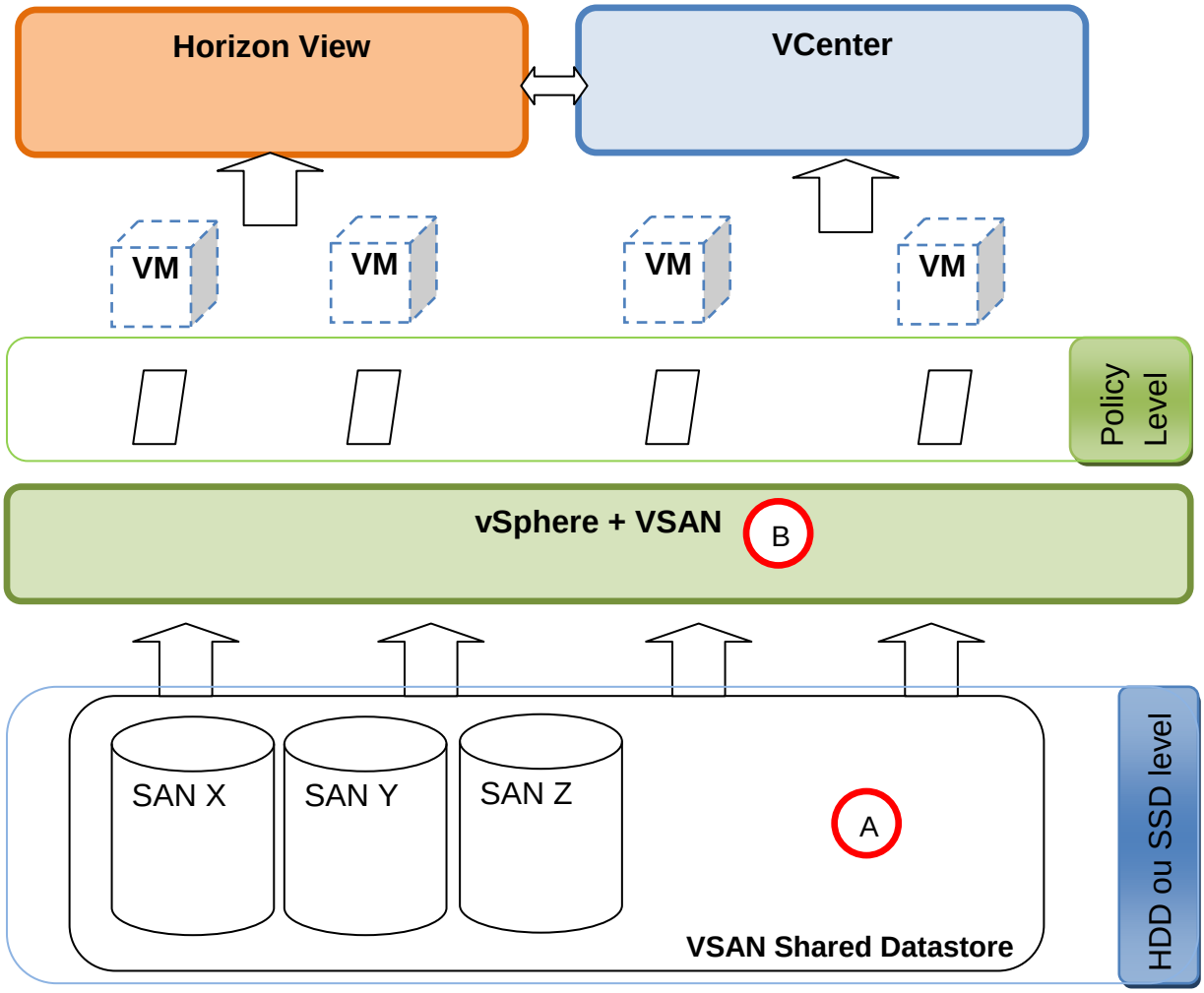
Les principales fonctionnalités de cette solution sont :

- Règle de provisionnement stockage en fonction des SLA
- Répartition selon la charge (QoS) par VM
- Mise en cache (r/w) côté serveur
    - SSD Cache
- Abstraction du matériel multimarque et / ou type différents de stockage
- Auto-tiring[22]
- RAID distribué (expliqué plus en détail au chapitre 7.3.1)

[22] Auto-tiring : Selon les besoins de performances, le déplacement des données s'effectue automatiquement sur le bon support (HDD ou SSD)

7.2.1 Le fonctionnement global :

Dans le schéma ci-dessous, le niveau « Shared Datastore » (A) représente notre partie stockage. Il peut s'agir de plusieurs types ayant de disques différents. Le but étant de créer une unité de stockage logique (Storage Pool). (B)



Il n'y a pas de notion de LUN ni de RAID dans le VSAN. En effet, VSAN de VMware est implémenté dans VSphere et n'as pas besoin qu'on lui affecte des LUN. La VM demande le stockage à VSAN puis à VSphere (qui lui a ses datastores). Il s'agit là de « storage pool » qui est ensuite distribué aux VM via les policy.

VSAN de VMware est capable selon les ressources demandées par une VM de plutôt privilégier le SSD au HDD.

Concernant la tolérance de panne, VSAN permet de mettre différents niveaux de criticités quant à la perte de certaines données (sous-entendu le nombre de copies que l'on a à disposition sur le SAN).

VSAN de VMware s'installe sous forme d'appliance sur n'importe quelle plateforme x86.

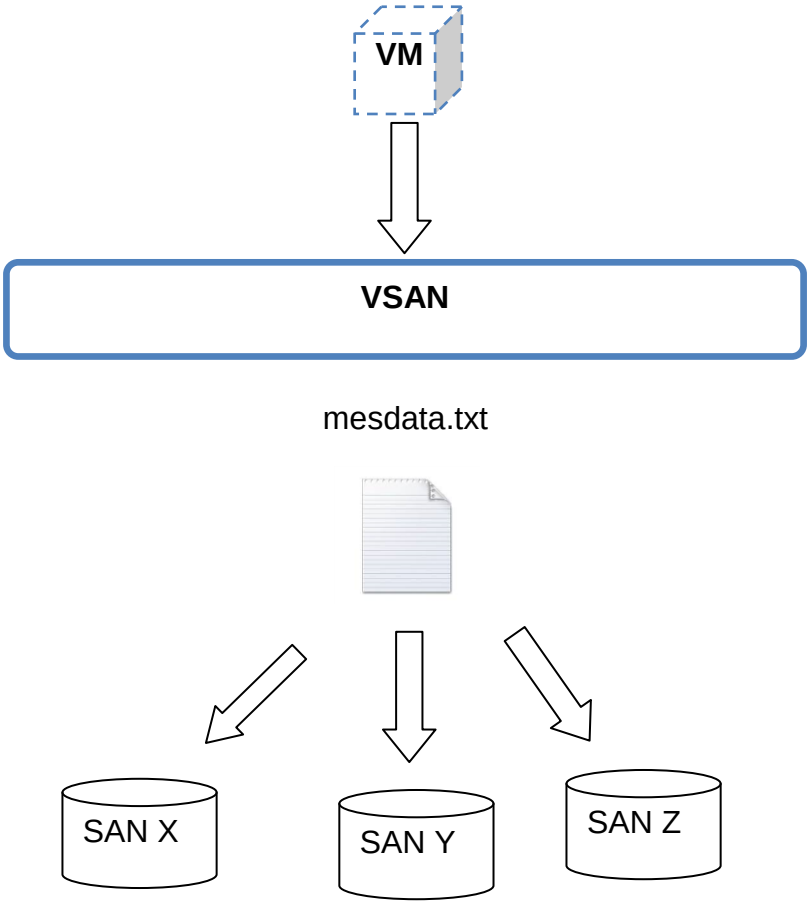
7.3 Spécificités

7.3.1 RAID distribué

Le RAID distribué permet de pallier aux pannes de disques, d'hôtes, ou du réseau. Ci-dessous, je vous présente un exemple avec le fichier « mesdata.txt »

La VM fait la demande de stockage à VSAN. Selon les stratégies appliquées à cette VM, il va, par exemple, dupliquer la donnée sur trois SAN différents.

La stratégie se paramètre comme suit :
Définir le nombre de panne toléré : n=2
Puis la solution va considérer que le nombre de copie est n+1 soit **3 copies**



Limitation des stratégies :
N = est compris entre 0 et 3 y compris

Nombre de copies :
Par défaut la valeur est de 1. L'avantage est que la donnée est sur deux espaces disque différents.

Les avantages :

- En cas de perte d'un disque ou d'un hôte, la donnée est préservée.
- En cas de maintenance d'un disque ou d'un hôte, la VM est rallumée plus rapidement car elle peut se servir de la copie pour remonter le service. En revanche, si la valeur de tolérance de panne est égale à zéro, il n'y a pas de copie donc le temps nécessaire à remonter celui-ci est plus long.

En plus des copies sur plusieurs espaces de stockage, il est possible de réserver un pourcentage par VM.

Limitations du produit :

Supported	Not Applicable	Futures
• VM snapshots • vSphere HA • DRS • vMotion • Storage vMotion • SRM/VR • VDP/VDPA	• SIOC • Storage DRS • DPM	• Horizon View • vCloud Director • 62TB VMDKs

Source VMware

7.3.2 Comparaison

Tableau de comparaison avec 1 autre produit en incluant une tarification approximative.

Fonctionnalité	VMware® Virtual SAN™V 1.0	Datacore SANsymphony™-V 10
Auto-Tiering	x	x
Distributed RAID	x	x
Syncro miroir	x	x
Hypervisor	ESXI	Tous

compatibility		
Taille max capacité	4.4 Petabytes	32 Petabytes
Nombre d'hôtes	3 à 32	2 à 32
Nombre de VM max	3200	?
Prix	2500$	A partir de 4000$

Avantages et inconvénients de la solution VSAN de VMware

Avantages	Inconvénients
Flexibilité (Multimarque de SAN / NAS ou attach direct)	Ajoute de la complexité
Autotiring : SSD ou HDD selon les besoins	Plus la maîtrise d'où sont stockées les données
Pas de LUN	
Intégration de VSAN dans vSphere, console unique de gestion.	
VSAN protection RAID	

Interface d'administration de VSAN VMware

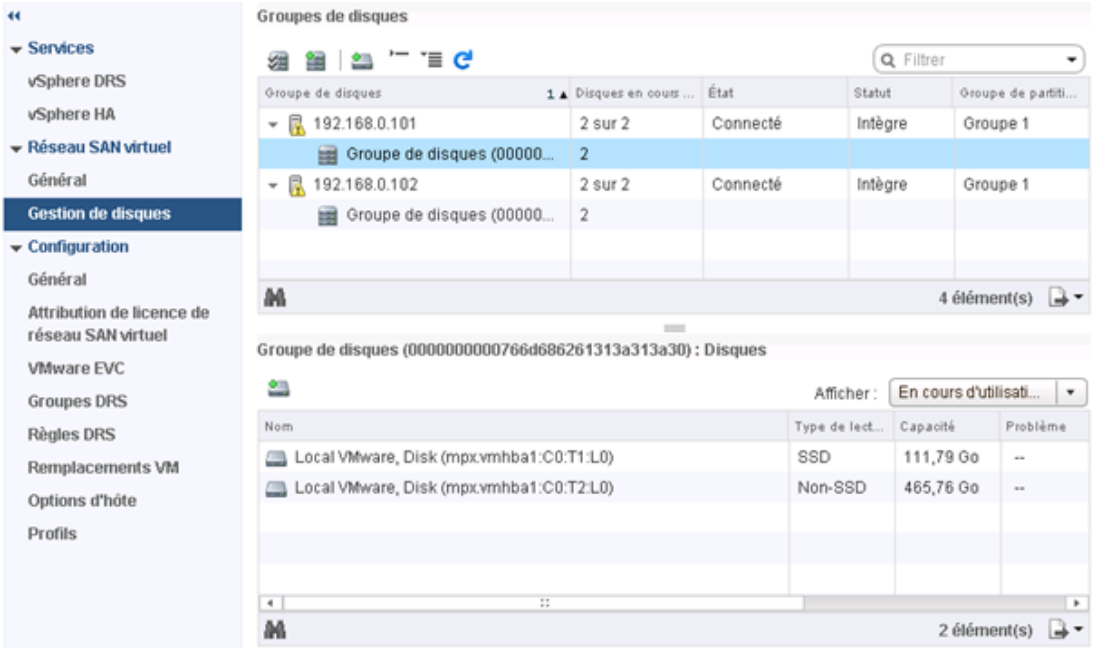


Figure 17 - VSAN groupe de disques

8 Bibliographie

VMware Persona Management

http://pubs.vmware.com/view-52/index.jsp?topic=%2Fcom.vmware.view.planning.doc%2FGUID-05B1BE12-8DD2-4EAE-A3E2-B52CDB6DFC32.html

VMware Persona Management vs Profil itinérant

http://pubs.vmware.com/view-50/index.jsp?topic=/com.vmware.view.administration.doc/GUID-E158A9D4-5FCD-4A61-B987-D01622A96FBF.html

Avantage du clone lié

http://www.vmware.com/files/fr/pdf/support/VMware-view401-architecture-planning-guide-FR.pdf

Explications des gains concernant le stockage en utilisant la technologie des clones liés.

VDI calculator

http://myvirtualcloud.net/?page_id=1076

Outils permettant de simuler les besoins en CPU, Storage, RAM.

Protocole blast

Lien expliquant le fonctionnement du protocole BLAST

http://www.blast.com/software/data_pump/DP_BLAST_Protocol.html

VMware administration guide

http://pubs.vmware.com/view-50/index.jsp?topic=/com.vmware.view.administration.doc/GUID-DD071C2C-316F-49D5-8361-8240CE85374E.html

Guide optimisation Windows 7 for VMware View

Lien permettant la personnalisation de Windows 7. En pièce jointe de ce fichier pdf, il y a des fichiers textes tout faits afin d'automatiser les modifications.

http://www.vmware.com/files/pdf/VMware-View-OptimizationGuideWindows7-EN.pdf

Persitent disk

Lien expliquant l'utilité du disque persistant pour les données utilisateurs en clone lié.

http://pubs.vmware.com/view-50/index.jsp?topic=/com.vmware.view.administration.doc/GUID-73C2B5E4-B983-4FEA-9B48-9568AC96DEC8.html

Gestion de la mémoire sous VMware ESX

Excellent document permettant de mieux comprendre le phénomène de sur allocation de mémoire (memory overcommitment). J'ai, par exemple, trouvé dans ce document la différence de temps d'accès entre de la mémoire vive et un fichier swap.

http://olbaum.free.fr/old/log/VMw/24-Fonctionnement%20et%20concepts-Gestion%20de%20la%20m%C3%A9moire%20sous%20VMware%20ESX.pdf

Installation guide ESX, vCenter

Dans ce lien, j'ai récupéré les prérequis pour l'installation de ESX sur les hôtes ainsi que les différentes possibilités de l'installer.

http://www.vmware.com/files/fr/pdf/support/VMware-ESX-and-vCenter-Server-Installation-Guide-PG-FR.pdf

VSphere, VCenter installation

http://pubs.vmware.com/vsphere-55/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-55-installation-setup-guide.pdf

Calculateur IOPS SSD / HDD en RAID

http://www.google.ch/url?sa=t&rct=j&q=iops%20read%20ssd%20raid%205&source=web&cd=1&ved=0CBwQFjAA&url=http%3A%2F%2Fwww.myvmwareblog.com%2Fwp-content%2Fuploads%2F2012%2F11%2FRAID-and-IOPS.xlsx&ei=XVq2U7mBPfGQ0QW9yYGgBA&usg=AFQjCNG0k7SW9vDCAH9RamFD5-20WgDYcA&bvm=bv.70138588,d.d2k

Editer profil par defaut Windows 7 (reg load)

http://blogs.technet.com/b/chad/archive/2012/04/25/tip-49-how-do-you-set-default-user-profile-registry-settings.aspx

Technical Specifications for SANsymphony™-V 10

http://www.datacore.com/products/technical-information/sansymphony-v-tech-specs

9 Conclusion technique

La virtualisation du poste de travail apporte un réel gain en terme de stockage, maintenance et mobilité. Cependant, elle porte à réfléchir sur d'autres conséquences, telles que l'impact d'une panne ou encore la dépendance des utilisateurs.

En ce qui concerne le stockage, l'image de base est enregistrée une seule fois. Seul le delta (dans mon cas ~16 % de l'image soit ~Go 8 Go par VM) est propre à chaque VM. En ajoutant la technologie de page sharing, l'on gagne encore du stockage sur la masse. Cependant à partir d'un certain nombre de VM l'on arrivera à la limite d'I/O accepté par le LUN replica, ce qui, engendrera un ralentissement général du système. Il faut donc prévoir un 2ème groupe de disques SSD physique afin de répartir la charge.

Il ne faut pas négliger la complexité de ce type d'infrastructure due à l'empilement des couches virtuelles sur du matériel. La détection de panne est plus complexe à identifier. Une formation des ingénieurs s'occupant de ce système est absolument nécessaire pour le support et la maintenance. Certes ceci a un coût mais les bénéfices que l'on en retira en seront supérieurs ; compétences, stabilité de la prestation et satisfaction du client.

Le gain de temps des maintenances est d'autant plus marqué que le nombre de VM's est grand. Par exemple, pour déployer 100 VM's, il ne faut que quelques minutes alors qu'il faut des jours pour installer 100 pc's physiques. De plus, lorsqu'il est nécessaire de mettre à jour les postes de travail, il suffit d'allumer notre VM parente, ajouter les mises à jour puis de régénérer les VM. Le tout est transparent pour l'utilisateur final puisque la régénération de la VM se fait à la fermeture de session. Le revers de la médaille et que si une erreur se trouve dans la VM parente, elle sera déployée sur l'ensemble des VM.

Tenant compte des ressources limitées en entreprise, il est préférable de restreindre le nombre de VM parente. Pour les utilisateurs ayant des besoins spécifiques en termes d'application il peut être intéressant de leur affecter une VM dédiée et de la gérer comme un poste physique (mise à jour, etc..), soit d'utiliser Thinapp[23]. Cette dernière offre la possibilité de virtualiser les applications.

Le ticket d'entrée du VDI est onéreux. Dans la réalité, le poste de travail virtualisé est plus cher que le poste physique. En effet, il est nécessaire de posséder des clients légers pour accéder au VDI ainsi que d'une console d'administration pour les gérer. Dans notre cas, cela est encore plus coûteux car ces postes virtuels sont complémentaires des machines physiques. Il ne faut pas partir dans le VDI en espérant faire des économies. Je pense

[23] Thinapp : Virtualisation d'application.

sincèrement que les avantages offert par le VDI sont pertinents à partir de 100 postes ou pour couvrir le besoin de mobilité.

Enfin, il est nécessaire de sensibilisé les utilisateurs sur les conséquences du télétravail. L'accès à l'environnement de travail en dehors du bureau est une intrusion à la vie privée et peut dans le pire des cas engendrer un « burnout ». Il est important de bien cadrer l'utilisation du VDI en faisant en sorte qu'entre l'employeur et l'employé des règles soient clairement établies avant l'utilisation (décompte des heures, rémunération, lieux de travail, etc.).

En ce qu'il concerne la virtualisation de SAN, deux points ont retenu mon attention. Le faite de ne pas savoir réellement où sont les données est à mon avis dangereux en cas de panne. Le faite de noyer l'information dans une « boîte noir » ajoute un niveau de complexité. Je dirai que dans le cas où l'infrastructure virtuelle est totalement maîtrisée et surtout dans un contexte d'optimisation, la virtualisation de SAN a sa place. En effet, la fonctionnalité « auto-tiring », qui n'est rien d'autre que l'adaptation du stockage en fonction des besoins est juste fabuleuse.

10 Conclusion personnelle

Ce travail de Bachelor m'as permis d'approfondir mes connaissances dans plusieurs disciplines : en virtualisation, stockage, réseau, matériel. Les notions étudiées en cours ont été une bonne base pour commencer ce travail, notamment pour le réseau. J'ai beaucoup appris sur la virtualisation tel que le comportement des VM's.

Humainement cela aura été très enrichissant. Par exemple, j'ai dû me battre pour avoir ce que je voulais avec un prestataire et non ce que lui voulait mettre en place. Toutes les personnes avec lesquelles j'ai collaboré tout au long de ce projet m'ont permis de réaliser ce dernier dans les meilleures conditions.

Les différents problèmes rencontrés m'ont appris à persévérer car la solution ne se trouve jamais en un coup de baguette magique. C'est en cherchant et surtout en comprenant les choses que l'on avance dans la résolution. Pour aider, j'ai utilisé la méthode telle que décrite dans le chapitre « problèmes rencontrés ».

En quelques mots, je vous résume les points simples / difficiles à réaliser de mon point de vue :

Simple :

- Personnalisation de l'image (importer l'image SIACG, activation Windows et office)
- Persona management
- Configuration des pools
- Installation de VMware View avec les différents rôles

Difficile :

- Sysprep
- Configuration base de données d'événements
- Personnalisation du profil par défaut de Windows 7

J'ai apprécié de gérer ce projet, notamment pour l'autonomie confiée et les aspects suivants :

Maintenir les délais, négociation avec les fournisseurs, gérer les processus d'acquisition et surtout la pression stimulante due au service attendu par les communes genevoises.

Concernant le suivi du projet, un journal de bord a été tenu du début jusqu'à la fin. Une planification a été réalisée et adaptée au fur et mesure que le projet avançait.

Les points forts du projet :

- Timing respecté (prestation cliente)
- Infrastructure fonctionnelle
- Cahier des charges respecté

Les points faibles du projet :

- Timing bachelor trop optimiste
- Sous dimensionnement du stockage (à terme)

J'espère que mon travail sera utile pour d'autres personnes afin de mieux comprendre la virtualisation de postes de travail qui n'est pas aussi simple qu'elle ne parait.

11 Annexes

11.1 Type de pool

Le type de VM a des conséquences non négligeables sur un projet VDI car il touche le stockage, la mémoire vive et le réseau.

Pour la partie stockage, il est intéressant d'utiliser le clone lié. En effet, les VM se partagent la même image de base (replica[24]) et créent seulement un disque propre à chaque VM qui est relativement petit et appelé également : delta-disk[25]

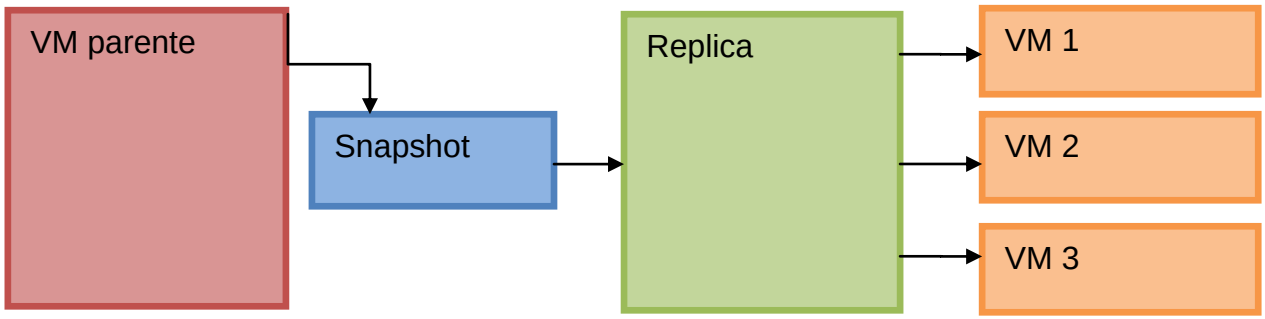
11.1.1 Pool Automatique

Il s'agit de la génération des VM automatique, soit à partir d'un template (VM dédiée), soit à partir d'une snapshot (clone lié).

11.1.1.1 Pool automatique - VM dédiée

11.1.1.2 Pool automatique -Clone lié

Le clone lié utilise le serveur composer pour créer les VM de type clone lié. Il s'agit de créer une VM avec notre image de base Windows 7, puis de réaliser un snapshot de celle-ci. Ce snapshot est ensuite affecté à notre pool. Un replica est automatiquement créé (à mettre sur disque rapide, type SSD). Ensuite à chaque provisionnement de VM, un delta est créé par VM.



Il y a lieu de noter que toutes les VM accèdent à la même image replica.

[24] Replica : image partagée par les VM
[25] Lien décrivant les différents fichiers lié à une VM
https://communities.vmware.com/blogs/ray.heffer/2013/02/25/understanding-vmware-view-51-linked-clones.

En plus du disque replica, chaque VM peut disposer de 3 disques supplémentaires qui sont :

1) OS disk (delta)

Sur ce disque il y a toutes les données propres à la VM, nom de machine, paramètre Windows, etc. Ce disque peut être supprimé à chaque déconnexion de l'utilisateur ou à une fréquence donnée (par exemple tous les samedis à 20h00). Il s'agit d'une bonne façon de garder nos VM propres.

2) Persistent disk (optionnel)

Il s'agit du disque utilisateur. Toutes les données utilisateurs telles que desktop, favoris, mes documents y sont enregistrées. Il peut se combiner avec « persona management » afin de sauver une copie de ce disque sur un fileserver.

4) Disposable disk (optionnel)

Dans ce disque, tous les fichiers temporaires y figurent (appdata\temp, c:\temp), hyberfile, etc).

À noter que les disques ci-dessus sont tous au format vmdk.

11.1.2 Pool manuel

- Utilisation de VM existante
- Utilisé dans des cas particuliers (par exemple reprendre une VM d'un administrateur système)

11.1.2.1 Assignement des machines

11.1.2.2 Dédiée

En mode dédié, l'utilisateur se connecte à son pool et se voit assigner une VM libre (spare) et la garde pour toujours. On peut aussi choisir d'assigner manuellement une VM à un utilisateur.

11.1.2.3 Float

En mode flottant, l'assignement d'une machine se fait de manière aléatoire. L'utilisateur ne reprendra pas forcément la même VM.

11.2 Profil utilisateur

La couche VMware « persona management » nécessite d'installer l'agent view sur le poste. De plus il faut activer la fonctionnalité « View persona Management » lors de l'installation. Ensuite cela se gère par GPO. Les modèles (ADM) sont fournis par VMware et permettent de faire de la redirection réseau de répertoires local (bureau, mes documents, etc.), activation / désactivation de la fonctionnalité, choix de l'intervalle de synchronisation.

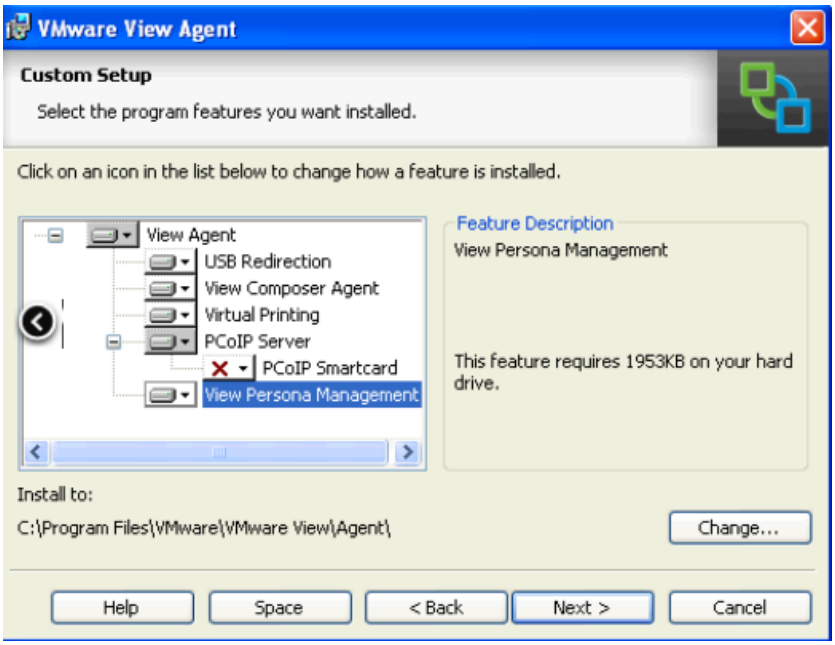


Figure 18 - Agent View persona

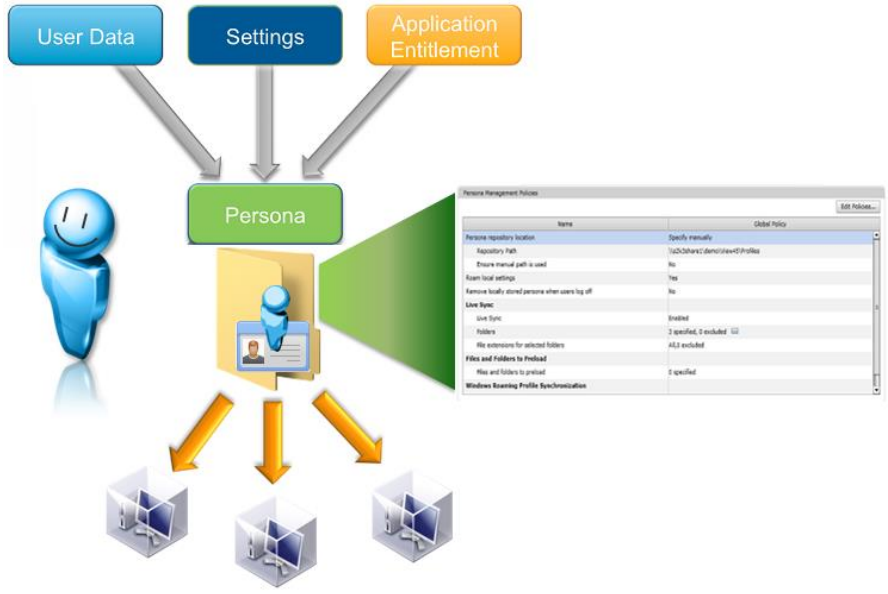


Figure 19 - VMware persona management

Il est également possible de fixer des priorités aux fichiers qui seront synchronisés lors de l'ouverture de session afin de gagner du temps lorsque l'on se connecte. Ceci est déjà une partie avancée de la configuration (tuning).

Un point important est à soulever. Persona management permet de faire soit de la synchronisation soit de la redirection. Dans le cas d'une synchronisation, on utilise un persistent disk qui est lié à l'utilisateur et à son pool. Cette synchronisation se fait par le biais d'un persistent disk sur un serveur de fichier.

Les avantages sont :

- Les données sont plus proches de la VM quant à l'accès (performances)
- Une copie sur le serveur de fichiers (sécurité)

On sauvegarde uniquement les données sur le serveur de fichier, ce qui permet de restaurer uniquement un fichier, un répertoire. A contrario du persistent disk qui lui se restaure en entier.

La redirection, quant à elle, est un simple chemin UNC [26]sur un serveur de fichier.

[26] Universal naming convention : Chemin unicode. A la place d'utiliser une lettre de lecteur, on spécifie le chemin réseau en entier, exemple : \\nomduserveur\nomdupartage.

11.3 View connection server

Le schéma ci-dessous illustre, dans un cas simple, la position du serveur. On verra par la suite le moyen de bénéficier d'une infrastructure sécurisée et redondante.

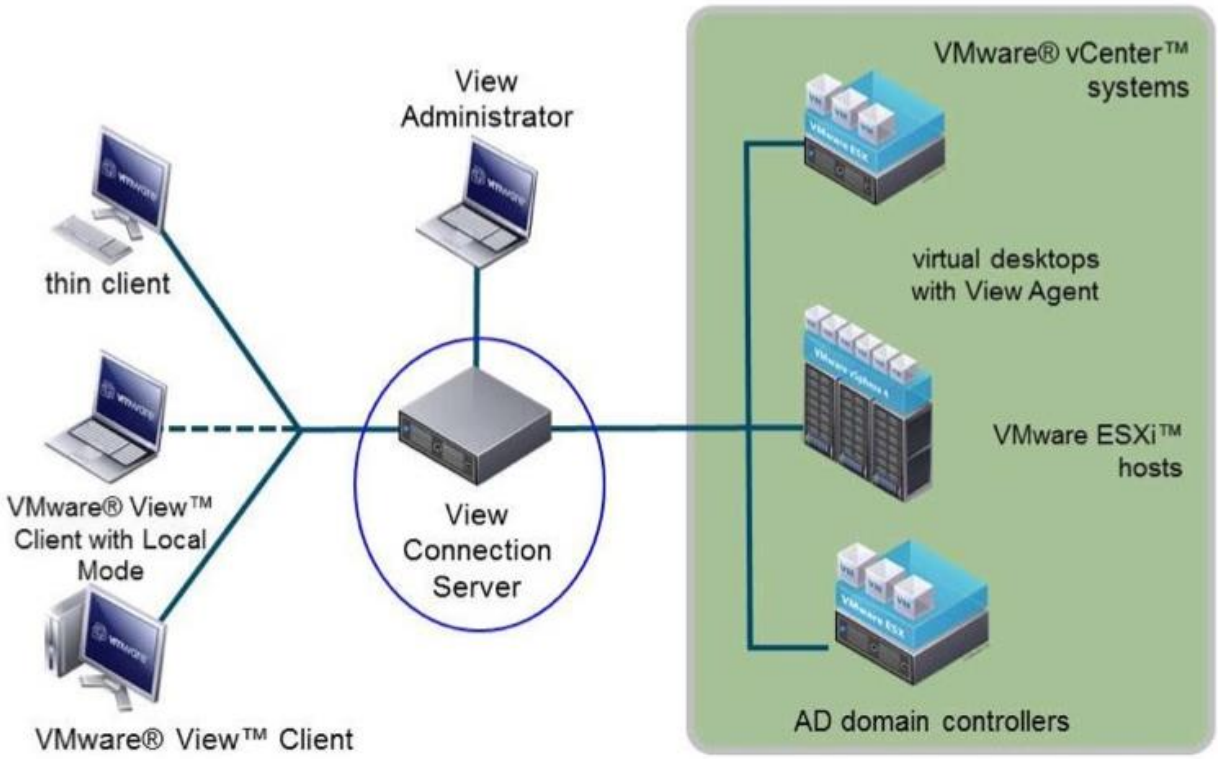


Figure 20 – VMware View Connection Server : Source Cours VMware Horizon View

Au niveau des journaux de ce serveur, 2000 évènements sont conservés par défaut. Cette limite a été fixée par l'éditeur afin de ne pas alourdir l'interface d'administration qui est au format web. Pour pallier à cette limite, il est nécessaire de renseigner une connexion sur un serveur SQL afin d'avoir d'avantages d'événements. Ci-dessous l'interface pour le faire :

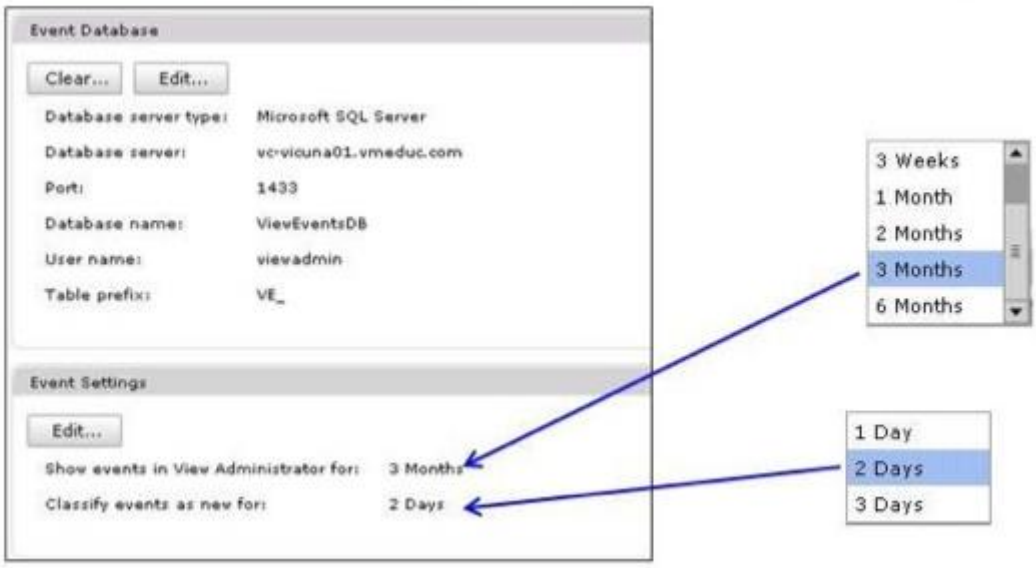


Figure 21 – Paramètres de journalisation

11.4 Security Server

Dans le cas où l'accès au VDI est uniquement fait depuis le réseau LAN de l'entreprise, on pourrait se passer du « security server ».

- Le connection serveur est le point d'entrée à l'accès VDI ainsi qu'à l'interface d'administration. Il est en conséquence nécessaire de le protéger des attaques.
- Le security server se place en DMZ (entre deux firewall) afin de ne pas impacter le réseau entreprise en cas d'attaque.

Ci-dessous le schéma incluant le security server

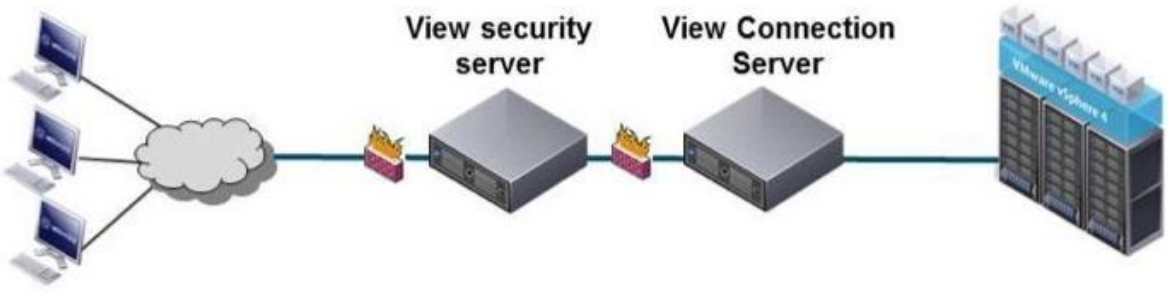


Figure 22 - View Security server : Source Cours VMware Horizon View

En ajoutant la redondance, nous avons un schéma du type :

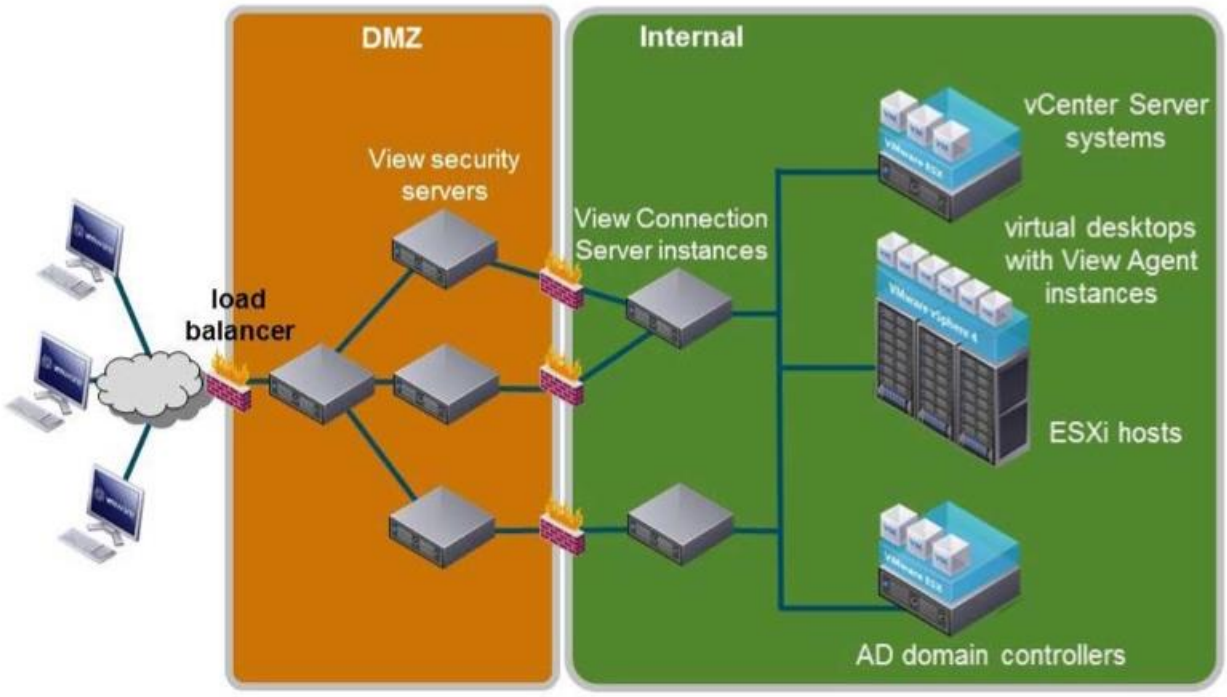


Figure 23 - View Securtiy Server : Source Cours VMware Horizon View

La solution de répartition de charge(loadbalancing) est intéressante afin de :

- proposer de la haute disponibilité
- en cas de maintenance ou arrêt des serveurs non volontaire (security et / ou connection server)

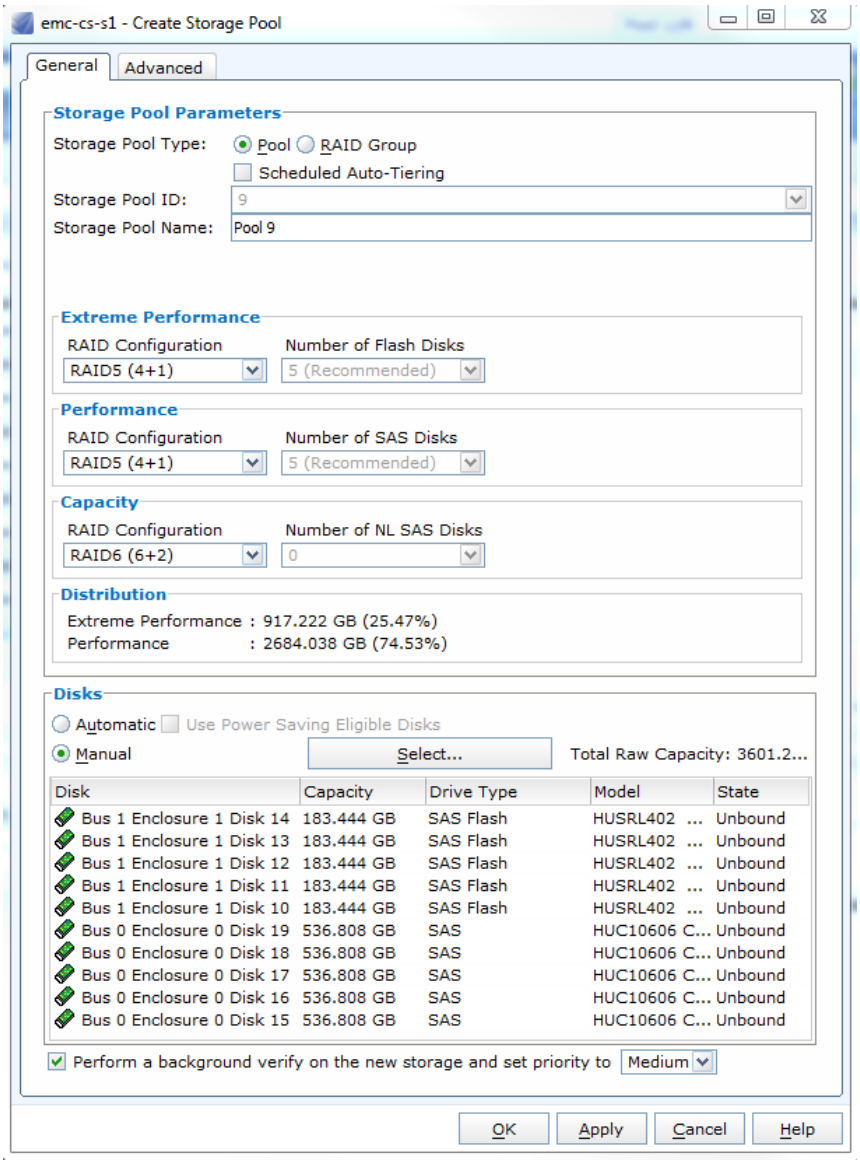
On peut par exemple, effectuer des requêtes snmp sur les view security et connection server afin d'établir un état de charge et répartir celle-ci (% utilisation CPU, % utilisation RAM) ou simplement du round-robin (une fois l'un, une fois l'autre).

Selon les recommandations VMware, un security server est relié à un seul connection server. Pour les lier, il suffit de générer depuis l'interface d'administration (connection server) un one time password où l'on doit choisir la durée de validité. Ceci se fait avant l'installation du security server. Une fois l'installation du security server lancée, on renseigne le mot de passe et les deux serveurs sont liés. Par défaut le security server tente une connexion ipsec entre lui et son connection server. On verra par la suite qu'il est intéressant d'activer cette fonctionnalité qui consiste a créer un tunnel sécurisé de point à point. Une autre fonctionnalité est à activer ; le mode tunnelé de bout en bout. Celle-ci permet, une fois la connexion acceptée entre le client et le connection server, de forcer le client à se connecter via le connection server. Car par défaut, une fois que le connection server a accepté la connexion, le client peut se connecter en direct sur l'infrastructure

View, que ce soit en RDP ou PCoip. VMware recommande d'utiliser le mode tunnelé pour des raisons de sécurité bien que les performances soient légèrement meilleures lors de l'utilisation du mode direct.

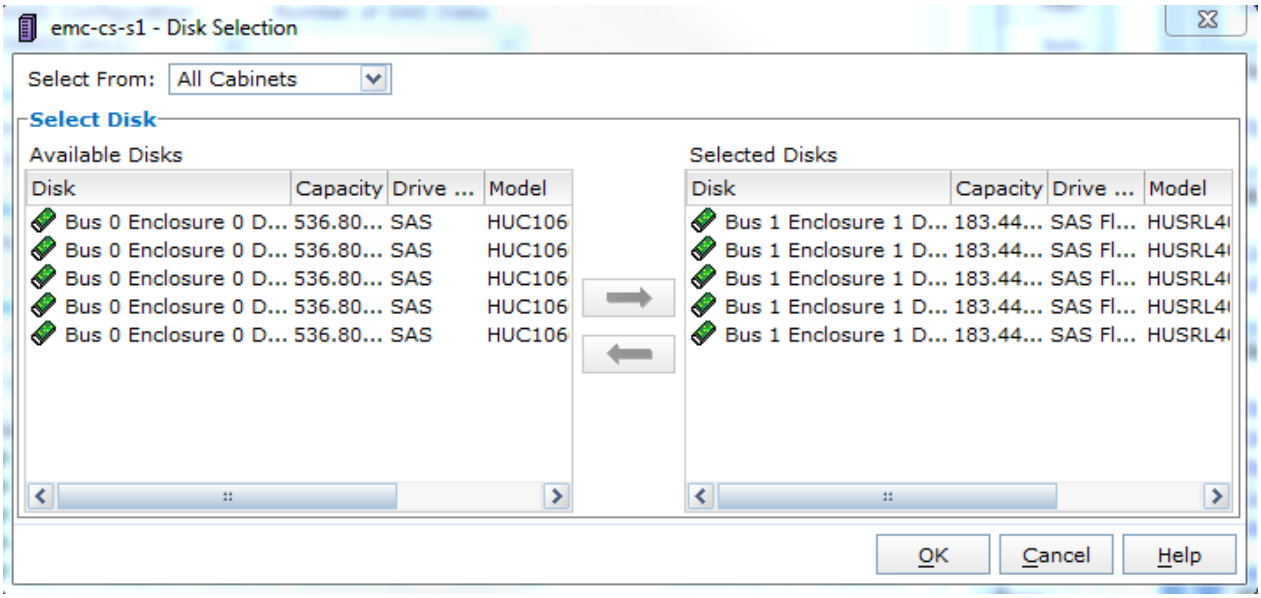
11.5 Création d'un pool de disques sur le SAN

Ci-dessous l'écran de création de pool sur notre SAN. Il permet d'y affecter les disques reconnus dans la baie et d'y choisir le type de RAID que l'on désire. Dans notre cas le RAID 5 (4+1) a été choisi. Il est, en effet un bon compromis entre performance et sécurité.

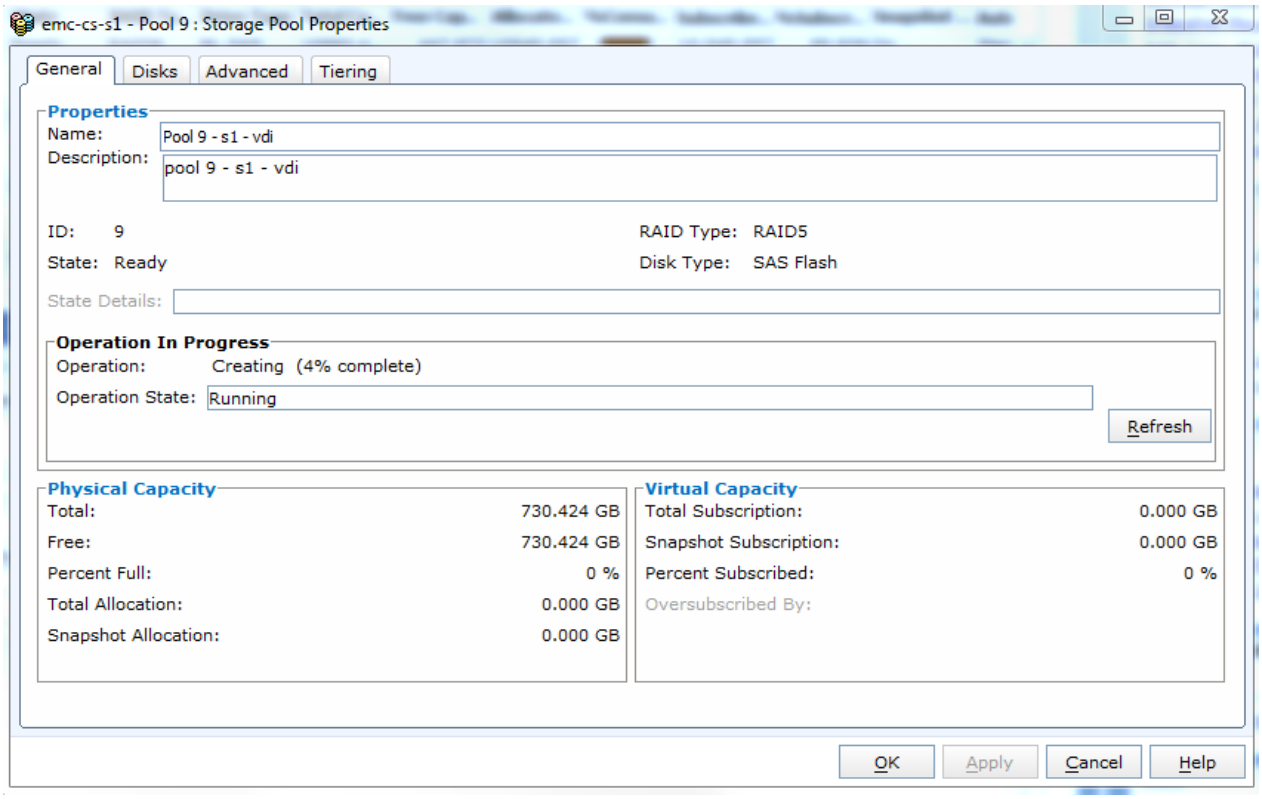


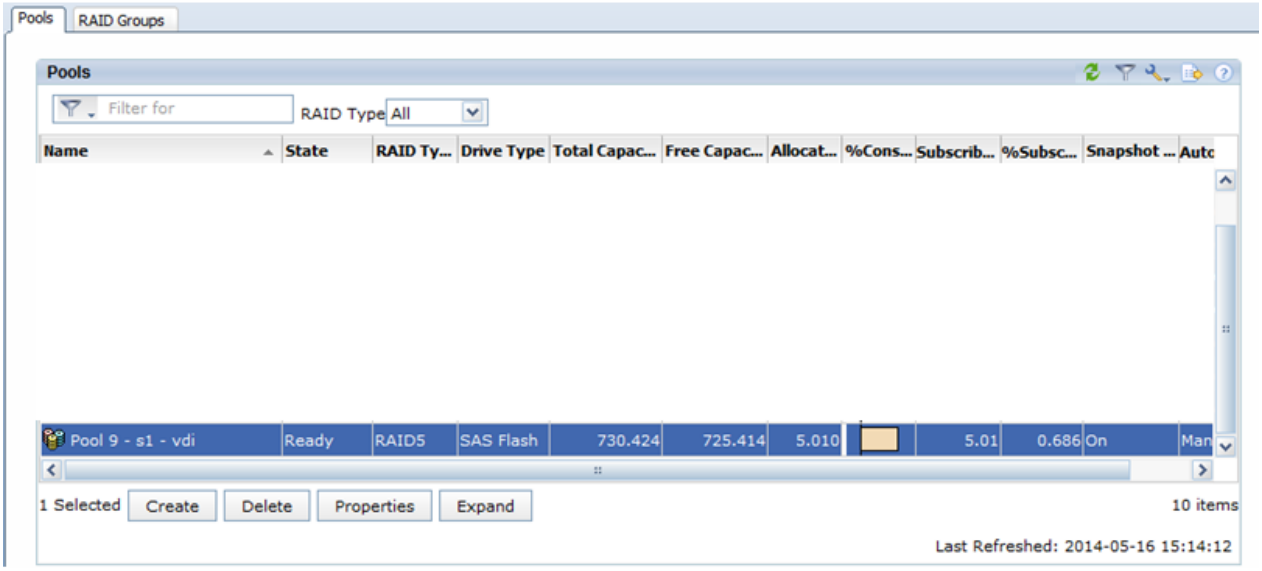
Cependant, par la suite, nous aurions pu faire un (3+1) pour la partie SSD c'est-à-dire 3 disques + 1 disque de parité + 1 disque de spare. Nous avons de la marge au niveau capacité.

Sélection des disques :



Résumé du pool :




Pools
RAID Groups
Pools
Filter for
RAID Type All
Name
State
RAID Ty...
Drive Type
Total Capac...
Free Capac...
Allocat...
%Cons...
Subscrib...
%Subsc...
Snapshot ...
Autc
Pool 9 - s1 - vdi
Ready
RAID5
SAS Flash
730.424
725.414
5.010
5.01
0.686
On
Man
1 Selected
Create
Delete
Properties
Expand
10 items
Last Refreshed: 2014-05-16 15:14:12

11.6 Photos du montage

Figure 24 - Serveurs Blade face avant

Figure 25 - Serveurs Blade face arrière

Figure 26 - UCS face avant

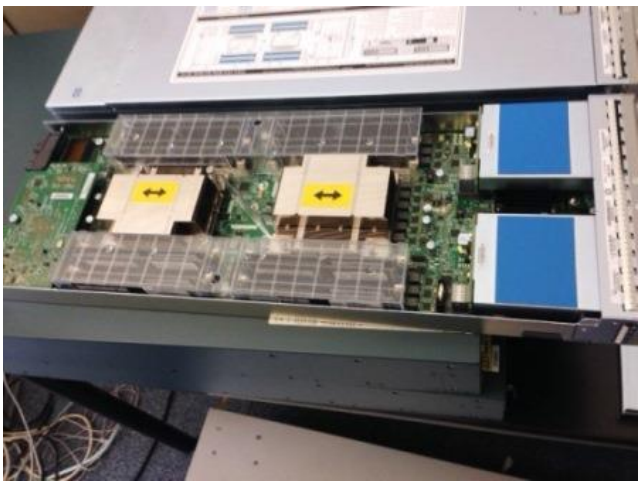


Figure 27 - Serveur Blade intérieur 1

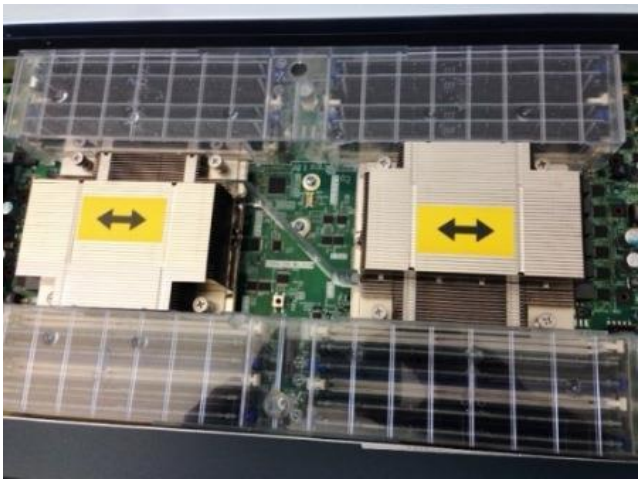


Figure 28- Serveur Blade intérieur 2

Figure 29 - Serveurs Blade + UCS