



HAL
open science

Étude et mise en place d'une plate-forme de cloud computing privé avec vCloud Director 5.1.2

Denis Foulon

► **To cite this version:**

Denis Foulon. Étude et mise en place d'une plate-forme de cloud computing privé avec vCloud Director 5.1.2. Autre [cs.OH]. 2015. dumas-01369231

HAL Id: dumas-01369231

<https://dumas.ccsd.cnrs.fr/dumas-01369231>

Submitted on 20 Sep 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

CENTRE REGIONAL DE LYON

MEMOIRE

présenté en vue d'obtenir

le DIPLOME D'INGENIEUR CNAM

SPECIALITE : INFORMATIQUE

OPTION : Réseaux et Systèmes et Multimédia

par

Denis FOULON

**Etude et mise en place d'une plate-forme de cloud computing privé
avec vCloud Director 5.1.2**

Soutenu le 17 avril 2015

JURY

PRESIDENT : Mr Christophe PICOULEAU *Professeur des Universités - Cnam Paris*

MEMBRES : Mr Bertrand DAVID *Professeur des Universités - ECL Lyon/
enseignant responsable - Cnam Lyon*

Mr Claude GENIER *Administrateur du CERN E.R./
enseignant-Cnam Lyon*

Mr Patrick PRONIEWSKI *Responsable pôle opérations de
l'Université Lyon 2*

Mr Azzedine ZERREL *Responsable secteur Usages et
Innovations pédagogiques par le
numérique à l'Université Lyon 2*

Remerciements

A ma famille pour son soutien lors des années de préparation de ce diplôme.

A tous ceux qui ont su me transmettre leur enthousiasme, leur énergie, leurs connaissances.

A mes collègues de l'université Lyon 2, évoluer parmi vous est un privilège.

Au CNAM et son personnel, cette institution est une chance incroyable pour ce pays.

A tous les membres du jury, c'est un honneur pour moi que vous jugiez mon travail.

Glossaire :

Bare Metal : un système d'exploitation Bare Metal est un système d'exploitation installé directement sur une machine physique. ESXi est un système d'exploitation Bare Metal.

Carte HBA : carte d'extension d'un serveur permettant de le connecter à son stockage. Les protocoles utilisés sont ISCSI ou FC.

Clones liés : technologie VMware permettant d'améliorer le temps nécessaire au clonage d'une machine virtuelle et de limiter l'espace disque utilisé par les clones.

Edge Gateway: (Enhancing Mobility) exosquelette conçu par le CEA dont le but est de redonner de la mobilité à des patients tétraplégiques.

EVC: Enhanced vMotion Compatibility.

ESXi: Hyperviseur de VMware utilisé par vSphere.

Hyperviseur : plate-forme de virtualisation qui permet l'exécution de plusieurs systèmes d'exploitation en même temps sur la même machine physique.

OVF : Open Virtual machine Format. Format utilisé par les éditeurs pour exporter des machines virtuelles entre les différents hyperviseurs et assurer la compatibilité.

SAN: Storage Area Network

vApp: ensemble de VM

vCenter: serveur qui centralise les fonctions de vSphere. On gère son infrastructure serveur en se connectant au serveur vCenter via un navigateur web ou le client vSphere lourd.

VM : Machine virtuelle (Virtual Machine)

vShield : Appliance de VMware qui gère le réseau pour vCloud Director. vShield n'a aucune autre vocation que d'être rattaché au serveur vCenter

vSphere : Suite logicielle de VMware qui englobe l'hyperviseur (ESXi) et le serveur vCenter.

Table des matières :

Introduction.....	1
I. Cloud computing.....	3
I.1. Définition du cloud computing	3
I.2. Les différentes familles de cloud (IaaS, PaaS et SaaS).....	4
I.2.1. IaaS.....	5
I.2.2. PaaS	5
I.2.3. SaaS	5
I.3. Les différents types de cloud.....	6
I.3.1. Le cloud privé.....	6
I.3.2. Le cloud public	6
I.3.3. Le cloud hybride.....	7
I.4. Liens entre virtualisation et cloud	8
I.5. Les apports de la virtualisation	9
II. Présentation du projet.....	11
II.1. Présentation de l'université Lyon 2 et sa DSI	11
II.2. Les besoins de l'université	11
II.3. Les solutions possibles	12
II.3.1. Les cloud publics.....	12
II.3.2 Les cloud privés à base de technologie Microsoft.....	12
II.3.3. Les cloud privés à base de projets Open source : Openstack, Cloudstack	12
II.3.4. Les cloud privés à base de technologie VMware: vCloud Director.....	12
II.4. Mon rôle dans le projet.....	13
II.5. Planning prévu	13
III. Présentation de la solution retenue : vCloud Director.....	15
III.1. La couche vSphere et l'infrastructure physique.....	15
III.1.1. La couche vSphere	15
III.1.2. L'infrastructure physique	15
III.2. La couche vCloud.....	16
III.2.1. Le serveur vCenter.....	16
III.2.2. Architecture générale de vCloud	17
III.2.3. Concept vCloud : les organisations.....	18
III.2.4. Concept vCloud : les vDC (virtual DataCenter) d'organisation.....	18

III.2.5. Concept vCloud : les VDC fournisseur (PvDC)	19
III.2.6. Concept vCloud : les Edge Gateway.....	19
III.2.7. Concept vCloud : Réseaux externes.....	19
III.2.8. Concept vCloud : Pool de Réseaux	19
III.2.9. Concept vCloud : vApp et VM	19
III.3. Les prérequis de vCloud.....	20
III.3.1. Choix des versions d'ESXi et de vSphere	20
III.3.2. vCenter	20
III.3.3. vShield	20
III.3.4. Bases de données	21
III.4. Chargeback.....	21
III.5. VCloud Connector	21
IV. Mise en œuvre de la solution vCloud	25
IV.1.0. Choix de la version de Red Hat	25
IV.2.0. Choix de la version d'Oracle	25
IV.3.0. Création de la base de données Oracle.....	26
IV.4.0. Déploiement et configuration de vShield Manager.....	26
IV.5.0. La génération des certificats auto signés	28
IV.6. Bilan de l'infrastructure à cette étape	28
IV.6.1. Points réalisés	28
IV.6.2. Points réalisés avant le début du projet.....	29
V. Mise en place d'une maquette de test.....	31
V.1.0. Les Objectifs	31
V.2.0. Création d'un nouveau VLAN.....	31
V.3.0. Aspect stockage.....	31
V.3.1. Les baies SAN utilisées	31
V.3.2. Création de LUNs sur la baie EMC VNX5300.....	34
V.3.3. Création de LUNs sur la baie HP EVA.....	35
V.3.4. Configuration des switchs fibres	37
V.3.5. Configuration dans vSphere au niveau du stockage.....	37
V.4.0. Installation du produit vcloud.....	41
V.5.0. Configuration de vCloud.....	44
V.6.0 Tests au niveau réseau.....	45

V.7.0. Recette de la plate-forme de test.....	47
VI. Mise en place de la production.....	49
VI.1.0. étude sur l'upgrade de la version vSphere de production et impacts sur la production	49
VI.2.0. Création d'une nouvelle base de données Oracle pour le nouveau serveur vCenter.....	50
VI.3.0. Installation de vCenter server	50
VI.4.0. Migration de vShield	55
VI.4.0. Mise en place du monitoring avec nagios et centréon	55
VI.5.0. Politique de backup des vms	57
VI.6.0. Modifications sur la base de données.....	58
VI.6.1. Passage en Archive Log des bases de données.....	58
VI.6.2. Démarrage automatique des bases de données	58
VII. Configuration de l'infrastructure de production.....	61
VII.1.0. Gestion des niveaux de service	61
VII.1.1. Gestion des niveaux de service pour le stockage.....	61
VII.1.2. Gestion des niveaux de service pour la RAM et le CPU	62
VII.1.3. Gestion des niveaux de service pour le réseau	63
VII.2.0. Utilisation des clones liés	63
VII.3.0. Customisation des vm.....	64
VII.3.1. Customisation des vm Windows	64
VII.3.2. Customisation des vm Linux.....	64
VII.4.0. Gestion des droits	65
VII.5.0. Gestion des licences (vSphere, vCloud et système d'exploitation)	66
VII.6.0. Phase de recette.....	67
VII.7.0. Documentation, partage des connaissances et présentations du produit .	67
VII.8.0. Migration vers la version vSphere 5.5 de l'infra serveur et impact sur vCloud	68
VII.9.0. Mise en place d'une vApp pour les serveurs qui gèrent vCloud.....	69
VII.10.0. Changement de serveurs ESXi.....	69
VII.11.0. Utilisation de EVC	70
VII.12.0. Backup des vm du cloud.....	71
VII.13.0. Packaging ThinApp.....	71
VII.14.0. Upgrade du serveur vCenter en 5.1	72

VII.15.0. Les difficultés rencontrées lors du projet.....	75
VII.15.1.Oracle	75
VII.15.2. Problème de gestion des objets vCloud	76
VII.15.3. Problème des licences.....	76
VIII. Les évolutions futures	77
VIII.1.0. Problématique liée au support	77
VIII.2.0. Les alternatives à vCloud.....	79
VIII.2.1. OpenStack.....	79
VIII.2.2. CloudStack	80
Conclusion.....	82
Annexes.....	84
Création de la base de données Oracle	84
Passage en Archive Log des bases de données.....	85
Script de démarrage automatique de la base de données :.....	87
Table des figures	90
Table des tableaux	94
Bibliographie.....	96

Introduction

L'informatique est un domaine qui connaît énormément d'évolutions depuis ses débuts. Ces évolutions sont parfois marquées par des ruptures. Depuis quelques années le « Cloud computing » se développe et s'impose aux professionnels mais aussi aux yeux du grand public. Rarement un terme supposé s'adresser uniquement au professionnel de l'informatique n'aura connu une telle démocratisation dans l'espace public.

L'objectif du projet est de mettre en place une infrastructure de cloud computing privée permettant de déployer rapidement des machines virtuelles préconfigurées. Ce projet s'inscrit dans la lignée d'autres projets menés précédemment et dont le but était de virtualiser la grande majorité des serveurs de la DSI de l'Université Lyon 2.

Le cloud computing s'appuyant sur la virtualisation il s'agit d'une évolution naturelle. L'outil retenu est vCloud Director de l'éditeur VMware. Cette infrastructure de cloud doit permettre au pôle études de déployer rapidement des serveurs qui ont une vocation de test dans un premier temps au moins. Ce projet a pour but de faire passer l'université Lyon 2 dans l'ère du cloud computing sans bouleverser l'existant.

Dans le chapitre 1, nous décrivons ce qu'est le cloud computing avant de présenter le projet au chapitre 2. Le chapitre 3 est consacré au fonctionnement de la solution retenue : vCloud Director. Ensuite nous étudions, au chapitre 4, la mise en œuvre de la solution vCloud puis la mise en place d'une maquette de test au chapitre 5. Nous présentons le passage en production dans le chapitre 6. Enfin nous analysons la configuration de l'infrastructure de production dans le chapitre 7 avant d'envisager les futures évolutions possibles du cloud à l'université au chapitre 8.

Chapitre 1

I. Cloud computing

I.1. Définition du cloud computing

Le cloud computing signifie littéralement « informatique en nuage ». C'est une façon d'envisager l'informatique différente de l'informatique traditionnelle qui met en avant les principes de flexibilité et de facilité d'accès pour l'utilisateur à des services informatiques. L'emplacement et le fonctionnement ne sont pas connus de l'utilisateur c'est pourquoi on parle d'informatique dématérialisée. Les services proposés sont très divers et vont du stockage de données à l'utilisation de logiciels en ligne.

Ce terme est parfois mal compris. Certains pensent à des services de stockage comme Dropbox ou Microsoft OneDrive. Pour d'autres, cela évoque des services de type Google_apps ou Office365. Pour d'autres encore, il s'agit de louer des machines virtuelles comme proposé par Amazon (EC2) ou Rackspace. Toutes ces idées sont justes et représentent à leur manière une facette du cloud aujourd'hui. Il existe une réelle diversité dans les services de cloud proposés au monde professionnel, mais aussi au grand public, qui est également une cible des fournisseurs de services de cloud.

Avant de distinguer chacune des différentes « familles de cloud », commençons d'abord par ce qui est commun à tous les exemples relevés ci-dessus. Pour ce faire le NIST (National Institute of Standards and Technology) a élaboré une liste de cinq caractéristiques du cloud computing qui sont les suivantes :

- service à la demande automatisé (On-Demand Self-Service)
- élasticité du service (rapid elasticity)
- service facturable en fonction de la consommation (measured service)
- accès via le réseau, capacité à utiliser des standards pour accéder via smartphone, pda, laptop... (broad network access)
- mutualisation des ressources entre consommateurs (resource pooling)

Le service à la demande automatisé représente la capacité de fournir le service sans intervention humaine de la part du fournisseur. L'élasticité du service vient de la nécessité de présenter le service de façon à ce qu'il soit extensible pour le client afin de gérer des montées en charge par exemple. Il faut bien entendu rendre ce service facturable en fonction de ce que consomme le client. On peut citer CloudWatt qui propose une gestion de la consommation des machines virtuelles à la minute et une tarification en conséquence. Le quatrième critère porte sur la capacité d'un service à utiliser des standards pour l'accès au service. Cet accès se fait via le

réseau pour assurer la compatibilité avec les tablettes, les smartphones ou les postes de travail. Enfin la mutualisation des ressources entre consommateurs s'appuie notamment sur la virtualisation et sa capacité à tirer les meilleures performances du matériel en mutualisant les machines virtuelles sur un même serveur physique.

I.2. Les différentes familles de cloud (IaaS, PaaS et SaaS)

Le cloud est divers de par la multitude de services existant. Le schéma suivant donne une meilleure idée de la classification observée entre IaaS (Infrastructure as a Service, PaaS (Platform as a Service) et SaaS (Software/Application as a Service). Traditionnellement dans l'informatique nous utilisons les « couches » afin de conceptualiser plus facilement. Ce découpage (I/P/SaaS) correspond à cela, l'ensemble du nuage constitue le cloud.

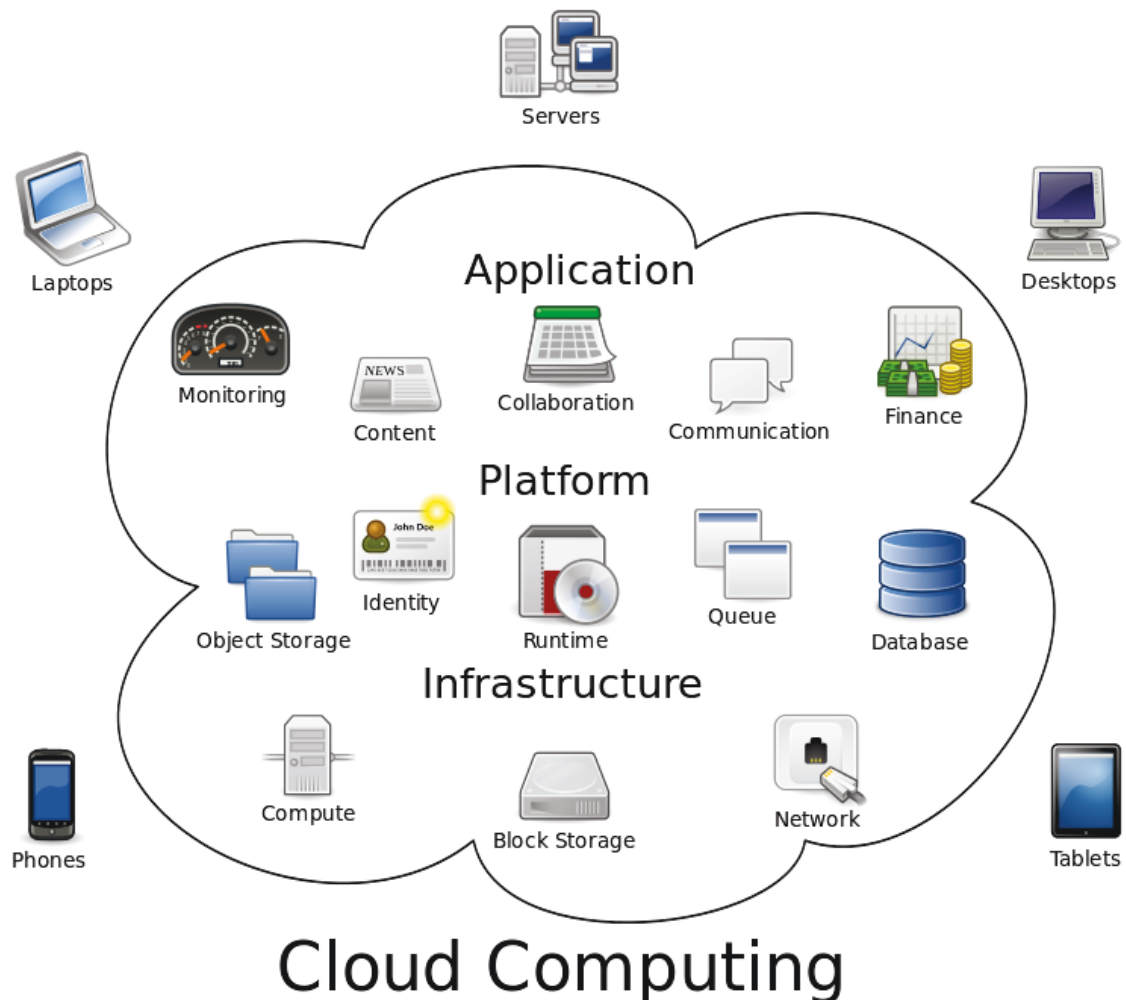


Figure 1 - Les différentes familles de Cloud, source [24]

La figure 1 et la figure 2 illustrent bien cette diversité. Afin de mieux comprendre les trois termes ci-dessus nous allons parler de chacune de ces catégories indépendamment.

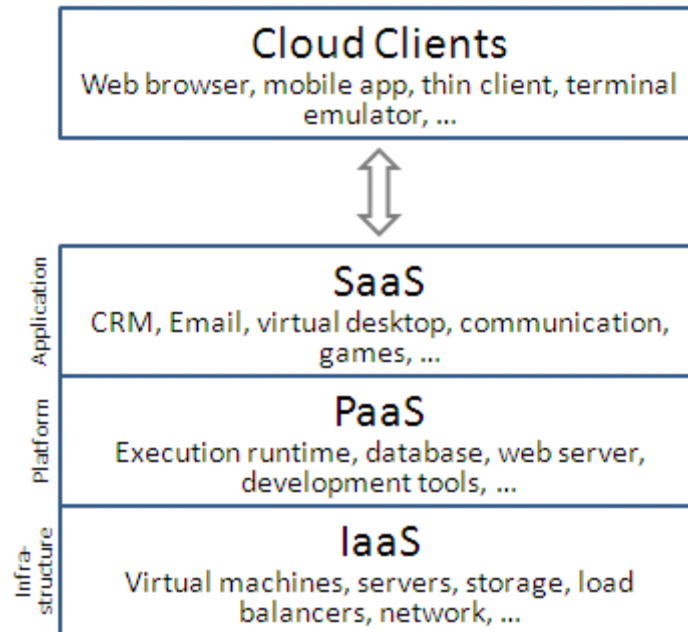


Figure 2 - Les différents modèles de services, source [24]

I.2.1. IaaS

vCloud Director, qui est la solution retenue pour ce projet, fait partie de la famille IaaS. Ce qui distingue l'IaaS des autres services c'est la capacité pour le client qui utilise ce service d'avoir la main sur l'OS de la machine virtuelle. C'est le cas pour des produits comme vCloud ou encore OpenStack. Pour les services de stockage qui apparaissent aussi dans cette famille, l'idée est de proposer un service « bas niveau ». C'est pourquoi le stockage en mode « block » apparaît dans cette catégorie.

I.2.2. PaaS

Le PaaS est un niveau intermédiaire. Le consommateur contrôle des applications fournies par les fournisseurs et peut les paramétrer. Parmi ces applications on peut trouver des bases de données ou encore du stockage orienté objet (par exemple Dropbox ou OneDrive).

I.2.3. SaaS

Le SaaS regroupe les services de « haut niveau ». On y trouve par exemple (Office365 ou google Apps). Ce sont des services « finis » mis à disposition en général par des éditeurs qui gèrent les mises à jour de l'application, ainsi que l'infrastructure bien évidemment.

I.3. Les différents types de cloud

I.3.1. Le cloud privé

Ce type de cloud a une vocation purement interne. La puissance de calcul, les capacités de stockage et le réseau sont accessibles uniquement en interne.

Un des premiers arguments en faveur du cloud privé est la possibilité pour une entreprise de pouvoir calculer précisément et par service ce que chacun consomme. C'est une donnée non négligeable car auparavant l'informatique ne permettait pas cela.

Un autre argument pour le cloud privé est le fait que l'entreprise n'est pas tributaire d'un grand fournisseur de services ni des aléas des changements de politique de ces fournisseurs. Ceci garantit un peu plus de souveraineté et d'indépendance pour une entreprise. De plus, les données sont stockées uniquement chez elle, cela permet (théoriquement) de ne pas voir les données sensibles être utilisées par quelqu'un de non habilité.

I.3.2. Le cloud public

Le cloud public est un cloud créé par un organisme dans le but de mettre à disposition ses ressources informatiques auprès d'autres entités. Des géants tels qu'Amazon, Google ou Microsoft proposent ce type de services. Ces services sont payants et facturés en fonction de la consommation des ressources. Il faut voir cela un petit peu comme une location que l'on peut ajuster en fonction de ses besoins.

Pour une petite entreprise, qui ne peut pas financièrement se permettre de payer une infrastructure redondante, le cloud apparaît comme une solution attractive au niveau du rapport qualité/prix. La flexibilité que le cloud procure donne de l'agilité et de la réactivité qui font la force des petites structures. De plus la forte disponibilité joue également en faveur de ce type de cloud. Assurer une disponibilité de haut niveau est quelque chose de coûteux.

L'un des deux gros défauts de ce modèle de cloud est l'hébergement de ses données sur des infrastructures parfois situées à l'étranger et donc soumises à des lois potentiellement différentes. Les différents scandales liés à la NSA et la volonté du gouvernement américain de mettre la main sur des données hébergées sur des sites en Europe par des entreprises américaines, dissuadent les décideurs à s'engager dans cette voie. Des « clouds souverains » sont apparus en France avec

notamment une entreprise comme Numergy qui propose du cloud « à la française ». Cependant rien ne garantit que les données ne sont pas accessibles par les services secrets français. Il faut noter que l'état français est actionnaire via la caisse des dépôts.

Le deuxième frein au développement du cloud public est la dépendance vis à vis du réseau. Malgré les progrès réalisés en termes de débits, beaucoup d'applications nécessitent une bande passante élevée et qui a tendance en plus à augmenter avec le temps et les mises à jour logicielles. Les temps de réponse inhérents au transport des données peuvent aussi freiner l'adoption du cloud. Enfin la disponibilité du réseau est un réel problème encore aujourd'hui. On le voit actuellement avec des attaques externes en DDOS (attaque par déni de service distribuée) qui peuvent facilement surcharger un réseau d'entreprise. Le cloud suppose donc la mise en place d'un réseau fiable au sein de son entreprise.

Enfin, il faut bien prendre en compte la sécurité et s'assurer que les échanges sont cryptés et que le prestataire est fiable et sérieux. Il n'y a pas nécessairement plus de risques liés à la sécurité sur ce type de cloud que sur un cloud privé. En effet, le fournisseur de cloud peut disposer de moyens supérieurs par rapport à une petite structure qui hébergerait en interne ses données. Il faut cependant bien prendre en compte que le cloud public nécessite de faire confiance à un acteur externe et que la sécurité concerne donc le client comme le prestataire.

I.3.3. Le cloud hybride

Ce type de cloud est un mélange des deux précédents. On peut par exemple imaginer faire héberger son site web chez un fournisseur de cloud tout en gardant son infrastructure de cloud privé en interne. Le cloud hybride a pour particularité d'apporter encore plus de flexibilité avec notamment cette possibilité d'agrandir virtuellement son propre Datacenter chez un fournisseur. Cela donne encore plus de réactivité en cas de gros pic de charge ou d'activité fluctuante.

Chez VMware, ce type de service est pris en charge depuis vSphere 5.5 avec la possibilité d'étendre son Datacenter chez l'éditeur en Europe (figure 3). VMware devient donc fournisseur de services cloud, en plus de son rôle d'éditeur.



Figure 3 - VMware vcloud hybrid service, source [23]

I.4. Liens entre virtualisation et cloud

Le cloud n'est pas en soi une révolution technologique, c'est d'avantage une évolution des usages. Si le cloud n'est pas une révolution technologique c'est aussi parce que les progrès techniques ont été réalisés avant son arrivée permettant ainsi son existence. Ainsi, la virtualisation et l'évolution constante des débits internet depuis son apparition mais aussi l'hébergement des données dans des baies SAN ; tous ces éléments rendent possible l'existence du cloud.

La virtualisation est une technologie utilisée dans les Datacenter du monde entier afin de tirer davantage parti de son matériel. C'est une couche d'abstraction qui découple le système d'exploitation du matériel afin de délivrer une meilleure utilisation et flexibilité des ressources de traitement. La figure 4 nous montre l'opposition entre l'ancienne architecture avec une relation « un serveur physique, un système d'exploitation » et l'architecture virtualisée avec plusieurs systèmes d'exploitation fonctionnant sur une seule machine physique.

VMware est la société leader en matière de virtualisation. Créée en 1998 puis rachetée en 2004 par EMC, VMware est une société qui s'est ensuite diversifiée dans le cloud computing mais aussi dans la virtualisation des postes de travail.

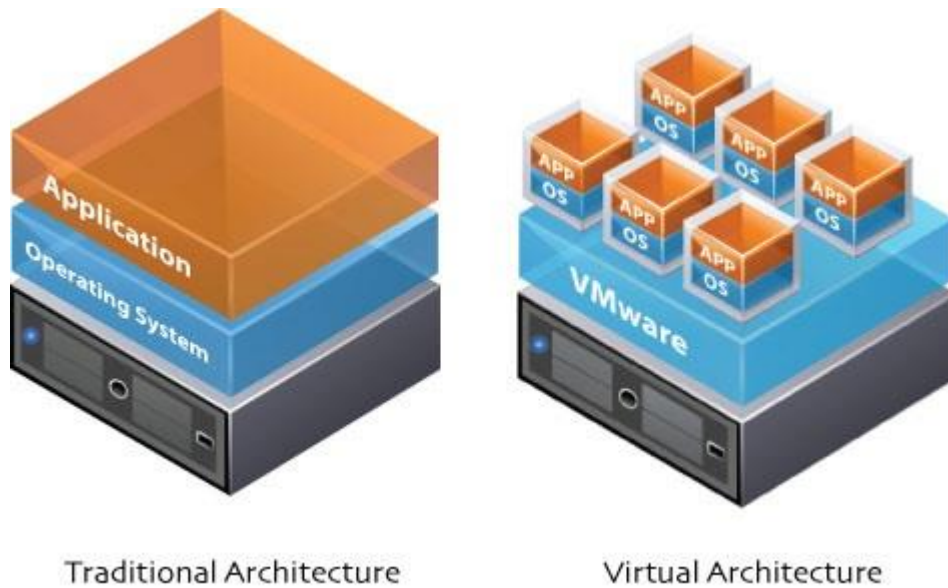


Figure 4 - Approche traditionnelle vs virtualisation, source [vmware.com]

I.5. Les apports de la virtualisation

La virtualisation s'est imposée pour trois raisons majeures dans le monde des Datacenter. D'abord, le premier argument tient aux gains financiers qui résultent de la diminution du nombre de serveurs physiques. Cette diminution du nombre de serveurs physiques a pour cause la concentration de plusieurs machines virtuelles sur un seul serveur physique. Les gains financiers ont motivé énormément d'entreprises à migrer vers une architecture virtualisée pour leur infrastructure.

Ensuite, les gains en termes de souplesse d'utilisation pour les administrateurs ont été le deuxième facteur clé du succès de la virtualisation. Les machines virtuelles sont des fichiers qui peuvent être copiés et cela génère un gain de temps pour cloner des machines très proches. On peut également changer d'hyperviseur alors que la machine virtuelle est en cours de fonctionnement, sans perte de données, ou encore ajouter un disque à chaud. Toutes ces possibilités rendent l'administration plus simple et plus pratique qu'auparavant, notamment pour des maintenances au niveau matériel.

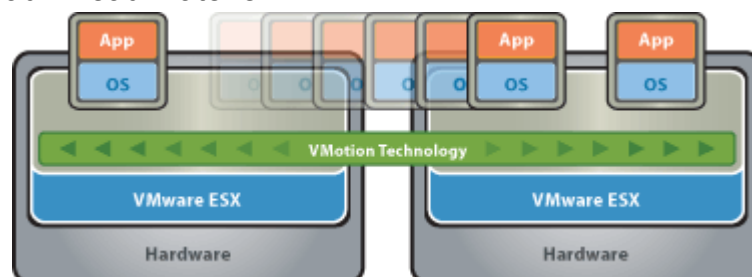


Figure 5 - Migration à chaud d'une machine virtuelle, vMotion, source [11]

Enfin, la virtualisation permet d'augmenter la disponibilité pour les services hébergés sur les serveurs. En effet, différents mécanismes permettent notamment un redémarrage de la machine virtuelle en cas d'incident matériel sur un autre serveur physique (module High Availability) ou bien de répliquer en temps réel une copie de la machine virtuelle et d'effectuer une bascule automatique sur un autre hyperviseur (Heartbeat, figure 6) en cas de problème matériel.

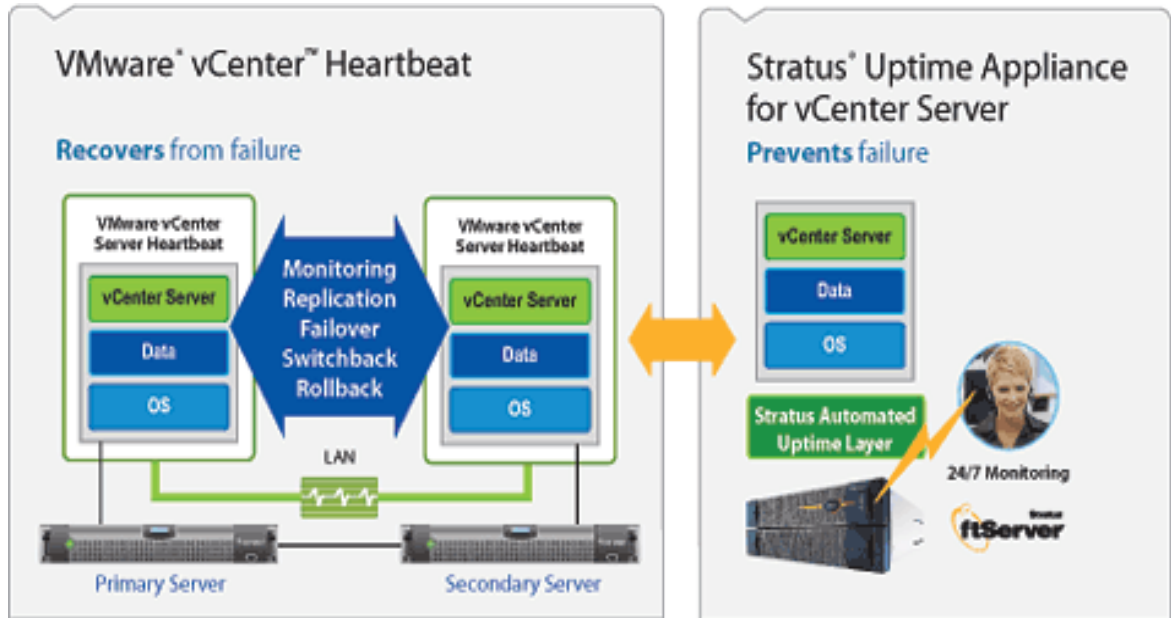


Figure 6 - Heartbeat, source [<http://www.yellow-bricks.com/2012/02/10/stratus-vcenter-uptime-appliance>]

On peut également mettre en place un Plan de Reprise d'Activité (PRA) en cas de problème majeur sur un site physique (module Site Recovery Manager). Ces mécanismes existent grâce à la virtualisation et ont eu pour effet de minimiser très fortement les temps d'indisponibilités des applications.

Le cloud computing présente de multiples aspects et s'appuie sur la virtualisation pour proposer ses services. Nous allons maintenant présenter le projet de cloud computing de l'université.

Chapitre 2

II. Présentation du projet

II.1. Présentation de l'université Lyon 2 et sa DSI

L'université Lumière Lyon 2 a été créée en 1973, elle est spécialisée en Langues, Lettres, Sciences humaines et sociales. Environ 30 000 étudiants répartis sur deux campus (Lyon et Bron) sont inscrits chaque année. La Direction des Systèmes d'Information, pour laquelle je travaille, est l'une des entités de l'université et possède des infrastructures sur chacun des deux sites.

La DSI est subdivisée en différents pôles. Je travaille pour le pôle opérations qui assure le bon fonctionnement de l'infrastructure et la mise en place des nouveaux serveurs. Le pôle étude regroupe les chefs de projet de la DSI et a en charge d'implémenter de nouvelles solutions. Le pôle support a pour fonction de s'occuper des problématiques liées aux postes de travail, et le pôle gestion et administratif des ressources humaines, des facturations et des commandes. La figure 7 rend compte de l'organisation de la DSI.

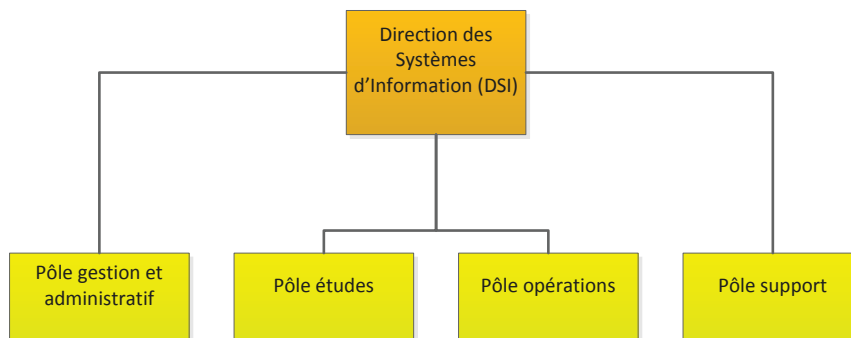


Figure 7 – Organigramme de la DSI

II.2. Les besoins de l'université

L'objectif initial était de proposer le déploiement rapide de serveurs préconfigurés pour le pôle étude afin qu'il teste et déploie plus rapidement certaines solutions sans avoir à faire des demandes au pôle opérations. L'objectif est de gagner du temps pour les nouveaux projets, d'améliorer l'efficacité en utilisant des serveurs standardisés et d'obtenir davantage de souplesse d'utilisation pour les utilisateurs du pôle étude. Il s'agit de mettre en place un cloud de type IaaS.

II.3. Les solutions possibles

II.3.1. Les cloud publics

Utiliser un cloud public est une option qui a été écartée par l'université. La maîtrise des données mises dans le cloud est l'argument majeur qui a poussé l'université à ne pas utiliser de cloud public.

II.3.2 Les cloud privés à base de technologie Microsoft

Microsoft propose des logiciels permettant de créer des cloud privés dans sa suite System Center. Même si l'hyperviseur de VMware (qui équipe le datacenter de l'université) est soutenu par System Center 2012 Virtual Machine Manager (SCVMM), il semblait plus compliqué de s'orienter vers cette solution. La relation de l'université avec cet éditeur n'est pas forcément des plus étroites et c'est un argument qui compte au moment de faire des choix techniques aussi structurants.

II.3.3. Les cloud privés à base de projets Open source : Openstack, Cloudstack

Le choix de ces solutions ne correspondait pas à la volonté de l'université d'utiliser un produit mature et soutenu par un grand éditeur. En 2012, s'orienter vers ces produits aurait été un peu compliqué, notamment parce que les compétences pour installer et administrer ces produits sont plus rares.

II.3.4. Les cloud privés à base de technologie VMware: vCloud Director

Vcloud Director est la solution retenue par l'université Lyon 2, c'est le choix de la continuité pour l'université. En effet le datacenter de l'université repose sur les technologies VMware et l'expérience acquise lors de la virtualisation des anciens serveurs physiques a servi de base pour se projeter vers le cloud.

La virtualisation a été popularisée par VMware, qui reste encore aujourd'hui le leader du marché avec son offre portant le nom de vSphere. vSphere tient historiquement une grande place au sein du datacenter de l'université Lyon 2. En s'orientant vers vCloud Director, l'université a fait le choix de s'appuyer sur son infrastructure existante car vSphere est indispensable pour vCloud.

Par ailleurs, le prestataire en contrat avec l'université maîtrisait cette technologie. Ce choix a été fait en 2012, aboutissant sur la création d'une maquette basée sur vCloud Director et non ouverte au public. Le but de la maquette était de démontrer la faisabilité du projet vCloud.

Ce choix implique des coûts de licence élevés. Chez VMware, on paye notamment une licence par CPU physique (socket) sur les hôtes ESXi, mais également le support annuel pour avoir accès aux différents patches et mises à jour de l'éditeur. Une autre licence concerne l'achat du serveur vCenter.

II.4. Mon rôle dans le projet

Mon rôle en 2014 a été de poursuivre l'implémentation du projet vCloud. A mon arrivée, la maquette de vCloud était réalisée et le prestataire avait terminé son travail. J'ai donc pris la suite en assurant le rôle de chef de projet en vue de mettre en production une plate-forme de cloud computing.

II.5. Planning prévu

Voici le planning du projet avec les étapes marquantes.

Jalon	Nom	01-oct	01-janv	15-févr	10-avr
J0	installation de vCloud	18-oct			
J1	livraison VLAN	01-nov	02-janv		
J2	configuration réseau dans vCloud	01-oct	31-janv		
J3	configuration stockage dans vCloud	20-déc	20-mars	20-mars	
J4	livraison environnement de préprod		31-mars	31-mars	
J5	recette environnement de préprod		15-avr	15-avr	15-avr
J6	définition des catalogues de vApp				10-mai
J7	livraison vCenter				30-avr
J8	mise en production				10-mai

Tableau 1 - Planning du projet

Les deux premières étapes ont coïncidé avec une montée en compétence sur le sujet et le produit dès la mi-octobre. Puis la livraison du VLAN a été effectuée par l'équipe réseau au début de l'année 2014. C'est une demande qui a pris un peu de temps du fait d'un planning chargé pour cette équipe. Le VLAN en question est le VLAN qui accueille les machines virtuelles issues du cloud.

La configuration du réseau dans vCloud dépend directement de la livraison du VLAN tout simplement parce qu'on ne peut pas configurer correctement le produit sans le VLAN. La configuration du stockage comprend la création des luns sur les baies de stockage, la configuration du stockage dans vSphere et aussi dans vCloud.

Ensuite viennent la livraison de l'environnement de pré production ainsi que la recette de cet environnement par des utilisateurs à la mi-avril. Après cela, la définition des catalogues de vApp, c'est-à-dire la création du contenu est prévue début mai. Bien entendu, le contenu est amené à évoluer non seulement à cause de l'obsolescence naturelle des vApp, mais aussi à cause des préférences et autres suggestions des utilisateurs.

L'étape « livraison vCenter » représente la mise en place d'un nouveau serveur vCenter dédié à vCloud. L'investissement représente environ 5 000€. Ce nouveau vCenter a pour objectif de cloisonner davantage l'infrastructure serveur de vCloud (ce qui est moins le cas pour tout ce qui concerne l'architecture de pré-production). Enfin la date de mise en production est planifiée pour le 10 mai 2014. C'est une date raisonnable qui laisse du temps pour corriger les derniers problèmes inhérents à ce genre de projet.

Le projet est maintenant cadré, nous allons désormais présenter la solution retenue à savoir vCloud Director.

Chapitre 3

III. Présentation de la solution retenue : vCloud Director

III.1. La couche vSphere et l'infrastructure physique

III.1.1. La couche vSphere

La couche vSphere correspond à la couche de virtualisation du cloud chez VMware. La machine physique, qui héberge les machines virtuelles, s'appelle un « hôte » ou hyperviseur. On l'appelle traditionnellement « hôte ESXi » à cause du système d'exploitation Bare Metal et de son nom (ESXi).

III.1.2. L'infrastructure physique

L'infrastructure physique est en lien direct avec la couche vSphere. Le stockage est déporté dans des baies SAN qui sont des équipements dédiés à cet effet. L'utilisation de ces baies SAN se fait en reliant les serveurs ESXi à des switchs « fibre » qui utilisent le protocole Fibre Channel. Le serveur doit être équipé pour cela d'une carte HBA (Host Bus Adapter) qui sert à communiquer avec le switch fibre.

Dans ce type d'architecture tout doit être redondant, c'est pourquoi on utilise deux cartes HBA par serveur, deux switchs fibre mais aussi deux Storage Processor par baie SAN. Les Storage Processor sont les interfaces de la baie qui gèrent les entrées/sorties d'une baie SAN (voir figure 8).

L'infrastructure qui a été mise en place avant mon arrivée repose sur ces technologies. C'est la raison pour laquelle je n'ai pas eu à mettre en place physiquement quoi que ce soit.

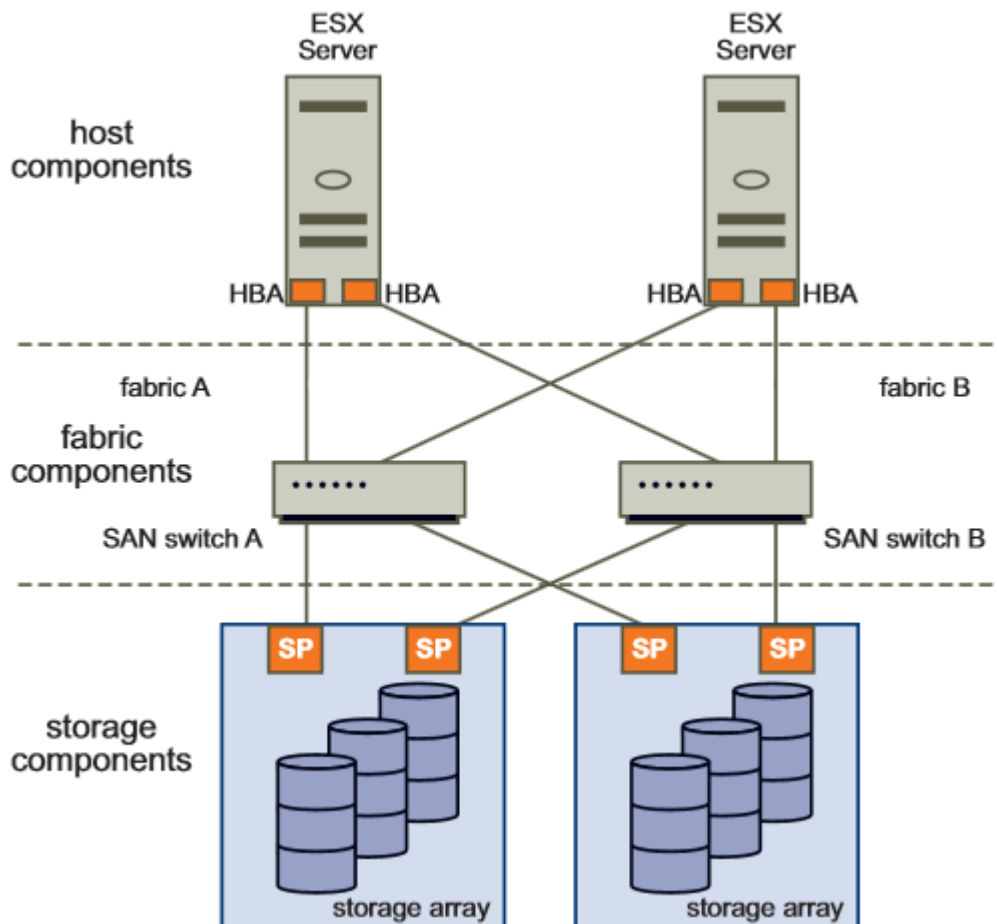


Figure 8 - Infrastructure physique, source [12]

III.2. La couche vCloud

III.2.1. Le serveur vCenter

VCloud, tout comme vSphere, nécessite d'utiliser un « serveur vCenter » pour fonctionner. A l'installation de vCloud, un serveur vCenter doit lui être rattaché pour fonctionner. Le rôle du serveur vCenter est de faire la passerelle entre vSphere qui gère le matériel (les serveurs ESXi ainsi que le réseau et le stockage) et vCloud qui va utiliser les ressources proposées par la couche vSphere, à laquelle il est rattaché. Dans une architecture vSphere classique sans vCloud, le schéma ressemble à la figure 9 :

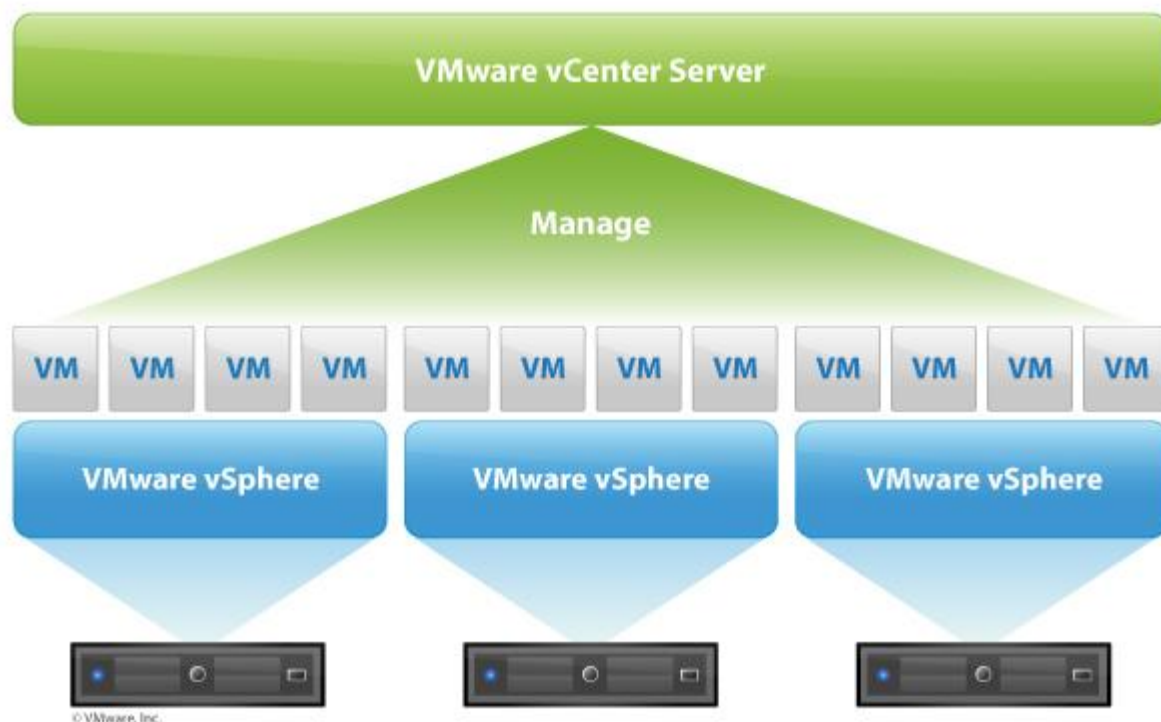
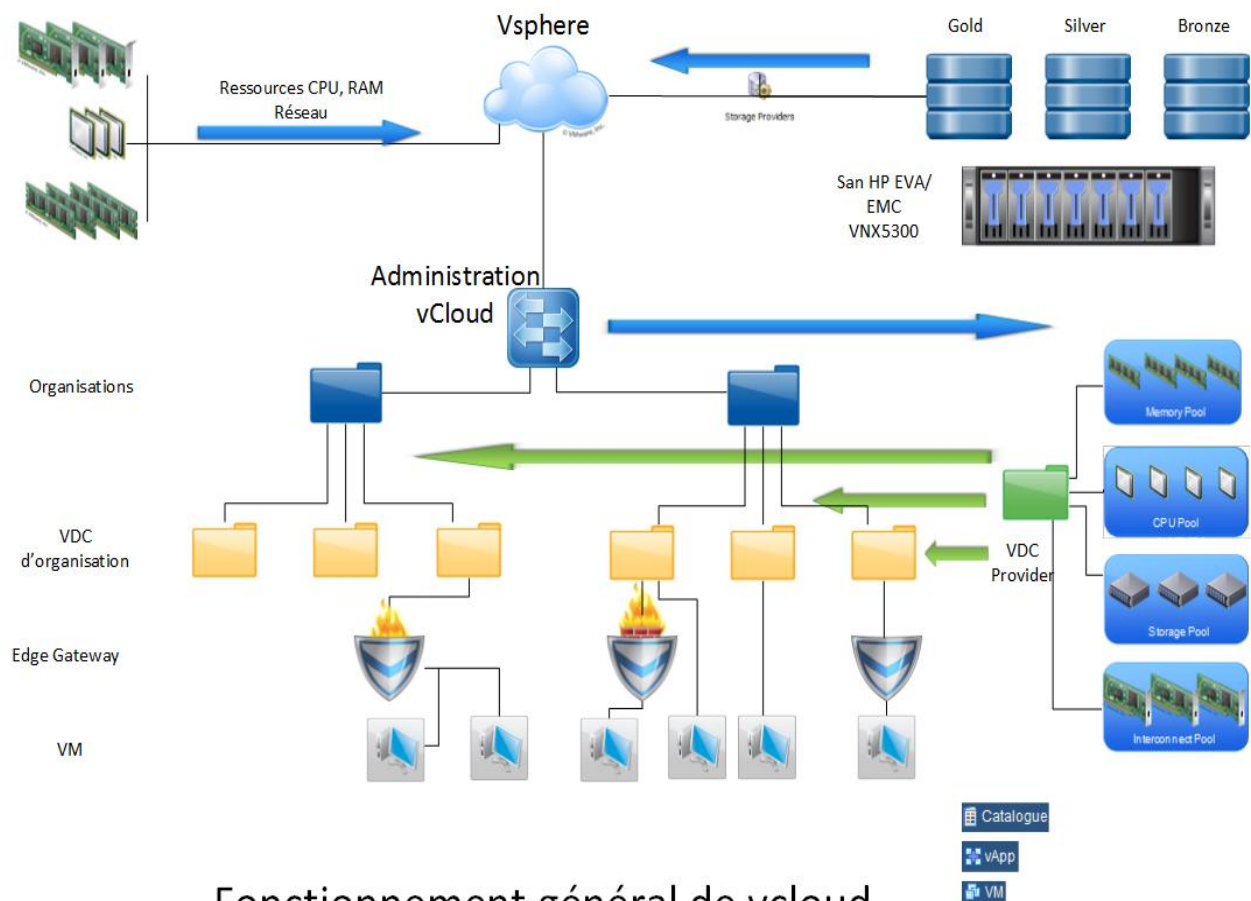


Figure 9 - vCenter au sein de l'infrastructure, source [<https://www.vmware.com/fr/products/vcenter-server/features.html>]

Concrètement le serveur vCenter est une machine (virtuelle ou non) qui gère les interactions entre serveurs ESXi. Dans le cadre du projet vCloud pour l'université Lyon 2, j'ai commencé par utiliser un de nos deux serveurs vCenter utilisé pour nos serveurs de production. Ce rattachement n'a que très peu d'impact pour le serveur vCenter.

III.2.2. Architecture générale de vCloud

Comme vu précédemment, le socle vSphere est très important et il faut le configurer en amont. En effet, vSphere présente des ressources et vCloud les utilise. Il faut voir vCloud comme une surcouche donneuse d'ordre. La figure 10 décompose l'outil vCloud en un certain nombre de concepts clés pour la compréhension que nous allons étudier juste après.



Fonctionnement général de vcloud

Figure 10 - Fonctionnement général de vCloud

III.2.3. Concept vCloud : les organisations

Les organisations sont des objets créés dans vCloud. L'organisation est un objet conteneur qui regroupe des utilisateurs. Ces regroupements se font par exemple au niveau d'un département pour une entreprise ou encore d'une division. Traditionnellement, on utilise des noms explicites pour les désigner par exemple : R&D, IT... Dans le cas de l'université 2, j'ai utilisé les organisations « opération » et « étude ». Les organisations permettent de cloisonner très fortement les droits et cela a un impact sur l'administration du cloud.

III.2.4. Concept vCloud : les vDC (virtual DataCenter) d'organisation

Les VDC d'organisation sont des sous-ensembles d'une organisation. L'idée est de leur associer ensuite un PvDC (Provider virtual DataCenter)

III.2.5. Concept vCloud : les VDC fournisseur (PvDC)

Les PvDC peuvent être vus comme des niveaux de service. Un des grands avantages du cloud est de pouvoir proposer aux utilisateurs différents ressources et de créer des niveaux de service différents en fonction de la personne qui utilise le service. Ainsi on peut privilégier certains groupes de personnes en leur donnant par exemple un stockage plus rapide ou encore davantage de RAM et de CPU. Ce découpage en niveaux de service se fait via les PvDC.

III.2.6. Concept vCloud : les Edge Gateway

Les « Edge Gateway » sont des passerelles créées et gérées par vShield. Ces passerelles ont pour objectifs de connecter les VDC d'organisation entre eux ou plus simplement de proposer un accès extérieur dans des réseaux différents.

Les Edge Gateway permettent de faire du DHCP, du NAT mais aussi une fonction firewall. Beaucoup de tests ont été réalisés à l'université Lyon 2 sur ces aspects réseaux, nous préciserons cela dans la partie relative à la période de tests.

III.2.7. Concept vCloud : Réseaux externes

Les réseaux externes sont les réseaux qui permettent à vCloud de sortir et de ne pas être isolé. Ces réseaux externes sont définis dans vSphere avant d'être configurés dans vCloud. Ils permettent l'accès internet par exemple.

III.2.8. Concept vCloud : Pool de Réseaux

Un pool de réseaux est un VLAN interne à vCloud. On affecte ensuite ce pool de réseaux à des vDC d'organisation.

III.2.9. Concept vCloud : vApp et VM

Une vApp (application virtuelle) est un objet de vCloud et vSphere (la notion existe aux deux niveaux). Une vApp est constituée d'une ou plusieurs VM. Par exemple, je pourrais créer une vApp « site web » contenant une machine virtuelle avec un serveur apache et une autre machine virtuelle disposant d'une base de données. Les notions de vm et de vApp sont donc à différencier.

VSphere propose par ailleurs une gestion avancée des vApp et permet d'aller plus loin en proposant un ordonnancement d'arrêt/démarrage des vm dans la vApp. Dans l'exemple précédent, on aurait la possibilité dans vSphere au démarrage de la vApp de lancer d'abord la base de données avant le serveur web tout en ajoutant un écart de deux minutes entre le démarrage des deux machines virtuelles.

III.3. Les prérequis de vCloud

III.3.1. Choix des versions d'ESXi et de vSphere

L'univers des produits VMware est vaste et connaître tous les produits de l'éditeur est compliqué. Au-delà de ce problème, il y a également les interactions entre ces logiciels qui selon les versions sont compatibles ou non. De plus, les versions de logiciels doivent également être compatibles avec les systèmes d'exploitations mais aussi avec le matériel. Avant d'installer quoi que ce soit il faut donc se pencher sur ces différentes compatibilités.

VMware propose pour cela un outil assez pratique qui permet de croiser différentes versions de logiciels entre elles et de valider ou non leur compatibilité : http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?

Les croisements à effectuer sont les suivants :

1. vérifier les compatibilités de versions entre vcloud et esx/vcenter
2. vérifier la compatibilité de versions entre vcloud et vshield
3. Vérifier la compatibilité entre la version de vcloud et la version de red hat
4. vérifier le matériel également

III.3.2. vCenter

Le serveur vCenter permet de gérer les serveurs physiques ESXi. C'est évidemment un pré-requis à vCloud. Dans le projet qui nous intéresse, l'infrastructure vCloud sera liée à notre serveur vCenter de production utilisée par l'UL2 pour les serveurs. C'est une machine virtuelle du nom de « nurn ». Le serveur vCenter a un coût de licence assez élevé (environ 5 000€ à lui seul).

III.3.3. vShield

VShield est un pré-requis de vCloud. Fourni sous forme d'Appliance que l'on déploie à partir d'un fichier .ova, vShield est la partie qui gère le réseau pour vCloud. Très concrètement, vShield s'occupe du NAT, du DHCP, des règles de routage et de Firewall dans vCloud. VShield est tributaire de la couche vSphere en dessous de lui. L'ajout d'un réseau dans vCloud nécessite de paramétrer vSphere pour prendre en compte ce nouveau réseau.

VShield est fourni gratuitement dans la version qui nous intéresse, puisqu'il nécessite le rattachement à un serveur vCenter pour fonctionner (serveur vCenter pour lequel on paye déjà une licence).

III.3.4. Bases de données

Comme beaucoup d'applications, vCloud nécessite une base de données afin d'être installé. Les informations stockées dedans sont vitales pour l'application. On y trouve notamment tous les objets vCloud (vDC d'organisation, vDC fournisseur, les pools de réseaux...). VCloud est compatible avec Oracle et SQL Server. Le choix se porte sur une base de données Oracle dans notre cas, car beaucoup d'applications l'utilisent à l'université. Les compétences de notre équipe sont plus axées sur Oracle et c'est également un facteur décisif dans le choix de ce SGBD.

Par ailleurs, au niveau des licences Oracle, nous avons le droit d'utiliser autant de bases de données que nous voulons, Oracle facturant le nombre total d'utilisateurs dans l'université. Une base de données en plus n'a donc aucun impact sur ce qui est payé à l'éditeur.

III.4. Chargeback

Chargeback est le module « facturation » de vCloud. Le package d'installation est prévu pour fonctionner uniquement sur Windows Server. De plus, Chargeback nécessite une énorme base de données afin de facturer au plus juste l'utilisation des ressources du cloud. Nous n'avons pas besoin de Chargeback à l'université et ce module est de toute façon une « option » de vCloud.

III.5. VCloud Connector

VCloud Connector est un plugin de vCloud qui permet de transformer un cloud privé en cloud hybride. Nous ne l'utiliserons pas dans l'architecture de l'UL2 qui a pour vocation d'être uniquement privé. La figure 11 illustre le concept.

vCloud connector permet également d'étendre son datacenter dans le cloud. Dans ce cas comme dans le cas de l'extension de son cloud, il faut d'abord déployer un serveur disponible sous format ovf (vCloud Connector Server), puis au minimum un autre serveur qui sert de « nœud » (disponible également au format ovf). Si on veut agrandir le datacenter, on déploie le nœud dans vSphere, sinon on le déploie dans vCloud pour agrandir son cloud (figure 12).

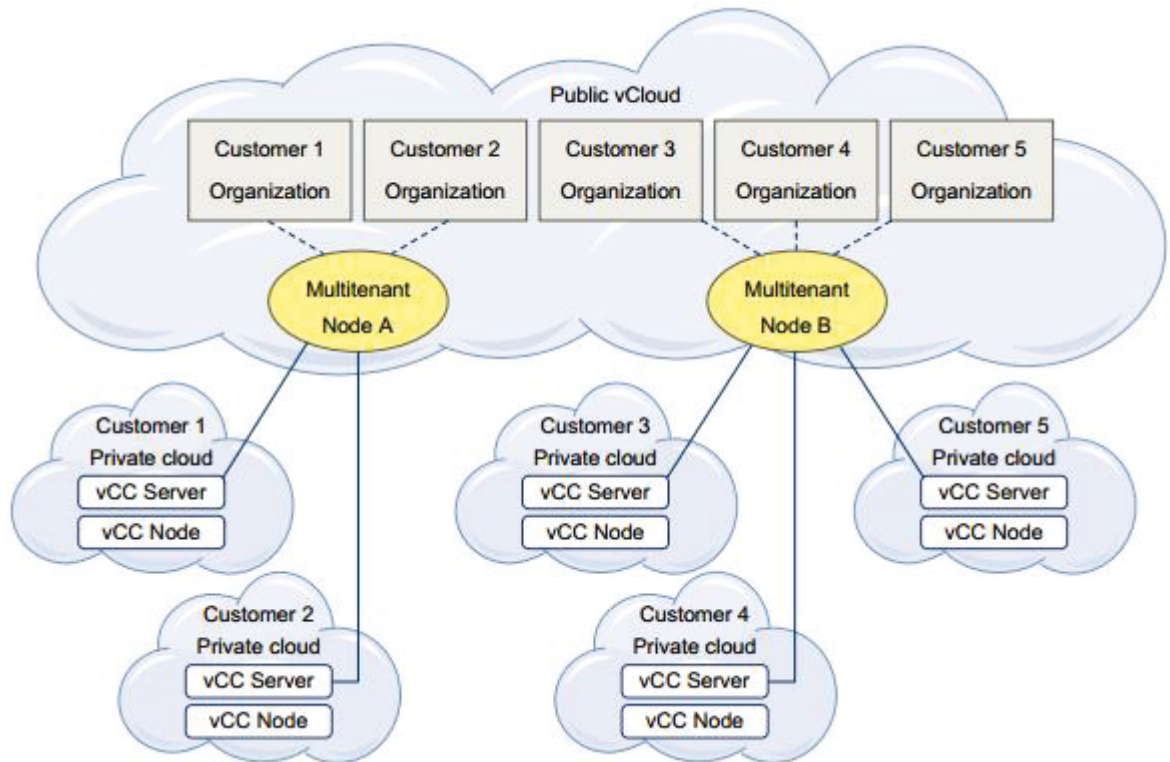


Figure 11 - Utilisation de vCloud connector, source [http://pubs.vmware.com/hybridcloud-26/index.jsp#com.vmware.vcc.install.doc_26/GUID-C2776581-4251-499C-86CF-84B2FD6B552F.html]

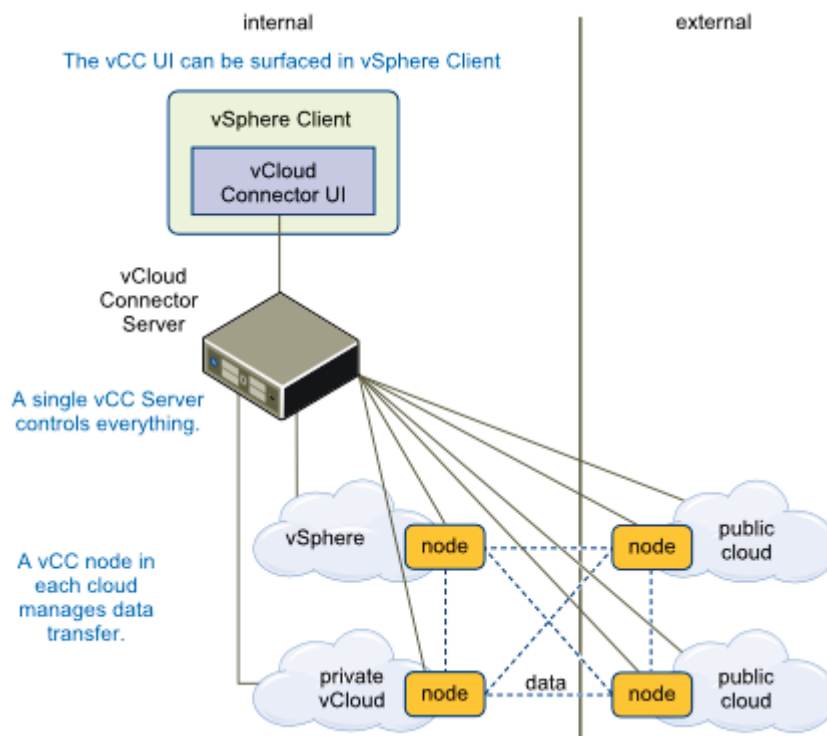


Figure 12 - Intégration de vCloud connector, source [http://pubs.vmware.com/hybridcloud-26/index.jsp#com.vmware.vcc.install.doc_26/GUID-C2776581-4251-499C-86CF-84B2FD6B552F.html]

Nous avons étudié la composition du produit vCloud Director ainsi que ses possibilités en matière de modules additionnels, nous pouvons désormais décrire la mise en œuvre de la solution vCloud.

Chapitre 4

IV. Mise en œuvre de la solution vCloud

IV.1.0. Choix de la version de Red Hat

Le choix de Red Hat pour la machine virtuelle qui accueille vCloud est imposé par VMware. C'est un choix cependant logique et plutôt intéressant pour l'université qui utilise déjà beaucoup de serveurs Red Hat. On peut utiliser Red Hat 5 ou 6 d'après la documentation officielle. Le choix se porte sur Red Hat 6 pour nous car nous utilisons cette version au quotidien.

Afin de gagner du temps, la création de la machine virtuelle « vCloud » se fait à partir de notre modèle de machine. Concrètement c'est une machine préconfigurée disposant d'options déjà paramétrées. Ceci permet également d'avoir des machines très homogènes dans un parc informatique.

Ainsi la problématique du lien entre la machine virtuelle et le serveur LDAP est géré dans le modèle de machine tout comme la configuration de SSH, la configuration du NTP ou encore les règles de firewall par exemple. Partir d'un modèle de machine implique en revanche de configurer le réseau de la machine virtuelle dans vSphere et dans la machine, d'installer les vmwaretools, de modifier le nom de la machine, de gérer les entrées dans le serveur DNS et d'enregistrer la machine chez Red Hat (licence).

IV.2.0. Choix de la version d'Oracle

Le choix de la base de données nous est laissé par VMware entre Oracle et SQL Server. Oracle Database est un SGBD qui a fait ses preuves dans le monde de l'entreprise tant en terme de performance que de fiabilité. Ce projet nécessite d'avoir les compétences de base sur Oracle et d'installer une base de donnée, c'est pourquoi j'ai suivi une formation d'administration de base de données Oracle en 2013 (DBA1 sur Oracle 11G).

Au niveau des licences, l'ajout de cette base de données ne coûte pas davantage d'argent à l'université. En effet nous pouvons installer autant de base de données que le souhaitons (à l'université) grâce à un accord avec Oracle.

La version Oracle Database 11GR2 est retenue car compatible avec vCloud et surtout c'est celle que nous maîtrisons le plus. Il existe une version Oracle 12c mais celle-ci n'a pas encore été intégrée dans notre production, ni dans nos tests. La compatibilité avec notre outil de backup, ainsi que son bon fonctionnement, est un travail à mener pour notre équipe avant d'intégrer Oracle 12c à nos outils validés.

IV.3.0. Création de la base de données Oracle

Nous utilisons le modèle de machine Red Hat intégrant un moteur de base de données Oracle Database. Ce modèle permet de gagner du temps à la création de la machine virtuelle, à sa configuration et à l'installation du SGBD. C'est une machine virtuelle qui a vocation à intégrer les bases de données Oracle de vCloud uniquement. Toutes les manipulations qui concernent la création de la base de données sont détaillées en annexes.

IV.4.0. Déploiement et configuration de vShield Manager

Une fois les sources de la bonne version de vShield téléchargées chez l'éditeur, il nous faut déployer l'Appliance dans vSphere. L'appliance apparaît dans vSphere au même niveau que les autres machines virtuelles de notre infrastructure serveur.

On se connecte via la console vmware comme sur une machine virtuelle standard et on lance la commande « setup » afin de configurer l'adresse IP de l'appliance, sa passerelle par défaut et le nom de la machine :

```
Hostname [vshield]:  
IP Address (A.B.C.D or A.B.C.D/MASK): 159.84.X.X  
Default gateway (A.B.C.D): 159.84.X.X  
Old configuration will be lost, and system needs to be rebooted  
Do you want to save new configuration (y/[n]): y  
Please log out and log back in again.
```

L'étendue des modifications applicables à vShield est relativement limitée d'un point de vue système. Une des particularités de vShield est d'avoir deux bases de comptes indépendantes. Il y a une interface web générée par l'Appliance qui a sa base de compte et une base de compte qui sert à la connexion en mode « console ». Le piège est que ces identifiants sont indépendants et pour le même login on peut avoir deux mots de passe différents au niveau du web et au niveau de la console.

Il faut tout d'abord configurer la console, se loguer en tant qu'admin et passer en « enable mode » puis en mode configuration du terminal. Ce procédé est très

largement inspiré des produits issus de chez Cisco (leader mondial des matériels réseaux). Voici comment changer le mot de passe de la console de vShield

```
manager login: admin
```

```
manager> enable
```

#on passe en mode configuration :

```
manager# configure terminal
```

#on crée un utilisateur temporaire

```
manager(config)# user tempadmin password plaintext pass007
```

#on enregistre la configuration actuelle

```
manager(config)# write memory
```

#on se délogue deux fois afin de revenir à la console en mode déconnecté

#on se relogue avec les identifiants de l'utilisateur temporaire nouvellement créé et on passe en « enable mode ». Puis on passe en mode configuration du terminal comme vu précédemment

#on supprime l'utilisateur admin

```
manager(config)# no user admin
```

On recrée l'utilisateur Admin en lui assignant un mot de passe fort

```
manager(config)# user admin password plaintext newPassXYZ
```

#On enregistre la configuration

```
manager(config)# write memory
```

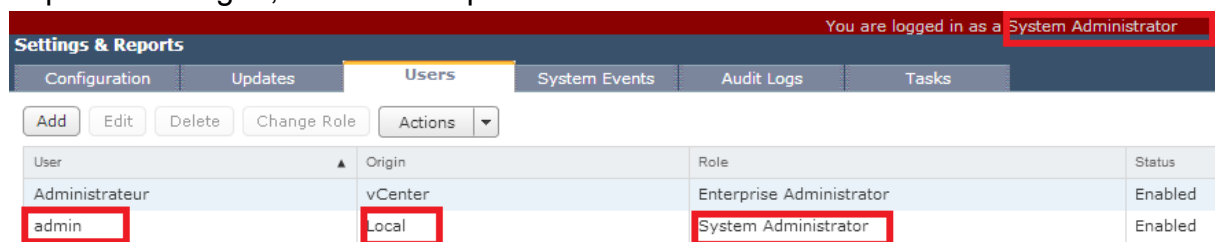
#on se délogue comme précédemment deux fois, on se relogue avec le nouvel utilisateur admin. On passe en enable mode puis en mode configuration du terminal et enfin on supprime l'utilisateur temporaire qui nous a permis de changer le mot de passe de l'utilisateur admin

```
manager(config)# no user tempadmin
```

#pour terminer on enregistre toute ces modifications sans quoi la configuration est perdu au prochain arrêt de la machine virtuelle :

```
manager(config)# write memory
```

A ce niveau-là, on a changé le mot de passe de la console mais en aucun cas celui de l'accès web. On y accède via : <https://vshield.univ-lyon2.fr> et ce grâce aux identifiants du compte admin (attention ce compte n'est pas celui de la console que l'on a changé auparavant). Admin correspond à l'utilisateur avec lequel on se logue, c'est un compte local.



The screenshot shows the vShield web interface. At the top, a red banner indicates the user is logged in as a System Administrator. Below this, the 'Settings & Reports' menu is visible, with the 'Users' tab selected. The 'Users' table lists two users: 'Administrateur' and 'admin'. The 'admin' user is highlighted with a red box, and its 'Origin' is 'Local' and 'Role' is 'System Administrator', both also highlighted with red boxes.

User	Origin	Role	Status
Administrateur	vCenter	Enterprise Administrator	Enabled
admin	Local	System Administrator	Enabled

Figure 13 - Interface graphique de vShield

Le compte Administrateur que l'on voit est issu du serveur vCenter
On change le mot de passe du compte « admin » de vShield directement dans l'interface.

IV.5.0. La génération des certificats auto signés

vCloud director est accessible une fois installé via le protocole https. Ce protocole utilise un système de cryptage des flux à base de clefs asymétriques. Il nous faut générer deux certificats afin de pouvoir installer vCloud (c'est un pré-requis à l'installation comme nous le verrons par la suite). Il y a deux manières de procéder : créer deux certificats signés par une autorité de certification ou bien générer deux certificats dit « auto signé ».

Nous opterons pour la deuxième option. Cela aura pour conséquence l'apparition d'un message à la première connexion dans le navigateur précisant que l'autorité de certification n'est pas reconnue par le navigateur. Voici les commandes utilisées pour générer les certificats :

```
./keytool -keystore certificates.ks -validity 1460 -storetype JCEKS -storepass monmotdepasse -genkey -keyalg RSA -keysize 2048 -alias http  
./keytool -keystore certificates.ks -validity 1460 -storetype JCEKS -storepass monmotdepasse -genkey -keyalg RSA -keysize 2048 -alias consoleproxy
```

Ces deux commandes génèrent via l'algorithme de cryptage RSA deux certificats ayant une période de validité de 1460 jours en utilisant une clé de 2048 bits.

IV.6. Bilan de l'infrastructure à cette étape

IV.6.1. Points réalisés

A cette étape nous avons mis en place ce qui est nécessaire pour installer vCloud Director. Nous avons créé :

- une vm qui héberge la base de données oracle
- une base de données accessible avec l'utilisateur vclouduser avec les bons droits positionnés
- une vm « vShield » qui sera jointe plus tard au vCenter et dont l'accès est verrouillé par des mots de passe qui ont été modifiés
- deux certificats qui seront utilisés par l'application vCloud

IV.6.2. Points réalisés avant le début du projet

Pour être clair il convient également d'effectuer un tour d'horizon des pré-requis qui étaient déjà atteints avant de commencer le projet :

- la création d'un service d'annuaire et plus particulièrement d'un Active Directory (LDAP Microsoft). C'est un pré-requis de vCenter
- la mise en place de serveurs physiques ESXi. En effet nous avons recyclé des serveurs décommissionnés de notre infrastructure serveurs. Ces serveurs étaient déjà installés et en partie configurés. Il faut noter que l'installation de ces serveurs ESXi est relativement triviale d'un point de vue logiciel.
- la mise en place d'un serveur vCenter. Là aussi nous capitalisons sur l'existant.
- la mise en place d'une baie san pour le stockage ainsi que les switchs fibre.
- la mise en place de switchs réseaux pour relier les serveurs

A ce stade, tout a été réalisé afin de rendre possible l'installation du produit vCloud Director. Nous pouvons décrire la mise en place de la maquette de test.

Chapitre 5

V. Mise en place d'une maquette de test

V.1.0. Les Objectifs

Le premier objectif de la plate-forme de test est de démontrer la faisabilité du projet à savoir créer une plate-forme de cloud pour l'université. Le deuxième objectif est de permettre de gagner de l'expérience avant de se lancer sur une plate-forme de production. C'est donc le bon moment pour pousser l'outil dans ses limites, ce que nous ne manquerons pas de faire notamment au point de vue du réseau.

V.2.0. Création d'un nouveau VLAN

La création d'un nouveau VLAN est nécessaire pour cloisonner d'un point de vue réseau l'infrastructure de cloud du reste de l'infrastructure. Le VLAN contiendra les machines créées par vCloud uniquement. Cela sous-entend que les machines virtuelles nécessaires à l'infrastructure (les ESXi, le serveur vCloud, le serveur de base de données, le serveur vShield) utiliseront des adresses IP « classiques » avec lesquelles nous adressons nos autres serveurs.

La création de ce nouveau VLAN a été confiée à l'équipe réseau de l'université qui est spécialiste de ces problématiques. Une charge de travail élevée ainsi qu'un effectif réduit dans cette équipe ont retardé la mise en place de l'infrastructure de test. C'est un imprévu qui peut survenir dans un projet tel que celui-ci où plusieurs personnes sont impliquées. Il faut toutefois souligner que le travail a bien été réalisé une fois l'équipe mobilisée sur ce sujet.

V.3.0. Aspect stockage

V.3.1. Les baies SAN utilisées

Le stockage est un aspect fondamental du cloud. Nous avons à l'université Lyon 2 la chance de disposer d'un matériel performant à ce niveau. En effet, notre infrastructure serveur fonctionne grâce à des baies SAN EMC VNX5300. Nous avons deux sites physiques (Lyon et Bron) contenant 2 baies de ce type, utilisant des « recover point » (figure 14) qui permettent la réplication en temps réel de ce stockage. Les « recover point » présents sur chaque site utilisent un « lien IP » direct

entre les deux sites, assurant ainsi de bonnes performances pour le stockage répliqué.



Figure 14 - Recover point d'EMC

Les baies EMC sont le fleuron de notre stockage. Celles-ci ont remplacé des baies HP d'ancienne génération (une baie HP EVA4000 et une baie HP EVA 4400). Ces baies ne sont plus supportées par le constructeur, c'est pourquoi seules nos machines de test uniquement les utilisent. Les baies HP en question ont l'avantage d'être simples d'utilisation et plus intuitives que les baies EMC qui sont plus complexes.

Dans le cadre du projet, nous utiliserons les baies présentes sur le site de Lyon (par opposition à celui de Bron), car c'est là où se situent les serveurs ESXi que nous prendrons pour soutenir l'activité des machines virtuelles issues du cloud. Pour fournir différents niveaux de service, nous utiliserons donc la baie EMC de Lyon ainsi que la baie HP 4000 de Lyon.

La figure 15 présente quelques concepts clés utilisés par la baie à savoir les disques physiques, les storage pools et les LUN. Les disques physiques sont de différents types, à l'université nous avons des disques SAS pour l'immense majorité et aussi quelques disques Flash. La configuration des storage pool est assez simple puisque nous n'en avons qu'un seul (l'avantage est que c'est plus simple à gérer comme cela). Dans ces storage pool on découpe des LUNs. C'est la plus petite unité logique que l'on peut présenter à un serveur.

La baie EMC permet une gestion très fine des performances grâce à sa technologie d'auto-tiering et grâce à la présence de disque ssd et sas. L'auto-tiering est une technologie qui permet de placer les données (blocks) les plus fréquemment accédées sur les disques les plus rapides (ssd). Concrètement chaque heure, la baie calcule quels blocks doivent être promus sur les disques ssd et les déplace une fois par jour (la nuit). Un système de statistiques interne à la baie permet cette opération. C'est une opération complètement automatisée. Tout ceci est fait dans l'optique d'améliorer les performances et les accès disques et in fine l'expérience utilisateur.

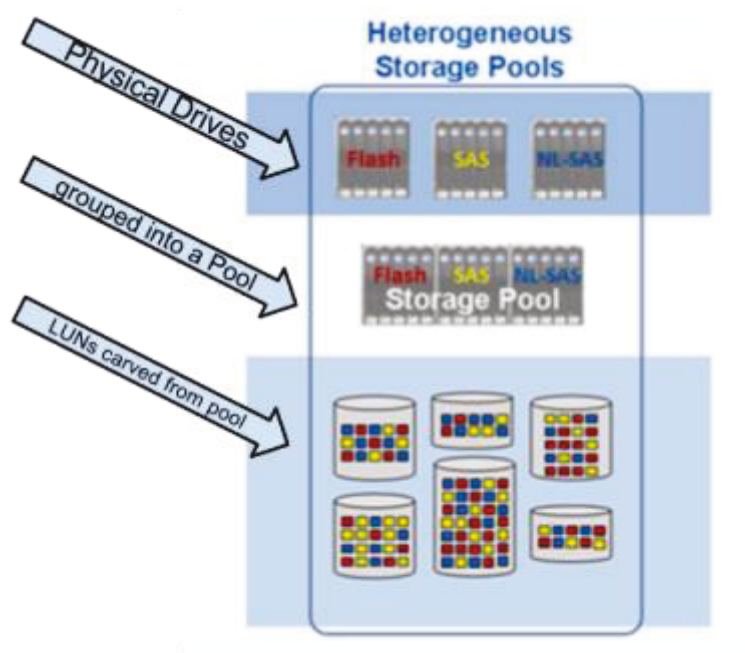


Figure 15 - Relations entre luns, pools et disques, source [1]



Figure 16 - Photo des disques de la baie EMC, pools et disques

Parmi les disques utilisés par la baie (figure 16), on trouve des disques SAS 15 000 tours ou 7 200 de différentes capacités : 300 GO et 600 GO pour les 15k et 1 TO pour les 7 200. Plus le nombre de tours est élevé, plus l'accès aux données est rapide. Il faut comprendre aussi que, plus la taille du disque est grande, plus les performances pour accéder à une donnée sont mauvaises. Il y a un équilibre subtil à

trouver entre l'espace de stockage qui doit être le plus grand possible et les performances en terme de temps d'accès qui doit être rapide. Par ailleurs mettre des disques différents permet de mieux tirer parti des capacités de la baie de stockage qui sait analyser les performances de ses disques et placer les données sur les bons disques.

Parmi les options intéressantes de la baie EMC utilisée, on notera également la création automatique de ticket chez le constructeur en cas de problème critique, la réplication de LUN, la souscription d'un abonnement chez EMC pour faire intervenir un technicien (pour remplacer les disques défectueux ou faire les mises à jour) et l'intégration au client vSphere de la gestion de la baie. Cette intégration des outils VMware/EMC trouve son origine dans le fait que VMware est une filiale d'EMC.

V.3.2. Création de LUNs sur la baie EMC VNX5300

La création d'une LUN sur la baie EMC est une opération plutôt aisée. On définit une taille mais aussi un niveau d'auto-tiering (figure 17). Ce niveau permet de prioriser certaines LUN par rapport à d'autres. A titre d'exemple, on pourrait imaginer créer une LUN dédiée à des bases de données dans l'idée de générer des entrées/sorties plus rapides.

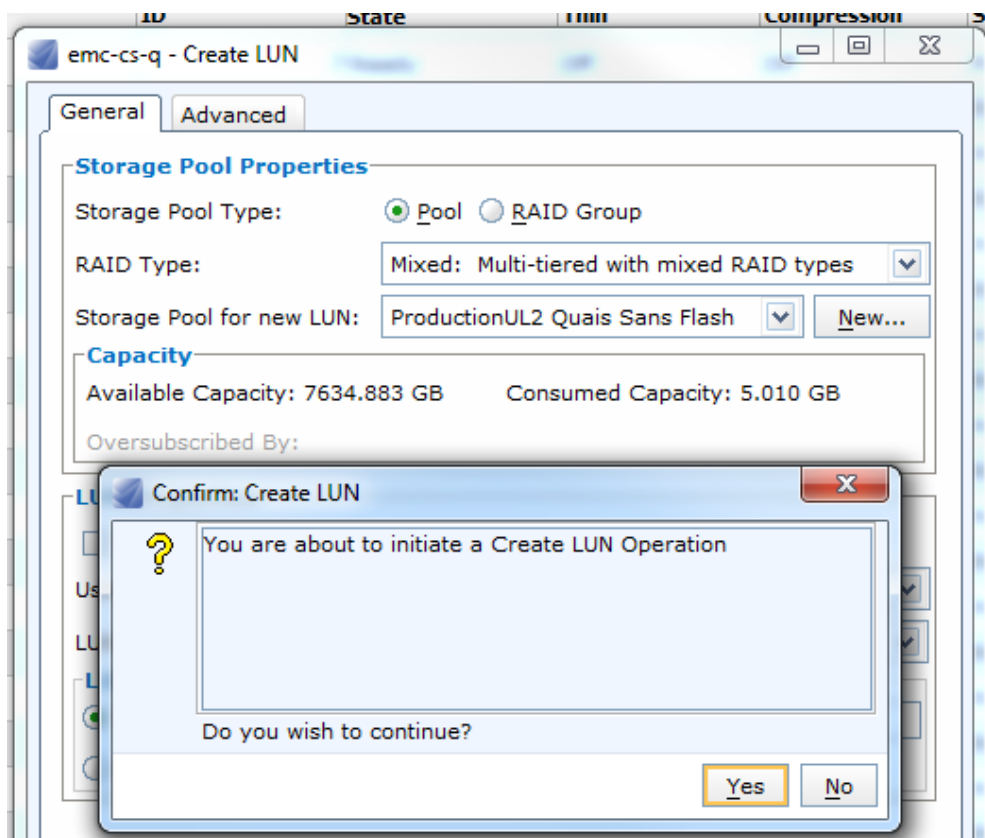


Figure 17 - Création d'une Lun sur la baie EMC

Il faut ensuite présenter la LUN nouvellement créée à un ou plusieurs serveurs. Sur la figure 18 nous choisissons de le présenter à notre ferme de serveurs ESXi.

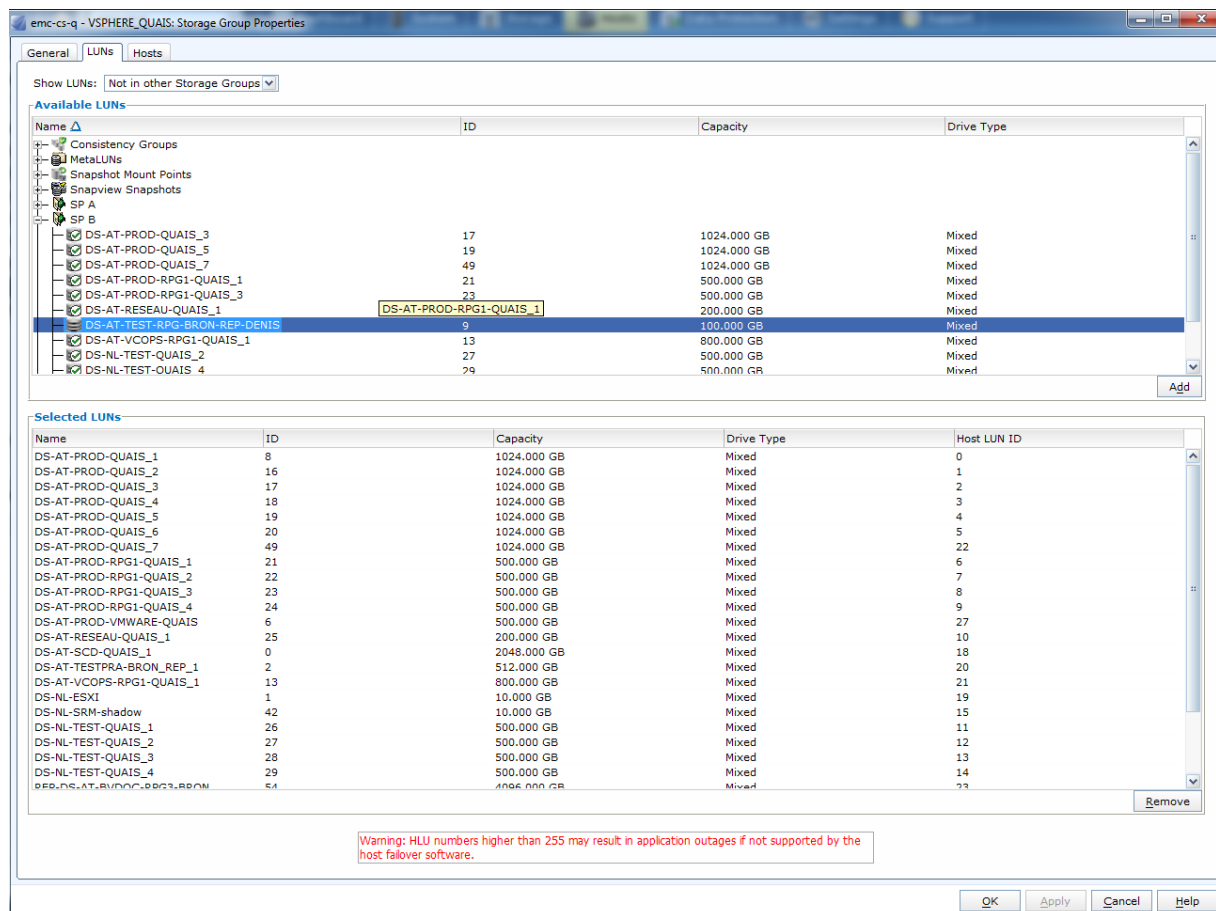
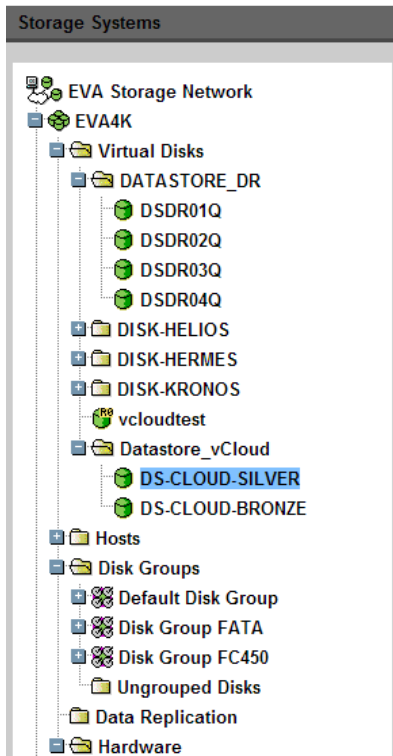


Figure 18 - Présentation d'une Lun aux serveurs

V.3.3. Création de LUNs sur la baie HP EVA

La création d'une LUN sur la baie HP EVA est plus facile encore que sur la baie EMC. L'interface est plus simple et présente globalement moins d'options. L'interface de la baie HP est visible sur la figure 18. Sur la figure 19 on crée une nouvelle LUN. Ensuite on présente la LUN aux serveurs ESXi, voir figure 20.



Vdisk Properties

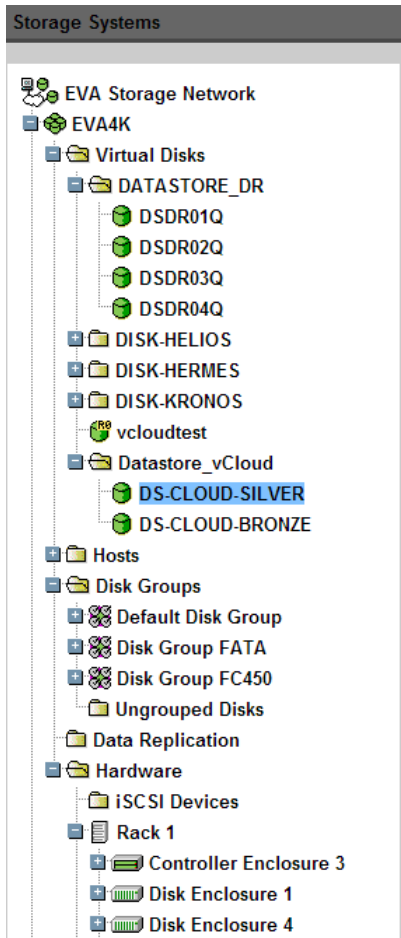
Save changes Create snapshot Create snapclone Delete ?

Create mirrorclone Convert to container Move

General Presentation Data Replication

Identification		Condition/State	
Name:	DS-CLOUD-SILVER	Operational state:	Good
World Wide LUN Name:	6005-08b4-0007-0946-0000-d000-0064-0000	Date/Time	
UUID:	6005-08b4-0007-0946-0000-d000-0064-0000	Created:	08-Aug-2012 10:06:08
Attributes		Cache Policies	
Type:	Original	Read cache:	On
Disk group:	Disk Group FC450	Mirror cache:	Mirrored
Redundancy:	Vraid5	Write cache:	
Capacity		Requested:	Write-back
Requested:	1235 GB	Actual:	Write-back
Allocated:	1235 GB		
Comments			

Figure 19 - Création d'une Lun sur la baie HP



Present Vdisk

Present Vdisk Select None Select All

Cancel

Select one or more hosts to which your Vdisk will be presented. Existing presentations to your Vdisk are shown. Click the **Present Vdisk** button after you have made your selection.

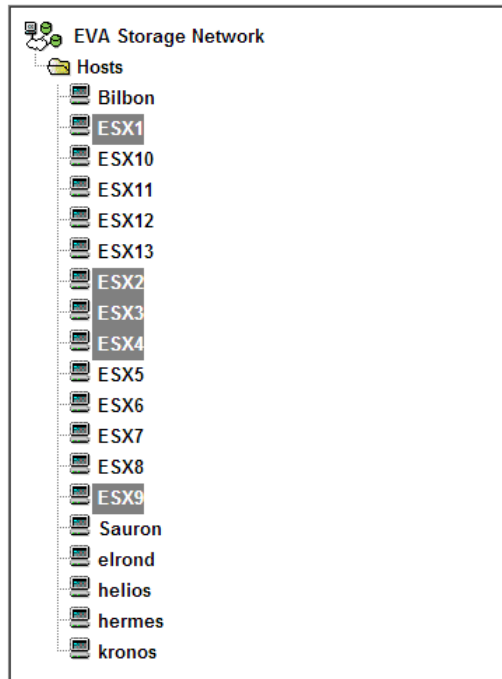


Figure 20 - Présentation d'une Lun sur la baie HP

V.3.4. Configuration des switchs fibres

Un switch fibre est un équipement utilisant le protocole FCP (Fibre Channel Protocol). Celui-ci permet d'associer un serveur à son stockage. L'université dispose de deux « fabriques » (ensembles des switchs FC) dans un souci de redondance. Ainsi la perte d'un switch FC ou d'un port n'entame pas le bon fonctionnement de l'infrastructure.

Le projet de cloud n'a pas nécessité de modification particulière au niveau des switchs fibres. Cependant j'ai déjà eu l'occasion de faire du zoning lorsqu'on m'a demandé de rajouter des serveurs physiques à notre ferme de serveurs ESXi à l'université. Ainsi, une bonne lecture de la configuration de ces switchs m'a aidé pour avancer rapidement sur les problématiques liées au stockage. Les modifications sur ces switchs sont à effectuer avec précaution car une erreur peut déconnecter un serveur de son stockage (ou plusieurs) et provoquer des corruptions en plus d'un arrêt du service délivré par le ou les serveurs impactés.

L'université utilise des switchs fibre Brocade 10Gb. La configuration se fait via l'interface web développée en java dont voici un aperçu sur la figure 21.

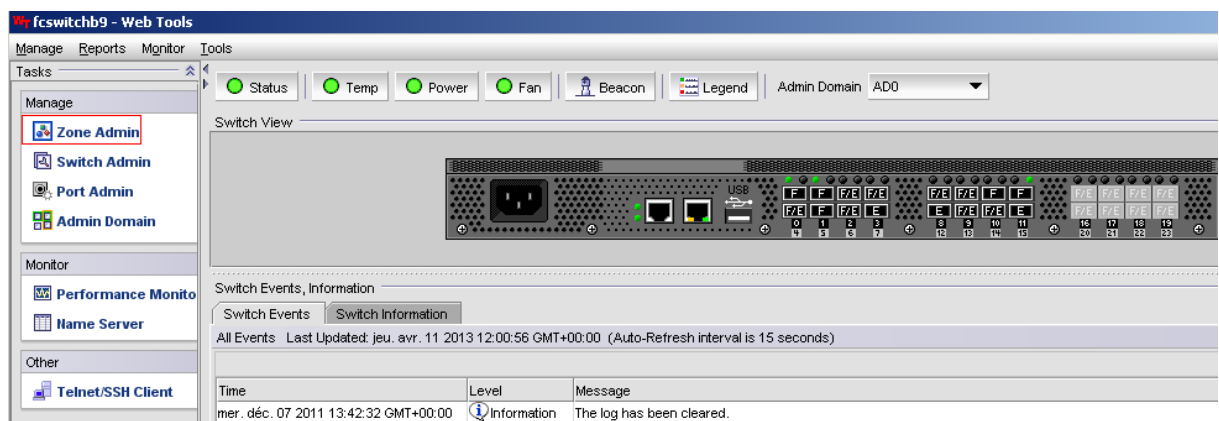


Figure 21 - Interface web de gestion des switchs fibres

V.3.5. Configuration dans vSphere au niveau du stockage

Il reste une opération à réaliser pour pouvoir utiliser le stockage dans des machines virtuelles et cela se situe au niveau de vSphere. On ajoute le stockage côté VMware :

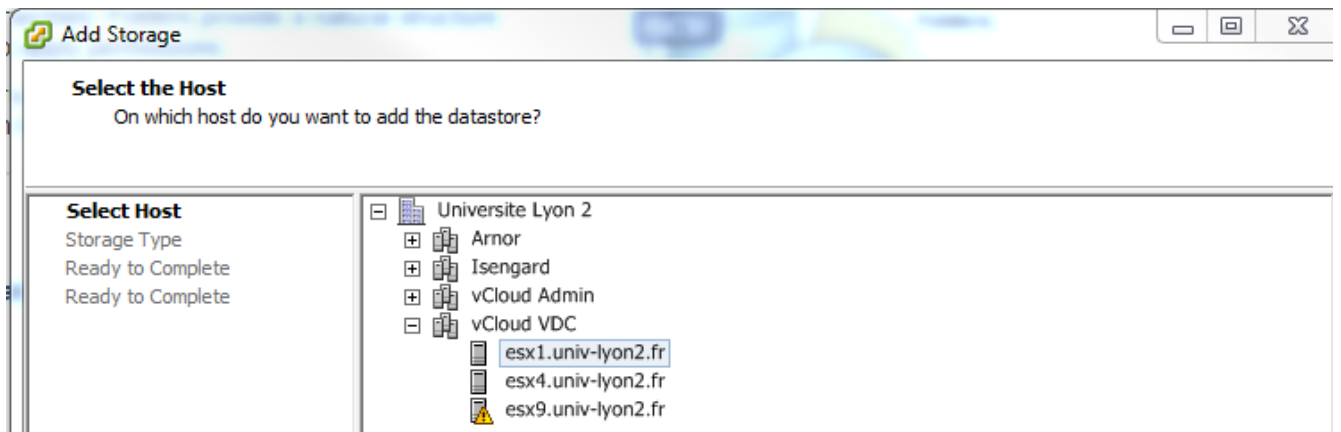


Figure 22 - Ajout du stockage dans vSphere

Il faut choisir un serveur à qui présenter le stockage (ici esx1 sur la figure 22). Ensuite, on choisit le type de stockage à savoir du NFS, un disque local ou une LUN.

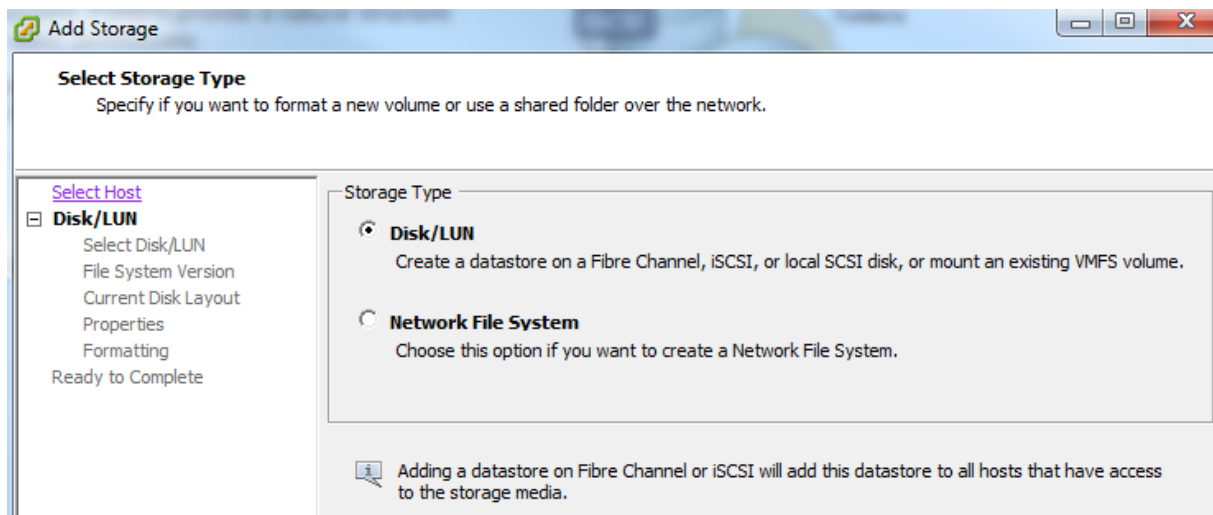


Figure 23 - Ajout du stockage dans vSphere (suite)

Si tout a bien été configuré avant, on choisit la LUN que l'on a créée (figure 23 et 24). Si on s'est trompé auparavant la LUN n'apparaît simplement pas.

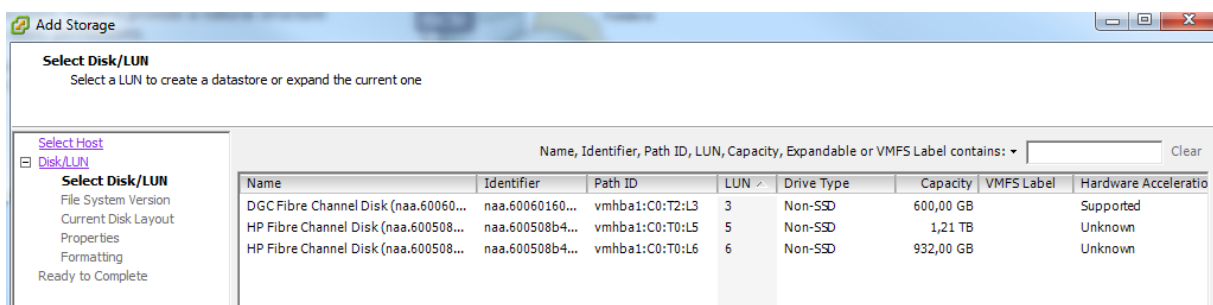


Figure 24 - Ajout du stockage dans vSphere, choix de la LUN

On choisit le type de formatage de la LUN sur la figure 25. Ici on prend VMFS-5 qui est plus récent que le VMFS-3 et qui présente l'avantage de créer des disques

virtuels de plus grande taille notamment (même si c'est inutile ici). L'idée est de choisir la version la plus haute pour éviter d'avoir à monter de version plus tard et ainsi éviter d'éventuelles surprises.

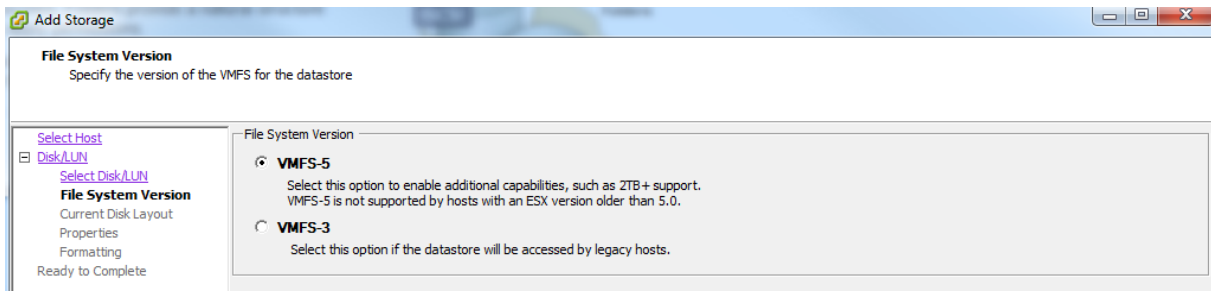


Figure 25 - Ajout du stockage dans vSphere, formatage du datastore

La LUN ainsi formatée devient un Datastore dans vSphere et il faut lui donner un nom sur la figure 26. Par convention, on utilise à l'université « DS » pour DataStore, « Cloud » pour désigner la vocation du Datastore et le distinguer des autres, « Gold » pour désigner la « qualité » du stockage (niveau de service délivré), « AT » pour auto-tiering et « Quais » pour sa géolocalisation.

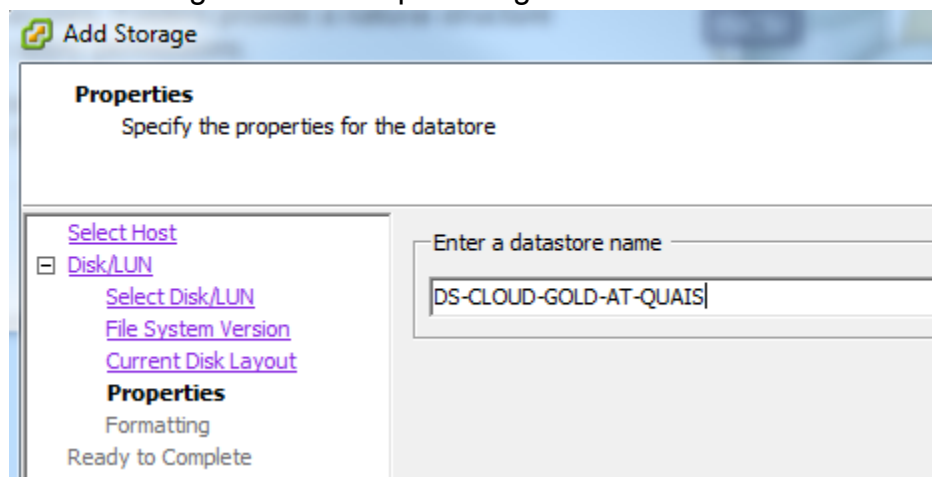


Figure 26 - Ajout du stockage dans vSphere, nommage du datastore

On alloue ici tout l'espace de la LUN au Datastore (figure 27), mais on pourrait avoir plusieurs Datastore pour une même LUN. Puis, on valide l'ensemble de l'opération (figure 28).

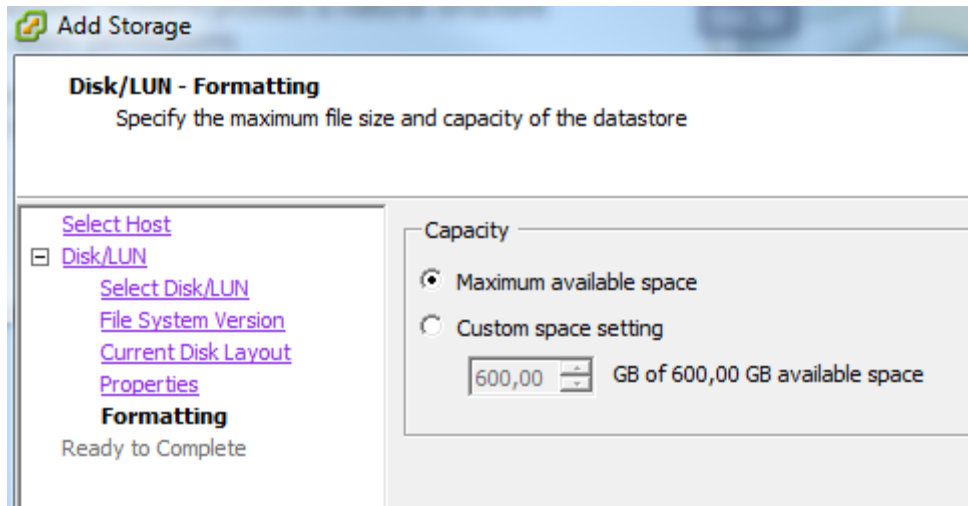


Figure 27 - Ajout du stockage dans vSphere, allocation de l'espace au datastore

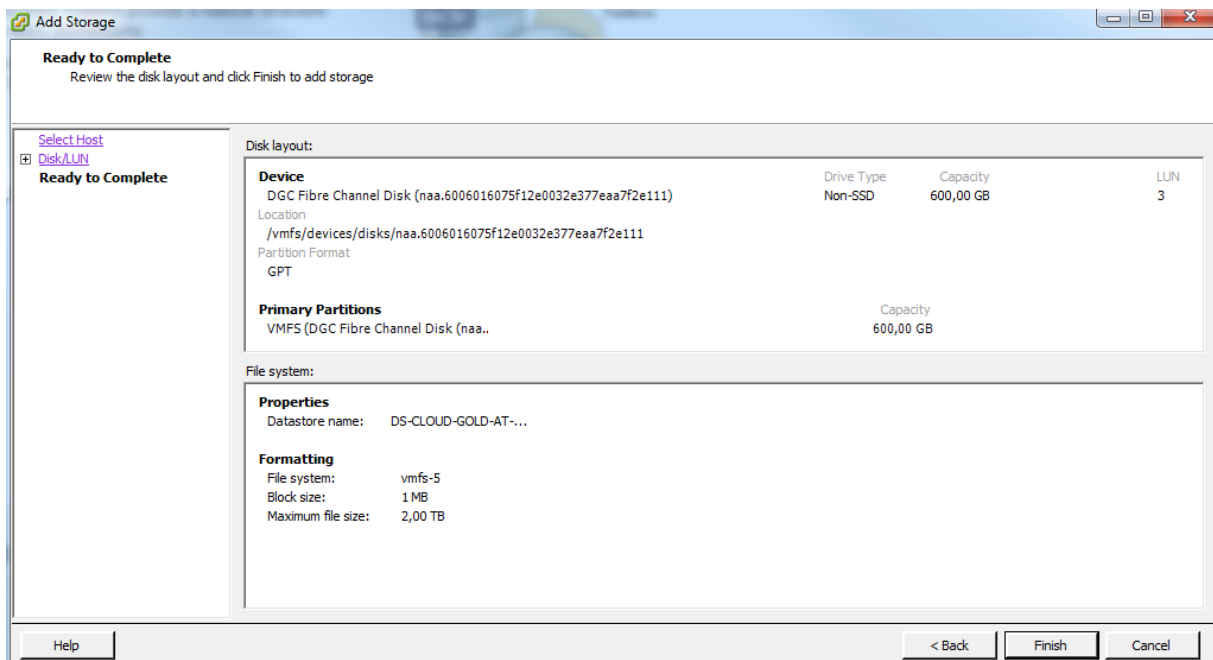


Figure 28 - Ajout du stockage dans vSphere, résumé avant validation de l'ensemble des opérations

On obtient ainsi nos différents «Datastore » dans vSphere que l'on utilisera ensuite dans vCloud. Ceci est visible sur la figure 29.

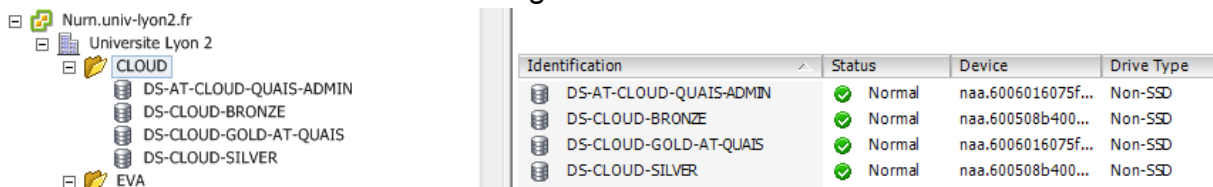
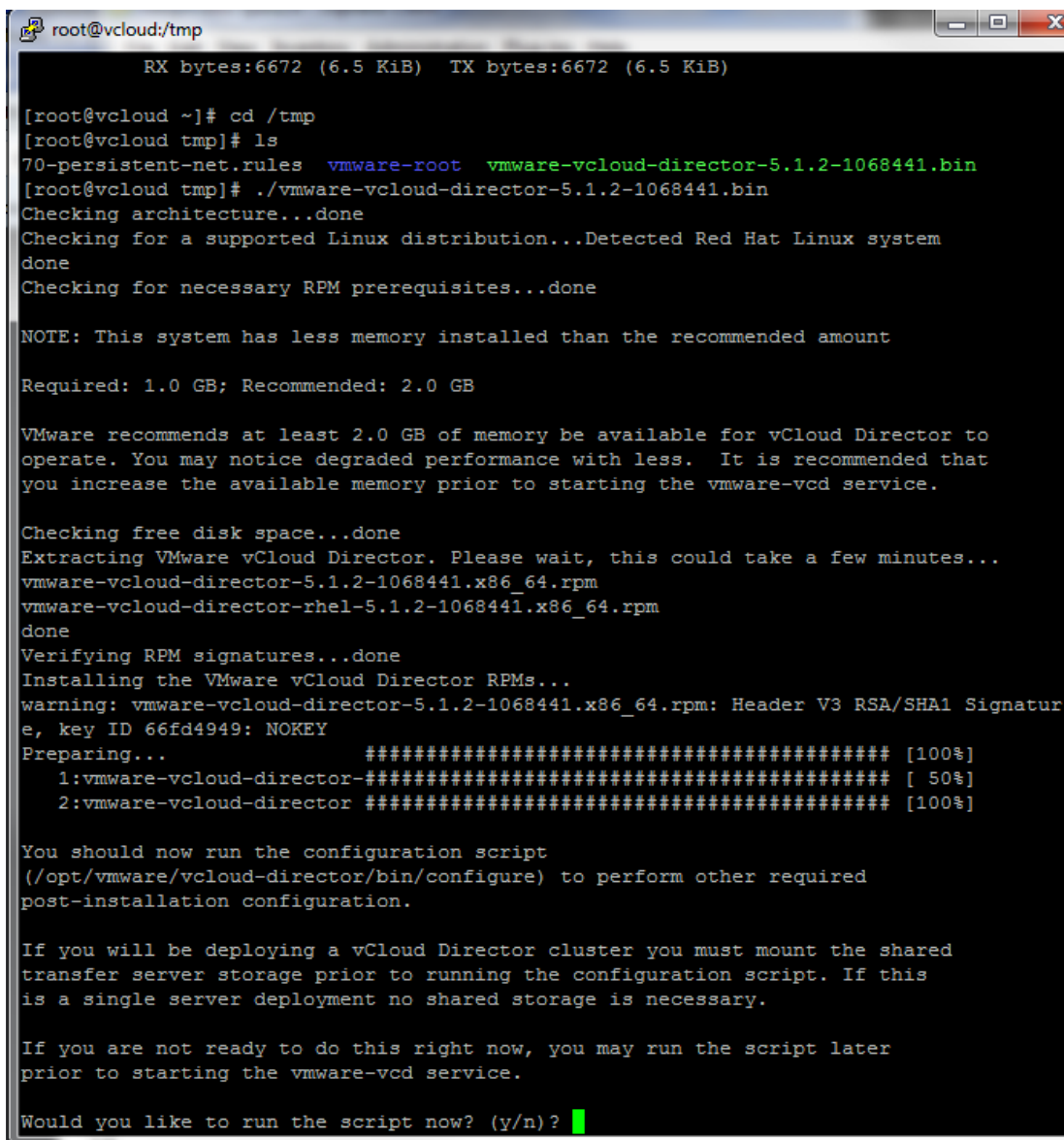


Figure 29 - Stockage dans vSphere alloué au cloud

V.4.0. Installation du produit vcloud

L'installation du produit vCloud se déclenche via un fichier exécutable binaire compatible avec Red Hat 6. J'ai utilisé notre modèle de machine virtuelle installée en Red Hat 6 64 bit. Pour cela il m'a fallu adresser une demande à notre équipe réseau afin qu'elle me fournisse une adresse ip, ainsi qu'une entrée dans notre dns (vcloud.univ-lyon2.fr).

Une fois le modèle cloné, j'ai installé les VMware Tools (qui ajoutent des fonctionnalités), entré le nom de la machine, modifié la configuration de la carte réseau afin de la faire correspondre à l'adresse que l'on m'avait fournie et modifié le nom de la machine (hostname). La préparation de la vm a été assez rapide au final. Après cela il faut ensuite installer le binaire fourni par VMware (figure 30).



```
root@vcloud:/tmp
RX bytes:6672 (6.5 KiB) TX bytes:6672 (6.5 KiB)

[root@vcloud ~]# cd /tmp
[root@vcloud tmp]# ls
70-persistent-net.rules  vmware-root  vmware-vcloud-director-5.1.2-1068441.bin
[root@vcloud tmp]# ./vmware-vcloud-director-5.1.2-1068441.bin
Checking architecture...done
Checking for a supported Linux distribution...Detected Red Hat Linux system
done
Checking for necessary RPM prerequisites...done

NOTE: This system has less memory installed than the recommended amount

Required: 1.0 GB; Recommended: 2.0 GB

VMware recommends at least 2.0 GB of memory be available for vCloud Director to
operate. You may notice degraded performance with less. It is recommended that
you increase the available memory prior to starting the vmware-vcd service.

Checking free disk space...done
Extracting VMware vCloud Director. Please wait, this could take a few minutes...
vmware-vcloud-director-5.1.2-1068441.x86_64.rpm
vmware-vcloud-director-rhel-5.1.2-1068441.x86_64.rpm
done
Verifying RPM signatures...done
Installing the VMware vCloud Director RPMs...
warning: vmware-vcloud-director-5.1.2-1068441.x86_64.rpm: Header V3 RSA/SHA1 Signatur
e, key ID 66fd4949: NOKEY
Preparing... ##### [100%]
 1:vmware-vcloud-director-##### [ 50%]
 2:vmware-vcloud-director ##### [100%]

You should now run the configuration script
(/opt/vmware/vcloud-director/bin/configure) to perform other required
post-installation configuration.

If you will be deploying a vCloud Director cluster you must mount the shared
transfer server storage prior to running the configuration script. If this
is a single server deployment no shared storage is necessary.

If you are not ready to do this right now, you may run the script later
prior to starting the vmware-vcd service.

Would you like to run the script now? (y/n)? █
```

Figure 30 - Installation de vCloud Director

Lors de l'installation du produit on configure l'accès à la base de données en utilisant l'utilisateur de la base de données que l'on avait créé au préalable et en renseignant son mot de passe.

Une fois installé le service vmware-vcd démarre et lance l'interface web par laquelle on configure ensuite l'outil : <https://vcloud.univ-lyon2.fr>. On peut cependant rendre le démarrage automatique afin qu'il démarre en même temps que la vm via la commande :

```
chkconfig --level 3 vmware-vcd on
```

L'accès web nécessite un navigateur compatible (internet explorer, firefox ou chrome) ainsi qu'adobe flashplayer et un plugin dédié VMRC.

La première connexion à l'interface web nous demande d'installer le certificat car nous utilisons un certificat auto signé. Nous aurions pu utiliser un certificat signé par une autorité de certification reconnu par le navigateur, ce qui a pour effet d'enlever le message d'alerte du navigateur lors de la première connexion. Il faut savoir que les certificats signés par une autorité de certification ont un certain coût.

La première connexion à vCloud (figure 31) permet d'installer la licence du produit qui dépend du nombre de processeurs utilisés par les machines physiques qui font tourner vCloud. Nous avons une licence pour 6 sockets de CPU soit 3 serveurs physiques possédant deux sockets chacun. Après la licence on crée un compte administrateur de l'outil en optant pour un mot de passe complexe, on ajoute l'adresse mail de l'administrateur et on donne un nom à la « cellule » du cloud que l'on vient d'installer.

Il faut noter que notre installation ne contiendra qu'une seule « cellule » mais il est possible d'en joindre plusieurs dans le cas d'énormes infrastructures réparties géographiquement sur plusieurs sites. Après cela, l'une des premières choses à faire est de joindre vCloud à vCenter. Cette opération nécessite un compte administrateur avec un niveau de droits élevé dans vSphere.

Ensuite il faut joindre vCloud à vShield, ce même vShield doit déjà être enregistré dans le vCenter en question sous forme de plugin. On utilise pour cette jonction le compte administrateur de vShield sur la figure 32.

Associer un nouveau vCenter

Nommer ce vCenter

Connecter à vShield Manager

Prêt à terminer

Nommer ce vCenter

Entrez les informations relatives à la connexion, le nom et la description pour le nouveau vCenter tel que vous souhaitez qu'elles apparaissent dans VCD.

Nom de l'hôte ou adresse IP : *

Numéro de port : *

Nom d'utilisateur : *

Mot de passe : *

Nom vCenter : *

Description :

URL de vSphere Web Client : Utiliser des services vSphere pour fournir cette URL
 Utiliser l'URL suivante :

Précédent **Suivant** Terminer Annuler

Figure 31 - Premier lancement de l'interface web de vCloud Director, association au serveur vCenter

Associer un nouveau vCenter

Nommer ce vCenter

Connecter à vShield Manager

Prêt à terminer

Connecter à vShield Manager

Connecter à vShield Manager

vShield Manager est nécessaire pour les services en réseau de VCD. Entrez les informations de connexion pour vShield Manager associé au vCenter en question. Vérifiez que vShield Manager est déjà enregistré avec le vCenter.

Nom de l'hôte ou adresse IP : *

Nom d'utilisateur : *

Mot de passe : *

Figure 32 - Premier lancement de l'interface web de vCloud Director, association au serveur vShield

A ce stade le schéma de l'infrastructure de test est visible figure 33.

Architecture vCloud de Test

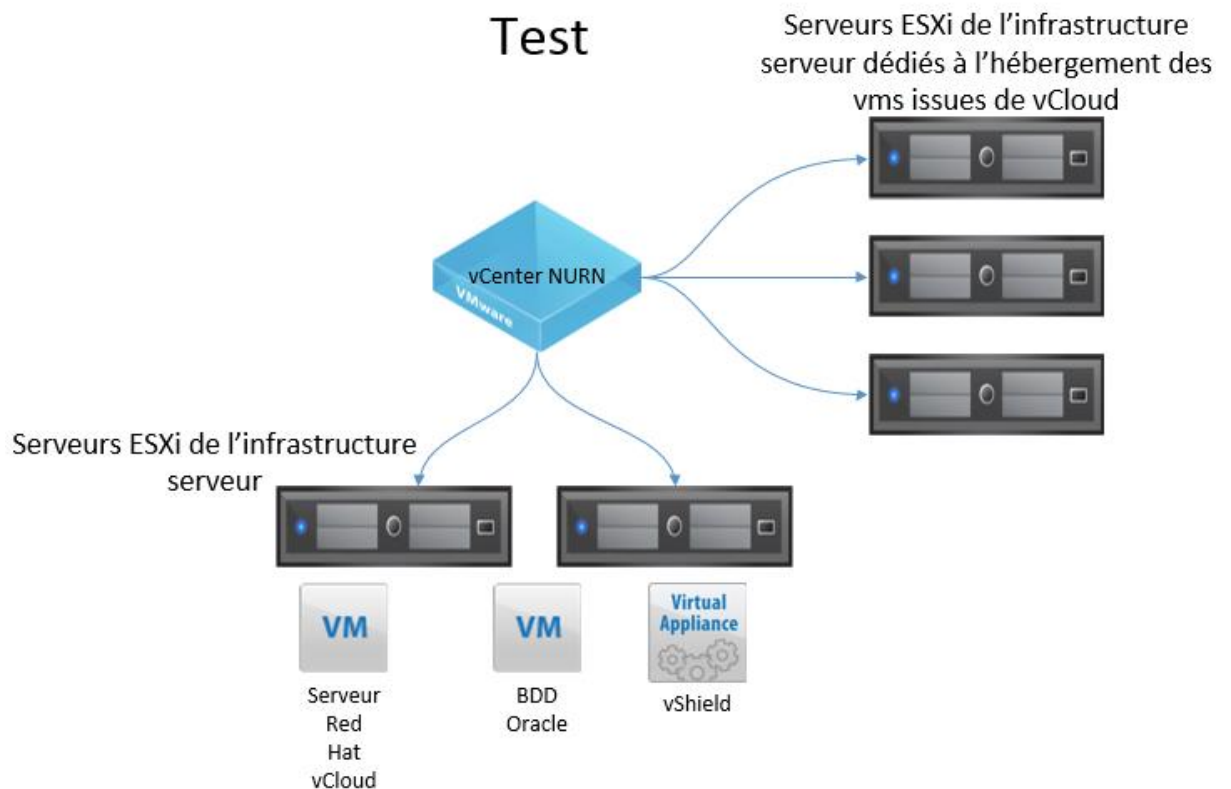


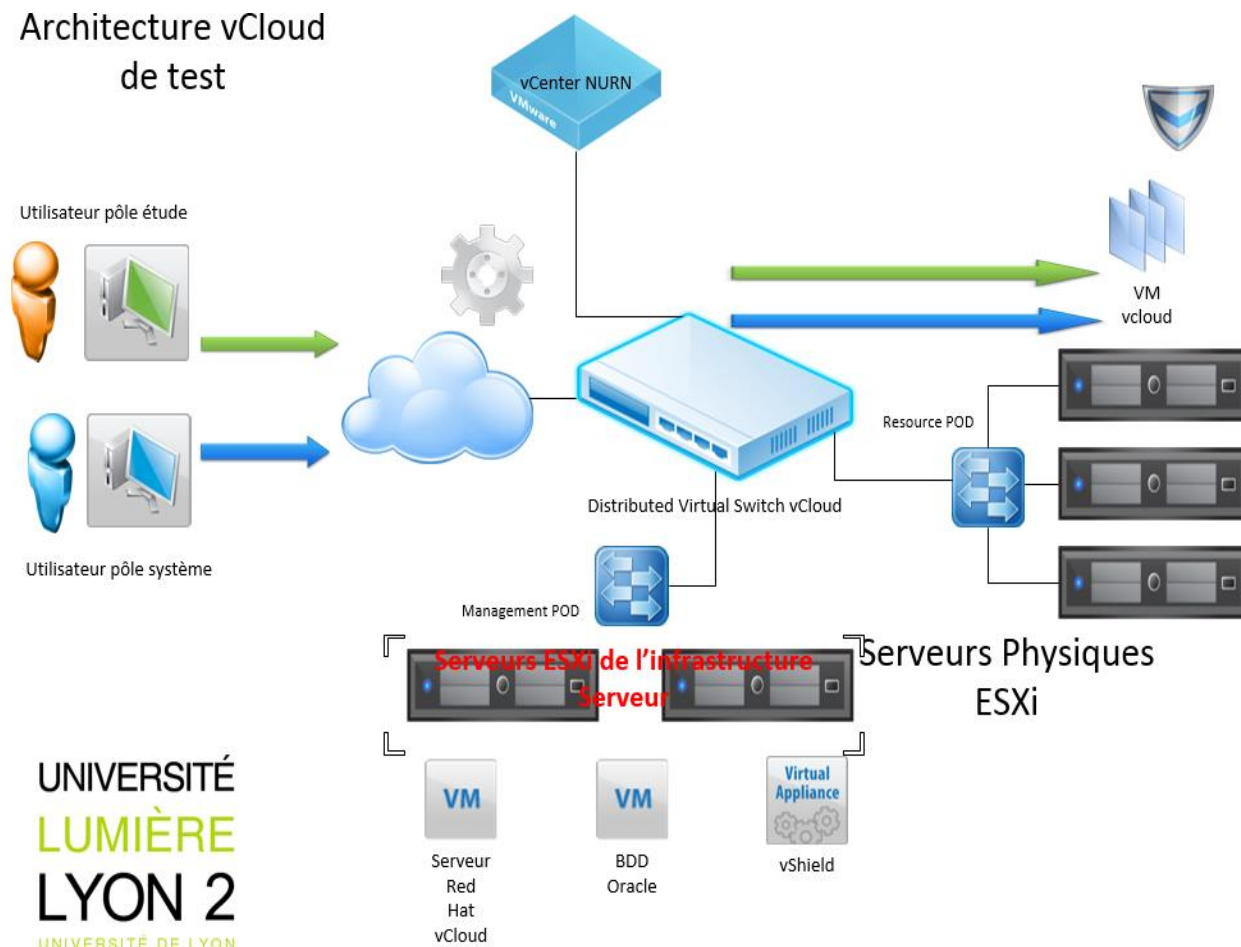
Figure 33 - Architecture de test

V.5.0. Configuration de vCloud

Parmi les premiers utilisateurs de vCloud il y a le « pôle étude » qui travaille à la DSI. Il s'agit d'une population de développeurs et de chefs de projets dont les besoins sont souvent les mêmes : un serveur d'application tomcat, un serveur apache, un serveur de base de données... Nous connaissions ces besoins avant le début du projet étant donné que le pôle opération pour lequel je travaille est fournisseur de ce type de serveurs assez régulièrement. Les besoins étant très spécifiques, j'ai choisi de créer une organisation au sens «vCloud » du terme pour le pôle étude.

Une deuxième organisation est dédiée au pôle opération auquel j'appartiens. La distinction entre les deux organisations repose sur les droits et la possibilité de publier des machines virtuelles pour le pôle opération, là où le pôle étude est tributaire du travail de notre pôle.

Architecture vCloud de test



UNIVERSITÉ
LUMIÈRE
LYON 2
UNIVERSITÉ DE LYON

Figure 34 - Architecture de test, gestion des utilisateurs

Les machines virtuelles issues du cloud doivent être isolées des machines virtuelles servant à l'infrastructure, c'est-à-dire la base de données, vShield et le serveur vCloud. D'un point de vue réseau, j'ai créé un switch virtuel distribué entre les serveurs ESXi, la figure 34 le décrit. Ceci permet de créer un objet de type switch distribué dans vSphere qui permet de partager des VLAN's entre les serveurs ESXi. Concrètement c'est une fonctionnalité de vSphere qui nécessite un haut niveau de licence contrairement à la fonctionnalité « switch standard ». Un des intérêts est par exemple de créer un VLAN sur x hôtes ESXi en une seule fois au lieu d'avoir à le créer individuellement sur chaque ESXi.

V.6.0 Tests au niveau réseau

J'ai réalisé plusieurs séries de tests au niveau réseau. Les tests effectués sur la plate-forme de test ont permis d'appréhender le produit et de concevoir une architecture cohérente avec les besoins de l'université. Les tests ont surtout été effectués au niveau réseau afin de comprendre comment isoler correctement le cloud. Ceci répond au besoin de sécurité.

Voici l'architecture la plus intéressante que j'ai pu tester (figure 35):

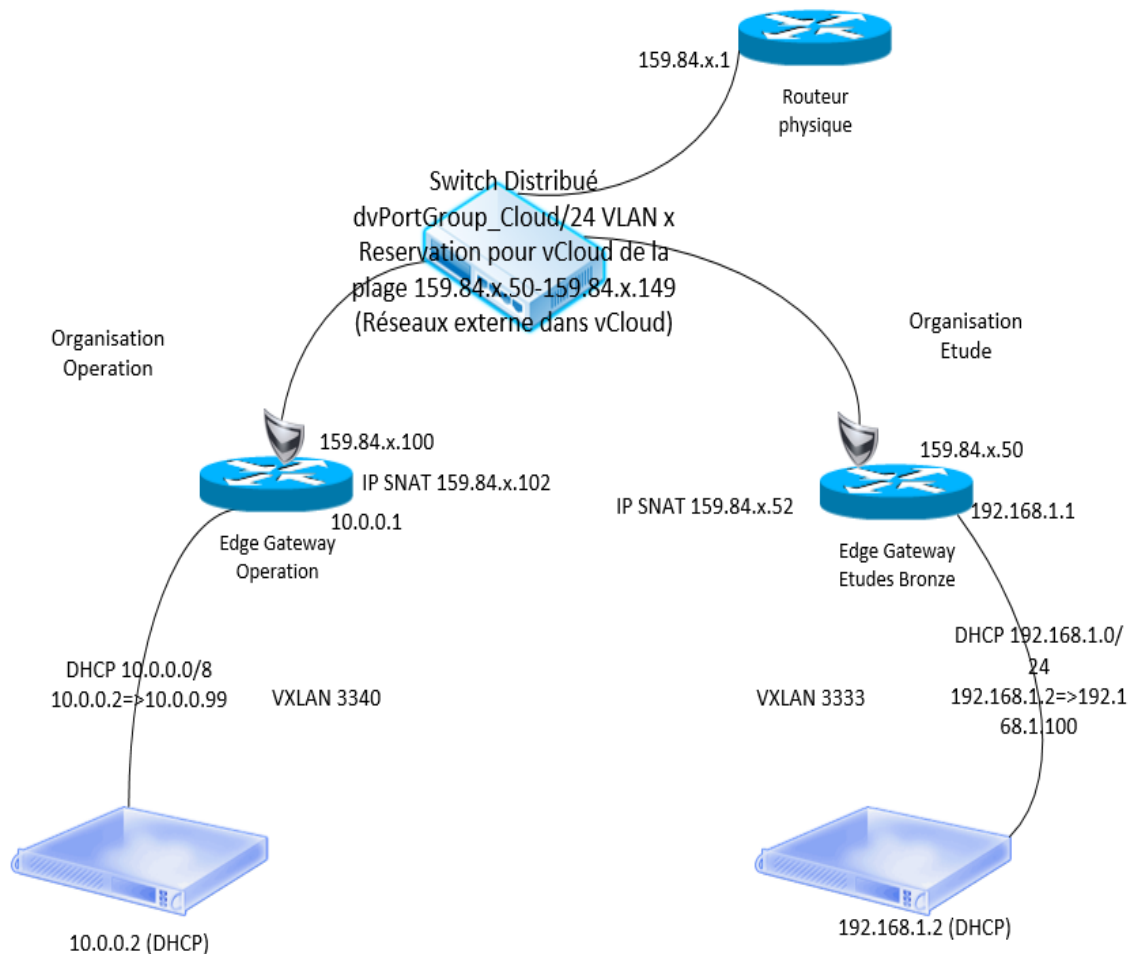


Figure 35 - Architecture réseau de test

Dans cette architecture j'ai testé la possibilité d'utiliser des adresses ip non routables sur internet (10.0.0.0/8 et 192.168.1.0/24). Dans cet exemple il a été possible de sortir sur internet malgré l'adresse IP 10.0.0.2. J'ai également testé s'il était possible de joindre une machine qui appartient à une autre organisation (la machine avec l'adresse 192.168.1.2). Il apparait que c'est possible, cependant il faut pour cela ajouter des règles de routage dans les « Edge gateway ». Ces « Edge Gateway » sont générées par vShield. Elles se matérialisent sous forme de machines virtuelles dans vSphere et s'associent à des VDC d'organisation dans vCloud. Les passerelles générées ainsi se configurent dans vCloud.

La configuration des Edge Gateway nécessitent de comprendre un minimum les problématiques classiques liées au réseau : routage, allocation d'adresses, règles de pare-feu, problèmes de congestions... Par ailleurs une des options intéressantes est de limiter la bande passante pour les machines virtuelles qui utiliseront ces Edge Gateway (figure 36).

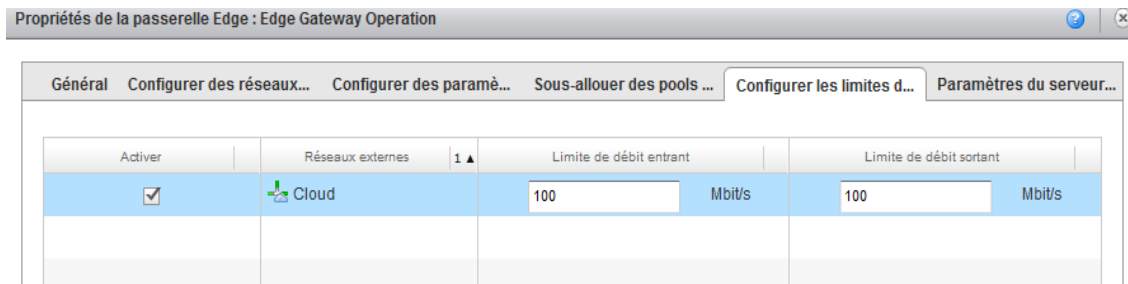


Figure 36 - Interface vCloud, limitation de la bande passante

Cette option peut s'avérer utile si l'on a une grande architecture et une qualité de service à assurer auprès de ses clients. Dans le cas de l'université je n'ai pas eu à l'utiliser. Des tests ont été réalisés afin de bien comprendre comment fonctionnait l'outil et pour connaître l'étendue des possibilités.

V.7.0. Recette de la plate-forme de test

Deux organisations ont été définies, c'est pourquoi j'ai choisi un utilisateur de chaque pôle afin de pouvoir faire tester l'ensemble de ce que j'allais créer dans vCloud. Bien sûr j'ai dû prendre le temps de les former à ces nouveaux outils. Même si l'interface web de vCloud est assez accessible, certains termes spécifiques au produit (vApp, catalogue...) le rendent moins facile à appréhender.

La mise en place de la plate-forme de test est terminée, les tests au niveau réseau ont notamment permis de dégager de bonnes pratiques en matière d'isolation des organisations. Nous pouvons décrire la mise en place de la plate-forme de production.

Chapitre 6

VI. Mise en place de la production

VI.1.0. étude sur l'upgrade de la version vSphere de production et impacts sur la production

Le projet vCloud a démarré avant le début du projet de montée de version de vSphere pour notre infrastructure serveurs. Cependant, il a fallu réfléchir à l'impact de l'un sur l'autre. Pour revenir aux sources du projet de montée de version vSphere, il faut savoir que notre version de vSphere (5.0) ne supportait pas par exemple des machines virtuelles en Windows 2012 Server. Pour avoir testé personnellement l'installation d'un serveur de test en Windows 2012 sur un ESXi en 5.0, l'opération se soldait par un « écran bleu » lourd de sens.

Au-delà de cette limitation, la montée de version vSphere nous a également permis de remplacer certaines machines physiques par des machines plus puissantes. A nombre de machines physiques égal, nous avons augmenté la puissance de calcul (CPU et RAM) de notre ferme de serveurs. Le calcul est intéressant car les licences chez VMware se basent sur le nombre de sockets physiques utilisé par les serveurs ESXi. Cette puissance de calcul accrue s'est faite sans augmentation des coûts de licence.

Notre prestataire a été chargé de mettre en œuvre ces changements, mais il l'a fait après la mise en production du cloud. C'est au moment de cette étude que j'ai préconisé l'achat d'un nouveau serveur vCenter dédié à vCloud. Ce choix impliquait 5000 euros de dépense en plus. Il se justifie par le cloisonnement qu'apporte un vCenter dédié. En termes d'architecture il est intéressant d'isoler les sources potentielles de problèmes. Nous connaissions à l'époque plusieurs plantages récurrents du serveur vCenter (avant la montée de version en 5.5) et je trouvais préférable de ne pas partager le même serveur vCenter entre le cloud et l'infrastructure serveur. Cela donne aussi un peu plus de souplesse et permet de mettre en maintenance le cloud sans impacter nos autres serveurs de production (l'inverse est vrai également).

Pour ce qui est de l'impact de la montée de version vSphere sur le cloud, il s'est résumé à une interruption du service d'environ une heure liée à la maintenance des vm. Aussi cette montée de version a permis de récupérer un matériel plus récent et d'abaisser le nombre de CPU utilisés pour le cloud de six à quatre. En réalisant cette opération, on abaisse aussi les coûts de licence lié au support annuel.

VI.2.0. Création d'une nouvelle base de données Oracle pour le nouveau serveur vCenter

Le choix de créer un nouveau serveur vCenter implique de créer une nouvelle base de données. Pour cela, trois options sont possibles : IBM DB2, Microsoft SQL Server ou Oracle. Le produit vCloud nous ayant déjà demandé d'installer une base de données Oracle, nous choisissons de créer une deuxième base de données sur le premier serveur de base de données utilisé par vCloud.

Techniquement la création de la base de données est très similaire à la première. Nous utilisons un « SID » différent. Le SID identifie la base de données dans Oracle.

VI.3.0. Installation de vCenter server

L'installation de vCenter se fait sur un serveur Windows 2008 R2. Il existe également une appliance Linux Suse qui peut remplacer un vCenter Windows. Cependant la version 5.0 de cet appliance est limitée au support de cinquante vm seulement. Très intéressant pour une organisation de petite taille notamment pour les gains en termes d'administration, l'appliance me semblait encore être un produit trop jeune et trop limité pour pouvoir l'utiliser à cet endroit. Historiquement le serveur vCenter est une application que l'on installe sur un serveur Windows et j'ai poursuivi dans cette voie.

Avant d'installer le produit vCenter j'ai donc utilisé un modèle de serveur Windows 2008 R2 que nous utilisons fréquemment. Rien de particulier à noter sur le déploiement, hormis le fait que je l'ai jointe à l'active directory (service d'annuaire Microsoft). La base de données de vCenter est donc déportée sur un autre serveur et cela nous oblige à installer le client oracle et à configurer un lien ODBC.

Il faut donc trouver les bonnes sources du driver ODBC sur le site d'Oracle. L'installation du client est assez triviale. On choisit la version 32 bit du driver ODBC.

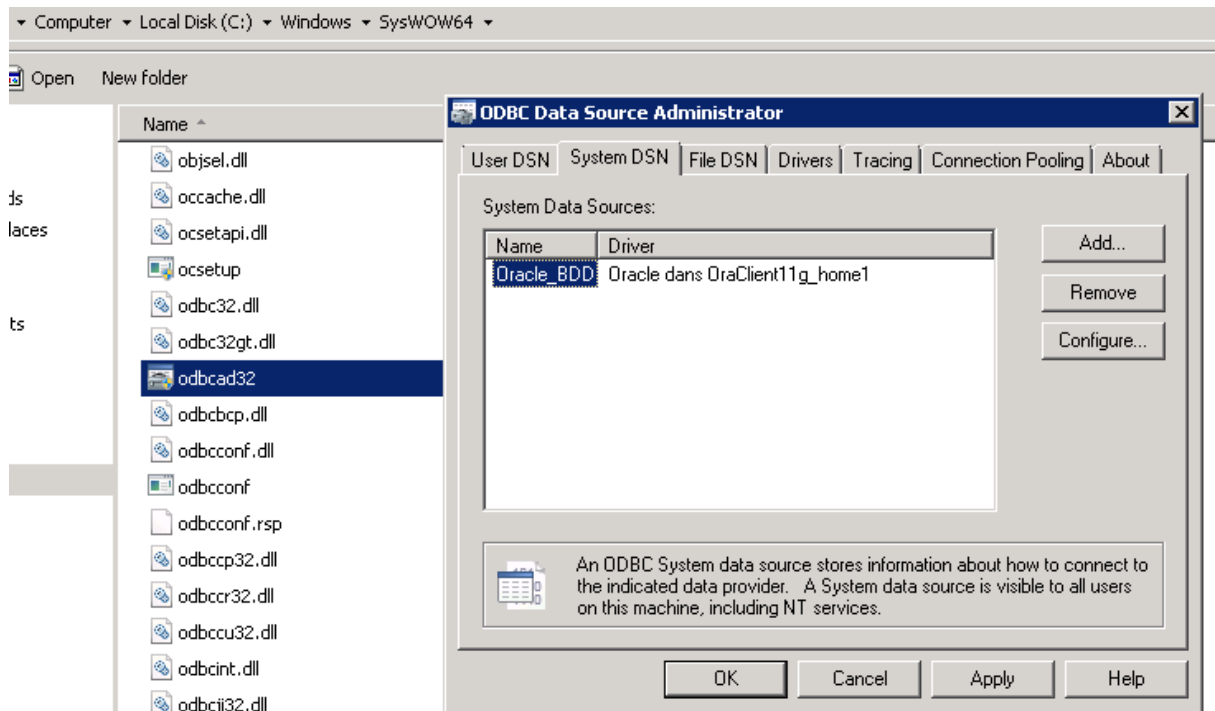


Figure 37 - Création du lien ODBC 32 bit dans Windows Server 2008 R2

Une fois installé on configure le lien ODBC (figure 37) et on teste la connexion à la base de données avant d'installer vCenter (figure 38).

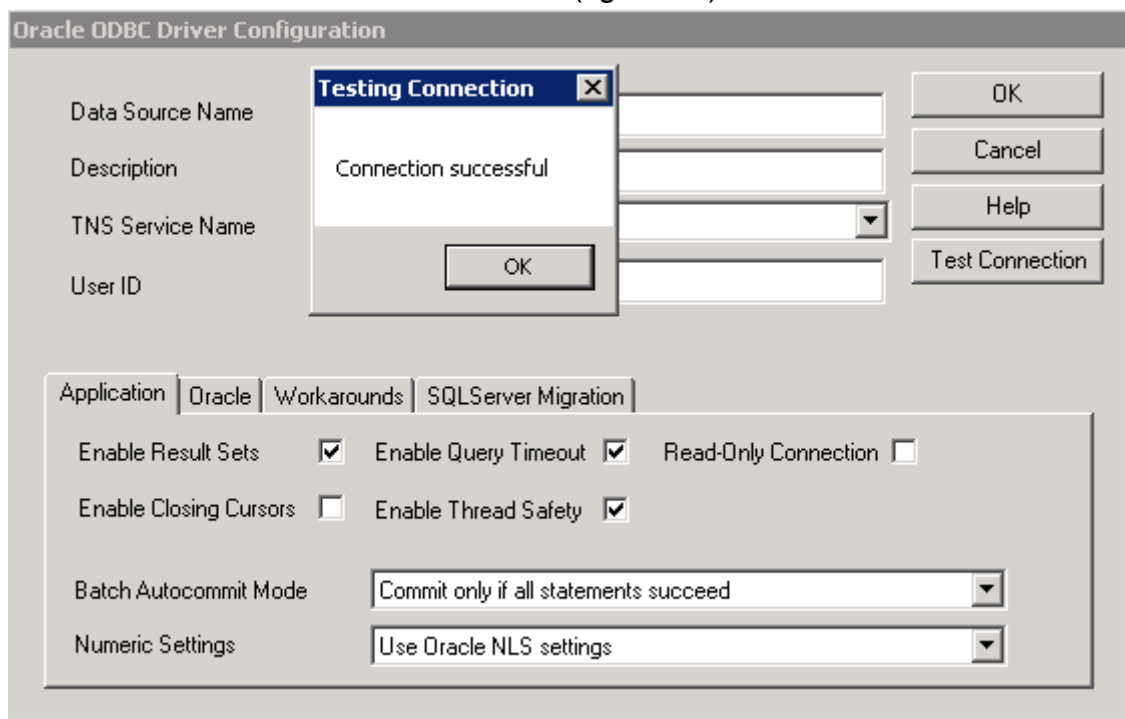


Figure 38 - Test de la connexion à la base de données en utilisant le lien ODBC

On installe ensuite vCenter :

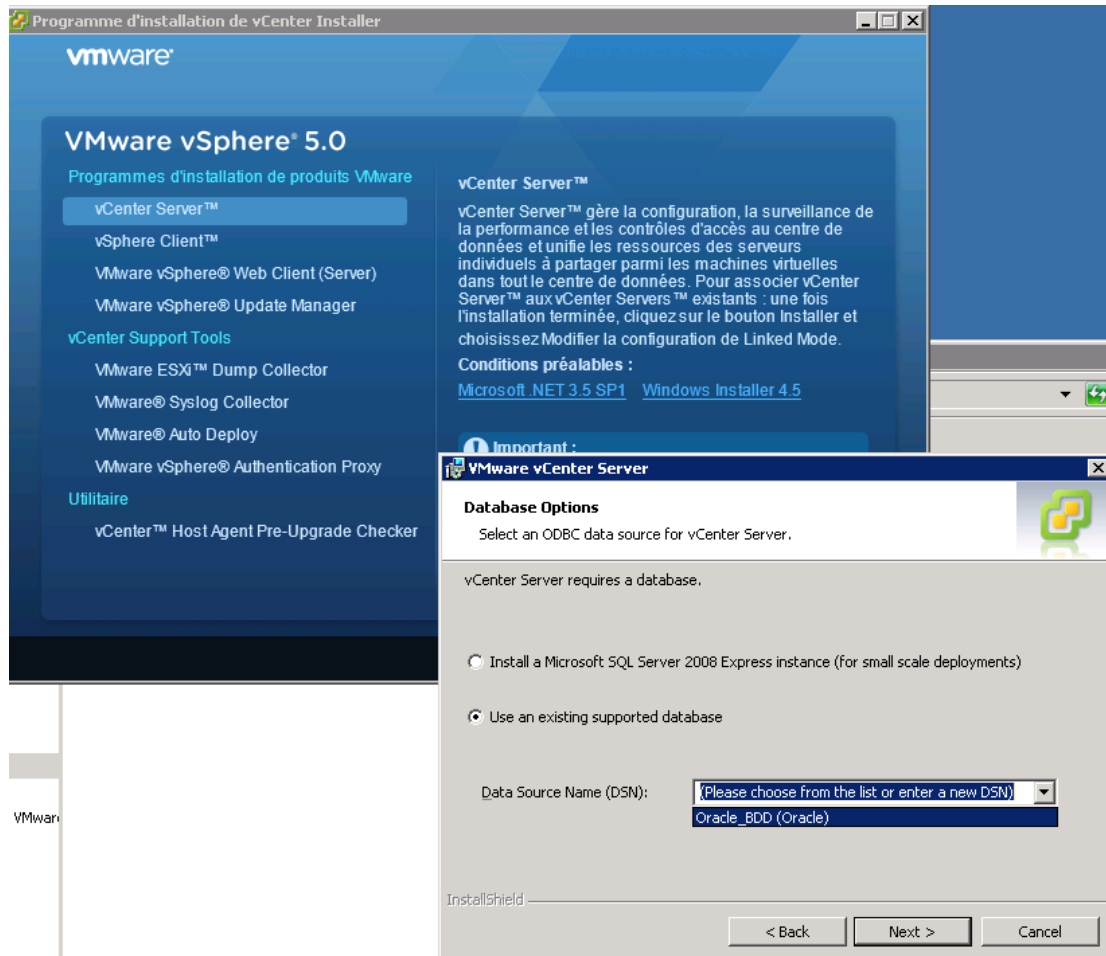


Figure 39 - Installation de serveur vCenter, sélection du lien ODBC

La bonne configuration du client oracle et du lien ODBC s'observe sur la figure 39, lorsque l'installer liste le DSN. On utilise ensuite les identifiants de l'utilisateur de la base de données afin de se connecter (figure 40).

On choisit le mode « standalone » plutôt que « linked mode » sur la figure 41. Le linked mode permet de lier deux serveurs vCenter et de gérer ainsi dans un seul client vSphere deux vCenter (ou plus). Cela apporte un confort d'utilisation mais dans notre cas ce n'est pas intéressant car nous ne voulons pas lier vCloud à notre infrastructure serveur.

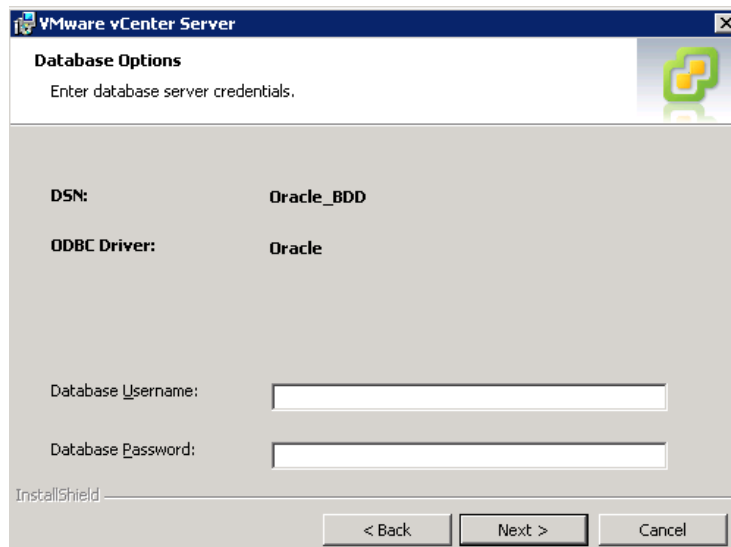


Figure 40 - Installation de serveur vCenter, connexion à la base de données déportée

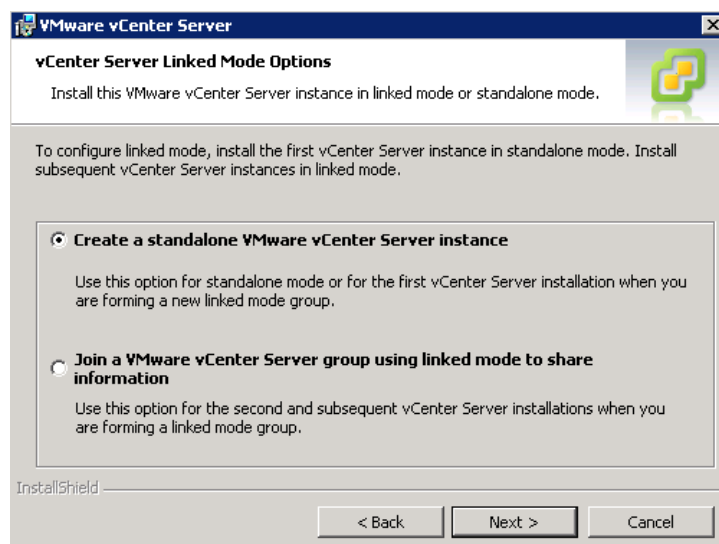


Figure 41 - Installation de serveur vCenter, sélection du mode "standalone"

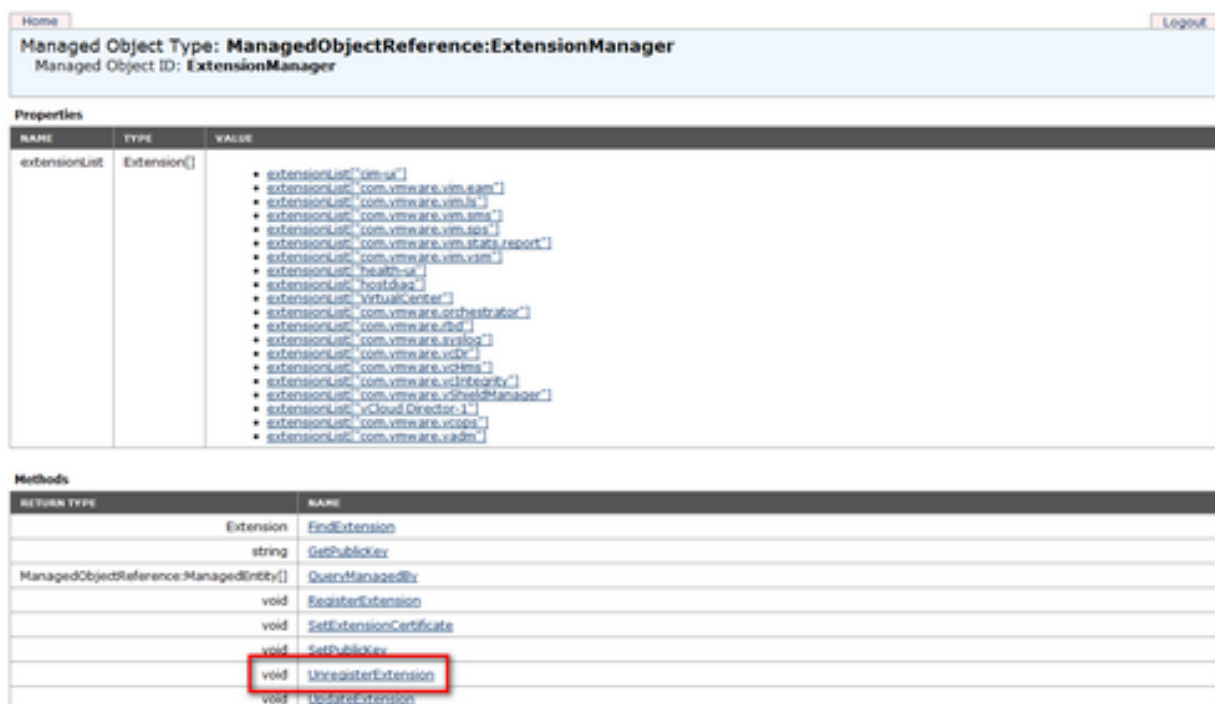
La taille de la JVM permet de dimensionner en fonction du nombre de vm. C'est un paramètre important car il dimensionne la ram allouée au service lancé par tomcat (figure 42). Une fois vCenter installé, on peut se connecter directement sur le serveur vCenter et intégrer les serveurs ESXi sur lesquels fonctionneront les vm issues de vCloud. La figure 43 présente l'architecture de production et l'utilisation des serveurs ESXi.

VI.4.0. Migration de vShield

L'appliance vShield était à ce stade encore rattachée à l'ancien serveur vCenter de notre infrastructure serveur (« Nurn » sur la figure 43). J'aurais pu me contenter de redéployer un nouvel appliance vShield sur le nouveau vCenter mais il me semblait intéressant de garder la configuration de l'outil tel que je l'avais faite et donc de réutiliser les modifications. C'est la raison pour laquelle j'ai décidé de migrer la vm vShield de vCenter.

Pour migrer vShield, il faut d'abord déréférencer vShield de l'ancien vCenter au niveau des plugins de vCenter (figure 44). Pour cela on utilise l'url de ce type : <https://vcenter.domain.local/mob>:

On arrive sur une page web référençant l'ensemble des plugins du vCenter, sur lequel on est connecté mais avec des noms un petit peu complexes. Par exemple vShield apparaît sous ce nom : com.vmware.vShieldManager,vShield Manager. On choisit unregisterExtension sur le plugin vShield puis invoke Method



Managed Object Type: **ManagedObjectReference:ExtensionManager**
Managed Object ID: **ExtensionManager**

Properties

NAME	TYPE	VALUE
extensionList	Extension[]	<ul style="list-style-type: none">extensionList["vm-ua"]extensionList["com.vmware.vim.sdm"]extensionList["com.vmware.vim.la"]extensionList["com.vmware.vim.sms"]extensionList["com.vmware.vim.scs"]extensionList["com.vmware.vim.stats.report"]extensionList["com.vmware.vim.vam"]extensionList["he-atn-ua"]extensionList["hpc-lua"]extensionList["virtualCenter"]extensionList["com.vmware.orchestrator"]extensionList["com.vmware.rbd"]extensionList["com.vmware.svslog"]extensionList["com.vmware.vdr"]extensionList["com.vmware.vchime"]extensionList["com.vmware.vchime"]extensionList["com.vmware.vchime"]extensionList["com.vmware.vchime"]extensionList["vCloud Director"]extensionList["com.vmware.vcloud"]extensionList["com.vmware.vcloud"]

Methods

RETURN TYPE	NAME
Extension	FindExtension
string	GetPublicKey
ManagedObjectReference:ManagedEntity[]	QueryManagedBy
void	RegisterExtension
void	SetExtensionCertificate
void	SetPublicKey
void	UnregisterExtension
void	UpdateExtension

Figure 44 - Interface permettant la désindexation de vShield des plugins de vCenter

VI.4.0. Mise en place du monitoring avec nagios et centréon

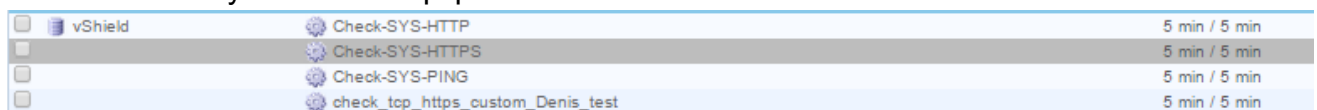
Le monitoring des équipements est assuré grâce au duo nagios/centréon à l'université. Nagios est un outil open source très répandu dans le monde professionnel qui utilise le protocole SNMP. Il peut se suffire à lui-même mais beaucoup d'organisations aiment lui ajouter une surcouche dont l'une des plus

connue est centréon. Centrion est en grande partie open source et quelques outils optionnels sont payants.

L'installation de nagios a été réalisée il y a quelques années à l'université et nous permet de monitorer notre infrastructure physique et virtuelle grâce notamment à certains plugins gratuits. On peut par exemple monitorer l'activité CPU d'une machine virtuelle ou d'un serveur ESXi ou encore monitorer l'activité d'une base de données oracle de manière assez fine.

Pour le projet vCloud, j'ai mis en place le monitoring pour les serveurs ESXi, les deux bases de données Oracle (celle de vCloud et de vCenter), les machines virtuelles red hat (pour le serveur vCloud et le serveur de base de données), mais aussi la machine Windows hébergeant vCenter et la machine virtuelle vShield. Nos modèles de vm sont configurés d'emblée pour prendre en compte le monitoring, toute la configuration se fait uniquement dans centrion pour ces machines.

En ce qui concerne le monitoring de l'appliance vShield (figure 45), j'ai dû me contenter d'un monitoring standard avec notamment un ping pour connaître la disponibilité du serveur au niveau réseau ainsi que le test des services http et https sur l'appliance. Concrètement si le service web tombe sans que la connectivité réseau soit en cause, nous sommes au courant via des alertes dans centrion et des mails sont envoyés à notre équipe.



<input type="checkbox"/>	vShield	Check-SYS-HTTP	5 min / 5 min
<input type="checkbox"/>		Check-SYS-HTTPS	5 min / 5 min
<input type="checkbox"/>		Check-SYS-PING	5 min / 5 min
<input type="checkbox"/>		check_top_https_custom_Denis_test	5 min / 5 min

Figure 45 - Contrôles de centrion concernant vShield

Le monitoring du serveur base de données intègre toutes les vérifications classiques pour un système red hat, à savoir : la connectivité réseau, la charge CPU, la charge mémoire, le remplissage des disques et l'activité réseau. En plus de cela, on supervise pour la base de données la connectivité jusqu'à la base de données, le remplissage des tablespaces ainsi que divers indicateurs sur l'activité de la base de données notamment au niveau de la gestion de la mémoire par oracle. Cette gestion de la mémoire est assez complexe, mais on peut par exemple savoir si une base de données est utilisée de manière performante ou si elle provoque des ralentissements. Dans le cas d'une base de données qui a tendance à ralentir, ces indicateurs nous aident à nous alerter, si par exemple une requête mal écrite amène trop d'informations en mémoire. Pour être très clair les indicateurs de centrion ne permettent pas de diagnostiquer la requête qui ralentit la base de données. En revanche, centrion nous alerte sur le fait qu'une base de données ralentit et qu'il faut donc l'analyser.

VI.5.0. Politique de backup des vms

Les backups sont effectués via avamar qui est un logiciel de sauvegarde édité par EMC. Nous utilisons la version 7.0 du logiciel. Avamar dispose de la particularité de s'intégrer avec vSphere. On peut ainsi sauvegarder des disques au sens vm du terme.

Par exemple, la machine virtuelle hébergeant vCloud est sauvegardée chaque nuit en « mode vm ». En cas de crash on peut restaurer l'ensemble de la vm.

Le serveur vCenter dédié à vCloud est lui aussi sauvegardé par avamar chaque jour en mode vm. L'appliance vShield n'est lui pas sauvegardé. Cependant, chaque nuit un export de la base de données de vShield est réalisé vers un autre serveur indépendant de vcloud. Cet export est effectué en SFTP (Secure File Transfer Protocol).

Le serveur de base de données Oracle est sauvegardé chaque semaine en mode vm. Ce serveur dispose également d'un agent avamar. Cet agent avamar sert à la sauvegarde chaque nuit des bases de données. Concrètement avamar lance rman (recovery manager) qui est un produit intégré à Oracle Database. L'interface avamar est visible sur la figure 46.

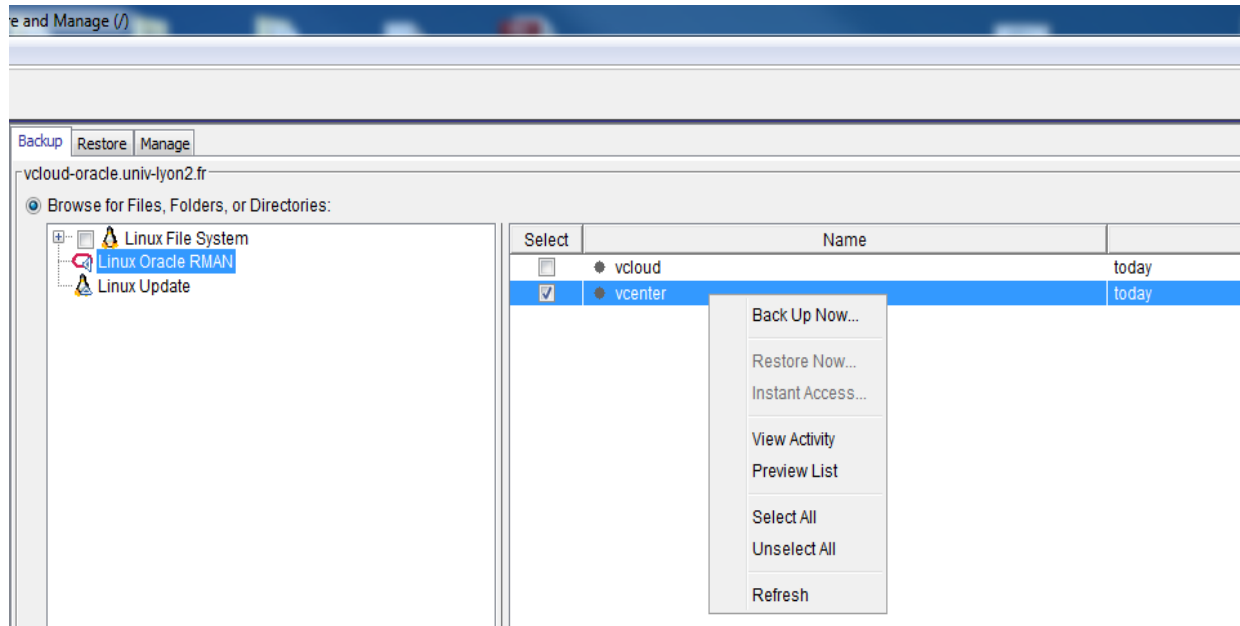


Figure 46 - Backup RMAN dans avamar des bases de données Oracle

Dans les faits, restaurer une sauvegarde de la vm suffit généralement à restaurer une machine virtuelle et sa base de données. C'est une technique non supportée par Oracle contrairement à Rman. Enfin il faut savoir que le support de Rman sur une base de données est conditionné au passage en « archive log » de la base de données.

VI.6.0. Modifications sur la base de données

VI.6.1. Passage en Archive Log des bases de données

La manipulation relative au passage des bases de données en archive log est placée en annexe dans la partie « Passage en Archive Log des bases de données ». Après cette manipulation, les archives sont générées au format « dbf » et visibles sur la figure 47.

```
sh-4.1# ls -lh /bases/archives/vcloud
total 160M
-rw-r----- 1 oracle dba 46M Nov 4 01:09 1_4183_828281005.dbf
-rw-r----- 1 oracle dba 39M Nov 4 01:48 1_4184_828281005.dbf
-rw-r----- 1 oracle dba 39M Nov 4 05:55 1_4185_828281005.dbf
-rw-r----- 1 oracle dba 39M Nov 4 10:00 1_4186_828281005.dbf
drwx----- 2 root root 16K Feb 21 2014 lost+found
sh-4.1# ls -lh /bases/archives/vcenter
total 160M
-rw-r----- 1 oracle dba 46M Nov 4 01:10 1_1557_846072894.dbf
-rw-r----- 1 oracle dba 38M Nov 4 01:14 1_1558_846072894.dbf
-rw-r----- 1 oracle dba 39M Nov 4 05:28 1_1559_846072894.dbf
-rw-r----- 1 oracle dba 38M Nov 4 09:39 1_1560_846072894.dbf
drwx----- 2 root root 16K May 13 11:06 lost+found
sh-4.1#
```

Figure 47 - Vision système des archives issues du passage en archive log

On obtient une base de données qui peut désormais être sauvegardée via rman. En cas de crash, le processus de restauration est de restaurer la machine virtuelle puis d'utiliser rman pour restaurer la sauvegarde journalière de rman. On peut ensuite utiliser rman pour rejouer les transactions qui ont été conservées dans les archives log. Chaque transaction est identifiée par un SCN (System Change Number) qui est unique et peut ainsi permettre de revenir à un état stable et cohérent d'avant crash tout en perdant un minimum d'informations. Rman permet de revenir à un SCN précis ou bien à une heure précise dans le temps. Toute transaction qui n'est pas valide, par exemple si elle s'est déroulée au moment du crash, n'est tout simplement pas rejouée par rman.

VI.6.2. Démarrage automatique des bases de données

Pour obtenir un serveur de bases de données qui démarre automatiquement les bases au démarrage du serveur (et qui arrête également les bases de données automatiquement), il faut appliquer quelques modifications. Pour cela oracle utilise le fichier /etc/oratab. On trouve dans ce fichier un récapitulatif des bases de données qu'on a créées sur le serveur. Il suffit de passer le paramètre de « no » à « yes » :

```
vcloud:/appli/oracle/product/11.2.0:N
```

Il faut ensuite faire des modifications au niveau du système et notamment créer le fichier /etc/init.d/dbora. Ce fichier (proposé en annexe dans ce dossier) est lancé au démarrage de la machine par le système. Il faut ensuite créer des liens symboliques entre ce script et les différents « runlevel » dans lesquels doivent être exécutés le script en question :

```
In -s /etc/init.d/dbora /etc/rc.d/rc0.d/K01dbora # Halting
In -s /etc/init.d/dbora /etc/rc.d/rc3.d/S99dbora
In -s /etc/init.d/dbora /etc/rc.d/rc5.d/S99dbora
In -s /etc/init.d/dbora /etc/rc.d/rc6.d/K01dbora # Rebooting
```

Le runlevel 0 (première ligne) correspond à un arrêt de la machine. Le runlevel 3 correspond au runlevel par défaut sans interface graphique contrairement au 5 (le runlevel 5 est cependant inutile sur un serveur de bases de données de ce type car on ne lui installe pas d'interface graphique). Enfin le dernier runlevel correspond à un redémarrage de la machine.

Cette procédure m'a été gracieusement fournie par une de mes collègues experte en bases de données Oracle. Je l'ai appliqué au serveur de bases de données sans encombre car tout était bien expliqué. Il faut savoir que l'arrêt d'un serveur de base de données est une opération qui peut s'avérer complexe (à cause des applications qui en dépendent notamment), c'est pourquoi ce type de modifications est très intéressant. Cette modification permet de réduire la complexité ainsi que le stress généré en cas de problème en allégeant l'administration.

La plate-forme de production est en place et nous pouvons décrire la configuration de cette infrastructure.

Chapitre 7

VII. Configuration de l'infrastructure de production

VII.1.0. Gestion des niveaux de service

VII.1.1. Gestion des niveaux de service pour le stockage

La gestion du niveau de service est un élément fondamental au niveau du concept de cloud. Dans le secteur public les choses sont différentes par rapport au secteur privé, mais l'idée de fond reste la même, à savoir proposer un service décliné en différents niveaux de qualités.

Ainsi pour le stockage, j'ai utilisé les deux baies SAN. L'ancienne baie HP, est très logiquement proposée dans le niveau de service le plus bas (Bronze) sur la figure 48. Le niveau de service intermédiaire se trouve également sur la baie HP, mais dispose de davantage de capacité de stockage. Enfin le niveau de service « Gold » est positionné sur la baie EMC.



Figure 48 - Stockage des données en fonction du niveau de service

VII.1.2. Gestion des niveaux de service pour la RAM et le CPU

Le niveau de service pour les problématiques de RAM et de CPU se configure au niveau du VDC d'organisation dans l'interface de vCloud (figure 49). Les paramètres suivants sont modifiables à tout moment et se configurent à la création des VDC d'organisation. Du côté de vSphere se sont des pools de ressources qui sont configurés en fonction des paramètres configurés dans vCloud. Concrètement cela influe sur l'expérience utilisateur car les contentions en matière de CPU et de RAM seront gérées via vSphere en fonction des paramètres qui sont dans les pools de ressource.

Configurer le modèle de pool d'allocation

Dans ce modèle, vous allouez des ressources au VDC d'organisation. Vous contrôlez également le pourcentage de ressources garanties pour le VDC d'organisation. Le facteur de ressources garanties est un moyen de surattribuer des ressources.

Allocation de processeur : GHz

Quantité maximale de processeurs disponible pour les machines virtuelles exécutées dans ce VDC d'organisation (prise du VDC fournisseur de soutien, vCloud VDC Provider Bronze).

Ressources de processeur garanties : % (5,57 GHz, 10 % de la capacité du vDC fournisseur disponible de 55,70 GHz)

Pourcentage des ressources garanti comme étant disponible pour les machines virtuelles exécutées à l'intérieur.

Allocation de mémoire : Go

Quantité maximale de mémoire disponible pour les machines virtuelles exécutées dans ce VDC d'organisation (prise du VDC fournisseur de soutien, vCloud VDC Provider Bronze).

Ressources de mémoire garanties : % (8,30 Go, 10 % de la capacité du vDC fournisseur disponible de 82,96 Go)

Pourcentage des ressources garanti comme étant disponible pour les machines virtuelles exécutées à l'intérieur.

Nombre maximum de machines virtuelles : 100 Illimité

Mesure de sécurité qui vous permet de contrôler le nombre maximum de machines virtuelles dans ce VDC d'organisation.

Ressources attribuées à partir du VDC fournisseur 'vCloud VDC Provider Bronze' à l'aide de ces paramètres d'allocation :

Indicateur	Total	Allocation	Réservation attribuée	Réservation utilisée
Processeur	55,70 GHz	11,14 GHz (20,00 %)	5,57 GHz (10,00 %)	0,00 GHz (0,00 %)
Mémoire	82,96 Go	16,59 Go (20,00 %)	8,30 Go (10,00 %)	0,00 Go (0,00 %)

Déplacez votre souris sur chaque en-tête de colonne pour voir plus d'informations.

Nombre typique de vApp ou de machines virtuelles susceptibles d'utiliser ces paramètres d'allocation :

- 11 'petites' VM : 1,0 GHz Processeur = 1 Processeurs virtuels * 1,0 GHz Évaluation du processeur virtuel, 512 Mo RAM
- 5 'moyennes' VM : 2,0 GHz Processeur = 2 Processeurs virtuels * 1,0 GHz Évaluation du processeur virtuel, 1,0 Go RAM
- 2 'grandes' VM : 4,0 GHz Processeur = 4 Processeurs virtuels * 1,0 GHz Évaluation du processeur virtuel, 2,0 Go RAM

Figure 49 - Association des ressources en fonction des niveaux de services dans l'interface de vCloud

Les « ressources garanties », sont des ressources qui seront tout le temps réservées pour le VDC d'organisation. Les « ressources allouées » sont-elles fluctuantes, si les ESXi ont la possibilité de donner toute la ressource allouée alors ils le font. En cas de contention, la ressource allouée réellement aux machines du VDC d'organisation peut baisser jusqu'au niveau des ressources garanties. Tout ceci permet de gérer les pics et de surallouer des ressources en donnant aux machines davantage de RAM ou de CPU que ce qu'on a réellement. On ne peut par contre pas

réserver davantage de ressource que ce qui existe réellement. Par ailleurs, il est possible également de limiter le nombre de machines générées.

VII.1.3. Gestion des niveaux de service pour le réseau

La gestion du niveau de service pour le réseau passe par le déploiement d'une edge gateway. Une fois déployé, on peut gérer des règles de pare-feu mais aussi par exemple limiter le débit utilisé au sein d'un vDC d'organisation (figure 50).

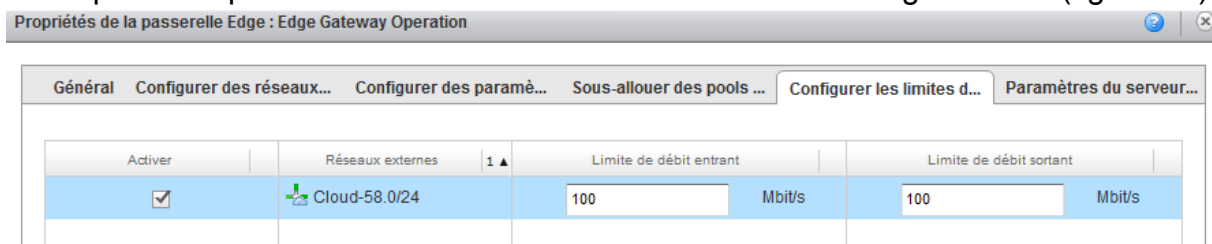


Figure 50 - Limitation de la bande passante en fonction du niveau de service

Ainsi on peut limiter ou privilégier certains vDC d'organisation par rapport à d'autres. Je n'ai pas utilisé cette option dans l'architecture de production car je n'ai pas forcé l'utilisation de passerelle Edge. C'est en revanche tout à fait possible d'ajouter cette option.

VII.2.0. Utilisation des clones liés

Pour le stockage des machines virtuelles issues de vCloud j'ai activé l'option pour l'utilisation des clones liés pour le niveau de service le plus bas. La technique des clones liés renvoie à la façon dont sont générées les VM du cloud. On peut de façon classique générer une machine virtuelle en copiant l'intégralité du disque de cette vm. On peut aussi grâce aux clones liés créer un nouveau disque delta dans lequel seront intégrés tous les changements opérés sur ce clone. Ces « changements sur le disque », ce sont concrètement les blocs du disque original qui ont été modifiés sur le disque delta du clone lié.

Cette technique, détaillée sur la figure 51, est issue de VMware View, un outil de VDI qui permet de générer des vm issues de clones liés pour des clients légers. Que ce soit dans View ou dans vCloud, cette technique a principalement deux avantages :

- générer des machines virtuelles plus rapidement que le clone classique (puisque l'on ne copie pas tout le disque d'origine)
- réduire la consommation d'espace sur le disque

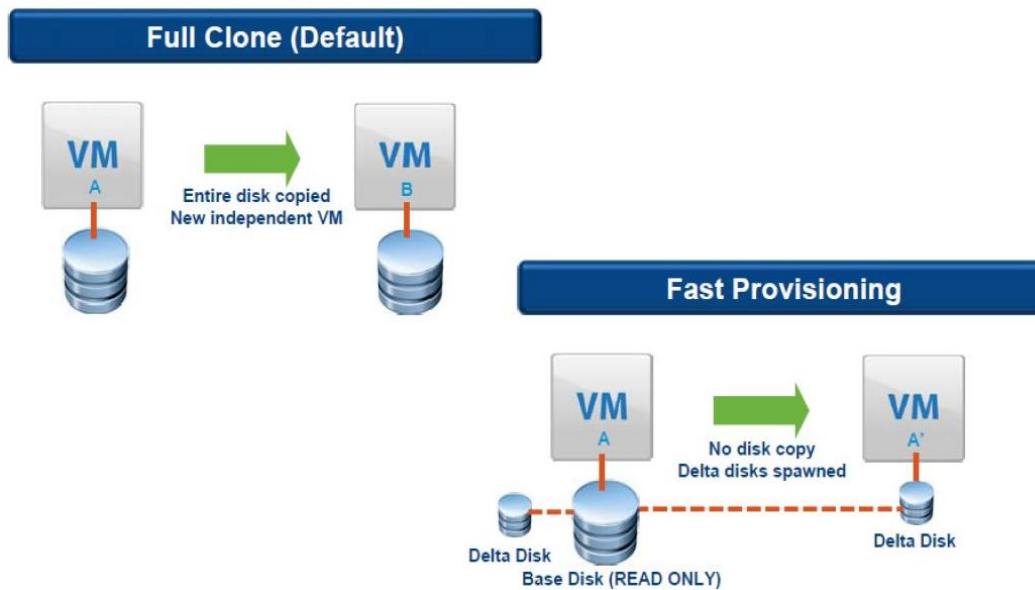


Figure 51 - Utilisation des clones liés, source [18]

VII.3.0. Customisation des vm

VII.3.1. Customisation des vm Windows

Les machines virtuelles que l'on déploie dans le cloud sont des machines préconfigurées. Pour cela il faut passer par une étape de personnalisation.

Pour les machines virtuelles de type Windows 2008 je pars de notre modèle de serveur type installé en Windows 2008 SP1 Entreprise. Je passe ensuite la carte réseau de la machine virtuelle en DHCP puis modifie le VLAN associé à cette carte de cette vm. Enfin je mets à jour le système via « windows update » puis je redémarre. Je passe également la licence de MAK vers KMS, concepts détaillés au point 5 de ce chapitre.

VII.3.2. Customisation des vm Linux

Le processus de personnalisation des machines virtuelles est relativement simple. Tout d'abord, je pars du template Linux que nous utilisons pour créer des server et je le clone. Je prends ce clone et passe la configuration en dhcp dans la vm et change son nom. Ensuite j'enregistre la vm chez Red Hat afin d'être en règle avec les licences de l'éditeur. Puis je modifie les droits dans la vm et j'ajoute les utilisateurs ciblés dans le groupe administrateur de la machine locale. Enfin je modifie éventuellement les disques attachés à la vm mais surtout le VLAN attachés à la carte réseau de la VM. Pour terminer, j'ajoute un serveur apache, par exemple si c'est une machine qui servira de serveur web ou encore mysql pour une base de données... Je termine en mettant à jour avec la commande yum update.

VII.4.0. Gestion des droits

La gestion des droits se joue à plusieurs niveaux. Les membres du pôle système, dont je fais partie, disposent de tous les droits partout. Les utilisateurs du pôle étude ont eux des droits limités à leur organisation. Si la publication de machines virtuelle dans le catalogue est permise pour le pôle système, elle ne l'est pas pour le pôle étude.

La politique de droits dans vcloud repose sur les comptes et groupes issus de l'active directory ou d'openldap. Pour cela on synchronise le ou les serveurs LDAP avec vCloud qui importe les comptes et les groupes. Une fois synchronisé, on retrouve ces comptes dans vCloud et on leur attribue un rôle (tout comme dans vSphere). Le rôle est un objet vCloud définissant tous les droits qu'un utilisateur a dans une organisation. On peut très bien avoir le rôle « administrateur de l'organisation » et être un simple « utilisateur de vApp » dans une autre. Il existe des rôles prédéfinis dans vCloud que l'on peut modifier à souhait ou bien en créer de nouveau. Pour ma part j'ai modifié le rôle « utilisateur de vApp », car il était assez proche des droits que je souhaitais attribuer aux utilisateurs du pôle étude.

On peut aller encore plus loin en enlevant aux utilisateurs la possibilité de faire des snapshots ou de supprimer certains objets... J'ai ajusté ces droits afin de faciliter l'utilisation en donnant beaucoup de droits dans l'environnement réservé aux utilisateurs du pôle étude. Un utilisateur standard de vApp disposera des droits visibles sur la figure 52.

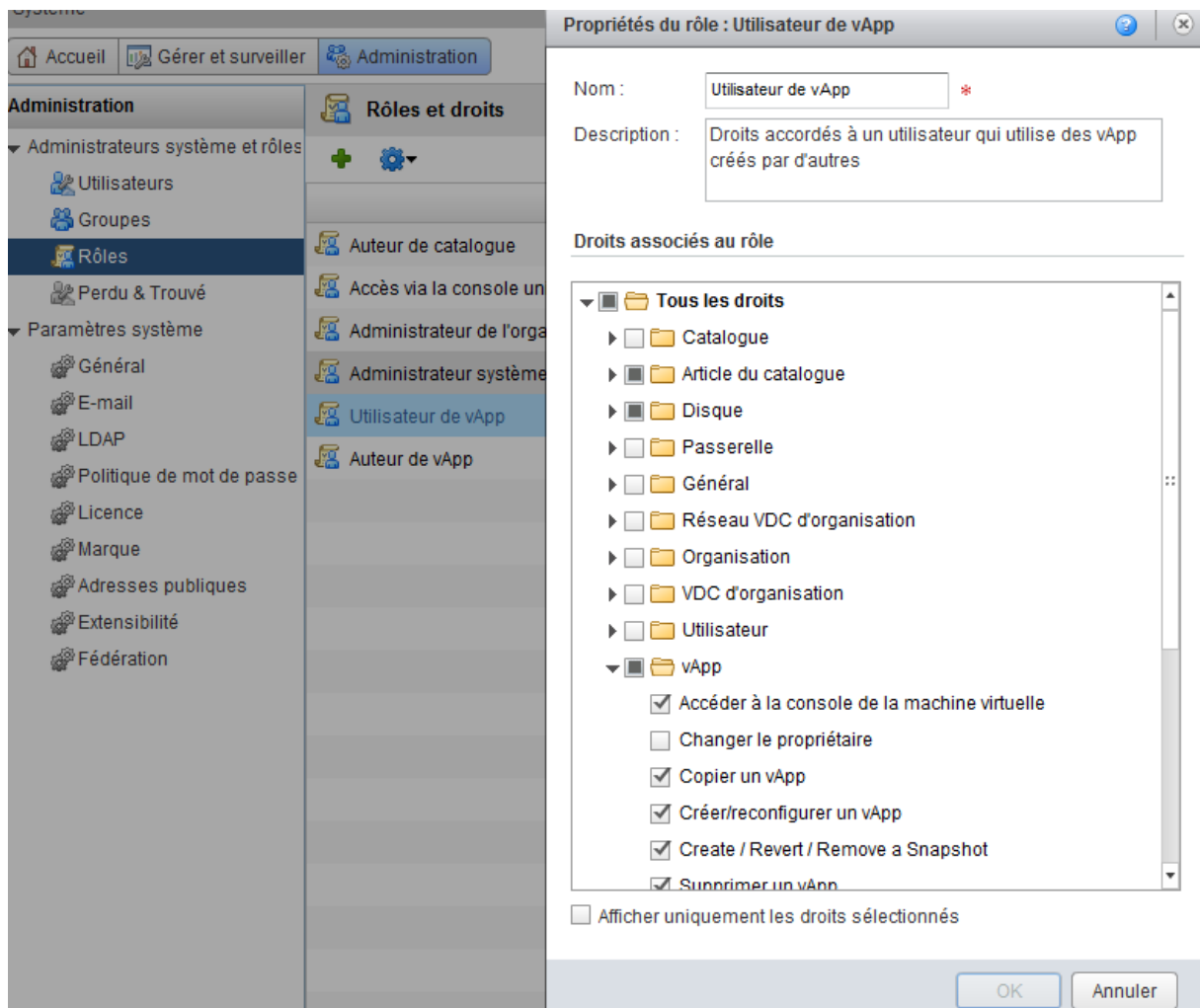


Figure 52 - Utilisation des rôles et des droits

VII.5.0. Gestion des licences (vSphere, vCloud et système d'exploitation)

Les licences dans vCloud reposent sur le nombre de sockets physiques de CPU utilisés par les ESXi dédié au cloud. Plus on en utilise, plus cela coûte cher. Il vaut donc mieux privilégier des serveurs avec des CPU rapides et beaucoup de RAM.

Nous sommes passés d'une licence 6 sockets CPU à une licence 4 sockets CPU suite au recyclage de serveurs ESXi plus puissants. C'est un point que j'aborde dans ce chapitre.

L'autre gestion des licences concerne celle des machines virtuelles du cloud. Pour les vm red hat, celle-ci sont pré-enregistrées au moment de leur incorporation dans le catalogue de vm disponibles.

L'enregistrement des machines virtuelles est plus complexe. Il existe deux types de licences Microsoft que nous utilisons : MAK et KMS. MAK correspond à un enregistrement classique chez Microsoft. KMS est un enregistrement local à l'université sur un serveur KMS interne. Si les serveurs de l'infrastructure (le serveur windows vCenter de l'infrastructure de cloud par exemple) utilisent l'enregistrement MAK, il est plus pertinent d'utiliser KMS pour les machines issues du cloud car leur nombre varie plus souvent. Par ailleurs, cela nous sécurise car on compartimente les licences entre l'infrastructure serveur et le cloud ce qui est une bonne chose.

VII.6.0. Phase de recette

La phase de recette a été plutôt rapide car j'ai trouvé un utilisateur motivé au pôle étude pour m'accompagner dans la démarche. Je lui ai simplement donné accès à la plate-forme et noté toutes ses remarques afin d'y répondre rapidement. Je lui ai également fait tester différents points parmi lesquels la connexion à la console web de vCloud, l'accès au catalogue de l'organisation, le déploiement de vApp et leur utilisation.

Le cloud comportant deux organisations, j'ai aussi demandé à un collègue du pôle système de tester les points mentionnés plus haut. De plus j'ai aussi demandé à cet utilisateur de tester la console d'administration où il a autant de droits que moi.

Au final tous ces tests ont été réalisés assez rapidement car les obstacles étaient minimes. J'ai surtout ajusté les droits au niveau des utilisateurs du pôle étude afin de leur donner davantage de libertés et d'autonomie.

VII.7.0. Documentation, partage des connaissances et présentations du produit

J'ai créé pour l'université deux documentations qui présentent la mise en place de l'infrastructure. Ces documentations ont été partagées pour les collègues du pôle système. J'ai également participé à un comité de pilotage afin de présenter l'avancement du projet à la DSI.

Par ailleurs nous avons pour tradition au pôle système de faire des présentations sur des sujets techniques précis afin de partager des connaissances pointues liés au projet sur lesquels nous travaillons. J'ai donc présenté vCloud et l'infrastructure mise en place dans ce cadre.

VII.8.0. Migration vers la version vSphere 5.5 de l'infra serveur et impact sur vCloud

La migration de l'infrastructure serveur a eu un impact sur le projet vCloud. En effet les serveurs nécessaires au bon fonctionnement du cloud sont des machines virtuelles : le serveur vCloud, le serveur vCenter lié à celui-ci, vShield et enfin le serveur accueillant les bases de données. Ces machines virtuelles fonctionnent sur l'infrastructure serveur de l'université. En tant que telle, la montée de version a donc eu un impact sur ces machines virtuelles.

Lorsque le prestataire est venu s'occuper de la montée de version de vSphere 5.0 vers la version 5.5 (changement très structurant pour l'université), je lui ai proposé de ne pas migrer les serveurs virtuels d'infrastructure du cloud afin de l'opérer moi-même un peu plus tard. J'ai préféré procéder ainsi parce qu'à l'époque je n'avais pas vraiment le temps de le faire et de traiter les éventuels effets de bord que son action pouvait provoquer.

Architecture vCloud de Production/migration vSphere 5.5

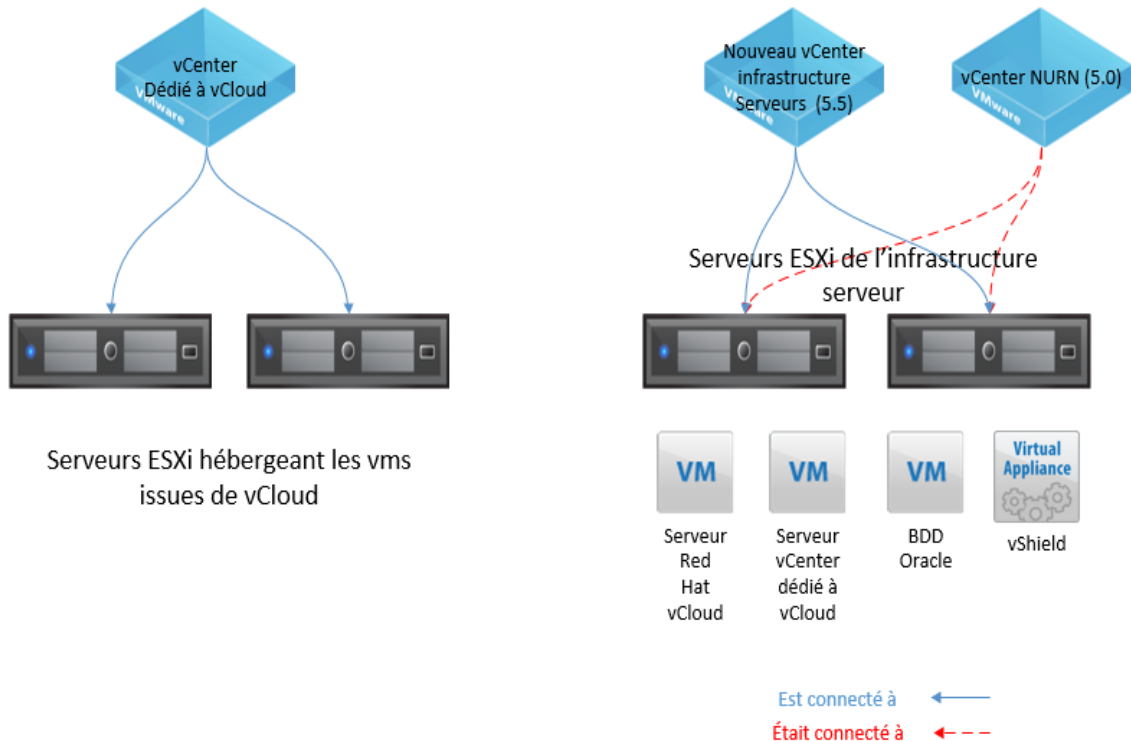


Figure 53 - Architecture vCloud de production, changement de serveur vCenter

Il m'a donc fallu migrer moi-même ces serveurs. J'ai prévu un arrêt de vCloud en alertant les utilisateurs de l'indisponibilité du service. J'ai migré les machines vers

un serveur ESXi encore rattaché à notre serveur vCenter 5.0 de l'infrastructure serveur. J'ai ensuite supprimé le serveur ESXi de ce même serveur vCenter. A ce moment-là les machines fonctionnaient toujours sur l'ESXi, qui était tout de même isolé. Puis j'ai rattaché cet ESXi sur notre nouveau serveur vCenter tout fraîchement installé en version 5.5. Puis j'ai arrêté les machines virtuelles et je les ai migrées à froid (éteintes) vers nos nouveaux serveurs ESXi plus puissants. Enfin j'ai redémarré les machines virtuelles et vérifié que tout était bon d'un point de vue applicatif sur vCloud. La figure 53 reflète cette manipulation.

VII.9.0. Mise en place d'une vApp pour les serveurs qui gèrent vCloud

VSphere permet de séquencer le démarrage des machines virtuelles via l'utilisation de vApp. J'ai utilisé cette option une fois sur le transfert des machines de l'infrastructure de vCloud migrées vers notre nouveau serveur vCenter 5.5. Cette opération permet de démarrer ou d'éteindre les machines dans le bon ordre tout en espaçant dans le temps le démarrage ou l'arrêt des machines virtuelles.

La machine virtuelle hébergeant les bases de données oracle démarre en premier car c'est un prérequis indispensable au bon fonctionnement de vCloud et du vCenter de vCloud. Puis le serveur vCenter dédié à vCloud démarre ensuite, suivi de vShield qui est lui-même rattaché à vCenter. Enfin le serveur dédié à vCloud démarre en dernier. Pour l'arrêt de la vApp de l'infrastructure vCloud le séquençage est exactement l'inverse, ce qui est parfaitement logique.

Au final, mes collègues qui n'ont pas autant de connaissances sur l'infrastructure vCloud que moi peuvent arrêter ou démarrer la vApp vCloud en trois clics de souris directement dans vSphere. Cette opération est très simple à réaliser et sécurisante pour l'utilisateur. Par ailleurs tout est prévu dans les machines virtuelles au niveau du système afin que tout ce qui est nécessaire au démarrage de l'application vCloud et à son fonctionnement démarre correctement. Par exemple les bases de données oracle sont configurées pour démarrer automatiquement, tout comme le service qui lance l'application vCloud.

VII.10.0. Changement de serveurs ESXi

Les serveurs ESXi sur lesquels tournent les machines virtuelles issues de vCloud portent les licences vCloud. Les licences vCloud sont calculées par socket de CPU. Nos serveurs blade utilisent deux sockets CPU physiques par serveur. Nous avons une licence six CPU et nous sommes passés à quatre, soit deux serveurs blade. Ainsi on économise un petit peu au niveau des licences. C'est un choix que j'ai porté, arguant du fait qu'on pouvait changer nos serveurs physiques par des serveurs plus puissant. Le changement d'ESXi est résumé sur la figure 54.

Architecture vCloud de Production/Changement

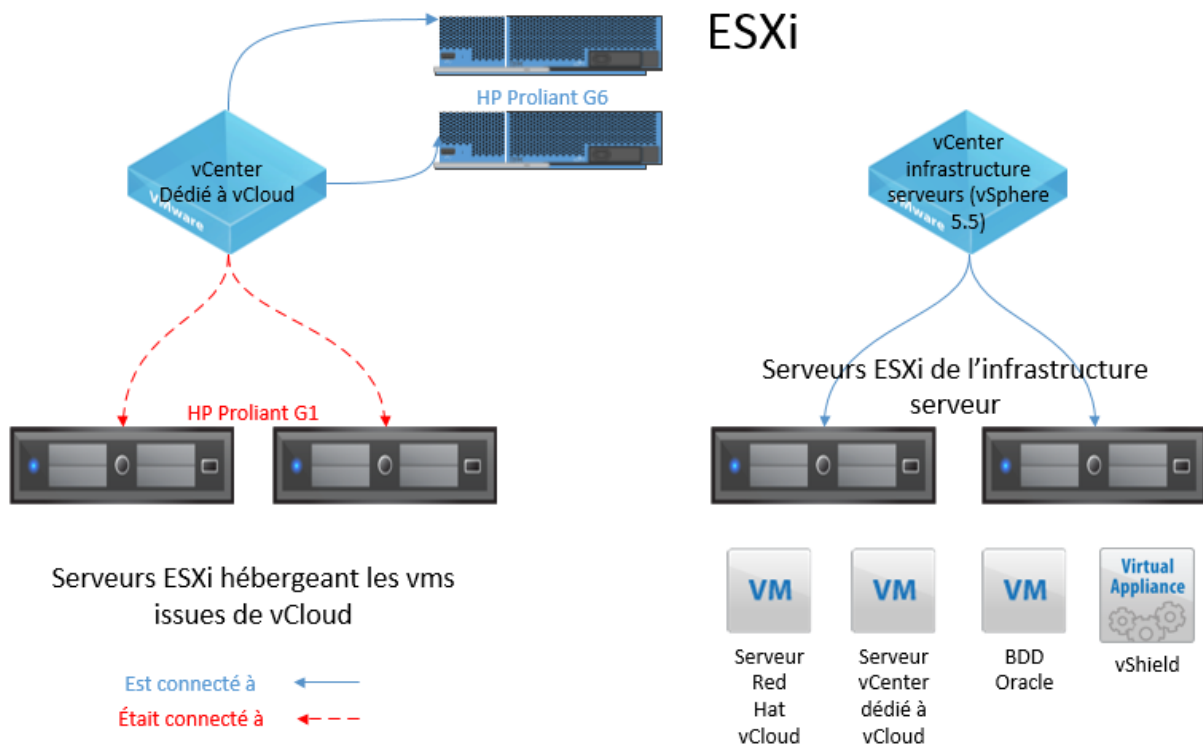


Figure 54 - Architecture vCloud de production, changement de serveurs ESXi

Le cloud de production était constitué de trois serveurs ESXi de modèle HP proliant G1 équipé de 32 GO de RAM. Nous sommes passés sur des Proliant G6, plus récents avec 64 GO de RAM. Ce changement de serveurs ESXi a été techniquement réalisé sans interrompre le service et ce grâce à la technologie EVC (Enhanced vMotion Compatibility) que nous allons découvrir.

VII.11.0. Utilisation de EVC

Historiquement, une des problématiques liée à l'utilisation des produits VMware est de changer de versions de produits assez régulièrement. Par exemple une sous-version majeure de vSphere sort chaque année environ, sans compter les « update » mineures entre ces sous-versions.

Il est indispensable que les montées de versions soient le plus transparentes possibles pour les machines virtuelles qui sont hébergées et qui représentent le cœur de l'activité. EVC répond à cette problématique. Ainsi il est possible de migrer des machines virtuelles en cours de fonctionnement entre deux serveurs physiques ESXi qui utilisent un matériel différent et de générations différentes. Pour réaliser

cela, on crée dans le cluster ESXi (au sens VMware) une modification qui permet d'aplanir les différences dans l'utilisation des jeux d'instructions des processeurs des serveurs ESXi pour permettre une migration à chaud. En clair, un serveur de dernière génération n'utilisera pas tous ses jeux d'instruction CPU mais la partie connue de ceux-ci par l'autre serveur ESXi de génération plus ancienne.

La principale limite à EVC réside dans l'incompatibilité entre serveurs utilisant des processeurs Intel et AMD. Une migration à chaud fonctionnera uniquement entre serveurs à base de processeurs Intel ou AMD, mais pas entre les deux. Dans notre cas, le problème ne se pose pas car nos serveurs sont tous équipés de processeurs Intel.

En résumé, pour changer les serveurs, j'ai donc récupéré les serveurs Proliant G6, formaté ceux-ci avec une version d'ESXi légèrement supérieure à la version utilisée sur les serveurs ESXi de production (à cause de patches nouvellement sortis). Puis j'ai ajouté ces nouveaux serveurs ESXi au serveur vCenter dédié au cloud. J'ai entré les serveurs ESXi dans mon cluster vSphere, puis configuré EVC dans ce cluster pour permettre la migration à chaud des machines virtuelles de mes anciens serveurs ESXi vers le nouveau. Dans vCloud j'ai ajouté un à un mes nouveaux serveurs ESXi et installé l'agent vCloud nécessaire à la bonne communication entre les ESXi et vCloud. Une fois bien configurés dans vCloud et dans vSphere, les ESXi étaient prêts pour recevoir les machines virtuelles du cloud, que j'ai donc migrées à chaud (grâce à EVC). Enfin, j'ai enlevé le lien entre vCenter et mes anciens ESXi, puis les licences utilisées par ces ESXi, puis j'ai éteint ces serveurs physiques pour ne pas consommer inutilement de l'électricité.

VII.12.0. Backup des vm du cloud

Le backup via avamar des machines virtuelles du cloud est possible en « mode vm » si elles ne sont pas générées via la technique des clones liés. Le backup n'était pas une priorité au début du projet. C'est peu à peu devenu quelque chose d'indispensable pour les utilisateurs. J'ai donc créé un VDC d'organisation qui n'utilise pas les clones liés et qui permet donc leur inscription dans la politique de backup avamar.

VII.13.0. Packaging ThinApp

Un des problèmes majeurs de vCloud director réside dans l'utilisation du plugin VMRC. VMRC est un plugin qui s'intègre dans les navigateurs internet explorer et firefox (sous windows et macintosh pour ce dernier). Ce plugin est malheureusement incompatible avec les dernières versions de firefox (versions 30 et plus). Ce plugin sert notamment pour afficher l'interface graphique. Pour ce qui est

des serveurs linux sans interface la plus-value de ce plugin est négligeable. En revanche, pour les serveurs linux avec une interface graphique ou les serveurs windows, VMRC est un outil intéressant.

ThinApp est une réponse aux problèmes de compatibilité entre certaines versions de firefox et le plugin VMRC. En effet, ThinApp permet de créer une bulle qui sépare l'application du système d'exploitation depuis lequel est lancé le logiciel. Je me suis tout naturellement tourné vers ce produit car l'université dispose de licences de ThinApp. Je me suis cependant heurté à des difficultés au niveau du packaging. L'idée était regrouper dans un seul package tous les outils nécessaire à l'utilisation de la console web de vCloud c'est-à-dire : Firefox, Flash Player, Java et VMRC.

Le processus de packaging est le suivant, on prend un système d'exploitation vierge (avec internet explorer désinstallé) en 64 bit. On installe ThinApp sur cette machine, puis on lance une capture. La capture scanne le système d'exploitation. Puis on rentre dans la phase d'installation des logiciels : d'abord firefox, puis flashplayer suivi de java et enfin vmrc. Suite à cela, ThinApp lance un nouveau scan et trouve le différentiel qu'il existe entre le premier et le second scan. Enfin on compile l'application et cela nous donne en définitive un package ThinApp contenant l'ensemble des logiciels installés.

Toutes ces phases ne posent pas de problème. En revanche, le lancement de l'application se termine par une erreur qui bloque l'exécution du navigateur packagé. J'ai soumis ce problème à mes collègues du pôle support qui sont davantage habitués à l'utilisation de ThinApp. Cependant ils ont buté sur le même problème que moi. J'ai donc enchainé en créant un ticket chez VMware sur ce sujet. Au final VMRC n'a pas pu être intégré au package ThinApp. Selon VMware, ThinApp est capable de capturer uniquement les modifications en « user mode » mais pas celles du « kernel mode ». VMRC fait des modifications dans le kernel et cela le rend impossible à packager via ThinApp.

VII.14.0. Upgrade du serveur vCenter en 5.1

J'ai créé un ticket chez VMware suite à un problème pour attribuer les licences sur les serveurs ESXi servant à faire tourner les vm du cloud. Le support m'a indiqué que dans une documentation officielle (dont le sujet principal est la gestion des licences) il apparaît que les licences de vCloud 5.1.2 sont incompatibles avec vCenter 5.0. J'ai évité involontairement pendant longtemps ce problème en laissant attribué des licences de notre infrastructure serveur aux serveurs ESXi. Cependant lors d'un tour d'horizon de nos licences, je me suis aperçu de cette méprise. En

enlevant les licences des serveurs ESXi, j'ai déclenché une période de 60 jours en mode d'évaluation. Je n'ai donc pas eu d'autre choix que de procéder à une montée de version de vCenter de la version 5.0 vers la version 5.1.

La version 5.1 de vCenter introduit une modification majeure qui s'appelle SSO (single sign on). Jusqu'ici, l'authentification sur vSphere était faite uniquement via Active Directory. SSO permet de centraliser l'authentification de différentes sources et d'utiliser OpenLDAP en plus d'active directory. Ce changement est perceptible sur la figure 55.

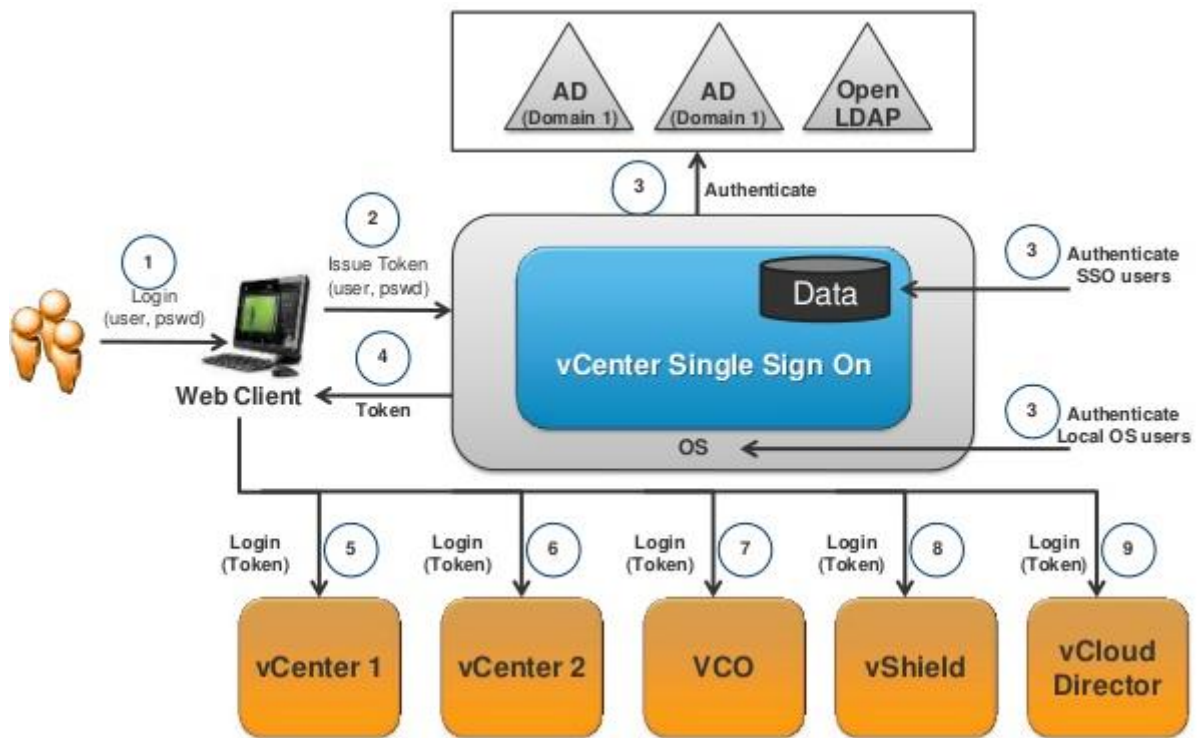


Figure 55 - Utilisation de SSO dans les produits VMware, source [21]

SSO utilise un jeton afin qu'un utilisateur authentifié par exemple sur la vCloud n'ait pas à se réauthentifier sur vSphere. On retrouve la liste des produits VMware intégrés à SSO ainsi que la feuille de route des développements autour de SSO sur la figure 56.

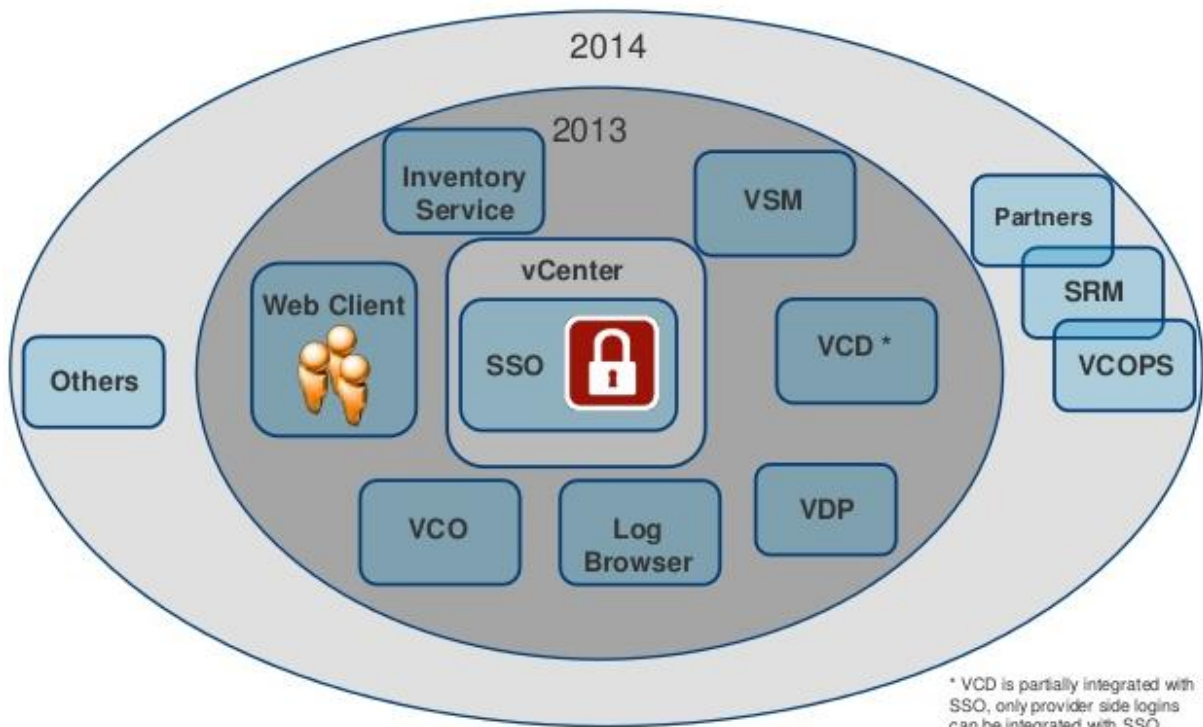


Figure 56 - Evolutions de SSO (roadmap), source [21]

SSO nécessite la création d'une base de données supplémentaire dédiée à l'authentification. C'est le principal problème de cette version de vSphere. J'ai donc créé une nouvelle base de données sur le serveur de base de données dédié à vCloud. Pour information la version 5.5 de vSphere (qui est sortie fin 2013) n'a plus ce problème car SSO ne nécessite plus de base de données.

Le processus de montée de version intègre plusieurs étapes résumées sur la figure 57 :

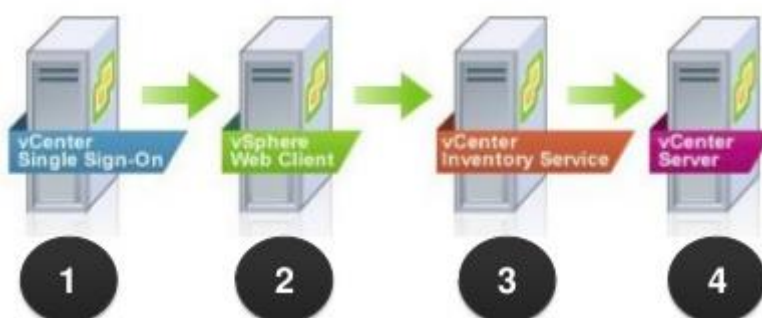


Figure 57 - Processus d'upgrade vCenter 5.0 vers vCenter 5.1, source [22]

On commence par installer le module SSO. Puis on upgrade le client web. Le client web est une alternative au client lourd Windows (historiquement utilisé). Le client web est désormais privilégié par VMware et les nouvelles fonctionnalités sont intégrées exclusivement sur le client web (depuis la version 5.5 avec vSan par exemple). On upgrade ensuite le service d'inventaire. Le service d'inventaire gère le cache du serveur vCenter en termes de gestion des objets vSphere (VM, ESXi...). Ce service permet de réduire la charge du service « VPXD » qui est lui le service

central permettant de lancer vCenter. Enfin on met à jour vCenter et par conséquent sa base de données également.



Figure 58 - Evolutions de la base de données de vCenter 5.1 par rapport à vCenter 5.0, source [22]

Les améliorations sur la base de données sont nombreuses (figure 58) et le résultat est de réduire le nombre d'entrées/sorties, ce qui est un paramètre critique pour une base de données. Ces améliorations sont intéressantes dans la mesure où nous avons par le passé identifié des problèmes dans la gestion de la base de données Oracle par vCenter en version 5.0.

VII.15.0. Les difficultés rencontrées lors du projet

VII.15.1.Oracle

Oracle est un produit assez austère et complexe et il m'a posé des difficultés. Le projet vCloud m'a permis de mettre à l'épreuve les connaissances que j'ai acquise sur Oracle Database depuis que je suis à l'université. J'ai notamment eu des difficultés sur la base de données du SSO, car j'ai eu à la créer dans l'urgence. La montée de version en vSphere 5.1 a notamment été compliquée à cause de la rapidité avec laquelle j'ai dû opérer les changements.

VII.15.2. Problème de gestion des objets vCloud

Mon premier ticket au support VMware a été ouvert pour des objets supprimés via vSphere. C'est une opération hautement déconseillée et c'est ce qui m'a valu d'appeler le support à l'aide. Tout objet ayant une existence dans vCloud doit être supprimé dans vCloud et non dans vSphere car sinon il reste des traces dans la base de données de vCloud qui ne sont pas nettoyées.

Le support de vCloud se fait en anglais uniquement et j'ai créé un ticket pour nettoyer les traces dans vCloud. L'ingénieur a pris la main grâce à webex (outil de prise en main de Cisco), s'est connecté à la base de données de vCloud et a supprimé les restes de l'objet qui n'existaient plus dans vSphere. Ce ticket m'a servi de leçon pour ce qui est du nettoyage de vCloud. J'ai aussi compris le mode de fonctionnement du support car je n'avais jamais fait appel à ce dernier. J'ai beaucoup apprécié leur efficacité.

VII.15.3. Problème des licences

Le problème des licences a empoisonné mon travail durant plusieurs semaines. Comme précisé auparavant ce problème m'a obligé à créer une base de données en plus de l'existant et de monter la version du vCenter de la version 5.0 vers la 5.1. Une fois ceci réalisé le problème d'attribution des licences était toujours présent alors qu'à priori rien ne devait empêcher ces licences de fonctionner.

Le support VMware a donc réexaminé mon ticket initial (pour lequel on m'avait préconisé d'upgrader vCenter). Ils ont pris la main sur mon client vSphere afin de rentrer la licence mais ils ont bien reconnu que cela ne fonctionnait pas. Le ticket a ensuite changé d'équipe chez VMware afin de passer dans l'équipe chargée des licences. Après examen et une nouvelle prise en main ils m'ont demandé de patienter afin de statuer dès le retour d'un de leur collègue.

Pendant ce temps les licences des ESXi du cloud étaient toujours en licence d'évaluation (60 jours par défaut). Puis après une bonne semaine le support m'a rappelé et a procédé à un « downgrade » de licence, me donnant suite à cette opération deux numéros de licence distincts contre un auparavant. Une de ces licences est attribuée à vCloud et l'autre aux serveurs ESXi. C'est ainsi que s'est terminé ce problème.

La configuration de vCloud est terminée à ce stade, nous pouvons maintenant étudier les évolutions futures du cloud de l'université et les différentes possibilités.

Chapitre 8

VIII. Les évolutions futures

VIII.1.0. Problématique liée au support

Au travers d'une KB [5] VMware annonce la fin du support de vCloud Director. L'éditeur n'aura assuré au total qu'un support de seulement deux ans, ce qui est très peu (figure 59).

Product Release	General Availability	End of General Support	End of Technical Guidance	Lifecycle Policy	End of Availability
VMware vCloud Director 1.5	2011/08/31	2013/09/10	N/A	EAP	
VMware vCloud Director 5.1	2012/09/10	2014/09/10	N/A	EAP	2013/09/19 as standalone product

Figure 59 - Fin du support de vCloud Director annoncé par l'éditeur, source [2]

Ce choix peut s'expliquer dans la volonté de VMware d'imposer un nouveau produit, vCAC, nouvellement rebaptisé vRealize (figure 60).

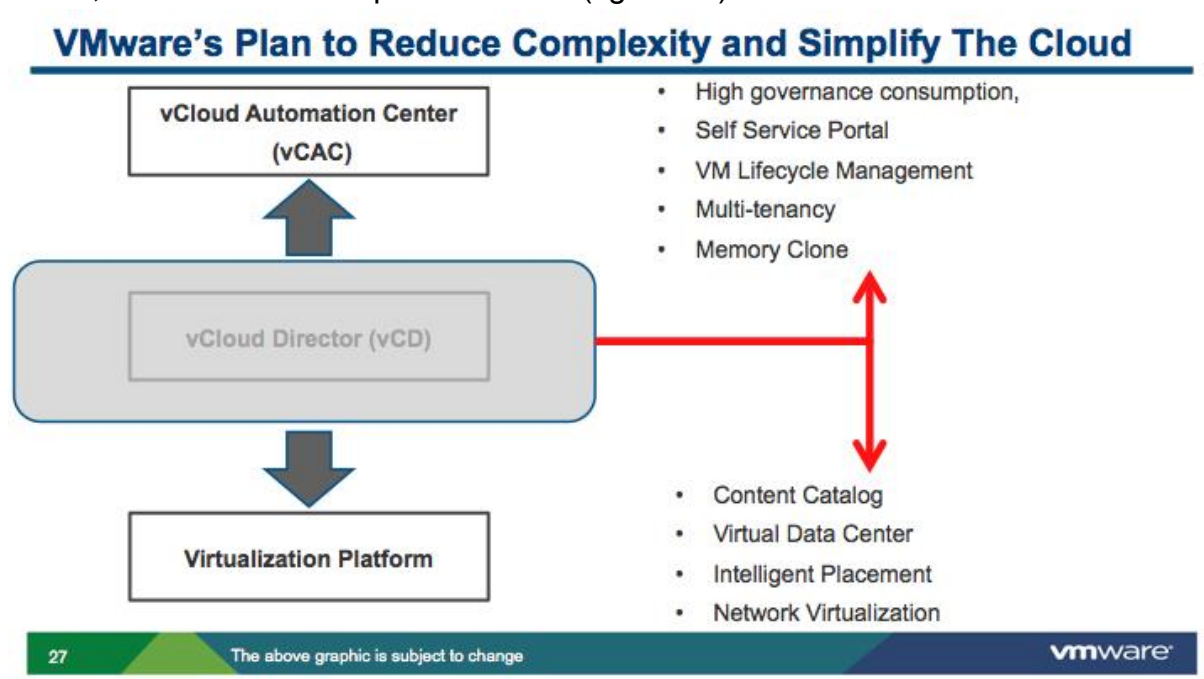


Figure 60 - Transition vCloud vers vCaC (vRealize), source [https://www.youtube.com/watch?v=giJOtba9IEA]

Passer de vCloud à vCAC ou vRealize est un changement majeur dans la stratégie Cloud de VMware. L'idée est de changer radicalement de produit pour le rendre plus attrayant plus efficace et mieux intégrable avec les outils comme SRM par exemple. La grande révolution de vCAC concerne le soutien des hyperviseurs

Xen, Hyper-v ou KVM en plus d'ESXi, on le remarque figure 61.

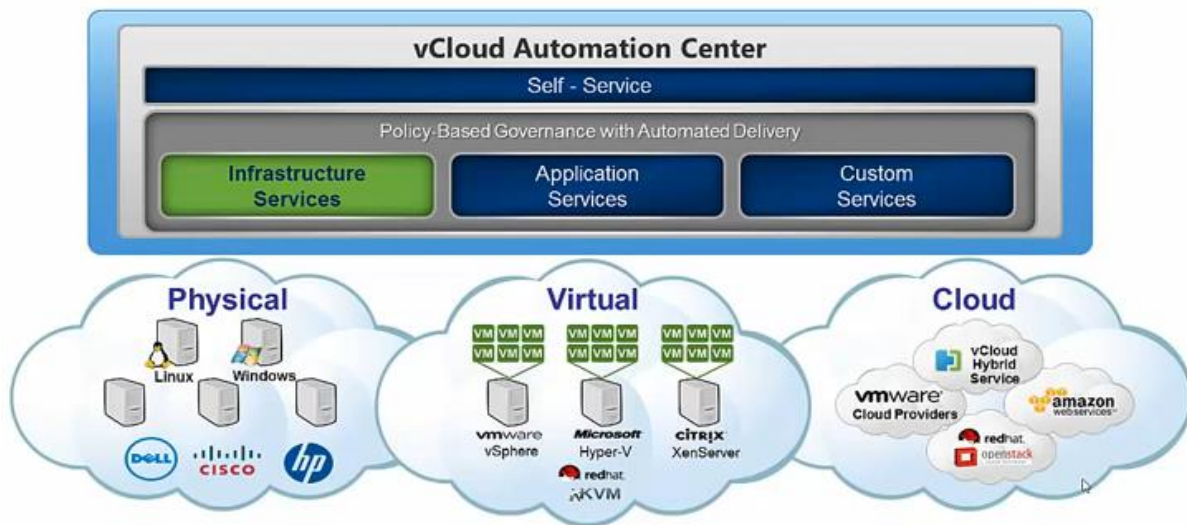


Figure 61 - VMware vCAC 6.x: Introduction, source [https://www.youtube.com/watch?v=giJOtba9IEA]

Enfin l'installation de vCAC est assez différente par rapport à vCloud. Il s'agit de déployer 3 machines dont un appliance qui joue le rôle de SSO, un autre appliance qui gère le portail web pour les utilisateurs (vCloud Automation Center Appliance) et un serveur windows (figure 62).

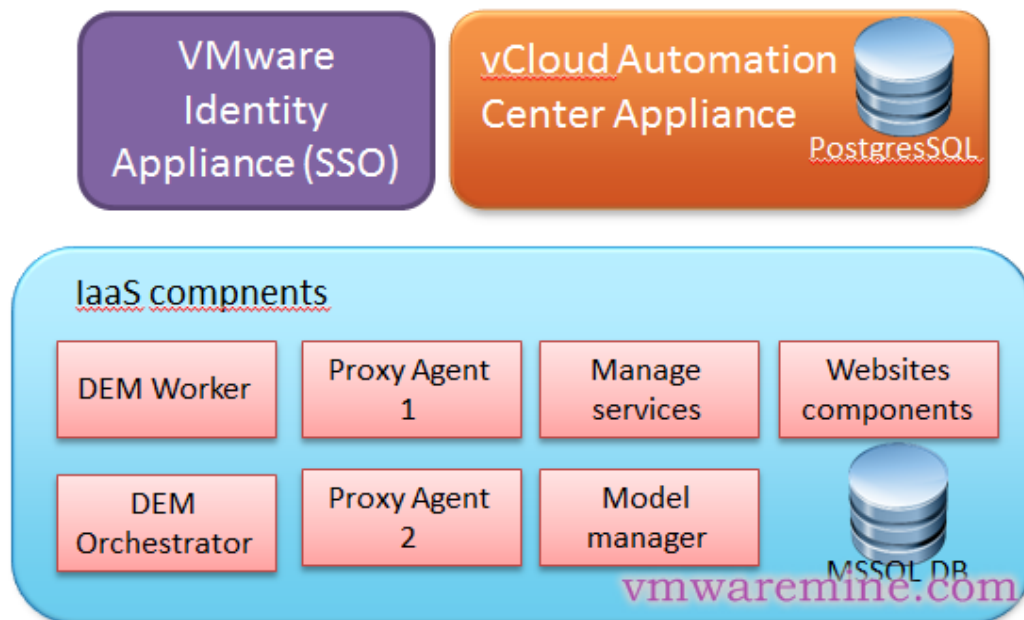


Figure 62 - Composants de vCAC 6.0, source [8]

Ce serveur windows héberge notamment la console d'administration (web), des agents proxy pour communiquer avec les ressources de l'infrastructure et le manager service qui communique la base de données, le serveur LDAP et le SMTP (messagerie).

VIII.2.0. Les alternatives à vCloud

VIII.2.1. OpenStack

OpenStack est le projet open source le plus connu dans le monde informatique. Lancé par un partenariat entre Rackspace et la NASA OpenStack a rapidement été intégré et soutenu par Debian, Ubuntu, SuSe et Red Hat. OpenStack est compatible avec les principaux hyperviseurs du marché (KVM, XEN, Hyper-V, QEMU et ESXi) et utilisent certaines de leurs caractéristiques. De très grandes entreprises soutiennent le projet parmi lesquelles on retrouve HP, IBM, Red Hat, AT&T, Rackspace, Yahoo, Intel, Cisco ou encore Dell.

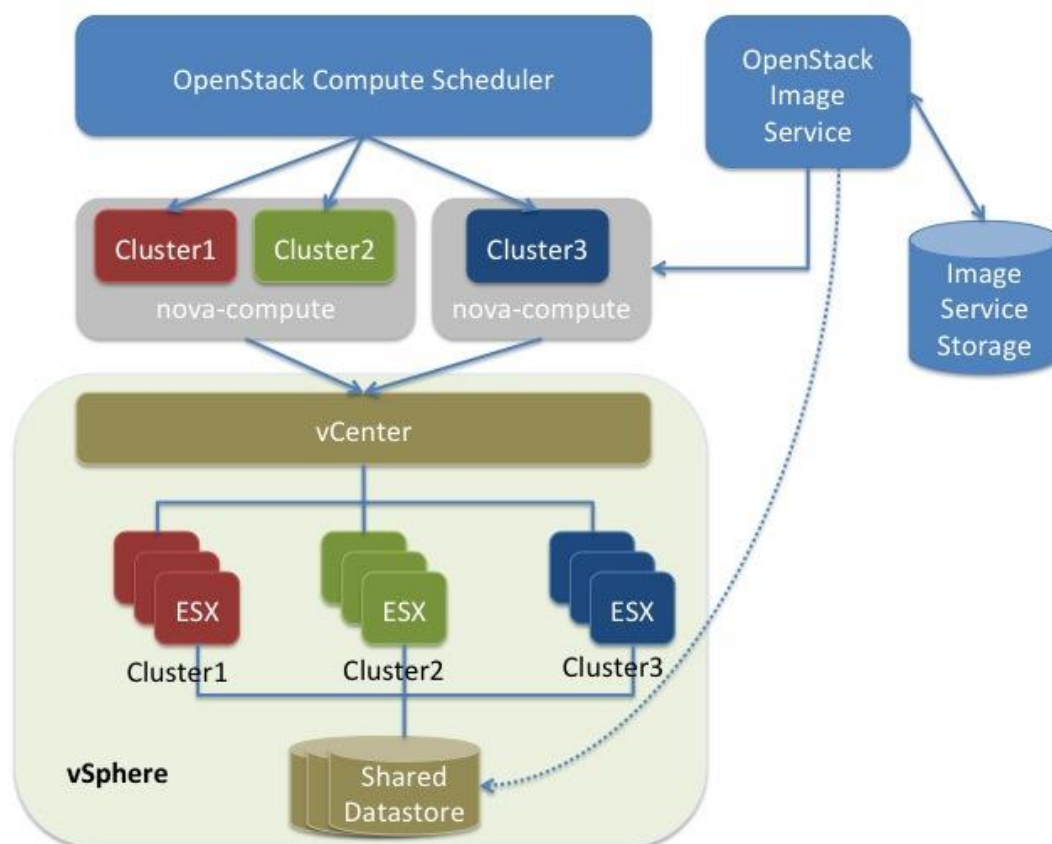


Figure 63 - Intégration d'OpenStack au-dessus de vSphere, source [19]

Intégrer OpenStack à l'infrastructure de l'université Lyon 2 est envisageable techniquement. Cependant, le gain en termes de licences serait assez faible si on part du principe de garder les ESXi et vCenter. Dans tous les cas OpenStack reste un projet à surveiller, ne serait-ce que pour son ambition ainsi que pour les noms prestigieux des entreprises associées au projet qui ne manqueront pas de le faire évoluer.

VIII.2.2. CloudStack

CloudStack est un projet en bonne partie soutenu par Citrix, l'autre leader historique de la virtualisation avec VMware. C'est un projet sous licence Apache parmi les plus actifs de la fondation du même nom un peu moins connu ou médiatique qu'OpenStack mais très intéressant. Historiquement c'est un projet lancé par cloud.com qui a été racheté ensuite par Citrix. Cloud Stack est compatible avec les hyperviseurs les plus importants du marché Hyper-v, ESXi, Xen, Oracle VM et KVM.

Huawei, Orange, Dell, Tata ou encore Walt Disney sont parmi les utilisateurs. CloudStack tire parti des outils hérités de la virtualisation tels que vMotion chez VMware ou vStorage chez Microsoft. De la même manière qu'avec OpenStack, l'intégration de CloudStack avec vSphere se fait au-dessus de vCenter :

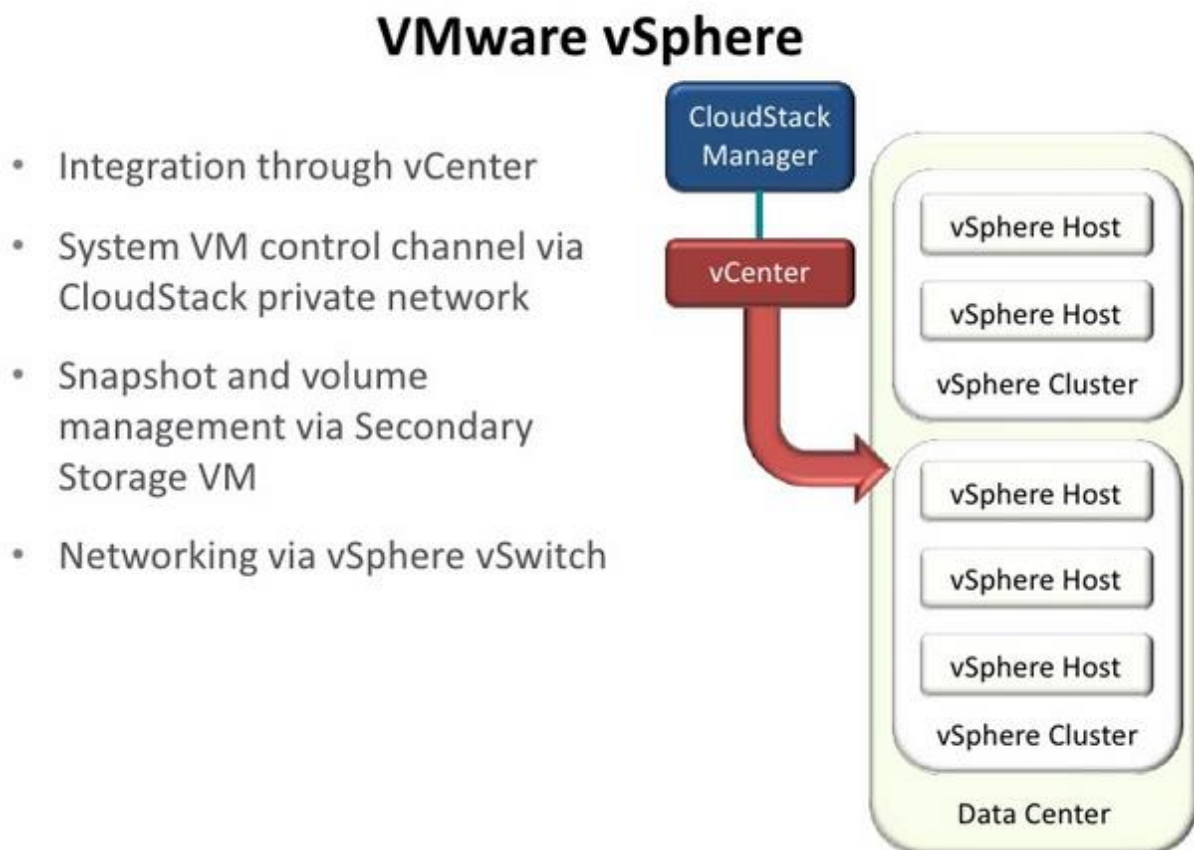


Figure 64 - Intégration de CloudStack au-dessus de vSphere, source [4]

La fin du support par VMware de vCloud et son changement de politique vis-à-vis du produit impliquent une réflexion globale sur le cloud de l'université et sur la viabilité potentielle d'autres solutions qui peuvent être intéressantes. Nous allons maintenant conclure.

Conclusion

L'université dispose maintenant d'une plate-forme de cloud de type IaaS et celle-ci est vouée à devoir évoluer pour répondre aux besoins des utilisateurs de façon plus rapide et plus précise. Une cinquantaine de VM peuvent tourner au même moment sur l'infrastructure de cloud actuelle mais c'est un chiffre qui peut rapidement évoluer à la hausse. Ces VM, Linux ou Windows sont déployables en quelques minutes après la création dans l'interface par l'utilisateur. Un travail encore important reste à réaliser pour rendre le cloud plus accessible pour les utilisateurs.

Plus globalement le cloud computing est voué à un bel avenir dans l'informatique. C'est un changement de modèle qui industrialise encore un peu plus l'informatique. Cette industrialisation se fera très probablement au détriment de l'emploi. Cette évolution est certainement inéluctable et ce, même si le « cloud-washing » est généralisé. L'utilisation du cloud n'est en soi pas forcément une réponse à tous les problèmes et ne garantit pas non plus un meilleur fonctionnement que l'informatique, tel qu'il était pratiqué jusqu'ici. Il faut être pragmatique et identifier les points forts du cloud afin d'en tirer le meilleur, mais ne surtout pas faire du cloud pour faire du cloud.

Enfin les problématiques liées à la sécurité risquent de mettre un frein au développement du cloud. L'une des réponses à cela pourrait se trouver dans le cryptage des données à l'aide d'algorithmes de chiffrement robustes, afin que les entreprises proposant du cloud n'aient pas potentiellement la main sur le contenu de leurs clients. Je pense que c'est une étape indispensable pour le cloud, faute de quoi il restera une mode.

D'un point de vue personnel, ce projet aura été l'occasion d'utiliser des technologies très différentes : Oracle Database, vSphere, vCloud, les baies SAN. Mes connaissances ont progressé en travaillant sur ce projet. Gérer un projet complexe comme celui-ci est réellement très gratifiant et je suis très heureux d'avoir pu faire partie intégrante de celui-ci.

Annexes

Création de la base de données Oracle

Nous créons 4 répertoires disposés sur des disques différents avant la création de la base de données :

```
/bases/oradata/vcloud  
/bases/redo/groupA/ vcloud  
/bases/redo/groupB/ vcloud  
/appli/oracle/diag/ vcloud
```

Le premier (« oradata ») doit accueillir les fichiers qui définissent la base de données. Les disques « redo » contiennent les redo logs. Ces « redo logs » sont destinés à être rejoués au besoin et contiennent les transactions SQL validées. Si le serveur de base de données connaît une défaillance et qu'aucun fichier de données n'est perdu, l'instance peut récupérer la base à l'aide des informations contenues dans ces redo logs. Chacun de ces deux répertoires est réparti sur un disque différent ; le fait d'avoir deux groupes de « redologs » permet d'être plus confiant pour parer à un problème de crash.

Enfin le quatrième répertoire « diag » sert à stocker des informations propres à oracle comme par exemple le fichier alert.log qui enregistre notamment les messages d'erreurs ou les drops de tablespace/database. Le répertoire diag conserve aussi les fichiers « trace » qui enregistrent des informations en provenance des processus d'oracle en arrière-plan. Ces fichiers sont une source de diagnostic en cas de problème mais aussi pour les prévenir.

Il faut ensuite s'occuper de l'accès à la base de données que l'on va créer. Pour cela il faut modifier le fichier `/appli/oracle/product/11.2.0/network/admin/listener.ora`. Le listener permet de donner l'accès à la base de données à l'application. C'est un service qui se lance de façon classique une fois configuré : `lsnrctl start |stop | reload`

Le démarrage du listener doit être automatisé au démarrage de la machine virtuelle qui l'héberge. Pour l'instant on se contente de modifier le listener afin qu'il permette une connexion entre le serveur de base de données et le serveur « vcloud ».

On lance la création de la base de données avec l'utilisateur oracle grâce à l'outil dbca (fourni par Oracle), on précise qu'on veut un encodage en UTF8

(obligation de vCloud) et en précisant les mots de passes des utilisateurs sys et system:

```
cd /appli/oracle/product/11.2.0/bin/  
./dbca -silent -createDatabase -templateName modeleDB.dbc -gdbName SID -  
sysPassword motdepasse -systemPassword motdepasse -emConfiguration NONE -  
storageType FS -characterSet AL32UTF8 -nationalCharacterSet AL32UTF8 -  
memoryPercentage 30
```

On lance le listener:

```
lsnrctl start
```

puis on se connecte avec sqlplus :

```
sqlplus / as sysdba
```

Puis on crée le tablespace :

```
Create Tablespace CLOUD_DATA datafile '/bases/oradata/vcloud/cloud_data01.dbf'  
size 1000M autoextend on next 500k;  
Create Tablespace CLOUD_INDX datafile '/bases/oradata/vcloud/cloud_indx01.dbf'  
size 500M autoextend on next 500k;
```

Création de l'utilisateur utilisé plus tard par l'application pour se connecter à la base de données en lui indiquant son mot de passe et en lui assignant un tablespace par défaut :

```
Create user vclouduser identified by monbonmotdepasse default tablespace  
CLOUD_DATA;
```

Il faut ensuite donner les droits suivant à l'utilisateur :

```
grant connect, RESOURCE, CREATE TRIGGER, CREATE TYPE, CREATE VIEW,  
CREATE MATERIALIZED VIEW, CREATE PROCEDURE, CREATE SEQUENCE to  
vclouduser;
```

Passage en Archive Log des bases de données

Le passage d'une base de données en archive log nécessite de rajouter un disque dans la vm pour stocker les archives. Cette opération se passe dans vSphere. Le disque est vu par le système d'exploitation comme un disque physique. On utilise ensuite lvm pour le formater et pour pouvoir l'utiliser.

```
sh-4.1# cat /proc/partitions  
major minor #blocks name  
8 0 16777216 sda  
8 1 512000 sda1  
8 2 16264192 sda2  
8 32 20971520 sdc  
8 16 15728640 sdb  
8 48 2097152 sdd  
253 0 12132352 dm-0  
253 1 4128768 dm-1  
253 2 1048576 dm-2  
253 3 1044480 dm-3  
253 4 10481664 dm-4
```



```

253    5  4194304 dm-5
253    6  4194304 dm-6
253    7  12578816 dm-7
253    8  2097152 dm-8
      8  64  10485760 sde
sh-4.1# pvcreate /dev/sde
Physical volume "/dev/sde" successfully created
sh-4.1# pvscan
PV /dev/sdd   VG VG_ORAREDO           lvm2 [2.00 GiB / 0   free]
PV /dev/sdc   VG VG_ORADATA           lvm2 [20.00 GiB / 2.00 GiB free]
PV /dev/sdb   VG VG_APPLI             lvm2 [15.00 GiB / 1.00 GiB free]
PV /dev/sda2  VG vg_systemrhel6ora11gr2 lvm2 [15.51 GiB / 0   free]
PV /dev/sde                   lvm2 [10.00 GiB]
Total: 5 [62.50 GiB] / in use: 4 [52.50 GiB] / in no VG: 1 [10.00 GiB]

```

On crée un volume groupe au nom évocateur.

```

sh-4.1# vgcreate VG_ORAARCH /dev/sde
Volume group "VG_ORAARCH" successfully created
sh-4.1# lvcreate -l 100%FREE -n lv_oraarch VG_ORAARCH
Logical volume "lv_oraarch" created
mkfs.ext4 /dev/VG_ORAARCH/lv_oraarch
sh-4.1# tune2fs -m 0 /dev/VG_ORAARCH/lv_oraarch

```

```

mkdir /bases/archives/
sh-4.1# ls -l /bases/
total 12
drwxr-xr-x 2 root  root 4096 Apr  2 10:25 archives
drwxrwx--- 5 oracle dba  4096 Jan  3 16:49 oradata
drwxrwx--- 4 oracle dba  4096 May  3 2013 redo
sh-4.1# chown oracle:dba /bases/archives
sh-4.1# ls -l /bases/
total 12
drwxr-xr-x 2 oracle dba 4096 Apr  2 10:25 archives
drwxrwx--- 5 oracle dba 4096 Jan  3 16:49 oradata
drwxrwx--- 4 oracle dba 4096 May  3 2013 redo
mkdir /bases/archives/VCLOUD
sh-4.1# chown oracle:dba /bases/archives/VCLOUD
sh-4.1# ls -l /bases/archives/
total 4
drwxr-xr-x 2 oracle dba 4096 Apr  2 10:28 VCLOUD
nano /etc/fstab

```

On ajoute la ligne suivante pour monter automatiquement au démarrage la partition dans /etc/fstab

```

/dev/mapper/VG_ORAARCH-lv_oraarch    /bases/archives/VCLOUD ext4
defaults        1 2

```

Puis on monte la partition :

```
mount /dev/mapper/VG_ORAARCH-lv_oraarch
```

On se connecte ensuite avec l'utilisateur système « oracle » :

```
sh-4.1# su - oracle
*****
serveur Prod DB VCLOUD - RHEL6-utilisateur oracle
-> base VCLOUD : setVCLOUD
-> base VCENTER : setVCENTER
*****
>[VCLOUD]
```

Puis on se connecte à la base de données

```
oracle@viewdb-bdr:oracle>[VCLOUD]sqlplus / as sysdba
SQL*Plus: Release 11.2.0.3.0 Production on Wed Apr 2 10:37:14 2014
Copyright (c) 1982, 2011, Oracle. All rights reserved.
Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
On précise le dossier du système où il faut placer les archives puis on arrête la base:
```

```
SQL> ALTER SYSTEM SET log_archive_dest = '/bases/archives/VCLOUD'
scope=both;
System altered.
SQL> shutdown immediate
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> startup mount
ORACLE instance started.
Total System Global Area 1202556928 bytes
Fixed Size          2227824 bytes
Variable Size       905970064 bytes
Database Buffers    285212672 bytes
Redo Buffers        9146368 bytes
Database mounted.
```

On place la base en mode « montée ». A ce moment la base de données est encore indisponible d'un point de vue applicatif. On active alors les archives logs.

```
SQL> alter database archivelog;
Database altered.
SQL> alter database open;
Database altered.
SQL>exit
```

On fait la même chose pour la base de données du vCenter.

Script de démarrage automatique de la base de données :

```
#!/bin/sh
# chkconfig: 345 99 1
# description: Oracle auto start-stop script.
#
# Set ORA_HOME to be equivalent to the $ORACLE_HOME
# from which you wish to execute dbstart and dbshut;
```

```

#
# Set ORA_OWNER to the user id of the owner of the
# Oracle database in ORA_HOME.
#
#/a placer dans /etc/init.d/dbora

ORA_HOME=/appli/oracle/product/11.2.0
ORA_OWNER=oracle

if [ ! -f $ORA_HOME/bin/dbstart ]
then
    echo "Oracle startup: cannot start"
    exit
fi

case "$1" in
'start')
    # Start the Oracle databases:
    # The following command assumes that the oracle login
    # will not prompt the user for any values
    su - $ORA_OWNER -c "$ORA_HOME/bin/lsnrctl start"
    su - $ORA_OWNER -c "$ORA_HOME/bin/dbstart $ORA_HOME"
    touch /var/lock/subsys/dbora
    ;;
'stop')
    # Stop the Oracle databases:
    # The following command assumes that the oracle login
    # will not prompt the user for any values
    su - $ORA_OWNER -c "$ORA_HOME/bin/dbshut $ORA_HOME"
    su - $ORA_OWNER -c "$ORA_HOME/bin/lsnrctl stop"
    rm -f /var/lock/subsys/dbora
    ;;
'restart')
    # Stop the Oracle databases:
    # The following command assumes that the oracle login
    # will not prompt the user for any values
    su - $ORA_OWNER -c "$ORA_HOME/bin/dbshut $ORA_HOME"
    su - $ORA_OWNER -c "$ORA_HOME/bin/lsnrctl stop"
    su - $ORA_OWNER -c "$ORA_HOME/bin/lsnrctl start"
    su - $ORA_OWNER -c "$ORA_HOME/bin/dbstart $ORA_HOME"
    ;;
esac
exit

```

Structures logiques et structures physiques d'une base de données

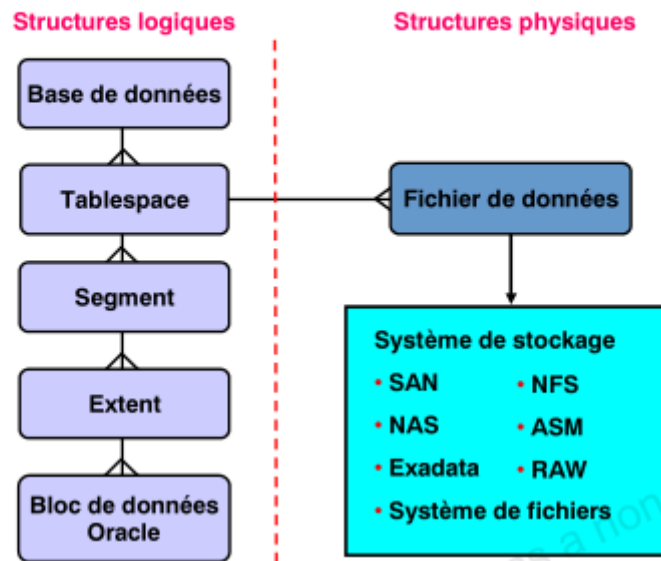


Figure 65 - Structures logiques et physiques d'une base de données Oracle, source [documentation officielle Oracle formation Oracle Database 11g : Workshop 1]

Table des figures

Figure 1 - Page 4 - Les différentes familles de Cloud, source
[http://en.wikipedia.org/wiki/Cloud_computing]

Figure 2 - Page 5 - Les différents modèles de services, source
[http://en.wikipedia.org/wiki/Cloud_computing]

Figure 3 - Page 8 - VMware vcloud hybrid service, source
[<http://www.virtualizationmatrix.com/2013/11/who-will-you-choose-cloud-management-strategic-battle-ground-for-vmware-and-microsoft/>]

Figure 4 - Page 9 - Approche traditionnelle vs virtualisation, source [vmware.com]

Figure 5 - Page 9 - Migration à chaud d'une machine virtuelle, vmotion, source
[<http://www.electricmonk.org.uk/category/vmware/vmotion/>]

Figure 6 - Page 10 - Heartbeat, source [http://www.yellow-bricks.com/2012/02/10/stratus-vcenter-uptime-appliance]

Figure 7 - Page 11 - Organigramme de la DSI

Figure 8 - Page 16 - Infrastructure physique, source
[http://www.vmware.com/pdf/esx_san_cfg_technote.pdf]

Figure 9 - Page 17 - vCenter au sein de l'infrastructure, source
[<https://www.vmware.com/fr/products/vcenter-server/features.html>]

Figure 10 - Page 18 - Fonctionnement général de vCloud

Figure 11 - Page 22 - Utilisation de vCloud connector, source
[http://pubs.vmware.com/hybridcloud-26/index.jsp#com.vmware.vcc.install.doc_26/GUID-C2776581-4251-499C-86CF-84B2FD6B552F.html] p53

Figure 12 - Page 22 - Intégration de vCloud connector, source
[http://pubs.vmware.com/hybridcloud-26/index.jsp#com.vmware.vcc.install.doc_26/GUID-C2776581-4251-499C-86CF-84B2FD6B552F.html]

Figure 13 - Page 27 - Interface graphique de vShield

Figure 14 - Page 32 - Recover point d'EMC

Figure 15 - Page 33 - Relations entre luns, pools et disques, source
[<http://vjswami.com/2012/12/17/a-study-in-vmx-vnx-auto-tiering/>]

Figure 16 - Page 33 - Photo des disques de la baie EMC, pools et disques

Figure 17 - Page 34 - Création d'une Lun sur la baie EMC

Figure 18 - Page 35 - Présentation d'une Lun aux serveurs

Figure 19 - Page 36 - Création d'une Lun sur la baie HP

Figure 20 - Page 36 - Présentation d'une Lun sur la baie HP

Figure 21 - Page 37 - Interface web de gestion des switchs fibres

Figure 22 - Page 38 - Ajout du stockage dans vSphere

Figure 23 - Page 38 - Ajout du stockage dans vSphere (suite)

Figure 24 - Page 38 - Ajout du stockage dans vSphere, choix de la LUN

Figure 25 - Page 39 - Ajout du stockage dans vSphere, formatage du datastore

Figure 26 - Page 39 - Ajout du stockage dans vSphere, nommage du datastore

Figure 27 - Page 40 - Ajout du stockage dans vSphere, allocation de l'espace au datastore

Figure 28 - Page 40 - Ajout du stockage dans vSphere, résumé avant validation de l'ensemble des opérations

Figure 29 - Page 40 - Stockage dans vSphere alloué au cloud

Figure 30 - Page 41 - Installation de vCloud Director

Figure 31 - Page 43 - Premier lancement de l'interface web de vCloud Director, association au serveur vCenter

Figure 32 - Page 43 - Premier lancement de l'interface web de vCloud Director, association au serveur vShield

Figure 33 - Page 44 - Architecture de test

Figure 34 - Page 45 - Architecture de test, gestion des utilisateurs

Figure 35 - Page 46 - Architecture réseau de test

Figure 36 - Page 47 - Interface vCloud, limitation de la bande passante

Figure 37 - Page 51 - Création du lien ODBC 32 bit dans Windows Server 2008 R2

Figure 38 - Page 51 - Test de la connexion à la base de données en utilisant le lien ODBC

Figure 39 - Page 52 - Installation de serveur vCenter, sélection du lien ODBC

Figure 40 - Page 53 - Installation de serveur vCenter, connexion à la base de données déportée

Figure 41 - Page 53 - Installation de serveur vCenter, sélection du mode "standalone"

Figure 42 - Page 54 - Installation de serveur vCenter, dimensionnement de la JVM

Figure 43 - Page 54 - Architecture de production

Figure 44 - Page 55 - Interface permettant la désindexation de vShield des plug-ins de vCenter

Figure 45 - Page 56 - Contrôles de centrion concernant vShield

Figure 46 - Page 57 - Backup RMAN dans avamar des bases de données Oracle

Figure 47 - Page 58 - Vision système des archives issues du passage en archive log

Figure 48 - Page 61 - Stockage des données en fonction du niveau de service

Figure 49 - Page 62 - Association des ressources en fonction des niveaux de services dans l'interface de vCloud

Figure 50 - Page 63 - Limitation de la bande passante en fonction du niveau de service

Figure 51 - Page 64 - Utilisation des clones liés, source
[<http://www.vmguru.com/2012/01/vmware-vcloud-director-design-guidelines>]

Figure 52 - Page 66 - Utilisation des rôles et des droits

Figure 53 - Page 68 - Architecture vCloud de production, changement de serveur vCenter

Figure 54 - Page 70 - Architecture vCloud de production, changement de serveurs ESXi

Figure 55 - Page 73 - Utilisation de SSO dans les produits VMware, source
[<http://fr.slideshare.net/VMworld/vmworld-2013-vsphere-vcenter-single-signon-best-practices>]

Figure 56 - Page 74 - Evolutions de SSO (roadmap), source
[<http://fr.slideshare.net/VMworld/vmworld-2013-vsphere-vcenter-single-signon-best-practices>]

Figure 57 - Page 74 - Processus d'upgrade vCenter 5.0 vers vCenter 5.1, source
[<http://fr.slideshare.net/VMworld/vmworld-2013-vcenter-deep-dive>]

Figure 58 - Page 75 - Evolutions de la base de données de vCenter 5.1 par rapport à vCenter 5.0, source [<http://fr.slideshare.net/VMworld/vmworld-2013-vccenter-deep-dive>]

Figure 59 - Page 77 - Fin du support de vCloud Director annoncé par l'éditeur, source [<https://www.vmware.com/files/pdf/support/Product-Lifecycle-Matrix.pdf>]

Figure 60 - Page 77 - Transition vCloud vers vCaC (vRealize), source [<https://www.vmware.com/files/pdf/support/Product-Lifecycle-Matrix.pdf>]

Figure 61 - Page 78 - VMware vCAC 6.x: Introduction, source [<https://www.youtube.com/watch?v=giJOtba9IEA>]

Figure 62 - Page 78 - Composants de vCAC 6.0, source [<http://vmwaremine.com/2014/01/19/vcac-60-series-part-1-architecture>]

Figure 63 - Page 79 - Intégration d'OpenStack au-dessus de vSphere, source [<http://docs.openstack.org/juno/config-reference/content/vmware.html>]

Figure 64 - Page 80 - Intégration de CloudStack au-dessus de vSphere, source [<http://docs.openstack.org/juno/config-reference/content/vmware.html>]

Figure 65 - Page 89 - Structures logiques et physiques d'une base de données Oracle, source [documentation officielle Oracle formation Oracle Database 11g : Workshop 1]

Table des tableaux

Tableau 1 - Page 13 - Planning du projet

Bibliographie

1. **VIJAY SWAMI**, A study in VMAX & VNX auto-tiering | on WordPress.com. En ligne : <http://vjswami.com/2012/12/17/a-study-in-vmax-vnx-auto-tiering/>, consulté le 24 janvier 2015.
2. **Bertina Nguyen**, Product-Lifecycle-Matrix. En ligne : <https://www.vmware.com/files/pdf/support/Product-Lifecycle-Matrix.pdf>, consulté le 24 janvier 2015.
3. **nVizor**, Changing VMware vShield Manager Default Passwords ». En ligne : <http://www.nvizor.com/?p=1401>, consulté le 24 janvier 2015.
4. **CloudStack Architecture**. En ligne : <http://fr.slideshare.net/cloudstack/cloudstack-architecture>, consulté le 24 janvier 2015.
5. **VMware KB**: End of Availability and End of Support Life for VMware vCloud Director 5.1 Standalone (2057589). En ligne : http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2057589, consulté le 14 février 2015.
6. **Eric BERTHELOT**, Memoire Online - Le cloud computing quel impact organisationnel pour les équipes informatiques des systèmes d'information ? En ligne : http://www.memoireonline.com/02/12/5216/m_Le-cloud-computing-quel-impact-organisationnel-pour-les-equipes-informatiques-des-systemes-d-infor1.html, consulté le 24 janvier 2015.
7. **Landry FOSSOUO NOUMSI**, Memoire Online - Etude et mise en place d'une solution "cloud computing " privée dans une entreprise moderne: cas de CAMTEL . En ligne : <http://www.memoireonline.com/01/13/6713/Etude-et-mise-en-place-d'une-solution-cloud-computing--privee-dans-une-entreprise-moderne-cas.html>, consulté le 24 janvier 2015.
8. **vCAC 6.0 series - Part 1 - Architecture**. En ligne : <http://vmwaremine.com/2014/01/19/vcac-60-series-part-1-architecture/>, consulté le 24 janvier 2015.
9. **vCenter Howto: Remove a plugin from the plugin manager (including a plugin list)** - viktorious.nl - Virtualization & Cloud Management. En ligne : <http://www.viktorious.nl/2012/05/06/vcenter-howto-remove-a-plugin-from-the-plugin-manager/>, consulté le 24 janvier 2015.

10. **vCloud Director Convergence and Transition Plan - What's the Scoop?** | VMware vSphere Blog - VMware Blogs. En
ligne : <http://blogs.vmware.com/vsphere/2013/09/vcloud-director-convergence-and-transition-plan-whats-the-scoop.html>, consulté le 24 janvier 2015.

11. **vMotion | Electric Monk**. En
ligne : <http://www.electricmonk.org.uk/category/vmware/vmotion/>, consulté le 24 janvier 2015.

12. **VMware SAN Conceptual and Design Basics**. En
ligne : http://www.vmware.com/pdf/esx_san_cfg_technote.pdf, consulté le 24 janvier 2015.

13. **VMware (2014) VMware KB: Backing up the VMware vShield database (1022135)**. En
ligne : http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1022135, consulté le 24 janvier 2015.

14. **VMware (2014) VMware KB: Installing and configuring a vCloud Director 5.1 or 5.5 database (2034540)**. En
ligne : http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2034540, consulté le 24 janvier 2015.

15. **VMware (2014) VMware KB: End of Availability and End of Support Life for VMware vCloud Director 5.1 Standalone (2057589)**. En
ligne : http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2057589, consulté le 24 janvier 2015.

16. **VMware (2014) VMware KB: Securing vShield CLI user accounts and the privileged mode (2064079)**. En
ligne : http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2064079, consulté le 24 janvier 2015.

17. **VMware vCloud Connector Documentation**. En
ligne : https://www.vmware.com/support/pubs/hybridcloud_pubs.html, consulté le 24 janvier 2015.

18. **VMware vCloud Director design guidelines**. En
ligne : <http://www.vmguru.com/2012/01/vmware-vcloud-director-design-guidelines/>, consulté le 24 janvier 2015.

19. **VMware vSphere - OpenStack Configuration Reference (2015).** En ligne : <http://docs.openstack.org/juno/config-reference/content/vmware.html>, consulté le 24 janvier 2015.

20. **VMware vSphere 5.1 - Upgrade Tips & Top New Features.** En ligne : <http://fr.slideshare.net/stcroixsolutions/vmware-vsphere-51-upgrade-tips-top-new-features>, consulté le 24 janvier 2015.

21. **VMworld 2013: vSphere vCenter Single Sign-on Best Practices.** En ligne : <http://fr.slideshare.net/VMworld/vmworld-2013-vsphere-vcenter-single-signon-best-practices>, consulté le 24 janvier 2015.

22. **VMworld 2013: vCenter Deep Dive.** En ligne : <http://fr.slideshare.net/VMworld/vmworld-2013-vcenter-deep-dive>, consulté le 24 janvier 2015.

23. **Who will Service Providers choose? Hybrid Cloud Management – Key Battle for VMware and Microsoft | Virtualization Matrix - Agnostic Vendor Comparison: vSphere, Hyper-V, XenServer.** En ligne : <http://www.virtualizationmatrix.com/2013/11/who-will-you-choose-cloud-management-strategic-battle-ground-for-vmware-and-microsoft/>, consulté le 24 janvier 2015.

24. **Wikipedia (2015) Cloud computing - Wikipedia, the free encyclopedia.** Wikipedia, éd. En ligne : <http://en.wikipedia.org/w/index.php?oldid=643498514>, consulté le 24 janvier 2015.

25. **Raynaud, Philippe** [dumas-00587661, v1] Déploiement d'une solution de virtualisation au sein d'une multinationale. En ligne : <http://dumas.ccsd.cnrs.fr/docs/00/58/76/61/PDF/2011.TH16880.raynaud.philippe.pdf>, consulté le 24 janvier 2015.

Etude et mise en place d'une plate-forme de cloud computing privé avec vCloud Director 5.1.2

Mémoire d'Ingénieur C.N.A.M., Lyon 2015

RESUME

Le cloud computing est devenu incontournable ces dernières années et s'impose aux professionnels mais aussi aux yeux du grand public.

L'objectif du projet était de mettre en place une infrastructure de cloud computing privée permettant de déployer rapidement des machines virtuelles préconfigurées. Ce projet s'inscrivait dans la lignée d'autres projets menés précédemment et dont le but était de virtualiser la grande majorité des serveurs de la DSI de l'Université Lyon 2.

Mots clés : cloud computing, vCloud Director, vSphere, SAN, IaaS.

SUMMARY

Cloud computing became inevitable these last years for the professionals, but also for the general public.

The project was to implement a private cloud infrastructure to quickly deploy preconfigured virtual machines. This project was part of other projects previously undertaken lineage and whose goal was to virtualize the majority of servers in the CIO of Lyon 2 University

Key words : cloud computing, vCloud Director, vSphere, SAN, IaaS.