

Table des matières

DEDICACES	4
REMERCIEMENTS	5
AVANT PROPOS.....	6
GLOSSAIRE.....	7
RESUME	10
LISTES DES TABLEAUX.....	11
LISTE DES FIGURES.....	12
LISTE DES CAPTURES.....	13
Introduction	16
PREMIERE PARTIE : Cadre de référence et approche méthodologique	19
1. Cadre de reference	19
1.1. Problématique	20
1.2. Objectifs de l'étude	21
1.3. Pertinence du thème	21
2. Approche Méthodologique.....	22
2.1. Délimitation du champ d'étude	22
2.2. Difficultés rencontrées.....	22
DEUXIEME PARTIE : ETUDE.....	24
1. Etude au préalable	24
1.1. Etude sur les Datacenter.....	24
1.1.1. Définition.....	25
2. Mécanisme de fonctionnement.....	25
2.1. Norme	25
2.1.1. CLASSEMENT DES DATACENTER	25
3. Notion générale de virtualisation	27
3.1. Définition.....	27
3.2. But de la virtualisation	28
3.3. Différents types de virtualisations	29
3.4. Différentes solutions de virtualisation	33
3.5. Etude comparative et choix de la solution de virtualisation	36
3.6. Solution de stockage	38

3.6.4.	Solution SAN.....	41
3.7.	Architecture VMware du Datacenter et ses différents modes d'accès	47
3.7.1.	Présentation de la solution de virtualisation des serveurs et poste se travail avec VMware	47
3.7.1.1.	VMware vSphere ESXI.....	47
3.7.1.2.	Description des différents composants de VMware View	48
TROISIEME PARTIE : Déploiement et Sécurisation		55
1.	Déploiement de l'infrastructure virtuelle du Datacenter	55
1.1.	Présentation de l'architecture Mise en œuvre	55
1.2.	Déploiement requise pour les différents composants en mode production. 55	
2.	Dispositif Materiel et Logiciel	56
3.	Exigence techninique	56
3.1.	Configuration requise pour les différents composants en mode production .. 56	
3.1.1.	Composants Serveur	56
3.1.2.	Composants Client	58
4.	Sécurisation du système d'information	60
4.1.	Risques éventuelles dans un environnement virtuel.....	61
4.2.	Menaces	65
5.	Définition et enjeu	66
5.1.	Définition.....	66
5.1.1.	Objectifs de la sécurité informatique	66
6.	Gérer les groupes et les utilisateurs avec VMware vSphere 5.0	68
QUATRIEME PARTIE : IMPLEMENTATION DE L'INFRASTRUCTURE.....		70
1.	Implémentation de l'infrastructure virtuelle.....	70
1.1.	Installation et configuration de VMware vSphere	70
1.1.1.	Installation	70
1.1.2.	Configuration du serveur ESXI	72
1.2.	Installation et configuration de view client	74
1.3.	installation et configuration deVMware vCenter Server	75
1.3.1.	Installation	76
1.3.2.	Configuration	77
2.	Installation et configuration de l'architecture VMware View	78
2.1.	Installation de Connection server	78
2.2.	Configuration de Connexion au serveur view.....	80

2.3. Composants clients	82
✓ Installation de view agent	85
3. INSTALLATION ET CONFIGURATION D'UN CLUSTER VMWARE VCENTER HA, DRS et DPM91	
4. Création et attribution des droits des utilisateurs et de groupes.....	100
5. Installation et configuration de l'architecture de stockage (FreeNas)	106
CONCLUSION	111
BIBLIOGRAPHIES	113
ANNEXES	116



DEDICACES

A

Mon père NGOMA MVOUNDI EMMANUEL, ma mère YEMBA DENISE, ma grande sœur NGOMA MVOUNDI JURLINE et à mon pasteur ETIENNE NYMILONGO dont l'encadrement, la motivation et les sacrifices consentis nous ont menés à ce niveau.

REMERCIEMENTS

La réalisation de ce travail a été possible grâce à l'encadrement, le soutien de et la bonne disposition des personnes à qui nous ne saurions manquer d'exprimer notre profonde gratitude.

Nos remerciements s'adressent :

- ✓ A Dieu Tout puissant pour la santé et le moral qu'il nous a accordés,
- ✓ Aux Membres du jury,
- ✓ Au **Pr. Djiby SOW**, notre responsable de formation,
- ✓ A **Mr. Ahmed YOUSSEF KHILL**, mon encadreur,
- ✓ Au corps administratif et professoral du laboratoire d'algèbre, de Cryptologie, de Géométrie, de Géométrie algébrique et application (**LACGAA**) du de département de mathématiques et informatiques(**DMI**) de la faculté des Sciences et techniques(**FST**) de l'université Cheikh Anta Diop de Dakar(**UCAD**),
- ✓ A Mon frère et ami de longue date **André MIALEBAMA BOUESSO SAINT-EUDES**,
- ✓ A mes amis et à tous ceux qui m'ont soutenu de près ou de loin.

AVANT PROPOS

Comme nous allons le voir tout au long de ce travail de diplôme, la virtualisation reste un domaine complexe dès qu'il s'agit de comprendre tous les mécanismes qui entrent en jeu. Les notions qui y sont rattachées sont également nombreuses et ne sont pas toujours simples à saisir, ce qui ne facilite pas l'apprentissage.

Néanmoins, la virtualisation a tendance à se populariser et à devenir indispensable pour ceux qui en ont compris les avantages et qui savent la maîtriser. Dans certains domaines du monde professionnel, on en arrive presque à n'avoir plus que des systèmes virtualisés et, c'est là, tout l'enjeu de comprendre et savoir comment configurer ces systèmes pour une optimisation parfaite des Datacenter.

GLOSSAIRE

AD	Active Directory
AMD	Advanced Micro Devices
AMD-V	Advanced Micro Devices Virtualization
APP	Application
CPU	Central Processing Unit
DAS	Direct Attached Storage
DDC	Desktop Delivery Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DPM	Distributed Power Management
DRS	Distributed Resource Scheduler
DVD	Digital Versatile Disc
EPT	Extended Page Table
ESX	Elastic Sky X
ESXi	Elastic Sky X integrated
Go	Giga octet
HA	High Availability
HDX	High Definition experience
IBM	International Business Machines
ICA	Independent Computing Architecture
IDC	International Data Conseil
IP	Internet Protocol
ISO	International Standard Organization
JVM	Java Virtual Machine
LAHF	load AH from Flags
MS	Microsoft
NAS	Network Attached Storage

ODBC Open Data Base Connectivity

OS Operating System

PC Personal Computer

PCoIP PC over IP

PKI Public Key Infrastructure

RAM Random Access Memory

RD Remote Desktop

RDP Remote Desktop Protocol

RDS Remote Desktop Services

RDS-V Remote Desktop Services-Virtualization

SAHF Store AH from Flags

SAN Storage Area Network

SC Serveur de Connexion

SP Service Pack

SPICE Simple Protocol for Independent Computing Environments

SQL Structured Query Language

URL Uniform Resource Locator

FT Fault Tolerance

VDI Virtual Desktop Infrastructure

VT-x Virtual Technology x

VCS View Connection Server

VLAN Virtual Local Area Network

VM Virtual Machine

VMHA Virtual Machine Hight Availability

RAID Redundant Array of Independent Disks (regroupement redondant des disques independants)

LUN espace de stockage crée sur les volumes RAID, permettant à une machine virtuelle VM de posséder un espace de stockage pour son installation et son propre fonctionnement.

iSCSI internet Small Computer System interface

DSI direction des services informatiques

Cluster grappe de serveur constituée de deux serveurs au minimum et partageant une baie de disques commune, pour assurer une continuité de service et/ou répartir la charge de calcul et/ou la charge réseau.

Baie de stockage (*diskarray* en anglais) est un équipement comportant principalement : un ensemble de disques regroupés par tiroir disque.

SLA (service level agreement) est un document qui définit la qualité de service requise entre un prestataire et un client.

RESUME

Ce mémoire qui porte sur l'étude, le déploiement et la sécurisation du Datacenter, s'emploie à traiter les aspects liés au problème de stockages et de la sécurisation des données informatiques. Dans ce mémoire nous avons fait un tour d'horizon sur les Datacenter et les solutions de virtualisation qui implémente cette technologie. Afin de consolider les serveurs.

Cette formation permet aux participants d'acquérir les connaissances et compétences nécessaires pour **déployer et gérer l'environnement de virtualisation du serveur à l'aide des technologies Microsoft (Hyper-V, SCVMM)**. Elle fournit les informations sur le déploiement et la gestion de Hyper-V et les services de bureau à distance sur **Windows Server 2008 R2**.

LISTES DES TABLEAUX

Tableau 1:comparatif technique pour les hyperviseurs de type1	38
Tableau 2: Comparatifs sur le coût entre MICROSOFT et VMware	38
Tableau 3:Différences essentielles entre le SAN et le NAS.....	46
Tableau 4: Vue générale des niveaux NAS et SAN	46
Tableau 5: Comparatif entre NAS et SAN	47
Tableau 6:Exigences matérielles de ViewConnection Server	58
Tableau 7: Systèmes d'exploitation prise en charge par ViewConnection server.....	58
Tableau 8: Systèmes d'exploitation prise en charge par View Agent.....	59
Tableau 9: Systèmes d'exploitation prise en charge par View Client.....	60
Tableau 10:Exigences matérielles des postes de travail en mode local	60

LISTE DES FIGURES

Figure 1 : Architecture réseau du Datacenter de la Régis de finances	27
Figure 2: hyperviseur de type 2	28
Figure 3:hyperviseur de type 1	28
Figure 4 : virtualisation d'applications	30
Figure 5 : virtualisation des postes de travail (VDI)	31
Figure 6 : Architecture ESX.....	34
Figure 7: ARCHITECTURE MICROSOFT HYPER-V	35
Figure 8:Architecture Citrix XenServer	36
Figure 9: Solutions de Virtualisations 2008.....	37
Figure 10: Architecture DAS.....	39
Figure 11: Schéma d'une architecture possible NAS	41
Figure 12:Architecture complexe du SAN (topologie fabric)	43
Figure 13:Baie de stockage de la Topologie Peer to peer.....	44
Figure 14: Baie de stockage de la Topologie en Boucle 1	44
Figure 15:Baie de stockage de la Topologie en Boucle 2.....	45
Figure 16:Architecture virtuelle de test de VMware	55
Figure 17:Stratégie de sécurité en entreprise	67
Figure 18: Architecture HA (High Availability)	91
Figure 19: Architecture DRS (Distributed Resource Scheduler).....	91
Figure 20: Architecture DPM (Dynamic Power Management)	92

LISTE DES CAPTURES

Capture 1:Installation de Vsphere ESXI	70
Capture 2:Interface d'installation de VMware ESXI 5.....	71
Capture 3:Interface de lecture de VMware ESX	71
Capture 4: Etape de l'installation.....	71
Capture 5:Espace de stockage de VMware ESXI5	71
Capture 6:Interface de configuration du mot de passe.....	72
Capture 7:Interface de configuration de la langue	72
Capture 8:Début de l'installation.....	72
Capture 9: Fin de l'installation	72
Capture 10:Interface d'authentification	73
Capture 11:Interface de configuration	73
Capture 12:Configuration paramètres IP	73
Capture 13 : Configuration de du nom et de l'adresse IP.....	74
Capture 14 : Configurations paramètres DNS.....	74
Capture 15 : Interface stable	74
Capture 16:Interconnexion a ESXI	75
Capture 17: Certificat SSL.....	75
Capture 18:Interface d'administration de VMware ESXI 5.....	75
Capture 19: Interface d'installation de vSphere	76
Capture 20:Assistant d'installation de vCenter Server	76
Capture 21:Informations sur le compte utilisateur vCenter.....	77
Capture 22:Création d'un ODBC	78
Capture 23:Organisation d'un Datacenter.....	78
Capture 24:Extraction de fichiers nécessaires	79
Capture 25:Assistant d'installation	79
Capture 26:Fin installation.....	80
Capture 27:Ouverture de vConnection Server	80
Capture 28:Interface de logging de View administrateur	80
Capture 29:Tableau de bord de view Administrateur	81
Capture 30:Utilisateur du domaine	81
Capture 31:Ajout d'un serveur vCenter sur le coursier de connexion	82
Capture 32:Configuration du Pool	82
Capture 33:Assistant d'installation de vSphere Client.....	83
Capture 34:Début installation.....	83
Capture 35:Fin installation.....	84
Capture 36:Interface de login de vSphereClient.....	84
Capture 37:Architecture du Mappage Réseau View.....	85
Capture 38:Assistant d'installation de view Agent	85
Capture 39:Assistant d'installation de view Agent en cours	86
Capture 40 : Extraction de fichiers nécessaires à l'installation.....	86
Capture 41: Indication du Broker par défaut.....	87

Capture 42:Installation de view Client en cours	87
Capture 43: Connexion au serveur de connexion.....	88
Capture 44:Configuration du ssl	88
Capture 45:Loggin de connexion à un bureau virtuel.....	88
Capture 46: Pool d'accès au bureau virtuel	89
Capture 47: Tentative de connexion au bureau virtuel	89
Capture 48: Image bureau sur pc.....	90
Capture 49:Image du bureau virtuel sur PC physique	90
Capture 50: Interface View agent	90
Capture 51:Interface de création d'un centre des données.....	92
Capture 52: Interface de fonctions HA et DRS du cluster.....	93
Capture 53:Interface DRS.....	93
Capture 54:Interface VMware HA.....	94
Capture 55 : Interface des règles d'applications du cluster VMware HA	94
Capture 56:Interface sur fixation de priorité de redémarrage	95
Capture 57:Capture sur VMware HA	95
Capture 58:Interface d'activation ou non d'EVC	96
Capture 59:Interface permettant de spécifier l'emplacement des fichiers	96
Capture 60:interface récapitulatif de la configuration du cluster	97
Capture 61:Interface d'administration de l'hôte.....	97
Capture 62: Certificat non identifié SHA1.....	98
Capture 63:Interface Pool Ressources de destination	98
Capture 64:Interface d'assignation de la licence.....	99
Capture 65:Interface d'assignation de la licence.....	99
Capture 66: Interface récapitulatif	100
Capture 67:Interface d'avancement de la configuration.....	100
Capture 68:Vue générale des hotes esxi dans un cluster	100
Capture 69:Connexion sur vClient	101
Capture 70:Création d'un Groupe sur ESX.....	101
Capture 71:Création d'un Groupe sur ESX.....	102
Capture 72:Création d'un utilisateur d'hôte.....	102
Capture 73:Interface d'ajout d'un utilisateur	103
Capture 74:Ajout d'un utilisateur dans un groupe	103
Capture 75:Attribution d'un rôle	104
Capture 76:Ajout d'une autorisation	105
Capture 77:Choix de l'espace du stockage de l'os de FreeNAS	106
Capture 78:Début de l'installation.....	106
Capture 79:Fin de l'installation	107
Capture 80:Configuration de l'espace de stockage (RAID)	107
Capture 81:Permission pour les groupes d'utilisateurs	108
Capture 82:Configuration du réseau	109
Capture 83:Configuration de l'espace de partage	109
Capture 84: Liaison de l'adaptateur réseau.....	110
Capture 85:Ajout du Stockage FreeNAS dans ESXi	110

Capture 86:Montage de FreeNas dans Esxi	110
---	-----

Introduction

L'avènement de la micro-informatique à partir des années 80 a fait entrer les ordinateurs dans tous les bureaux mais n'a pas diminué le besoin de surfaces dédiées aux serveurs qui offrent les garanties nécessaires pour réduire au minimum les défaillances. Au contraire, l'utilisation des micro-ordinateurs reliés aux réseaux privés ou à l'Internet a fait exploser le besoin en serveur. Ainsi le développement de cette connectivité a permis l'installation des serveurs dans des bâtiments dédiés distants des sites des entreprises qui offrent un environnement contrôlé, une alimentation électrique garantie, un bon niveau de sécurité physique et une large connectivité communément appelé **Datacenter**. Aux yeux de l'immensité des utilisateurs, l'existence d'un **Datacenter** est occultée par les autres maillons (*services, applications, plateformes, serveurs...*). Le Datacenter est au sommet de la pyramide des services informatiques.

Une seule fraction des utilisateurs est consciente de la mesure dans laquelle les Datacenter concourent à la fiabilité et à la performance de l'outil informatique des entreprises.

Pour l'utilisateur qui a la capacité et la volonté de gérer indépendamment ses serveurs, le recours à des Datacenter s'inscrit dans une politique de rationalisation et de la fiabilité de l'outil informatique.

En effet l'exigence sans cesse et croissante de fiabilité des serveurs et des services qu'ils fournissent aux entreprises, à leurs salariés, leurs clients et au public, s'accompagne d'une complexité accrue de la conception et la gestion des **Datacenter**. Face à ces exigences, une offre de service de colocation est apparue pour permettre aux entreprises de toute taille d'avoir l'accès aux Datacenter garantissant des conditions optimales pour héberger les serveurs.

Dans le cadre de notre travail nous allons nous appesantir sur le déploiement et la sécurisation des applications et des services du Datacenter monté sur une plateforme de virtualisation.

Compte tenu de la complexité accrue de la conception et de la gestion des Datacenter, la virtualisation s'introduit, voire même s'impose, de plus en plus dans les parcs de serveurs, les systèmes de stockage et les réseaux des organisations.

Comme lors de l'avènement de toute nouvelle technologie, la sécurité reste trop souvent négligée. Pourtant, les risques existent et ne doivent pas être négligés.

Grâce à la virtualisation, l'efficacité et la disponibilité des ressources et applications informatiques seront améliorées. On commence par abandonner l'ancien modèle "un serveur, une application" et exécute plusieurs machines virtuelles sur chaque machine physique. On allège la tâche des administrateurs informatiques, qui passent plus de temps à gérer les serveurs qu'à innover. Dans un Datacenter non virtualisé, près de 70 % du budget informatique type sont consacrés à la simple maintenance de l'infrastructure existante, ce qui laisse peu pour l'innovation.

Un Datacenter automatisé, reposant sur la plate-forme de virtualisation éprouvée en production, permettons de répondre de façon plus efficace et plus rapide à l'évolution du marché.

C'est dans ce contexte que s'inscrit notre projet de fin d'étude. C'est à dire déployer un Datacenter s'appuyant sur une technologie de virtualisation et mettre en place une sécurité s'adaptant sur la technologie de virtualisation en question.

Pour une bonne compréhension de notre sujet, il convient de subdiviser ce travail en quatre grandes parties.

Dans la première partie nous parlerons du : «cadre de référence et de l'approche méthodologique» c'est-à-dire que nous allons présenter le laboratoire qui nous permis de réaliser ce projet ensuite adopté une démarche pour aborder notre thème, dans la deuxième partie il convient d'axer notre travail sur «l'étude» c'est-à-dire une étude préalable sur : le Datacenter ; les différentes solutions de virtualisations ; étude comparative et le choix de la solution à déployer puis les solutions de stockages.

Quant à la troisième partie nous parlerons du déploiement et sécurisation. C'est ici que nous allons citer les exigences à respecter pour le déploiement, le dispositif matériel et logiciel utilisé, ainsi que le niveau de sécurité des serveurs et applications. Enfin la quatrième et dernière partie concerne « l'implémentation ». C'est ici que nous mettrons en place toutes les configurations ainsi que notre plateforme de test.

PREMIERE PARTIE :

Cadre de référence et approche méthodologique

PREMIERE PARTIE : Cadre de référence et approche méthodologique

1. Cadre de reference

La Faculté des Sciences de l'université Cheikh Anta Diop, devenue Faculté des Sciences et Techniques en 1990 par la réforme de l'Université, est un établissement d'enseignement et de recherche. Elle compte six départements, parmi lesquels le département de **Math-info**, dont nous faisons partis, et qui en son sein se trouve la filière de **cryptologie, tatouage, génie logiciel et base des données (MAGA/CTGBD)** dont le but est de former des ingénieurs et chercheurs dans le domaine des mathématiques et de l'informatique.

Par ailleurs cette filière dispose aussi d'un laboratoire de renommé mondial avec un corps professoral dynamique :

LABORATOIRE D'ALGÈBRE DE CRYPTOLOGIE DE GÉOMÉTRIE ALGÈBRIQUE ET APPLICATIONS(L.A.C.G.A.A)

Qui a pour objectif :

- D'une part, la formation à la recherche fondamentale et appliquée de la Cryptographie, de la Théorie des codes, de l'algèbre et de leurs applications(en logique, en informatique, en sécurité de l'information, en biologie, en robotique, etc.) par :
- Des enseignements pour les jeunes doctorants durant leur première année d'inscription en thèse ;
- L'encadrement des jeunes doctorants durant toute leur thèse ;
- D'autre part, des formations professionnelles qualifiantes sur divers domaines de l'informatique. Conscients de la nécessité de ses technologies et de leur importance dans le développement, les responsables ont vite compris de se mettre dans une dynamique d'ouverture vers des nouveaux types d'informations qui leur a permis de répondre aux exigences de qualité en ressources humaines dont font preuve les entreprises. C'est dans ce cadre que le Master de cryptologie, tatouage, génie logiciel et Base des données (MAGA/CTGBD) a vu le jour.

Globalement, ce Master forme en cryptologie et en sécurité des systèmes d'information sur deux ans. Cette formation est destinée au moins pour des étudiants titulaires d'une licence en mathématique ou en informatiques ou équivalent, mais aussi des ingénieurs informaticiens d'entreprises.

Cette formation offre beaucoup des débouchés aux étudiants dont les principaux sont :

- Développeur des logiciels Cryptographiques;
- Spécialiste en audit et Sécurité;
- Expert en sécurité réseau;
- Administrateur des sites de commerces sécurisé;
- Administrateur des bases de données sécurisées;
- Responsable dans un corps du chiffre etc...

A cet effet, à la fin du Master il est proposé des thèmes de mémoire de fin de cycle. Chaque étudiant sera assisté pendant toute la période de travail par un encadreur qui le guide et le conseille pendant l'élaboration de son mémoire.

1.1. Problématique

Depuis quelques années, le contexte économique devient de plus en plus difficile, avec l'augmentation des applications, des serveurs et des postes de travail dans l'entreprise, l'administration et la gestion des infrastructures informatiques (serveurs, applications, réseau, ...) deviennent fastidieuses.

Ainsi pour être compétitif les entreprises semblent se diriger vers l'optimisation des ressources, l'augmentation de la flexibilité, la réduction des coûts, la sécurité et la diminution d'interruption des services. Ces aspects sont des points critiques jouant fortement sur la production. Il est très compliqué d'appliquer des stratégies de sécurités pour les machines physiques encore plus pour les nomades. Avec ces derniers, il est indispensable de protéger les données qui sortent de l'entreprise pour qu'en cas de vol ou de pertes du matériel, elles ne soient pas accessibles par des personnes mal intentionnées.

Beaucoup de solutions ont été mise en œuvre pour apporter des éléments de réponse aux problèmes sus mentionnés. On citera la virtualisation des serveurs et de réseau de stockages qui aident à limiter la prolifération des serveurs et des espaces de stockages, de simplifier l'administration, de réduire les couts des ressources et surtout de minimiser les besoins énergétique et de refroidissement (Datacenter). Les entreprises veulent dépasser ce stade de virtualisation des serveurs pour aussi passer à la virtualisation des postes de travail.

Mais l'avènement de toute nouvelle technologie est toujours lié à un certain nombre des problèmes notamment d'ordre sécuritaire; ce qui nous pousse néanmoins à nous interroger sur l'impact de la virtualisation sur le système d'information ou du parc informatique d'une entreprise ? En outre, les Datacenter ont-ils permit de créer un maximum de sécurité des données au sein d'une entreprises ? A ces questions se greffe une autre non moins importante : peut-on réellement affirmer que l'introduction des Datacenter dans le monde de l'entreprise a permis de révolutionner à celle-ci et de combler ses lacunes en matière de sécurisations des données informatiques ?

La virtualisation des postes de travail, des serveurs et des applications offre-t-elle la possibilité au directeur des systèmes d'information de relever le challenge en terme

d'efficacité ; de fiabilité, d'économie, de disponibilité, qualité de service et sécurisation des données ?

1.2. Objectifs de l'étude

Notre étude consiste à mettre en place une plateforme de virtualisation de poste de travail et de serveur contenu dans le **Datacenter** afin de permettre une gestion centralisée du parc informatique de l'entreprise, tout en permettant aux utilisateurs nomades de se connecter sur la plateforme via une authentification unique afin de récupérer les postes agents virtualisés via un coursier de connexion ou session Broker . Ses Utilisateurs ouvrent une session via leurs comptes créés dans le contrôleur de domaine pour s'authentifier à la plateforme de virtualisation à travers la session Broker et récupère le poste agents pour les différentes tâches.

Un concept uniformisé de la virtualisation n'est pas viable en ce qui concerne la sécurité; c'est pourquoi l'un des avantages de cette approche, c'est que les outils de sécurité peuvent être introduits selon les besoins. Cela contribue également à gérer les coûts.

1.3. Pertinence du thème

De nos jours l'activité de l'entreprise se résume directement sur des informations stockées sous forme numériques, et sur des systèmes informatiques et des réseaux de télécommunications chargés de mettre ces informations à la disposition des utilisateurs qui en ont besoin. A l'endroit et au moment où ils en ont besoin c'est-à-dire vingt-quatre heures sur vingt-quatre (24/24h) soit 365 jours par ans. S'ils ne peuvent accéder à ces informations et aux systèmes informatiques pour les traiter, les utilisateurs perdent tout pouvoir et l'entreprise s'arrête de fonctionner.

Si cette situation se produit, le cout sera astronomique. Il varie d'une entreprise à l'autre, mais en cas de l'immobilisation de toute l'entreprise, il peut se chiffrer à des dizaines de milliers, voire en millions de francs CFA pour chaque heure d'indisponibilité.

Pour faire face à ce problème des offres de collocation des espaces dédiés aux stockages sont apparus fournissant cette disponibilité appelés Datacenter.

D'où l'importance et le rôle essentiel d'un Datacenter pour fournir les informations et les services informatiques aux utilisateurs, à des niveaux de fiabilité stratégiques. Ces niveaux de disponibilités sont sans précédent dans le secteur de l'informatique commercial.

C'est pour cela que nous accordons une grande importance sur la virtualisation des serveurs, des postes de travail et des applications pour la réalisation de ce travail.

2. Approche Méthodologique

2.1. Délimitation du champ d'étude

La sécurisation du réseau de stockage et des applications contenues dans le Datacenter est un aspect de la sécurité informatique. Les problèmes que soulèvent ces dernières s'étendent à tous les points que traite la sécurité informatique ainsi que la télécommunication. Nous étudierons les aspects théoriques (*technologies, services, protocoles...*) et pratiques.

2.2. Difficultés rencontrées

Comme pour toute entreprise, la réalisation d'un projet nous pousse à être confronté à un certain nombre de difficultés qui ont plus ou moins rendu certaines tâches difficiles ou empêcher leur réalisation. Pour réaliser ce travail technique et scientifique, les outils sont d'une importance capitale si l'on veut produire des résultats. Nos principales difficultés étaient d'ordre matériel et logiciel. Mais nous avons pu trouver des compromis pour contourner certaines et arriver à produire ce travail.

DEUXIEME PARTIE : ETUDE

DEUXIEME PARTIE : ETUDE

1. Etude au préalable

L'objet de notre étude sur les Datacenter sera basée sur une plateforme de virtualisation car dans une infrastructure non virtualisée, plus de 70% du budget informatique type sont consacrés à la maintenance de l'infrastructure existante, ce qui laisse peu pour l'innovation. Alors qu'une infrastructure automatisée repose sur une plateforme de virtualisation éprouvée en production, permettant de répondre de façon efficace et rapide à l'évolution du marché, mais avant de rentrer dans le vif du sujet, il paraît important de s'intéresser d'abord sur la genèse de la virtualisation, car c'est n'est pas, aussi étrange que cela puisse paraître, une idée nouvelle, bien au contraire.

Nous détaillerons cela dans un premier temps. Dans un second temps nous allons nous consacrer à la définition des principaux termes en rapport avec la virtualisation afin de bien assimiler les principes de base.

Enfin nous clôturerons cette partie par un aperçu des buts de la virtualisation, nous verrons ainsi qu'il existe des nombreux avantages et bénéfices quant au déploiement d'une telle technique et cela suivant les différentes implémentations.

1.1. Etude sur les Datacenter

Ce sujet présente un intérêt considérable dans la mesure où au cours de la dernière décennie avec la généralisation de l'Internet, le développement des réseaux à haut débit, la location d'application, le paiement à l'usage et la quête sociétale de mobilité peuvent expliquer l'avènement des Datacenter. Celui-ci consiste en une interconnexion et une coopération de ressources informatiques, situées au sein d'une même entité ou dans diverses structures internes, externes ou mixtes. Et dont les modes d'accès sont basés sur les protocoles et standards Internet. Les solutions Datacenter reposent sur des technologies de virtualisation et d'automatisation. Trois caractéristiques clés du Datacenter le différencient de solutions traditionnelles:

- Services à la place de produits technologiques avec mise à jour en continu et automatiquement
- Mutualisation et allocation dynamique de capacité (adaptation élastique aux pics de charge). Vu des entreprises utilisatrices (du grand compte multinational à la PME locale), le Datacenter peut se définir comme une approche visant à disposer d'applications, de puissance de calcul, de moyens de stockage, etc. comme autant de « services ». Ceux-ci seront mutualisés, dématérialisés (donc indépendants de toutes contingences matérielles, logicielles et de communication), contractualisés (en termes de performances, niveau de sécurité, coûts...), évolutifs (en volume, fonction, caractéristiques...) et en libre-service.

- Consolidations des serveurs, plusieurs serveurs regroupés sur une seule unité de stockage.

Les machines, applications et données pourront être disséminées ou centralisées dans un, ou dans différents sites internes, chez des prestataires, dans un Datacenter situé à l'autre bout de la planète ou sur une myriade de serveurs appartenant à un même «Datacenter ».

1.1.1. Définition

La définition française du DATACENTER est : centre de traitement de données. Il se présente comme un lieu, où se trouvent des serveurs, des équipements électroniques et équipements de télécommunications.

Son but est de traiter les informations nécessaires aux entreprises. Concrètement, seules les entreprises moyennes et les grandes entreprises ont recours à de telles pratiques.

Il peut héberger plusieurs types de données et d'applications informatiques dans un environnement sécurisé. Il répond à des exigences et à un cahier des charges extrêmement stricts (normes : électrique, hygrométrique, accessibilité...).

2. Mécanisme de fonctionnement

2.1. Norme

Le DATACENTER doit être proche de points stratégiques. À proximité d'un point d'accès de très forte puissance électrique et d'un point d'accès de très forte bande passante en télécommunications. La conception des DATACENTER nécessite deux conditions principales : la haute disponibilité et une consommation électrique optimisée afin d'impacter au minimum la consommation en CO2.

2.1.1. CLASSEMENT DES DATACENTER

Une association américaine a créé une classification des DATACENTER pour en mesurer la fiabilité. Cette classification permettra de choisir au mieux le DATACENTER en corrélation avec ses exigences informatiques.

✓ Niveau 1 (Basic)

Désigne les DATACENTER n'ayant qu'une seule voie pour l'alimentation électrique et le refroidissement sans redondance des éléments ; son niveau de disponibilité est de 99,671 % (28,8 h/an d'indisponibilité).

✓ Niveau 2 (composants redondants)

Idem niveau un, mais ayant des éléments redondants (onduleurs, générateurs). Niveau de disponibilité 99,749 % (22 h/an d'indisponibilité).

✓ **Niveau 3 (maintenance de façon concurrente)**

DATACENTER plus évolué, il comporte plusieurs voies d'alimentation et de refroidissement. Les éléments sont doublés et la maintenance faite à chaud (sans interruption de service) la disponibilité est de 99,928 % (1,6 h/par an d'indisponibilité).

✓ **Niveau 4 (tolérance aux pannes)**

Le plus haut des niveaux, plusieurs voies actives en parallèle pour l'alimentation et le refroidissement. Des éléments d'infrastructure sont doublés et tolérants aux pannes. Disponibilité est de 99,995 % (24 mn/an d'indisponibilité).

En lieu et place de niveau un à quatre, on peut trouver la terminologie « ntiers un à quatre ». Quel niveau choisir en fonction de ses activités et de la sécurité ? La répartition par niveau est la suivante :

Niveau	1
Services informatiques en support sans SLA* (Industrie, administration, PME-PMI)	
Niveau	2
Services informatiques généraux avec des exigences d'interruption de service modéré. (Commerce, industrie, administration, PME-PMI)	
Niveau	3
Services informatiques de production avec des exigences de disponibilité importante. (Industrie, services télécoms, administration, santé, finance, université de recherche, service public exigeant)	
Niveau	4
Services informatiques de production nécessitant une haute disponibilité. (Multinationale, sécurité, Défense)	

*SLA : Service Level Agreement ; engagement que le DATACENTER prend envers son client pour lui assurer un service.

Il convient donc de bien choisir son DATACENTER en regard de ces exigences et de ces disponibilités. Outre les infrastructures du DATACENTER, il est nécessaire de bien étudier son niveau de sécurité.

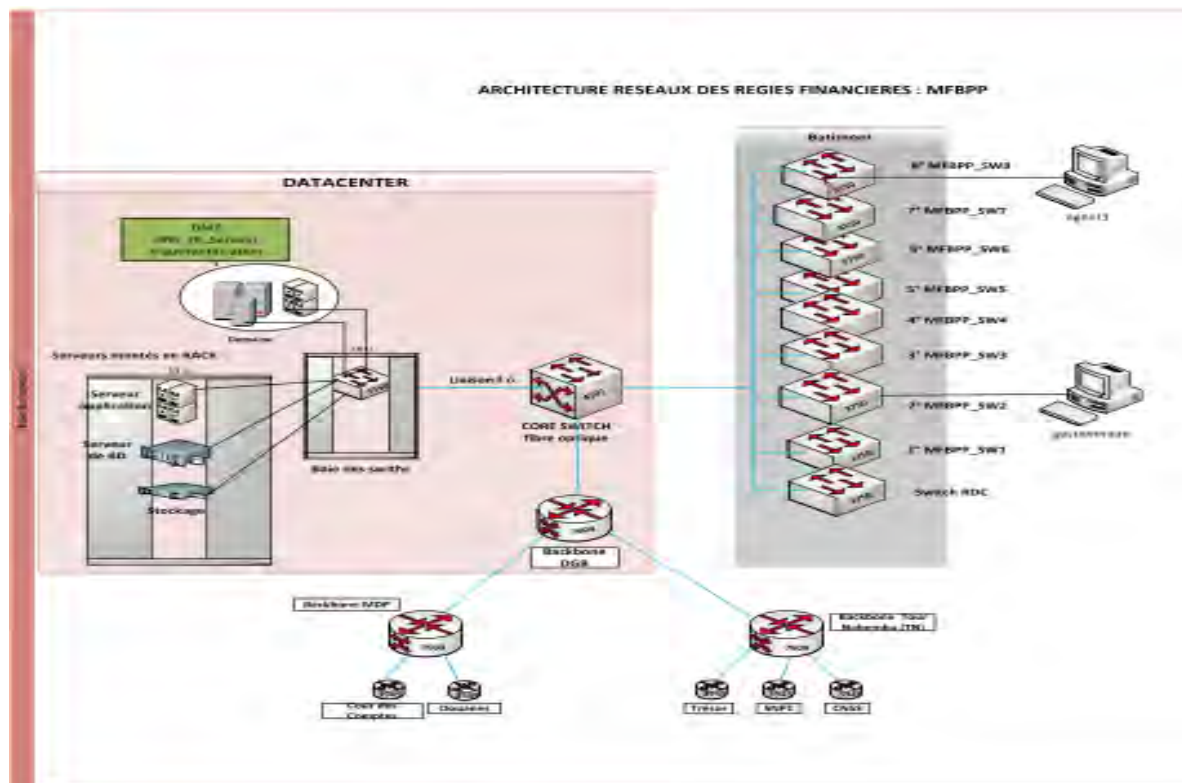


Figure 1 : Architecture réseau du Datacenter de la Régis de finances

3. Notion générale de virtualisation

3.1. Définition

La virtualisation est « l'ensemble des techniques matérielles et logicielles qui permettent de faire fonctionner sur une seule machine plusieurs systèmes d'exploitations ou plusieurs applications, séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes. Les outils de la virtualisation servent à faire fonctionner ce qu'on appelle communément des serveurs privés virtuels (Virtual Private Servers ou VPS) ou encore environnements virtuels (Virtual Environments ou VE) ».

Dans notre étude nous nous intéressons uniquement à la virtualisation de systèmes, basé sur des techniques principalement logicielles. Dans ce cas l'environnement matériel est complètement virtualisée au sein d'une machine virtuelle, afin qu'elle puisse accueillir un système d'exploitation complet.

Le logiciel qui permet de gérer la virtualisation s'appelle « **hyperviseur** » qui est la couche logicielle qui s'intègre entre le matériel et les différents systèmes invités. Il existe deux types d'hyperviseurs:

- ✓ **Hyperviseur de type 2** ou **architecture « hosted »** : dans ce système de virtualisation un système d'exploitation doit-être au préalable installé sur le matériel comme le montre la figure ci-dessous. Un système d'exploitation invité s'exécutera donc en troisième niveau au-dessus du matériel, les

systèmes d'exploitation invités n'ayant pas conscience d'être virtualisés (exemple VMware Player, Virtual PC et Virtual Box...).



Figure 2: hyperviseur de type 2

- ✓ **Hyperviseur de type 1**, ou **natif**, ou **para-virtualisation**, voire « **baremetal** » (littéralement "*métal nu*"), est un logiciel qui s'exécute directement sur une plateforme matérielle ; cette plateforme est alors considérée comme outil de contrôle de système d'exploitation. Un système d'exploitation secondaire peut, de ce fait, être exécuté au-dessus du matériel. L'hyperviseur de type 1 est un noyau hôte allégé et optimisé pour ne faire tourner initialement que des noyaux de systèmes d'exploitation invités adaptés et optimisés à cette architecture spécifique, ces systèmes invités ayant conscience d'être virtualités (exemple VMware ESX, Xen et Hyper-V, ...).



Figure 3: hyperviseur de type 1

3.2. But de la virtualisation

Tout d'abord, le premier but de la mise en place virtualisation au sein du système d'information (SI) d'une entreprise est bien entendu la réduction des coûts liés à l'achat des serveurs. Il n'est pas rare de trouver au sein d'un SI un serveur dédié pour telle fonction, un autre pour tel service de l'entreprise, pour des raisons aussi historiques que technologiques.

Avec la virtualisation, on peut ainsi avoir une machine physique regroupant un ensemble de machines virtuelles fonctionnant sous différents systèmes d'exploitation.

C'est d'autant plus vrai qu'une partie des serveurs sont sous employés. Le cas de serveurs WEB des Intranet des entreprises est le plus représentatif. Fonctionnant le

plus souvent environ 10 heures par jour, et cela, sans utiliser le maximum de leurs capacités, ces serveurs sont autant des ressources inexploitées.

En virtualisant par exemple trois serveurs Web sur un seul ordinateur, on économise au niveau de l'achat du matériel et cela permet de diminuer de façon négligeable la consommation électrique des Datacenter et climatisation associés. Un serveur fonctionnant à 15% ne consomme pas beaucoup plus d'énergie qu'un serveur pleine puissance.

Ensuite, la virtualisation peut fournir de nombreux services et faciliter grandement le quotidien des administrateurs. Lors des migrations de système, il est ainsi possible d'éviter le coûteux redéveloppement d'une application (nécessaire car le matériel était obsolète ou que la mise en place d'un nouveau système d'exploitation rendait l'application inutilisable) en virtualisant le système complet. De plus des environnements de tests ou de pré-production très fidèles à l'environnement futur peuvent être mis en place avec un minimum de ressources physiques. Dans le cadre de l'hébergement, Internet notamment, les hébergeurs ont la possibilité de fournir un système virtualisé en toute indépendance des autres machines virtuelles, les clients pouvant avoir un contrôle total sur le serveur virtuel (type de système d'exploitation, redémarrage, de la machine sans aucune restriction, etc.) la virtualisation s'avère très intéressante dans le domaine de la haute disponibilité. Grace à elle, il est possible de déplacer une machine virtuelle d'un serveur vers un autre (dans la maintenance, etc.) tout cela sans interruption des services. Des machines virtuelles peuvent aussi être activées lors de plan de secours.

Enfin, pour que la virtualisation prenne tout son sens, il faut absolument l'associer à une technologie de stockage partagé en réseau, SAN notamment, afin de profiter de tous les services possible (continuité de service, déplacement d machines virtuelles, etc.).

3.3. Différents types de virtualisations

Une fois convaincu de la nécessité de la mise en place d'une solution de virtualisation au sein d'un SI, encore faut-il choisir la technologie la plus appropriée à celui-ci. Car toutes solutions disponibles sur le marché offrent des approches différentes tant en terme de fonctionnalité qu'en terme de performance.

Il existe de nombreux types de virtualisation: d'application, de plate-forme, de réseau et de stockage. Généralement, quand quelqu'un mentionne la virtualisation, il fait référence à la virtualisation de plate-forme. Celle-ci correspond à l'utilisation de matériel serveur pour héberger plusieurs machines virtuelles invitées. La virtualisation s'applique aux différents composants du système d'information. On peut décliner le principe de virtualisation sur les composants de l'infrastructure informatique suivant :

✓ Virtualisation de la plateforme

Dans cette partie, nous explorerons plusieurs stratégies de virtualisation populaires et nous expliquerons comment chacune d'entre elles fonctionnent.

Le but est d'apporter des informations pratiques dont on aura besoin afin de prendre des décisions éclairées pour notre stratégie. Les logiciels de chaque éditeur ont tous leur propre interface (console), leurs méthodes de créer, d'importer et de modifier des machines virtuelles, et leurs propres idiosyncrasies, astuces et outils.

Cette partie nous offre un aperçu indépendant de l'éditeur, mais technique, des types de virtualisation disponibles. Nous approchons ces différents types à partir des applications et des performances. En d'autres termes, il s'agit d'une approche pratique de chaque technologie et de ce qu'elle implique pour nous. Chaque section inclut également au moins deux représentants de la technologie en question.

✓ Virtualisation d'applications

La virtualisation d'application est une technologie logicielle qui va permettre d'améliorer la portabilité et la compatibilité des applications en les isolant du système d'exploitation sur lequel elles sont exécutées. Elle consiste à encapsuler l'application et son contexte d'exécution système dans un environnement cloisonné. La virtualisation d'application va nécessiter l'ajout d'une couche logicielle supplémentaire entre un programme donné et le système d'exploitation; son but est d'intercepter toutes les opérations d'accès ou de modifications de fichiers ou de la base de registre¹ afin de les rediriger de manière totalement transparente vers une localisation virtuelle (généralement un fichier). Puisque cette opération est transparente, l'application n'a pas notion de son état virtuel. Le terme virtualisation d'application est trompeur puisqu'il ne s'agit pas de virtualiser l'application mais plutôt le contexte au sein duquel elle s'exécute (registres du processeur, système de fichiers, ...).

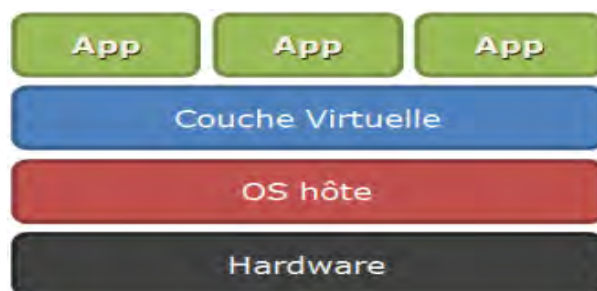


Figure 4 : virtualisation d'applications

La base de registre est utilisée par les systèmes Windows qui y renseignent les données de configurations du système d'exploitation et des autres logiciels installés.

Cette solution permet le **déploiement d'applications** sans intervention sur le système d'exploitation, ce qui rend leur suppression sans risque et propre. Il existe

trois approches populaires de virtualisation de serveurs: le modèle de machines virtuelles, le modèle de para-virtualisation et la virtualisation au niveau du système.

✓ Virtualisation de poste de travail (VDI)

La virtualisation de poste de travail est un terme relativement nouveau qui décrit le processus de séparation du bureau personnel (ses applications, fichiers et données) de la machine physique. Le bureau virtuel est stocké sur un serveur central distant plutôt que sur le disque dur de l'ordinateur personnel local. Cela signifie que lorsque les utilisateurs travaillent depuis leur bureau, tous les programmes, applications, processus et données utilisés par le bureau sont centralement conservés et exécutés, permettant aux utilisateurs d'accéder à distance à leurs postes de travail sur n'importe quel appareil capable d'afficher le bureau, tels qu'un PC classique, souvent peu puissant, recyclé pour ne faire que de l'affichage déporté, un ordinateur portable, un Smartphone ou client léger qui sont de petits terminaux démunis de disque dur. Cette solution banalise donc le poste de travail classique, ce qui fait que l'utilisateur retrouve tout son environnement de travail et ses données quel que soit le poste qu'il utilise en mode connecté ou pas.

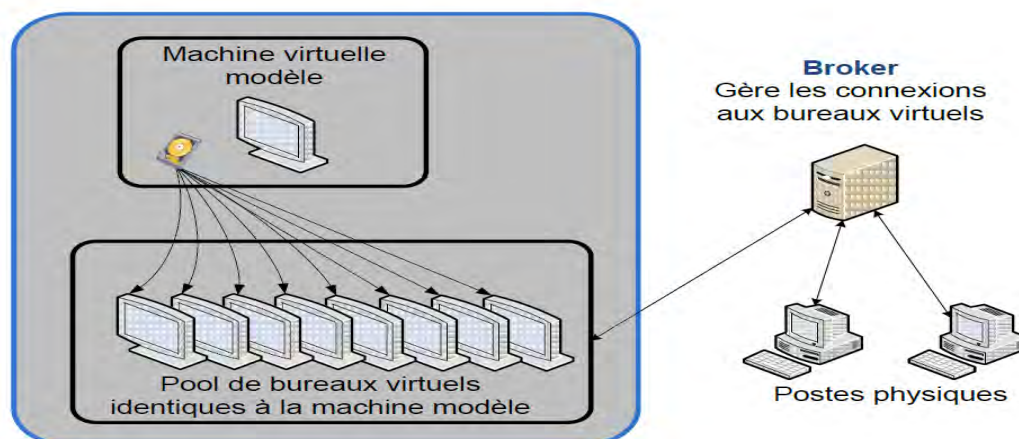


Figure 5 : virtualisation des postes de travail (VDI)

✓ La virtualisation des serveurs

La virtualisation des serveurs consiste à masquer les ressources du serveur, c.-à-d., le nombre et les caractéristiques de chaque machine physique, de chaque processeur et de chaque système d'exploitation pour les utilisateurs de ce serveur. L'administrateur du serveur va utiliser un logiciel grâce auquel il va diviser un serveur physique (constitué ou non de plusieurs machines distinctes) en plusieurs environnements virtuels isolés les uns des autres.

Ces environnements isolés sont parfois appelés serveurs privés virtuels, hôtes, instances, conteneurs ou émulations.

La plupart des serveurs sont sous-utilisés et achetés de façon massive afin de pouvoir disposer de plusieurs environnements par exemple ou encore isoler des données ou des espaces utilisateurs. La virtualisation de serveurs vient répondre à cette sous-utilisation des serveurs en permettant de regrouper sur une seule machine l'ensemble des applications tournant sur plusieurs serveurs tout en conservant une isolation entre celles-ci. Un autre avantage est de pouvoir assurer la continuité de service en transférant facilement les serveurs virtuels d'une machine physique à l'autre. Cette solution permet des **économies d'énergie** en diminuant le nombre de serveurs et ouvre la porte à l'informatique à la demande. La virtualisation de serveurs peut aussi être vue comme une méthode de partitionnement d'un serveur physique en plusieurs serveurs afin que chacun ait l'apparence de fonctionner sur sa machine dédiée, chaque serveur virtuel pouvant exécuter son propre système d'exploitation à part entière, disposer de ressources propres qui lui sont attribuées et chaque serveur pouvant être redémarré indépendamment. La virtualisation de serveurs s'inscrit dans une tendance globale qui tend à promouvoir la virtualisation au sein des entreprises en faisant notamment appel à la virtualisation de stockage et à la virtualisation de réseaux. Cette tendance est une composante dans le développement de systèmes autonomes. Un système est dit autonome si il est capable de s'autogérer sur base de l'activité qu'il perçoit, sans aucune intervention externe, et en conservant les détails de son implémentation invisibles pour l'utilisateur. La suite de ce document concerne plus particulièrement la virtualisation des serveurs.

✓ Virtualisation du réseau

La virtualisation du réseau consiste à combiner des ressources réseau matérielles et logicielles dans une seule unité administrative. L'objectif de la virtualisation du réseau est de fournir aux systèmes et utilisateurs un partage efficace, contrôlé et sécurisé des ressources réseaux. Le résultat de la virtualisation du réseau est un réseau virtuel. Les réseaux virtuels sont classés en deux grandes catégories : externes et internes. Les réseaux virtuels externes sont composés de plusieurs réseaux locaux administrés par le logiciel comme une entité unique. Les blocs de construction des réseaux virtuels externes standard sont le matériel de commutation et la technologie logicielle VLAN. Les réseaux virtuels externes comprennent par exemple les grands réseaux d'entreprise et les centres de données. Un réseau virtuel interne se compose d'un système utilisant des machines virtuelles ou des zones configurées sur au moins une interface pseudo-réseau. Ces conteneurs peuvent communiquer les uns avec les autres comme sur le même réseau local, fournissant un réseau virtuel sur un seul hôte.

✓ Virtualisation de stockage

La virtualisation de stockage, procédé aussi dénommé abstraction du stockage, c'est la mise en commun logique d'éléments de stockage qui étaient indépendants à l'origine. On peut rassembler dans un stockage virtuel des éléments dissemblables

(DAS, NAS, SAN...), provenant de constructeurs différents et utilisant des protocoles de gestion de fichiers différents. La virtualisation de stockage est donc une réponse à la gestion de la disparité des ressources de stockage : équipements, protocoles d'accès, environnements d'exploitation. Elle permet à tout client (serveur, application, poste de travail) d'accéder à tout équipement de stockage par tout protocole. D'une part, elle organise les ressources de stockage sous la forme d'une capacité unique, comme un disque de grande taille, qu'exploitent les applications, les serveurs et machines virtuels. D'autre part, elle distribue les données en mode bloc sur l'infrastructure de stockage. La virtualisation de stockage consiste à masquer la disparité des ressources de stockage, et à les présenter comme un volume logique homogène. Cette couche d'abstraction intermédiaire agit comme un courtier de capacité : elle fournit de l'espace de stockage aux applications, fait cohabiter des environnements hétérogènes dans une même représentation, permet l'adjonction de capacité à la volée, et laisse l'administrateur appliquer une politique unifiée de gestion des données. La suite de ce document concerne plus particulièrement la virtualisation des serveurs et stockage. C'est sur ce dernier type de virtualisation, d'actualité, que nous allons nous appesantir dans la suite de ce mémoire.

3.4. Différentes solutions de virtualisation

Les solutions de virtualisations présentes sur le marché sont assez nombreuses, diverse et variées. Il existe, comme nous l'avons vu précédemment, plus d'une dizaine de systèmes de virtualisation disponibles, que ce soit dans le monde de l'open-source ou dans le monde des éditeurs.

Dans le but d'être suffisamment concis et sans parti pris pour telle ou telle technologie, nous allons analyser les trois solutions les plus utilisées au sein des SI, selon *l'institut Gartner* à commencer par le leader du marché VMware avec ESX (89% de part de marché), puis Microsoft (7%) avec hyper-v, et nous terminons par Citrix (2%) avec XenServer. De plus, chaque éditeur dispose d'une offre globale liée à son hyperviseur fournissant une multitude d'outils variés aux fonctionnalités multiples. Chaque solutions dispose d'une solution de stockage SAN, que ce soit iSCSI ou Fiber Channel.

3.4.1. Solution VMware

Présent sur le marché de la virtualisation depuis la fin des années 1990 et leader actuel sur incontesté, VMware infrastructure trois, dispose en 4 versions (VMware ESXI standalone gratuit, VMware Infrastructure Fondation, VMware Infrastructure Standard, VMware Infrastructure Entreprise) et son hyperviseur associé, ESX.

L'hyperviseur ESX est un hyperviseur de type 1, s'exécutant directement sur le matériel et propose ainsi des machines virtuelles pour les systèmes invités. Elle repose sur une virtualisation complet, compatible avec la plupart des systèmes d'exploitation.

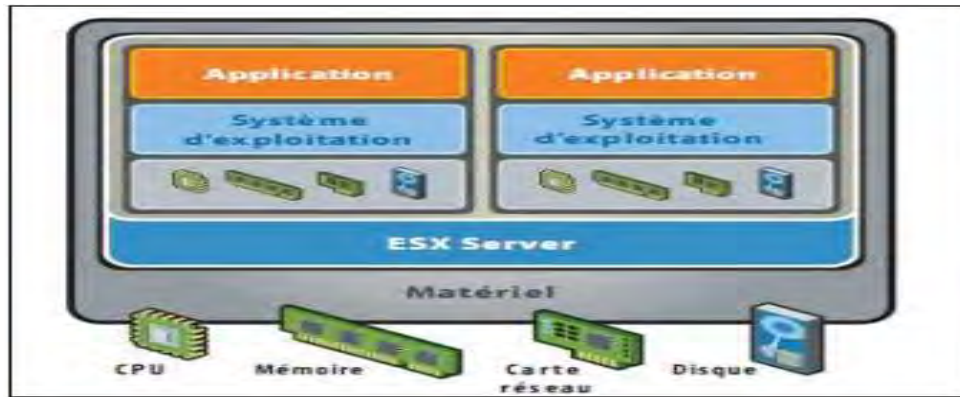


Figure 6 : Architecture ESX

Concernant la partie spécification technique, un serveur ESX est capable de faire tourner jusqu'à 128 machines virtuelles, d'allouer 64 Go de RAM et CPU physiques (soit 16 cœurs) par VM. Le serveur physique peut lui compter jusqu'à 128 Go de RAM et 32 cœurs.

Lié à l'hyperviseur ESX, VMware Infrastructure propose les services suivants :

- **VMFS** : système de fichiers en cluster très performant qui permet à plusieurs installations d'ESX Server d'accéder simultanément aux ressources de stockage d'une même machine virtuelle.
- **Virtual SMP** : améliore les performances des machines virtuelles en permettant à une seule machine virtuelle d'utiliser simultanément plusieurs processeurs physiques.
- **VMotion** : permet de migrer à chaud des machines virtuelles d'un serveur physique à un autre sans interruption.
- **VMware HA** : offre une haute disponibilité à l'ensemble de l'environnement virtualisé.
- **VMware DRS** : équilibre la puissance de calcul entre les pools de ressource et l'infrastructure virtuelle.
- **VMware Consolidated Backup** : permet de sauvegarder les machines virtuelles à partir d'un serveur Windows 2003.
- **VMware FT** : Cette option de Virtual Center consiste à créer un cluster de serveurs ESX, en les associant sous la forme d'un "Fault Tolerant Cluster". La technologie "LockStep" sur laquelle repose le cluster FT permet à la VM du serveur secondaire d'exécuter en parallèle la VM du serveur principal.

3.4.2. Solution Microsoft

Arrivé très tardivement sur le marché des solutions de virtualisation (la première version a été finalisée au début de l'été 2008), Microsoft et son hyperviseur hyper-v n'e demeure pas moins le deuxième virtualiseur utilisé dans les SI des entreprises. Inclus dans le nouveau système d'exploitation Windows server 2008, Hyper-v a de quoi séduire une partie des DSI.

Etant plus jeune que son concurrent VMware, la plupart des services offerts par Hyper-v sont éprouvés. Mais ceux-ci sont inclus dans les différentes offres (Hyper-v, hyper-v R2 et Windows server 2008 R2 Entreprise Edition et Datacenter) et nécessite pas d'achat de licence supplémentaires. L'hyperviseur hyper-v est un de type 1 fonctionnant en mode natif et en mode para virtualisation, mais cependant limité a peu de systèmes d'exploitation. Ainsi, hyper-v ne supporte que les OS suivants :

- Windows XP SP3 x86 et x64
- Windows Vista SP1 x86 et x64
- Windows Server 2000 SP4
- Windows Server 2003 SP3 x86 et x64
- Windows Server 2008 x86 et x64
- Suse Linux Entreprise Server 10 SP1 et SP2x86 et x64.

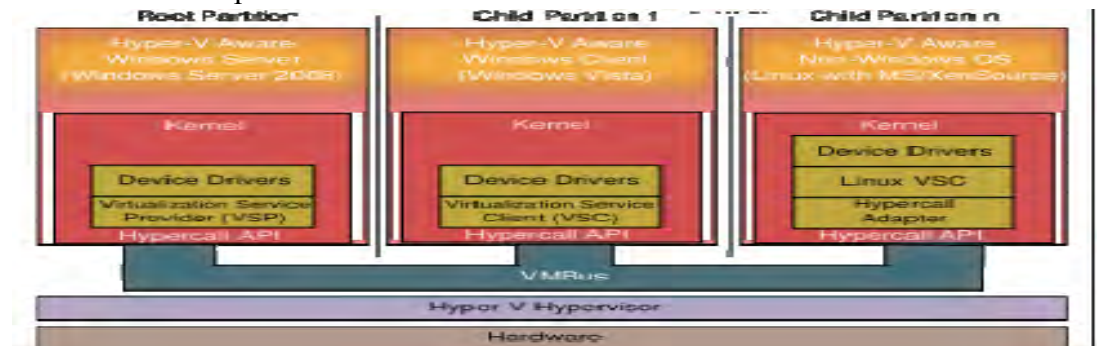


Figure 7: ARCHITECTURE MICROSOFT HYPER-V

Mais il est important de noter que tout cela reste théorique, et bien loin de l'utilisation « typique » d'un server virtuel.

Comme pour ESX, Hyper-v offre les services suivants :

- **FailoverClustering** : Haute disponibilité des machines virtuelle en cas de panne d'un host, les machines sont relancées sur un host survivant.
- **Live Migration** : permet le déplacement des machines virtuelles d'un host a un autres sans arrêt de service et cela au sein d'une famille de processeurs
- **Updated Hyper-V configuration Utility** : cet utilisateur permet de simplifier la configuration hyper-v. Les nouvelles de configurations incluent :
 - La configuration à distance.
 - Configuration des clusters
 - Outils de mises à jour supplémentaires.
 - Et bien sûr, allocation dynamique des ressources (CPU, RAM).

3.4.3. Solution Citrix

La solution Citrix, XenServer, est basée sur Xen, un hyperviseur de machine virtuelle, issu de la communauté open-server, récupéré lors de l'achat de XenServer en 2007. Il a été développé, dans un premier temps, par l'université de Cambridge au

Royaume-Uni en 2001. De plus, Xen est activement soutenu par une vingtaine de grandes entreprises dont AMD, HP, Intell et Novell.

XenServer 5, est proposé en quatre versions (Express qui est gratuit, Standard, Entreprise et Platinum). Même si il parait plus jeune qu'ESX et plus mature qu'Hyper-V, XenServer n'en demeure pas moins un concurrent sérieux de par les services fournis.

XenServer est un hyperviseur de type 1, s'exécutant directement sur le matériel et propose ainsi des machines virtuelles pour les systèmes invités. La technologie utilisée par XenServer repose sur la para virtualisation (non compatible avec les systèmes dits fermés) ainsi qu'un mode virtualisation complète ou HVM (mais qui nécessite les technologies Intel VT ou AMD-V pour les systèmes Microsoft). Il est ainsi possible de virtualiser la plupart des systèmes d'exploitation. De plus, le partenariat de Citrix avec Microsoft permet notamment le support de Windows Server 2008 en tant qu'OS invité.



Figure 8:Architecture Citrix XenServer

A l'instar d'ESX ou d'Hyper-V, XenServer dispose d'une gamme étendue de services :

- **XenMotion**: permet le déplacement de machines virtuelles à chaud et sans interruption.
- **Xen Center** : interface à l'administration, à l'infrastructure et aux processus existants.
- **Xen API** : intégration, à l'infrastructure et aux processus existants.
- **Citrix Essentials for XenServer and Hyper-V** : offre un ensemble de fonctionnalités de gestion et d'automatisation qui étend les capacités de Citrix XenServer et de Microsoft Hyper-V.
- Et bien entendu, des fonctionnalités de continuité de services (haute disponibilité automatique et reprise après sinistre).

3.5. Etude comparative et choix de la solution de virtualisation

3.5.1. Etude comparative

Nous venons de terminer notre tour d'horizon sur les différentes solutions de virtualisations, au travers trois principaux systèmes les plus utilisés au sein des

DSI. Le premier point commun est sans doute le fait que les hyperviseurs soient tous de type 1, en directe avec le matériel pour des meilleures performances.

Deuxièmement, tous utilisent une technologie de virtualisation complète et de para-virtualisation, ce qui leur permet d'accueillir la plupart des systèmes d'exploitation en tant qu'invités mais c'est à partir de là que la différence commencent à émerger.

De ce fait, le choix d'un système de virtualisation adapté à ses besoins, apparaît assez complexe. Chaque solution possédant ses points forts et ses points faibles.

Pour essayer d'éclaircir un peu tout cela, nous pouvons dans un premier temps nous baser sur le classement pour l'année 2008 effectué par *l'institut Gartner* qui a publié le tableau ci-après, regroupant plusieurs critères de sélections des cinq premières solutions de virtualisation du marché. Ainsi le leader du marché (VMware) possède tous les atouts pour être retenu par la plupart des DSI. Sauf peut-être le prix.

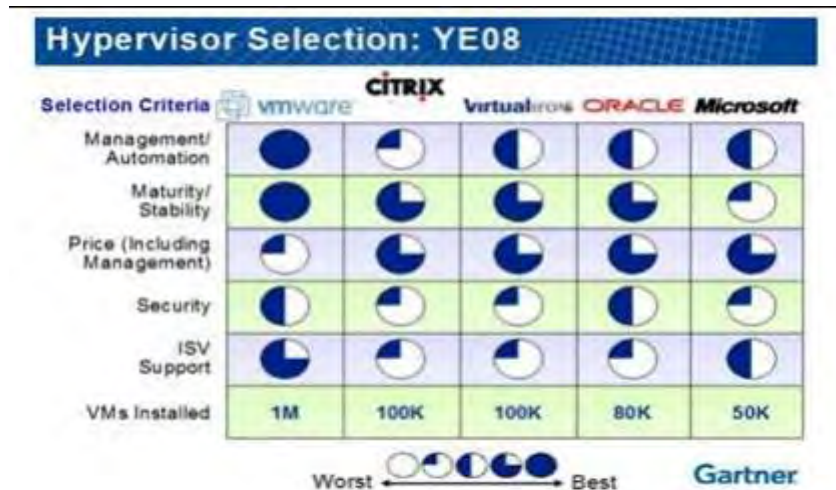


Figure 9: Solutions de Virtualisations 2008

Dans un second temps nous pouvons aussi nous appuyer sur ce comparatif technique regroupé dans le tableau ci-dessous.

	VMware ESX3.5	Microsoft Hyper-V R2	Citrix XenServeur5.0
Over Head	5 à 10%	inconnu	2 à 5%
Type d'hôtes invités	Quasiment tous	Tous les systèmes Microsoft et uniquement Suse Linux Entreprise server	Quasiment tous
Compétences requises	Connaissance Unix de base	Compétences Microsoft	Connaissance Unix
Nombre maximum	32	64	32

de cœurs			
Quantité de RAM maximale		1To	128 Go
Nombre de VM	128	>384	Illimite
Nb/RAM par VM	16 cœurs/64 Go	Illimite	8 cœurs /32 Go

Tableau 1:comparatif technique pour les hyperviseurs de type1

MICROSOFT		VMWARE		
Version	Prix liste	Version	Prix liste pour 1 processeur. 1 an support gold	Avec 3 ans support Gold/platinum
Standard (1 vm)	\$999 (includes 5 CALs)	Standard	1068\$	1491\$/1618\$
Enterprise (jusqu'à 4vm)	\$3999 (includes 25 CALs)	Advanced	2717\$	3448\$/3675\$
Datacenter (nombre de vm illimités)	\$2999 (per socket)	Enterprise	3479\$	4415\$/4708\$
Itanium	\$2999 (per socket)	Enterprise plus	4229\$	5366\$/5723\$
Web Server	\$469 (no CALs required)			
Storage Server	TBD			
Compute Cluster Server	\$469 (per node)			

Tableau 2: Comparatifs sur le coût entre MICROSOFT et VMware**3.5.2. Choix de la solution de virtualisation**

Eu égard à ce qui précède notre choix c'est porté sur la technologie VMware bien que couteux par rapport à Microsoft, mais il reste néanmoins le leader incontesté dans ce domaine avec une technologie de pointe éprouvé en production et largement avancé par rapport aux autres.

Cependant la pénétration de la virtualisation dans des entreprises de toutes de tailles confondues est seulement entre 15 et 20 % ce qui représente un marché colossale à conquérir et notamment les PME qui n'ont pas beaucoup virtualisé principalement pour des raisons de prix des licences VMware.

3.6. Solution de stockage

Le développement du commerce électronique, des datawarehouses ainsi que l'augmentation du nombre d'applications au sein des entreprises, notamment celles liées à la gestion de la relation client, sont autant de facteurs qui contribuent à l'accroissement exponentiel du volume des données et alourdit le réseau de l'entreprise. Pour répondre aux besoins de stockage considérables qui en découlent, des solutions apparaissent à un rythme soutenu, dans un secteur, celui du stockage, en pleine explosion. Nombre d'acteurs de l'industrie informatique, jusque-là présents sur d'autres segments, abordent ce marché fort en perspectives de profits importants à moyen et long terme. A l'heure actuelle, plus de 95% de tous les systèmes de stockage informatiques, tels que les disques durs, les systèmes AID, etc., sont directement reliés à des ordinateurs clients à travers divers adaptateurs SCSI, Fibre Channel, ou autres. Ce type de stockage, ou attachement direct, est généralement

appelé DAS (Direct Attached Storage). Toutefois, la tendance à la consolidation des données ainsi que les besoins croissants d'un accès plus rapide à ces dernières dans les réseaux d'entreprises a conduit au développement de deux architectures de stockage: les serveurs de stockage en réseau, ou NAS (Network Attached Storage), et le SAN (Storage Area Network).

3.6.1. Architecture centralisée: Les problèmes.

Plusieurs problèmes se posent lorsque l'on centralise les données. L'intérêt de la centralisation devient un piège pour la gestion et l'administration : le volume des données augmente et nécessite une sécurité accrue.

De plus une haute sollicitation d'entrée et sortie nécessite une technologie avancée à tous les niveaux (CPU, bus, accès disques, transferts bandes).

Mais ce n'est pas tout, les applications deviennent critiques et sensibles du fait de la centralisation et la sauvegarde est rendue difficile car les Batch augmentent et la fenêtre de sauvegarde diminue, sans oublier bien sûr que la production est de 24h/24.

3.6.2. L'architecture classique

Le modèle classique couramment mis en place dans les organisations informatiques est né de l'assemblage d'un nombre de serveurs et machines personnelles connectées par le réseau. Des postes de travail individuels ont trouvé grâce à la connexion sur le réseau, la possibilité de mettre en place l'échange de données et le travail coopératif.

Un tel réseau est représenté par la figure suivante.

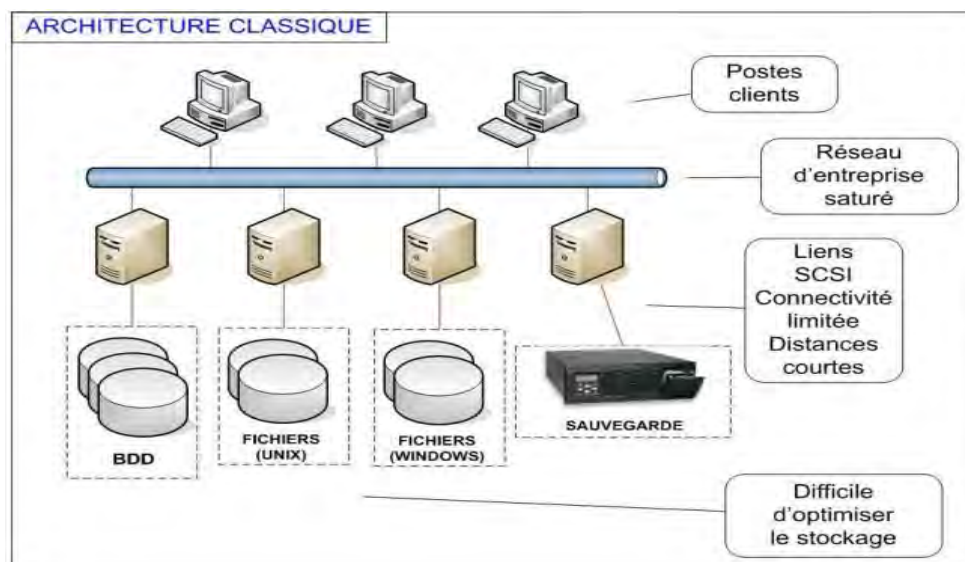


Figure 10: Architecture DAS

Le réseau s'est étendu, mais les principes qui régissent les échanges de données restent identiques. Les données sont stockées sur disque dur, l'accès à ces données est piloté par le serveur local. Les partages ou échanges de données entre les machines, est basé sur un protocole client/serveur (NFS ou FTP). Sollicité par un

client, le serveur est le passage obligé de tous les flux concernant ses espaces disques locaux. Le débit du réseau devient rapidement un point sensible de l'architecture, mais ce n'est pas le seul. Le protocole SCSI limite le nombre de périphériques connectés, les performances de la machine hôte et les applications hébergées ont un impact direct sur les performances des entrées/sorties. Une panne de la machine, entraîne l'indisponibilité des données. On peut aussi ajouter que cette topologie, en favorisant le morcellement des espaces, rend difficiles les évolutions (en volume ou en débit). Cette architecture a tendance à être limitée aux configurations de taille réduite. L'évolution naturelle de cette topologie est le serveur de fichiers. Elle consiste à dédier un gros serveur aux fonctions de stockage. Les aspects spécifiques sont développés sur ce serveur pour une meilleure efficacité et un meilleur service. Chaque machine réserve la totalité de ses ressources aux applicatifs qu'elle héberge. La fonction de gestion de données, centrée sur un tel serveur, permet une économie de moyens (matériels et humains) et un service plus souple et plus efficace. On doit veiller cependant à soigner particulièrement les aspects débits– réseaux, ...

Dans cette configuration, on tire les avantages classiques d'une solution centralisée :

- Une réponse efficace à l'augmentation des besoins en espace disque.
- Mise en place plus avisée de la sécurité.
- Intégration de matériels fiables (comme des éléments matériels redondants, la technologie AID).
- Le partage des données est aisé.

Cependant, du choix de la configuration dépendront directement les performances des entrées/sorties, les possibilités d'extension, la sécurité des données. Des moyens matériels appropriés doivent être intégrés afin d'assurer la meilleure disponibilité des données, le serveur. Il devient un point central de l'architecture, et indispensable à la bonne marche des applications.

3.6.3. Solution NAS

Un NAS ou Network Attached Storage (Serveur de stockage en réseau) désigne un périphérique de stockage (généralement un ou plusieurs disques durs) relié à un réseau par un protocole de communication tel que TCP/IP par exemple.

3.6.3.1. Principe

Un NAS définit un produit spécifique possédant sa propre adresse IP (statique) et directement connecté au réseau local de l'entreprise. Par conséquent, l'installation d'un matériel de ce type ne nécessite pas la mise en place d'une infrastructure spécifique ce qui est un avantage en terme de coût, de temps et de mains d'œuvre surtout pour les PME / PMI. Grâce à l'utilisation de son propre système d'exploitation et de deux systèmes de fichiers, les serveurs de stockage en réseau NAS permettent le partage d'un même fichier entre de multiples serveurs et clients

dans un environnement hétérogène, sous Windows NT/95/98/2000/2008, Novell, Netware, Apple ou bien encore les systèmes basé sur UNIX. L'utilisation d'un NAS est adaptée aux applications faisant appel au service de fichiers comme l'hébergement de sites WEB ou encore les serveurs de fichiers ou de messagerie.

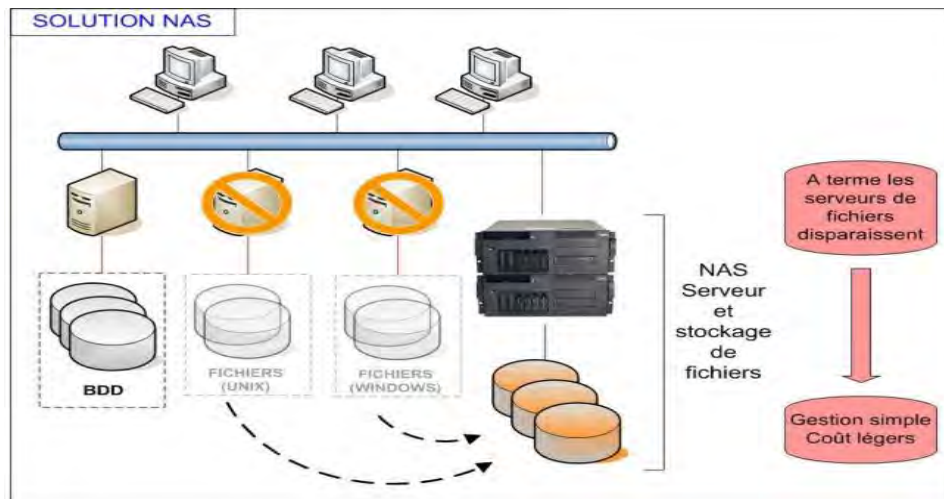


Figure 11: Schéma d'une architecture possible NAS

Les serveurs de fichiers tendent à disparaître au profit des NAS, plus simples à sauvegarder, plus adaptables aux besoins et plus facilement administrable. De plus, un seul serveur de stockage est maintenant nécessaire puisque les NAS supportent plusieurs types de système de fichiers.

La mise en place d'une solution NAS ne nécessite pas l'achat de beaucoup de matériel et reste abordable pour une PME ou PMI. Comme dit auparavant, les serveurs de stockage NAS sont connectés directement à une infrastructure réseau existante de type LAN ou WAN.

Le plus souvent présenté sous sa forme «rackable», le type de NAS le plus « simple » contient des disques durs IDE (4 pour le basic dont la taille varie) et il est muni d'une ou deux interfaces réseaux (J-45). Il suffit alors d'alimenter le NAS, le connecter au LAN, par exemple, et de lui donner une adresse IP statique afin de le rendre opérationnel.

Une interface WEB permet alors à l'administrateur du réseau de créer de nouveaux partages réseaux accessibles par les utilisateurs et les serveurs possédant les droits nécessaires sur le système de fichiers.

L'utilisation du NAS permet de limiter le risque de perturbation des tâches cruciales qui étaient auparavant servies par la même machine que le serveur de fichiers.

3.6.4. Solution SAN

Un SAN (Storage Area Network) est un réseau spécialisé permettant de partager de l'espace de stockage à une librairie de sauvegarde et à des serveurs.

3.6.4.1. Principe

Basé sur la Fibre Channel, topologie indépendante et multicouches fonctionnant en série et se comportant exactement comme une liaison téléphonique, le SAN est un réseau de stockage ouvert et évolutif qui relie, à des périphériques de stockage, des serveurs, stations et postes de travail, par ailleurs reliés au réseau d'entreprise.

Le SAN constitue une plate-forme de communication qui exploite les protocoles SCSI sur des technologies d'interconnexion à haut débit. Il virtualise totalement l'espace de stockage et travaille au niveau des blocs (et non des fichiers comme les serveurs NAS); ceci permet le partage centralisé des données via des "switches" intelligents Fibre Channel.

Pour information, les SAN peuvent ainsi être connectés à des milliers de serveurs pour constituer des systèmes de calcul évolutifs et surpuissants présents au sein des laboratoires de recherche dans les domaines industriels, environnementaux, militaires, financiers,...

Un SAN se différencie des autres systèmes de stockage tel que le NAS par un accès bas niveau aux disques. Pour simplifier, le trafic sur un SAN est très similaire aux principes utilisés pour l'utilisation des disques Internes (ATA, SCSI). C'est une mutualisation des ressources de stockage. Dans le cas du SAN, les baies de stockage n'apparaissent pas comme des volumes partagés sur le réseau. Elles sont directement accessibles en mode bloc par le système de fichiers des serveurs. En clair, chaque serveur voit l'espace disque d'une baie SAN auquel il a accès comme son propre disque dur. L'administrateur doit donc définir très précisément les LUN (unités logiques) et le zoning, pour qu'un serveur Unix n'accède pas aux mêmes ressources qu'un serveur Windows utilisant un système de fichiers différent.

3.6.4.2. Architecture

Les SAN sont bien adaptés aux applications demandant un stockage dédié, comme les bases de données, qui demandent une mise à jour permanente, et le traitement des transactions en ligne (OLTP).

Il y'a encore peu de temps on ne trouvait des SAN que dans les grands centres informatiques de société ayant besoin d'un grand volume de stockage très sécurisé. Les prix devenant plus raisonnable, des centres informatiques plus modestes s'équipent d'architectures SAN plus simples (tel que représenté dans le schéma ci-dessous).

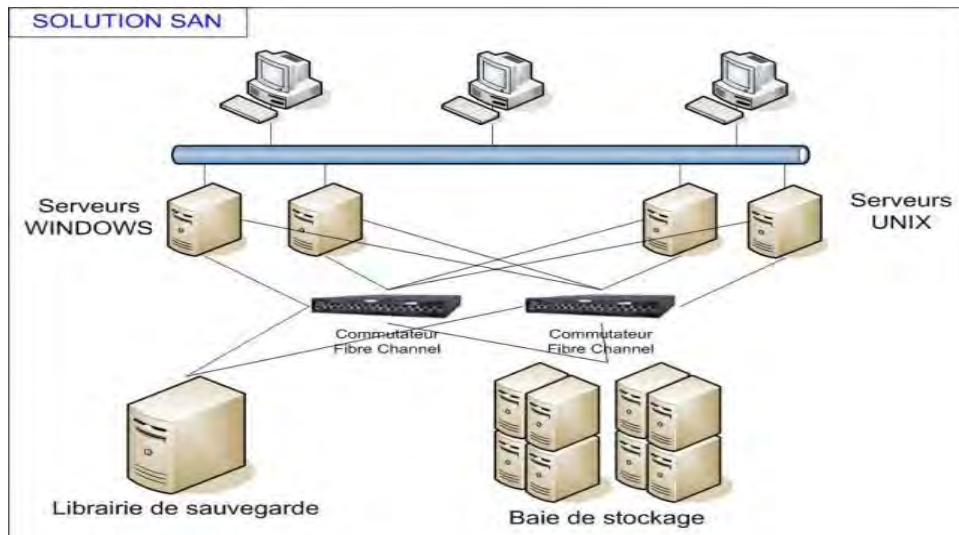


Figure 12: Architecture complexe du SAN (topologie fabric)

Un site plus grand mettra en place une architecture plus complexe, composée de plusieurs SAN reliés entre eux. Chaque SAN pouvant être équipé d'un grand nombre de baies de disques.

Cette architecture (figure ci-dessus) est basée sur la constitution d'un réseau performant dédié aux entrées/sorties avec les périphériques de stockage. Ce réseau est totalement indépendant du réseau classique. Les données sur disques ou bandes sont accessibles via le réseau dédié, déchargeant ainsi le réseau local.

3.6.4.3. Constitution du réseau SAN

Le réseau SAN est basé sur le protocole Fibre Channel (FC). Le SAN est un réseau sur lequel sont connectés des serveurs et des périphériques de stockage. Chaque serveur peut accéder à chaque périphérique.

La majorité des SAN sont basés sur un réseau de transport en fibre optique, mais on peut aussi utiliser le cuivre. Les standards FC définissent une architecture en couches FC0-FC4. Les couches FC0 et FC1 transportent les données, FC4 établit l'interface entre FC et les applications.

Le protocole utilisé pour le transfert des données est le SCSI série (SCSI-3).

L'implantation actuelle autorise des débits de 100Mo/s, des distances jusqu'à 10 Km, et des centaines (voire des millions suivant la topologie) de périphériques sur un même réseau.

Trois topologies ont été définies :

–La topologie «*point à point*» : c'est la topologie la plus simple qui relie deux entités. Dans ce cas se sont un serveur et une unité de disques. Les deux entités ainsi reliées disposent de la totalité de la bande passante.

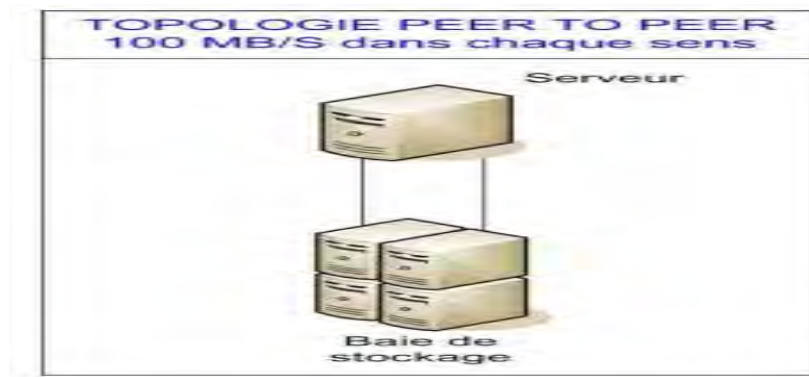


Figure 13: Baie de stockage de la Topologie Peer to peer

Les configurations «point à point» sont souvent les plus anciennes. Le protocole était alors limité à 25Mo/s à cause des performances des serveurs et des disques. Les configurations «point à point» sont encore tout à fait adaptées à des environnements simples, bien que l'augmentation des débits, et le développement des switches FC aient favorisé l'émergence des deux autres topologies.

– La boucle arbitrée: c'est la topologie la plus fréquente. Elle est moins limitée que la topologie «point à point», et moins onéreuse que la topologie «Fabric».

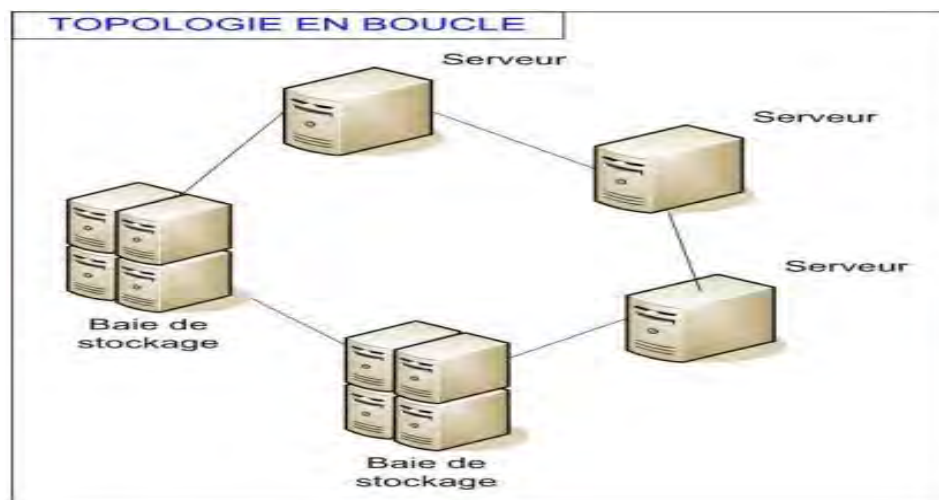


Figure 14: Baie de stockage de la Topologie en Boucle 1

Les premières boucles ont été réalisées comme l'indique la figure ci-dessus. Si un composant est défaillant, la boucle est cassée et les composants de la boucle sont hors circuit.

Les boucles sont actuellement réalisées à l'aide d'un hub qui réalise une topologie en étoile pour une configuration en boucle. Ceci permet de mettre hors circuit un élément défaillant sans casser la boucle.

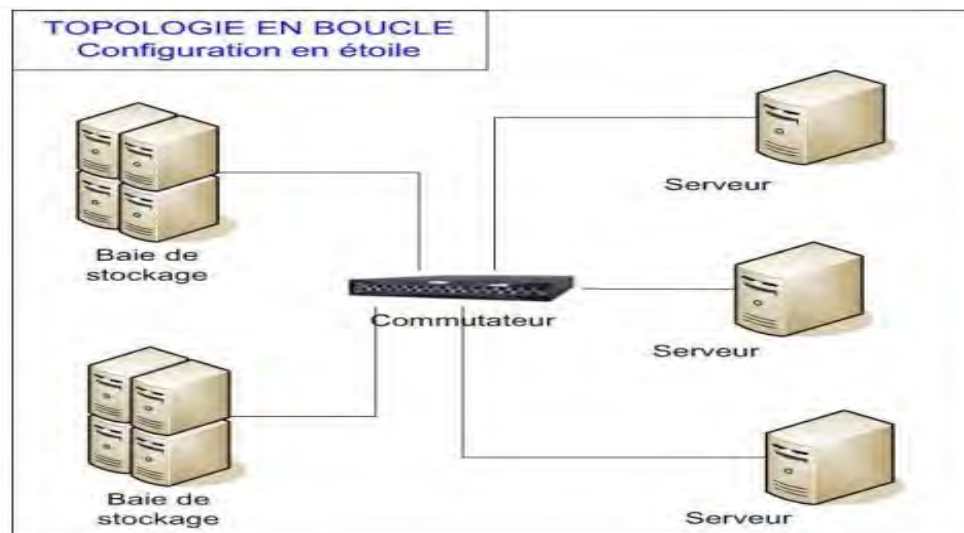


Figure 15: Baie de stockage de la Topologie en Boucle 2

Cette topologie est assez souple. Elle permet la connexion de 126 périphériques. Elle est relativement peu coûteuse, mais impose le partage de bande passante.

La topologie «fabric»: dans une telle configuration, les éléments du SAN sont reliés entre eux par un ou plusieurs switches. Dans ce cas, chaque port a un débit de 100Mo/s et chaque serveur accède aux données stockées sur le disque. Il peut également accéder aux lecteurs de bandes.

On peut aussi réaliser des combinaisons de ces configurations: des topologies fabric en connectant plusieurs switches en cascade et des boucles arbitrées sur une ossature fabric.

3.6.5. Avantages et inconvénients

	NAS	SAN
Disponibilité	Données accessibles en permanence	Données accessibles en permanence par n'importe quel serveur du réseau
Interopérabilité	Système supporte plusieurs os	Partage des données milieux hétérogènes
Fiabilité	Architecture interne équipée de dispositifs redondants	Architecture interne conçue contre les risques de panne totale ou partielle
Evolutivité	Capacité pouvant atteindre plusieurs téraoctets	Capacité pouvant atteindre plusieurs téraoctets
Simplicité	Mise en œuvre rapide	Conception et installation nécessitant souvent présence d'un expert
Administration	Centralisation sur le poste de l'administrateur	Centralisation sur le poste de l'administrateur
Sécurité	Accès par mot de passe	Réplication local ou

		distant
Ouvert	Facilité d'intégration et de migration	
Performance	Vitesse suivant le débit du réseau local en place	Risque de saturation faible débit (200Mo/s)

Tableau 3: Différences essentielles entre le SAN et le NAS**3.6.6. Vue générale de niveau NAS et SAN**

NAS	SAN
Orienté fichiers	Orienté paquets SCSI
Basé sur le protocole Ethernet	Basé sur le protocole fibre Channel
Conçu spécifiquement pour accès client général	Le stockage est isolé et protégé de l'accès client général
Support des applications client dans un environnement NFS/CIFS hétérogène	Support des applications serveur avec haut niveau de performance SCSI
Peut être installé rapidement et facilement	Le déploiement est souvent complexe

Tableau 4: Vue générale des niveaux NAS et SAN**3.6.7. Comparatif entre NAS et SAN**

	NAS	SAN
Fonction Principale	Serveur spécialisé qui sert les fichiers et les données stockées et aux autres serveurs à travers le réseau	Le stockage est accessible à travers le réseau qui lui est spécialement dédié. Sa principale fonction est de fournir au serveur un stockage consolidé basé sur la fibre Channel
Application bien adaptée	Idéal pour servir les fichiers	Idéal pour les bases des données et le traitement des transactions en ligne
Transfert des données	A travers un LAN et un WAN	A travers le SAN vers un serveur vers un LAN ou un WAN
Ressources de stockage et de sauvegarde	Les sauvegardes peuvent être attachées directement à des Appliance NAS intermédiaires ou être un LAN ou un WAN	Les ressources de stockage et de sauvegardes peuvent être attachées directement au serveur ou à travers une structure Fibre Channel
Disponibilité	Des alimentations et des ventilateurs redondants sont couramment utilisés	Des composants matériels et logiciels redondants donnent au système une haute disponibilité. Le système peut être configuré sans le moindre point de panne
Scalabilité	Plusieurs serveurs NAS peuvent être ajoutés au	Le stockage peut être étendu par l'ajout des

	réseau, et du stockage peut être aux serveurs NAS intermédiaires	switches Fibre Channel et de dispositifs de stockage
Réseau	Réseau d'entreprise existant (Ethernet, FDDI,...)	Réseau spécialisé Fibre Channel
Fonction des unités de stockage	Serveur de fichiers, gestion multi-protocole	Serveur de ressources de stockage. Aide à la protection, partage et mouvement de données.
Protocole d'échange	Type messages: TCP-IP	Type canal d'entrée/sortie SCSI
Bande passante	Liée au réseau existant	Liée à la vitesse du média Fibre Channel
Administration du stockage	Le stockage est administré à travers le serveur	Administration directe, incluant l'infrastructure SAN

Tableau 5: Comparatif entre NAS et SAN

3.7. Architecture VMware du Datacenter et ses différents modes d'accès

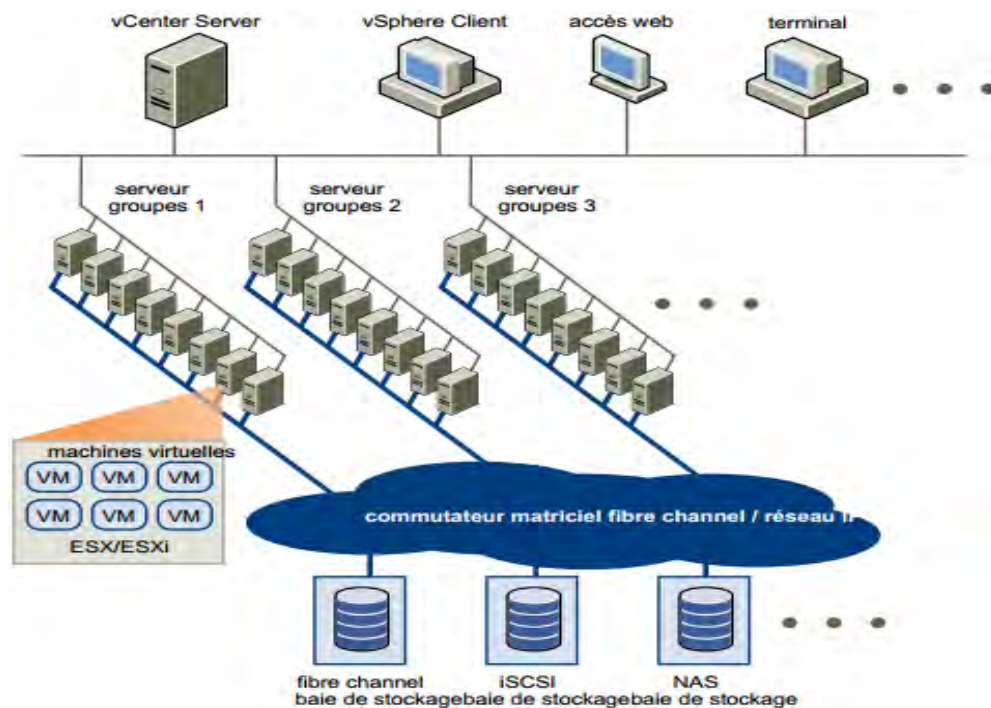


Figure 16: Architecture du Datacenter

3.7.1. Présentation de la solution de virtualisation des serveurs et poste de travail avec VMware

3.7.1.1. VMware vSphere ESXi

Grâce à la virtualisation, améliorez l'efficacité et la disponibilité de vos ressources et applications informatiques. Commencez par abandonner l'ancien modèle « un

serveur, une application » et exécutez plusieurs machines virtuelles sur chaque machine physique. Allégez la tâche de vos administrateurs informatiques, qui passent plus de temps à gérer les serveurs qu'à innover. Dans un Datacenter non virtualisé, près de 70 % d'un budget informatique type sont consacrés à la simple maintenance de l'infrastructure existante, ce qui laisse peu pour l'innovation.

Un Datacenter automatisé, reposant sur la plate-forme de virtualisation VMware, éprouvée en production, vous permet de répondre de façon plus efficace et plus rapide à l'évolution du marché. VMware vSphere fournit les ressources, les applications et même les serveurs nécessaires, quand vous en avez besoin et là où vous en avez besoin. Généralement, les clients VMware réduisent leurs coûts informatiques globaux de 50 à 70 % en consolidant leurs pools de ressources et en distribuant des machines hautement disponibles grâce à VMware vSphere.

Les composants et l'architecture globale d'ESXI sont conçus pour garantir la sécurité du système ESXI entier.

Sous l'angle de la sécurité ESXI comprend trois composants principaux : la couche de virtualisation, les machines virtuelles et la couche réseau virtuelle.

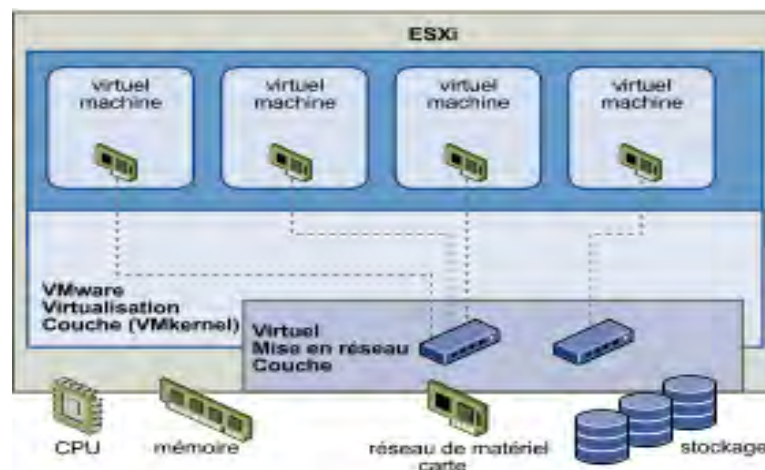


Figure 17: Architecture ESXI

3.7.1.2. Description des différents composants de VMware View

✓ View Connection Server

Ce service logiciel agit comme un broker pour les connexions client. View Connection Server authentifie les utilisateurs via Windows Active Directory et dirige la demande vers la machine virtuelle appropriée, le PC physique ou lame, ou le serveur Windows Terminal Services. View Connection Server fournit les fonctions de gestion suivantes :

- L'authentification d'utilisateurs ;

- L'autorisation d'utilisateurs sur des postes de travail et des pools spécifiques
- L'attribution d'applications fournies avec VMware ThinApp à des postes de travail et des pools spécifiques ;
- La gestion des sessions de postes de travail locales et distantes;
- L'établissement de connexions sécurisées entre utilisateurs et postes de travail ;
- L'activation de l'authentification unique ;
- La définition et l'application de règles.

✓ **View Client**

Le logiciel client pour accéder à des postes de travail View peut s'exécuter sur une tablette, un PC ou un ordinateur portable Windows, Linux ou Mac, un client léger, etc. Les utilisateurs exécutent View Client pour :

- se connecter à View Connection Server ou à un serveur de sécurité ;
- se connecter à leur poste de travail View dans le Datacenter ;
- modifier la liste de serveurs auxquels ils se connectent.

Installez View Client ou View Client with Local Mode sur chaque périphérique. Chacun d'entre eux doit fonctionner sur un système d'exploitation pris en charge ;

✓ **View Agent**

Vous installez le service View Agent sur l'ensemble des machines virtuelles, des systèmes physiques et des serveurs Terminal Service que vous utilisez comme sources pour les postes de travail View. Sur des machines virtuelles, cet agent communique avec View Client pour fournir des fonctions comme le contrôle des connexions, l'impression virtuelle, Gestion de persona View et l'accès à des périphériques USB connectés en local.

Si la source de postes de travail est une machine virtuelle, vous devez d'abord installer le service View Agent sur cette machine virtuelle et utiliser la machine virtuelle comme un modèle ou un parent de clones liés.

Lorsque vous créez un pool depuis cette machine virtuelle, l'agent est automatiquement installé sur chaque poste de travail virtuel.

Vous pouvez installer l'agent avec une option pour l'authentification unique. Avec cette option, les utilisateurs sont invités à ouvrir une session uniquement lorsqu'ils se

connectent à View Connection Server et ne sont pas invités une deuxième fois à se connecter à un poste de travail virtuel.

✓ **ViewAdministrator**

Cette application Web permet aux administrateurs de configurer ViewConnection Server, de déployer et de gérer des postes de travail View, de contrôler l'authentification utilisateur et de résoudre des problèmes d'utilisateur.

Lorsque vous installez une instance de View Connection Server, l'application ViewAdministrator est également installée. Cette application permet aux administrateurs de gérer des instances de ViewConnection Server depuis n'importe quel endroit sans avoir à installer d'application sur leur ordinateur local.

✓ **View Composer**

Vous pouvez installer ce service logiciel sur une instance de vCenter Server qui gère des machines virtuelles ou sur un serveur séparé. View Composer peut alors créer un pool de clones liés à partir d'une machine virtuelle parente spécifiée. Cette stratégie réduit les coûts de stockage de 90 % au maximum.

Chaque clone lié agit comme un poste de travail indépendant avec un nom d'hôte et une adresse IP uniques.

Pourtant, le clone lié requiert beaucoup moins de stockage car il partage une image de base avec le parent.

Comme les pools de postes de travail de clone lié partagent une image de base, vous pouvez rapidement déployer des mises à jour et des correctifs en ne mettant à jour que la machine virtuelle parente. Les paramètres, les données et les applications des utilisateurs finaux ne sont pas affectés. Vous pouvez également utiliser la technologie de clone lié pour des postes de travail View que vous téléchargez et empruntez afin de les utiliser sur des systèmes locaux.

Même si vous pouvez installer View Composer sur son propre hôte serveur avec View 5.1, un service View Composer peut fonctionner avec une instance unique de vCenter Server. De même, une instance de vCenter Server peut être associée à un service View Composer unique.

✓ **vCenter Server**

Ce service agit comme un administrateur central des serveurs VMware ESX/ESXi qui sont connectés sur un réseau.

VCenter Server, connu précédemment sous le nom VMware Virtual Center, fournit le point central pour la configuration, l'approvisionnement et la gestion de machines virtuelles dans le Datacenter.

En plus de l'utilisation de ces machines virtuelles comme sources de pools de postes de travail View, vous pouvez utiliser des machines virtuelles pour héberger des composants du serveur de VMware View, y compris des instances de Connection Server, des serveurs Active Directory et des instances de vCenter Server.

Vous pouvez installer View Composer sur le même serveur que vCenter Server pour créer des pools de postes de travail de clone lié. vCenter Server gère ensuite l'attribution des machines virtuelles aux serveurs physiques et au stockage et gère l'attribution de CPU et de ressources de mémoire aux machines virtuelles.

Vous installez vCenter Server dans un serveur Windows Server 2008, de préférence sur une machine virtuelle VMware.

✓ **View Transfer Server**

Ce logiciel gère et rationalise des transferts de données entre le Datacenter et des postes de travail View qui sont empruntés afin d'être utilisés sur des systèmes locaux d'utilisateurs finaux. View Transfer Server est requis pour prendre en charge des postes de travail qui exécutent View Client with Local Mode (connu précédemment sous le nom Offline Desktop).

Plusieurs opérations utilisent View Transfer Server pour envoyer des données entre le poste de travail View dans vCenter Server et le poste de travail local correspondant sur le système client.

Lorsqu'un utilisateur restitue ou emprunte un poste de travail, View Manager autorise et gère l'opération.

View Transfer Server transfère les fichiers entre le Datacenter et le poste de travail local.

View Transfer Server synchronise des postes de travail locaux avec les postes de travail correspondants dans le Datacenter en répliquant les modifications générées par l'utilisateur dans le Datacenter. Les répliquations se produisent à des intervalles que vous spécifiez dans des règles de mode local. Vous pouvez également initier des répliquations dans ViewAdministrator. Vous pouvez définir une règle qui permet aux utilisateurs d'initier des répliquations à partir de leurs postes de travail locaux.

View Transfer Server distribue des données système communes à partir du Datacenter vers les clients locaux. View Transfer Server télécharge des images de base de View Composer à partir du référentiel de Transfer Server vers des postes de travail locaux.

✓ **View Client with Local Mode**

Il permet à un utilisateur de transférer son poste de travail virtuel afin que ce dernier s'exécute sur son ordinateur local, tout en étant déconnecté du réseau. Une version spéciale de View Client, View Client with Local Mode, est requise pour activer cette fonctionnalité. View Client with Local Mode est pris en charge uniquement sur les machines physiques Windows. Avec cette version de View Client, les utilisateurs peuvent accéder à leur poste de travail avec ou sans connexion réseau. Les utilisateurs hors ligne, quant à eux, peuvent synchroniser les modifications de leur poste en le « remplaçant » dans le Datacenter lors de leur reconnexion au réseau. Toutes les règles de sécurité informatiques régissant ce poste virtuel continuent de s'appliquer indépendamment de la connexion réseau ;

✓ **View Portal**

C'est une page d'accès à Internet installée avec ViewConnection Server. Les utilisateurs peuvent accéder à un serveur ViewConnection Server puis à View Portal pour installer View Client. Ils peuvent télécharger View Client pour Macintosh, View Client pour Windows ou View Client with Local Mode ;

✓ **Un serveur de sécurité VMware View**

Il fournit une couche de sécurité supplémentaire aux utilisateurs externes d'internet se connectant à un serveur ViewConnection Server pour accéder à votre réseau interne. Le serveur de sécurité gère les fonctions SSL ;

✓ **View Persona Management**

Il fournit des profils utilisateur permanents et dynamiques pour les sessions des utilisateurs sur différents postes de travail. Les données des profils utilisateur sont téléchargées selon les besoins afin d'accélérer la connexion et la déconnexion, et les nouveaux paramètres utilisateurs sont envoyés au référentiel de profils utilisateurs automatiquement durant l'utilisation du poste de travail ;

✓ **ThinApp**

Il permet de créer des packages d'applications virtualisées que vous pouvez placer sur le poste de travail ou vers lesquels vous pouvez être redirigé à partir de raccourcis sur le poste de travail afin d'exécuter des applications disponibles en continu à partir d'un lecteur partagé. Les applications que vous placez sur les postes de travail virtuels View peuvent être :

- des applications installées en natif ;
- des packages d'applications virtuelles ThinApp ;
- des raccourcis vers les packages ThinApp en continu.

Les applications virtualisées avec ThinApp sont stockées dans le référentiel d'applications ThinApp sur un partage réseau du déploiement de VMware View. L'administrateur peut copier un package ThinApp complet à partir du référentiel vers le poste de travail virtuel. L'administrateur peut également placer un raccourci sur le poste de travail virtuel, qui diffusera un package ThinApp en continu à partir du référentiel.

TROISIEME PARTIE :

Déploiement et Sécurisation

TROISIEME PARTIE : Déploiement et Sécurisation

1. Déploiement de l'infrastructure virtuelle du Datacenter

1.1. Présentation de l'architecture Mise en œuvre

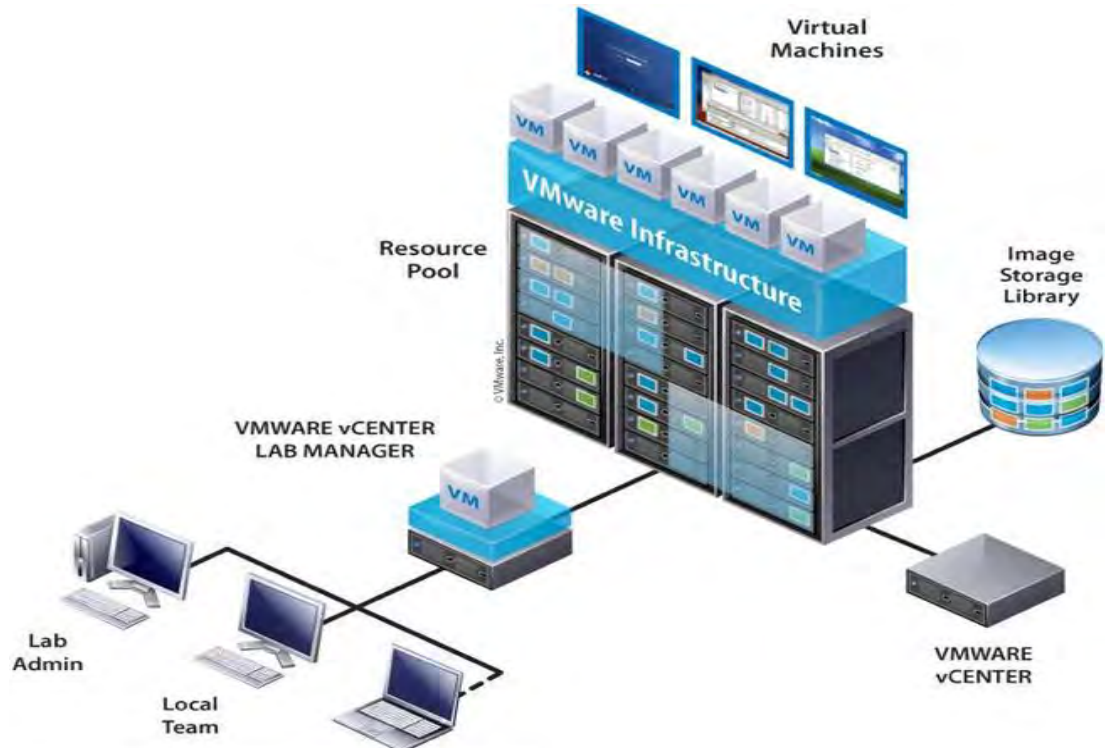


Figure 16: Architecture virtuelle de test de VMware

1.2. Déploiement requis pour les différents composants en mode production

Notre architecture va permettre dans un premier temps aux utilisateurs de pouvoir récupérer le poste agent virtualisé dans le Datacenter dans laquelle se trouve des applications et de les utiliser, dans un second temps de pouvoir Migrer à chaud les VM d'un des hôtes du cluster.

Elle comporte en effet :

Sept Machines Serveurs dont :

- ✓ Un serveur de stockage pour la sauvegarde (FreeNAS)
- ✓ Deux Serveurs VMware ESXi 5.0 comportant chacune des Machines virtuelles
- ✓ Un Serveur VMware vCenter fonctionnant sur Windows server 2008 R2
- ✓ Un coursier de connexion fonctionnant sur Windows server 2008 R2
- ✓ Un serveur messagerie Exchange 2010 fonctionnant sur Windows server 2008 R2
- ✓ Une Machine Windows server 2008 R2 faisant office de contrôleur de domaine.

Deux Machines Windows:

- ✓ Une Machine client Windows XP
- ✓ Une Machine Agent Windows 7

2. Dispositif Matériel et Logiciel

✓ Dispositif Matériel

Comme équipement et système dont nous disposons :

- Un point d'accès Wifi
- Un PC Core i3 8Go de RAM et 500Go de disque dur
- Un PC Intel Celeron de 2Go de RAM
- L'ISO de Microsoft Server 2008 R2 64 bits
- L'ISO de Windows Seven Edition Intégrale
- L'ISO de Windows XP Professionnel

✓ Dispositif Logiciel

Pour mener à bien notre projet nous avons besoin d'un dispositif logiciel qui est accessible sur le site de VMware. Pour cela il faut au préalable ouvrir un compte sur VMware pour avoir accès à un espace membre. Grâce à ce compte, nous avons eu droit aux téléchargements des différents produits suivants et leurs clés de licence de 60 jours. Voici la liste des produits qui nous ont aidés pour la réalisation de notre projet :

- VMware-workstation-full-9.0.1
- VMware-VMvisor-Installer-5.0.0 (hyperviseur ESXi)
- VMware-vSphereclient-all-5.0.0
- VMware-vCenter-ServerSetup-all-5.0.0
- VMware-viewconnectionserver-x86_64-5.1.0
- VMware-viewagent-x86_64-5.1.0
- VMware-viewclient-5.1.0

Notre architecture sera déployer sur Workstation qui est un hyperviseur de type 2 dans lequel nous avons installé trois machines serveurs (un contrôleur de domaine, un vCenter serveur) et un contenant un viewclient, un viewagent,

3. Exigence technique

3.1. Configuration requise pour les différents composants en mode production

3.1.1. Composants Serveur

- Exigences matérielles de vSphere (ESXi)

L'utilisation d'ESXi exige des ressources matérielles et système spécifiques.

Processeur 64 bits

- VMware ESXi ne peut s'installer et fonctionner que sur les serveurs dotés de CPU x86 à 64 bits.
- Processeurs 64 bits connus :
- Tous les AMD Opterons admettent le 64 bits.
- Tous les Intel Xeon 3000/3200, 3100/3300, 5100/5300, 5200/5400, 7100/7300 et 7200/7400 admettent le 64 bits.
- Tous les Intel Nehalem (aucun numéro de marque Xeon attribué à ce jour) admettent le 64 bits.

Mémoire vive

- Minimum de 2 Go de mémoire vive
- Pour les mises à niveau, 2 Go de RAM sont nécessaires si l'hôte ESXi est géré par vCenter Server.

Réseau

Une ou plusieurs cartes réseau. Les adaptateurs réseau pris en charge incluent :

- Contrôleurs BroadcomNetXtreme 570x gigabit

Cartes Intel PRO 1000

○ Exigences matérielles de vCenter Server

Le système vCenter Server est une machine physique ou virtuelle ayant accès à une base de données prise en charge. Le système vCenter Server doit correspondre à des conditions spécifiques. Aussi, assurez-vous que les machines vSphere Client correspondent aux conditions de matériel requises.

- CPU : deux CPU 64-bits ou un processeur 64-bits à double cœur.
 - processeur Intel ou AMD de 2,0 GHz ou plus rapide. Les spécifications du processeur doivent être supérieures si la base de données s'exécute sur la même machine.
 - Mémoire : RAM 3 Go. Les spécifications de la mémoire doivent être supérieures si la base de données s'exécute sur la même machine.
VCenter Server inclut un service appelé VMware Virtual Center Management Web services. Ce service nécessite de 512 Mo à 4,4 Go de mémoire supplémentaire. La mémoire maximum de la JVM pour Web services peut être spécifié lors de l'installation selon la taille de l'inventaire.
 - Stockage disque – 3 Go. Les spécifications du disque doivent être supérieures si la base de données s'exécute sur la même machine.
 - Spécifications disque pour Microsoft SQL Server 2005 Express – Jusqu'à 2 Go d'espace disque libre pour décompresser l'archive d'installation. Environ 1,5 Go de ces fichiers sont supprimés une fois l'installation soit terminée.
 - Connexion réseau : Connexion Gigabit recommandée.
- Exigences matérielles de ViewConnection Server**

Il y a plusieurs types d'installations pour ce serveur notamment l'installation standard, de réplica et de serveur de sécurité. Ils doivent tous être installés sur une machine physique ou virtuelle dédiée respectant la configuration matérielle du tableau ci-dessous.

Composant matériel	Requis	Recommandé
Processeur	processeur Pentium IV 2 GHz ou plus	4 CPU
Réseau	Une ou plusieurs cartes réseau De 10/100 Mbits/s	Des cartes réseau de 1 Gbit/s
Mémoire Windows Server 2008 64 bits	RAM de 4 Go ou plus	Au moins RAM de 10 Go pour les déploiements de 50 postes de travail View ou plus

Tableau 6:Exigences matérielles de ViewConnection Server

La machine physique ou virtuelle qui héberge Serveur de connexion View doit utiliser une adresse IP statique.

Le serveur de connexion View doit être installé sur un système d'exploitation Windows Server 2008 R2. Les systèmes d'exploitation suivants prennent en charge tous les types d'installations du Serveur de connexion view.

Système d'exploitation	Version	Edition
Windows server 2008 R2	64 bits	Standard Entreprise
Windows server 2008 R2 SP1	64 bits	Standard Entreprise

Tableau 7: Systèmes d'exploitation prise en charge par ViewConnection server

Le serveur de connexion View nécessite certaines versions du logiciel de virtualisation de VMware. Si c'est vSphere qui est utilisé, les versions prises en charge à utiliser sont les suivantes :

- vSphere 4.0 Update 4 ou versions supérieures
 - vSphere 4.1 Update 2 ou versions supérieures
 - vSphere 5.0 Update 1 ou versions supérieures
- Les hôtes ESX et ESXi sont pris en charge.

3.1.2. Composants Client

Les systèmes exécutant des composants client View doivent satisfaire certaines exigences matérielles et logicielles.

✓ Prérequis de vSphere client

Afin d'assurer un bon fonctionnement de vSphere client les conditions minimales suivantes doivent être requises

- Nombre de CPU : 1 CPU
- Processeur : processeur Intel ou AMD de 500 MHz ou plus rapide (1 GHz recommandé).
- Mémoire : RAM 1Go
Stockage sur disque : 1,5 Go d'espace disque libre pour une installation complète comprenant les composants suivants :
- Microsoft .NET 2.0
- Microsoft .NET 3.0 SP1
- Microsoft Visual J#
- Connexion réseau : connexion Gigabit recommandée.

✓ Prérequis de View Agent

Le composant View Agent facilite la gestion des sessions, l'ouverture de session unique et la redirection de périphérique. View Agent doit être installé sur toutes les machines virtuelles, systèmes physiques et serveurs Terminal Server qui seront gérés par View Manager.

Système d'exploitation client	Version	Edition	Service pack
Windows 7	64 bits et 32 bits	Enterprise et Professional	Aucun et SP1
Windows Vista	32 bits	Business et Enterprise	SP1 et SP2
Windows XP	32 bits	Professional	SP3
Windows 2008 R2 terminal server	64 bits	Standard	SP1
Windows 2008 terminal server	64 bits	Standard	SP2

Tableau 8: Systèmes d'exploitation prise en charge par View Agent

✓ Prérequis de View Client et View Client en Mode Local

Les utilisateurs exécutent View Client pour se connecter à leurs postes de travail View. View Client ou View Client with Local Mode doit être installé sur un système d'exploitation pris en charge. Le tableau suivant répertorie les systèmes d'exploitation Microsoft Windows pris en charge par View Client.

Système d'exploitation client	Version	Edition	Service pack
Windows 7	64 bits et 32 bits	Home, Enterprise,	Aucun et SP1

		Professional et Ultimate	
Windows XP	32 bits	Home et Professional	SP3
Windows Vista	32 bits	Home, Business, Enterprise et Ultimate	SP2

Tableau 9: Systèmes d'exploitation prise en charge par View Client

Lorsqu'il est emprunté un poste de travail View pour être exécuté sur un ordinateur local, le matériel sur l'ordinateur client doit prendre en charge à la fois le système local et la machine virtuelle qui s'exécute maintenant sur lui.

Configuration de l'ordinateur client	Description
PC	compatible 64 x86 Support LAHF/SAHF en mode long
Nombre de CPU	Les systèmes multiprocesseurs sont pris en charge
Vitesse de CPU	Pour un poste de travail local Windows XP, 1,3 GHz ou plus ; 1,6GHz recommandé. Pour un poste de travail Windows 7, 1,3 GHz ou plus ; pour des effets Aero, 2 GHz ou plus
Processeurs Intel	Processeurs Pentium 4, Pentium M (avec PAE), Core, Core 2, Core i3, Core i5 et Core i7. Pour Windows 7 Aero : Intel Dual Core
Processeurs AMD	Athlon, Athlon MP, Athlon XP, Athlon 64, Athlon X2, Duron, Opteron, Turion X2, Turion 64, Sempron, Phenom et Phenom II. Le processeur AMD doit avoir un support de limite de segment en mode long. Pour Windows 7 Aero : Althon 4200+ et supérieur

Tableau 10: Exigences matérielles des postes de travail en mode local

4. Sécurisation du système d'information

La sécurité des données est devenue et sera de plus en plus **une condition absolue** dans l'échange des données sur les réseaux locaux et sur le réseau mondial.

Les technologies et les modes de conception des infrastructures réseaux **évoluant rapidement**, il est **indispensable**, pour un **administrateur**, de **connaître** et de **réévaluer** en permanence les risques potentiels qu'encourt son système.

Les premières étapes dans la sécurisation d'un réseau informatiques se concentrent sur l'accès aux **dispositifs communs du réseau (routeurs, switches...)** et dans la mise en place et **la configuration d'un pare-feu**. En définitive sécurisé une entreprise consiste à mettre en place une politique de sécurité. Pour protéger une infrastructure virtuelles ; il est important de connaître les éventuelles risques et menaces qui pèsent sur celle-ci afin de les combattre.

4.1. Risques éventuelles dans un environnement virtuel

Il est donc important de connaître l'ensemble des risques pour en maîtriser l'impact en termes de confidentialité, d'intégrité et de disponibilité des données et des applications.

✓ **Risque 1 : Risque accru de compromission des systèmes**

On entend ici par «compromission» la prise de contrôle par un acteur malveillant d'une brique utilisée dans le système virtualisé. Il peut s'agir d'une compromission d'un système invité depuis un autre système invité, ou de la couche d'abstraction depuis un système invité.

On remarque qu'une compromission de la couche d'abstraction peut éventuellement entraîner une compromission de l'ensemble des systèmes s'exécutant sur la machine. On note également que plus la compromission touche le système en profondeur, plus elle aura de conséquences sur les capacités de remise en service ultérieure du système.

Si une instance est compromise, comment décider si les autres instances qui s'exécutaient sur la machine hôte doivent être considérées comme compromises. En cas de mise en œuvre de techniques de migration, comment déterminer précisément le domaine de propagation des instances compromises ?

Le principal événement redouté suite à une compromission est la fuite d'informations sensibles ou, dans certains cas, des perturbations engendrées par une modification du système pouvant aller jusqu'à l'indisponibilité d'un service.

Les solutions permettant d'empêcher une compromission sont souvent délicates à mettre en œuvre. Il s'agira de diminuer au maximum la surface d'attaque. Il conviendra notamment que chaque brique (matériel, système d'exploitation hôte, systèmes d'exploitation invités etc.) soit à jour de tous les correctifs de sécurité.

Plus généralement, l'application stricte du principe de défense en profondeur est indispensable.

Enfin, s'il peut généralement être aisé de « remonter » un système invité défaillant sur une autre machine physique à partir d'une image saine, seule la

mise en œuvre du principe de défense en profondeur permettra une localisation précise de l'origine de la compromission (système invité, système hôte, matériel, données, etc.).

✓ **Risque 2 : Accroissement du risque d'indisponibilité**

Comme évoqué précédemment, une compromission peut engendrer une indisponibilité d'un service.

Cependant, ce risque peut apparaître, même en l'absence de compromission. Ainsi, si un atout de la virtualisation est l'utilisation plus intensive des ressources informatiques, la panne d'une ressource commune pourra engendrer l'indisponibilité simultanée de plusieurs systèmes. De même, une attaque en disponibilité sur un des systèmes (ou plus généralement sur une ressource commune) impactera potentiellement tous les services hébergés sur la même machine.

Là encore, les préconisations faites au point précédent s'appliquent. Si des besoins en disponibilité diffèrent sensiblement d'une application à une autre, il peut même être préférable de regrouper sur une machine dédiée celles ayant le besoin en disponibilité le plus élevé.

✓ **Risque 3 : Fuite d'information par manque de cloisonnement**

Bien que les solutions de virtualisation mettent généralement en œuvre des mécanismes de cloisonnement des instances se partageant une même ressource, ces instances ne sont en pratique jamais totalement isolées. Dans certains cas, des flux existent entre les différentes instances (systèmes d'exploitation, applications, systèmes de stockage de données, ...), flux qui peuvent engendrer des vulnérabilités.

La maîtrise des différents échanges internes à une même machine physique est par ailleurs particulièrement difficile. En effet, il sera généralement délicat de garantir que les ressources bas niveau partagées n'introduisent pas de possibilité de fuite d'information.

La défense en profondeur consiste à mettre en place plusieurs techniques de sécurité complémentaires afin de réduire l'impact lorsqu'un composant particulier de sécurité est compromis ou défaillant.

Pour illustrer ces propos, prenons l'exemple de l'accès au réseau d'une machine informatique. Dans une architecture sans virtualisation, les machines communiquent sur des réseaux physiques au moyen, par exemple, d'une carte réseau spécifique. Les flux de données sont ainsi traités, au niveau des machines, par chaque carte réseau et peuvent être identifiés précisément.

Dans une architecture avec virtualisation, les machines virtuelles peuvent par exemple communiquer sur des réseaux physiques par le biais d'une carte unique appartenant à la machine physique qui les héberge. Les flux de données de chaque machine virtuelle sont donc traités par cette unique carte réseau. Dès lors, il n'est pas possible de garantir un cloisonnement des flux au niveau de la

ressource partagée. La carte réseau a la possibilité, en cas d'erreur ou de compromission, de mélanger les différents flux d'information.

Dans ce contexte, pour mieux répondre au besoin de cloisonnement, le choix peut être fait d'avoir autant de cartes réseau que de machines virtuelles hébergées sur une machine physique. Il conviendrait idéalement de vérifier, mais une telle vérification est en pratique irréaliste, que les composants impliqués dans la chaîne de traitement du flux de données entre une machine virtuelle et la carte réseau attribuée gèrent correctement le cloisonnement des données suivant leur appartenance.

En effet, une mauvaise implémentation d'un contrôleur d'entrées/sorties pourra échanger les flux issus des machines virtuelles différentes. Un canal caché pourra ainsi apparaître et engendrer des fuites d'informations. L'utilisation d'un chiffrement au niveau IP (IPsec) géré intégralement par chaque instance permettra, dans une certaine mesure, de réduire ce risque.

La problématique est similaire pour les supports de mémoire de masse de la machine physique dans le cas où celle-ci est partagée par plusieurs machines virtuelles.

Enfin, s'il s'avère que les objectifs de sécurité fixés en matière de cloisonnement ne sont pas remplis par l'une ou l'autre des techniques évoquées précédemment, certains domaines ne devront pas s'exécuter dans l'environnement virtualisé. Le choix d'un retour partiel à une solution classique (c'est à dire sans virtualisation) pourra alors être plus adapté à un bon cloisonnement des flux. Par exemple, lorsque les données traitées par différentes instances ont des sensibilités différentes, une séparation physique au niveau réseau sera à retenir.

✓ **Risque 4 : Complexification de l'administration et de la mise en œuvre**

Lorsqu'une solution de virtualisation est utilisée, il est nécessaire d'administrer d'une part les différents systèmes invités, mais également la couche d'abstraction. Des exemples d'opérations d'administration nouvelles, induites par l'utilisation de technologies de virtualisation, sont les suivants :

- ☐ Mise en place des quotas sur les ressources partagées entre différents systèmes ;
- ☐ Gestion de l'ajout d'un disque ou d'un périphérique de stockage réseau (NAS) sans remise en question du cloisonnement mis en place entre machines virtuelles;
- ☐ Sauvegardes spécifiques liées aux opérations de virtualisation, protection de ces sauvegardes, opérations de restauration. La mobilité éventuelle des machines virtuelles lors des sauvegardes doit être prise en compte, ainsi que les corrélations fortes qui peuvent exister entre les sauvegardes des différents systèmes et des données.

Les tâches d'administration classiques peuvent également s'avérer plus complexes car les interventions sur la machine physique proprement dite

(administrateur du système hôte), sur les instances qui y sont hébergées (administrateur(s) des systèmes invités), sur les périphériques de stockage physiques et virtuels (SAN / NAS) et sur les équipements réseau physiques et (éventuellement) virtuels peuvent devoir être réalisées séparément. En effet, si comme dans de nombreuses organisations de taille importante, les équipes gérant les serveurs, le stockage, le réseau et les sauvegardes sont disjointes, l'identification des responsabilités de chacun dans l'administration d'un système virtualisé est indispensable afin de limiter, autant que faire se peut, les erreurs de configuration, comme par exemple, le positionnement d'une machine virtuelle dans le mauvais réseau virtuel (VLAN).

L'administration des machines peut s'opérer localement ou à distance. S'il est généralement difficile d'administrer localement les systèmes invités, la question se pose pour la couche d'abstraction.

Le choix d'administration d'un système à distance ou non doit être fait en considérant tous les risques induits. Parmi de tels risques, on trouve l'usurpation du rôle d'administrateur permise suite à la mise en place d'un mécanisme d'authentification trop faible, la perte de confidentialité et/ou d'intégrité d'une commande circulant sur le réseau, la perte de traçabilité des opérations d'administration.

Si l'organisation utilise des technologies d'informatique en nuage (Cloud Computing), une attention toute particulière doit être portée sur la gestion des machines virtuelles qui peut, dans certains cas, être très automatisée (guichet de demande d'une nouvelle machine virtuelle par un utilisateur métier, avec livraison immédiate, par exemple). Il convient ainsi de bien sécuriser l'ensemble des interfaces de gestion et de tracer toute action réalisée par leur biais.

✓ **Risque 5 : Complexification de la supervision**

De même que pour l'administration, les opérations de supervision peuvent aussi s'avérer complexes, en particulier du fait de l'incompatibilité entre le cloisonnement nécessaire des machines virtuelles et la vision d'ensemble souhaitée lors des opérations de supervision. Compte-tenu des cloisonnements induits par la solution de virtualisation, il peut être difficile de tracer un événement ou une action de bout en bout.

De plus, la nécessité de disposer d'une vision d'ensemble impose que le personnel opérant les moyens de supervision soit autorisé à accéder aux informations du niveau de sensibilité le plus élevé des données traitées.

✓ **Risque 6 : Prolifération non souhaitée des données et des systèmes**

La virtualisation rend les systèmes invités moins adhérents aux équipements. Leur migration sur différentes machines est donc possible, et la plupart du temps souhaitée. En conséquence, la localisation précise d'une donnée est complexifiée.

De même, il sera généralement plus difficile d'empêcher la copie frauduleuse d'une information. Par ailleurs, les principes de migration des instances impliquent généralement que ces dernières soient sous forme « d'objets migrables ». Les risques de copie non maîtrisée (non-respect des licences logicielles) des instances, de perte, de vol, de modification ou de perte de maîtrise des versions des instances (régression) sont importants.

✓ **Risque 7 : Incapacité à gérer voire à comprendre les erreurs**

Les problèmes de fonctionnement et les erreurs peuvent être complexes à gérer techniquement dans une architecture s'appuyant sur une solution de virtualisation.

Par exemple, les erreurs qui pourraient survenir lors de l'arrêt puis la relance d'une instance seront soit rapportées au système hôte que l'instance quitte, soit au système hôte qui est en train de l'accueillir. Sans la prise en compte globale des erreurs pouvant apparaître sur un système s'appuyant sur la virtualisation, il se peut que des informations pertinentes permettant d'identifier leur cause soient perdues, ou a minima, que leur synthèse ne puisse pas être réalisée. Il convient donc de mettre en place une centralisation et une corrélation des journaux sur l'ensemble des systèmes. Cette corrélation pose évidemment des problèmes identiques à ceux identifiés.

✓ **Risque 8 : Investigations post incident plus difficiles**

Les principes sur lesquels reposent les techniques de virtualisation peuvent rendre difficiles certaines investigations après un incident du fait du partage de ressources matérielles par plusieurs systèmes.

Ainsi, l'optimisation de la gestion de la mémoire vive effectuée par la solution de virtualisation rend plus délicate toute analyse de l'historique des états de la machine et donc le traitement d'un incident.

L'optimisation qui consiste à réallouer à d'autres machines virtuelles l'espace en mémoire d'une machine virtuelle dès qu'elle n'est plus utilisée pose potentiellement des problèmes en matière d'analyse post mortem. Seule la connaissance précise du mode de fonctionnement des solutions de virtualisation permettra de retenir celles qui gèrent le plus rigoureusement les accès mémoire et facilitent des investigations post incidents.

4.2.Menaces

Il existe deux types de menaces : la menace numérique et la menace physique.

✓ **Les menaces numériques**

Les menaces numériques sont notamment, le piratage informatique, les virus, les goulots d'étranglement réseau et toutes attaques malveillantes ou accidentelles de sécurité ou de flux de données. Il est donc nécessaire de mettre en place d'antivirus et des firewalls de dernières générations.

On comprend encore mieux l'avantage de déporter son informatique dans un Datacenter.

En effet, de plus en plus d'entreprises font l'objet d'attaques sur leur système informatique. Le niveau de sécurité des serveurs en place nécessite une veille des plus actives, afin de réduire les menaces. Et il est courant de s'apercevoir que le niveau de sécurité des entreprises est des plus bas : pour des raisons économiques ou de personnels non qualifiés.

Les Datacenter ont l'obligation de maintenir une vigilance des plus accrues pour veiller à une sécurisation optimale des serveurs.

✓ Les menaces physiques

Les serveurs informatiques deviennent des machines hyperpuissantes dans des volumes de plus en plus réduits. Il est donc indispensable de mettre en place des systèmes de refroidissement sophistiqués nécessitant une alimentation électrique sécurisée.

Des menaces humaines peuvent exister, ou tout simplement des erreurs de manipulation engendrant des effets catastrophiques sur le système d'information. Les incendies, les inondations sont des menaces susceptibles d'entraîner des pertes de données importantes pour la vie de l'entreprise. Les Datacenter ont mis en place des normes de sécurité leur permettant de répondre à ces types de menaces. Une entreprise est-elle prête à investir dans de telles protections ? De plus, ce sont des investissements qui n'ont pas une incidence immédiate sur la rentabilité de l'entreprise. Il est donc parfois difficile de la convaincre d'investir dans des procédures n'impactant pas la rentabilité immédiate de l'entreprise.

5. Définition et enjeu

5.1. Définition

Un système d'information permet à une organisation des activités consistant à acquérir, stocker, transformer, diffuser, exploiter et gérer des informations. Les systèmes informatiques sont au cœur des systèmes d'informations.

5.1.1. Objectifs de la sécurité informatique

Les systèmes informatiques regorgent de vulnérabilités et sont exposés à des risques et des menaces. La sécurité informatique a principalement cinq objectifs à garantir :

✓ l'intégrité

C'est la propriété d'une donnée dont la diffusion doit être limitée aux seules personnes autorisées. Les menaces sont : l'écoute du réseau (à l'extérieur ou à l'intérieur), le vol de fichiers (données, mots de passe...), l'espionnage et l'ingénierie sociale.

Pour les prévenir, on peut recourir à la cryptographie (chiffrement de données et des communications), aux contrôles d'accès logique (mot de passe) ou physique (biométrie).

✓ La confidentialité

C'est la propriété d'une donnée dont la valeur est conforme à celle définie par son propriétaire. Les menaces possible sont : des attaques malicieuses (*vers, virus, bombes logiques*), la des informations et les erreurs humaines. Les contre-mesures sont : l'utilisation de la cryptographie (*signature, authentification*), les systèmes de détections (Antivirus, systèmes détection d'intrusion).

✓ Disponibilité

C'est la propriété d'un système d'information capable d'assurer ses fonctions sans interruption, sans délai ou sans dégradation, au moment même de la sollicitation. Les menaces sont : des attaques malicieuses (DOS, SPAM) des attaques accidentelles, les pannes et les coupures d'électricité. Les contre-mesures à appliquer sont : le déploiement de pare-feu ; de systèmes de détections d'intrusions, d'alimentation de secours, le clustering et la formation des administrateurs.

✓ Non- Répudiation

Elle garantit qu'une entité à l'origine d'une action ne puisse par la suite réfuter sa responsabilité en tant que telle. L'utilisation de signature avec des mécanismes de chiffrement asymétrique permet de l'assurer.

✓ Authentification

C'est la procédure qui consiste, pour un système informatique, à vérifier d'identité d'une entité à des ressources (systèmes, réseaux, applications...)

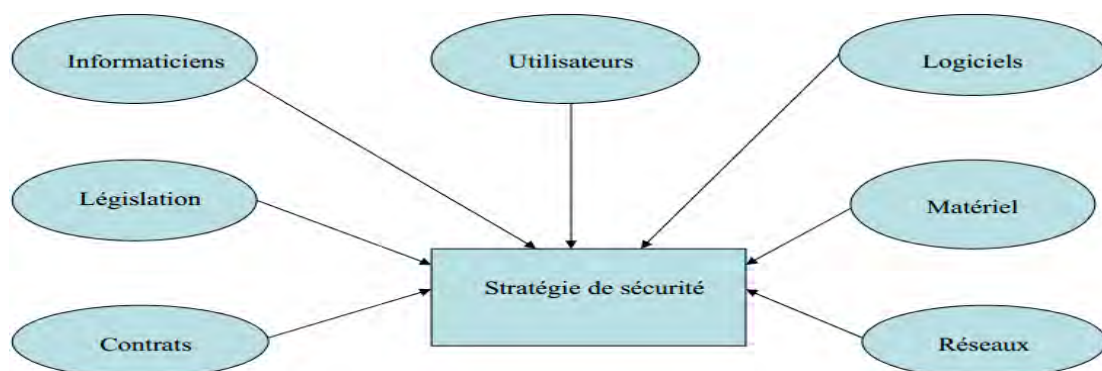


Figure 17:Stratégie de sécurité en entreprise

(Sécurité Informatique _<http://w.w0ducrot.org>)

✓ Définition d'une politique de sécurité

La politique de sécurité contient des énoncés généraux dictés par les cadres supérieurs et décrivant le rôle de la sécurité au sein de l'entreprise afin d'assurer les objectifs d'affaire. Pour mettre en œuvre cette politique, une organisation doit être mise en place et une définition des rôles, des responsabilités et des imputabilités doit être effectuée. Elle comporte des compromis sécurité-fonctionnalités qui impliquent :

- **La définition des besoins** permettant de déterminer les actifs à protéger et leurs propriétaires (*quelles sont les valeurs, quelles sont leurs criticités, quelles sont leurs propriétés*), la détermination des menaces représentant des risques (*acteurs, attaquants, moyens*), la détermination des objectifs à atteindre (*actifs à protéger*).
- La proposition des solutions permettant de déterminer les contremesures à mettre en place.
- L'évaluation des risques résiduels permettant de déterminer quelles sont les vulnérabilités toujours présentes et leurs impacts sur les objectifs initiaux.

Elle inclut aussi des audits, des tests d'intrusion, des mécanismes de détection d'incidents, de réaction et de restauration. Il existe aussi des méthodes permettant d'établir la mise en œuvre d'une politique de sécurité comme :

- **EBIOS** (*Expressions des Besoins et Identification des Objectifs de Sécurité*)
- **MEHARI** (*Méthode Harmonisée d'Analyse de Risques*)
- **La norme ISO 17799**

6. Gérer les groupes et les utilisateurs avec VMware vSphere 5.0

Avec VMware vSphere il est possible de gérer des groupes et des utilisateurs auxquels on affecte des autorisations sur un serveur vCenter, sur un centre de données, un pool de ressources ou sur un hôte VMWare ESX/ESXi uniquement. En ce qui concerne les utilisateurs et les groupes, il y'a ceux de votre hôte ESX local, c'est à dire des utilisateurs et des groupes Linux et ceux du vCenter qui correspondent aux utilisateurs et aux groupes du système d'exploitation sur lequel le vCenter est installé (Voir la partie implémentation).

QUATRIEME PARTIE : IMPLEMENTATION DE L'INFRASTRUCTURE

QUATRIEME PARTIE : IMPLEMENTATION DE L'INFRASTRUCTURE

1. Implémentation de l'infrastructure virtuelle

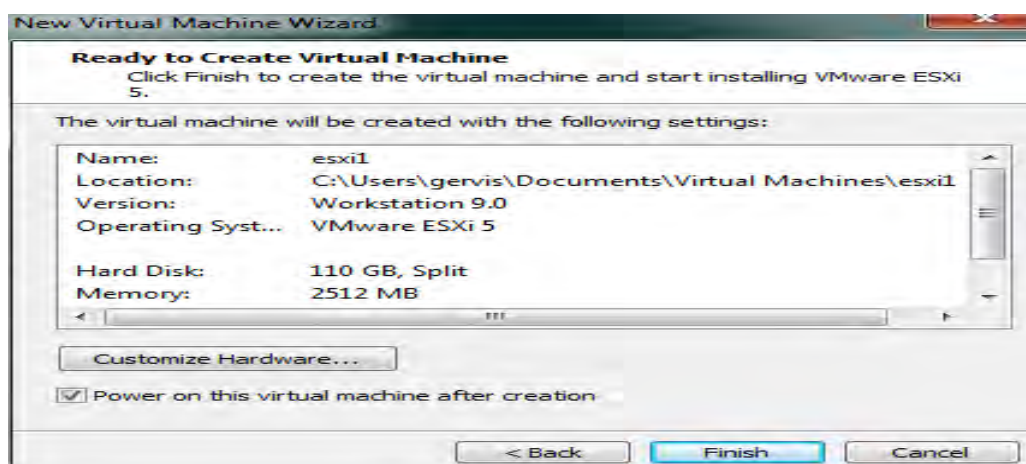
1.1. Installation et configuration de VMware vSphere

1.1.1. Installation

Pour l'installation, nous avons téléchargé la version d'évaluation de 60 jours de l'image de l'ESXi sur le site de VMware après création d'un compte.

ESXi est un hyperviseur de type 1. Il s'installe donc comme un OS sur une machine physique ou sur une machine virtuelle. Dans notre cas nous l'avons déployé dans VMware Workstation version 9 en tant que machine virtuelle. Dans VMware Workstation, nous sélectionnons le chemin **Fichier → Nouvelle Machine virtuelle** pour avoir l'assistant de création d'une nouvelle machine virtuelle.

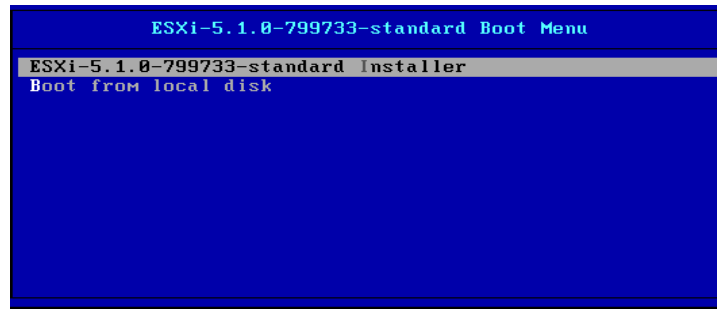
- Ici nous choisissons une installation de type avancé pour pouvoir définir nous même les spécificités du serveur en termes de ressources nécessaires et on fait **Next**.
- Nous laissons la compatibilité matérielle telle quelle c'est-à-dire Workstation 9 et on fait **Next** pour choisir le type d'installation de l'OS invité.
- Nous cochons l'installation via un fichier image ISO que nous sélectionnons depuis un emplacement sur la machine physique et on fait **Next** pour nommer et localiser notre serveur virtuel.
- Vient ensuite le choix de la configuration matérielle du serveur à savoir le nombre de CPU et la taille de la RAM, le nombre de cartes réseaux, le type de réseau à connecter, le type d'adaptateur réseau, le type de disque et sa capacité. Le résumé des différents choix que nous venons de faire figure sur la capture suivante :



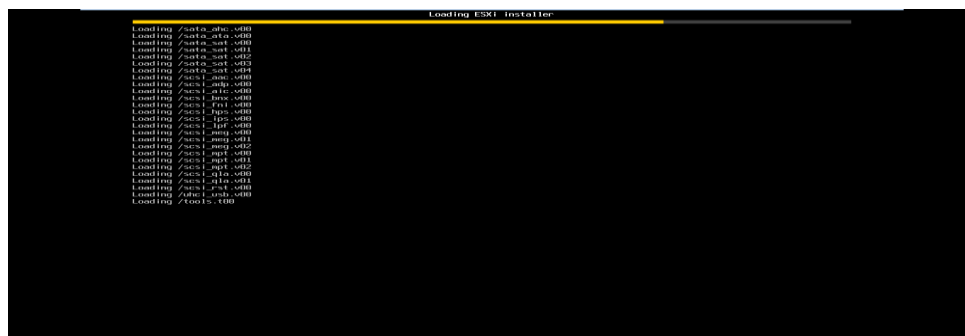
Capture 1: Installation de Vsphere ESXI

Téléchargeable sur le site VMware sous forme « VMware ESXI 5 »

Pour commencer on lance l'exécutable.

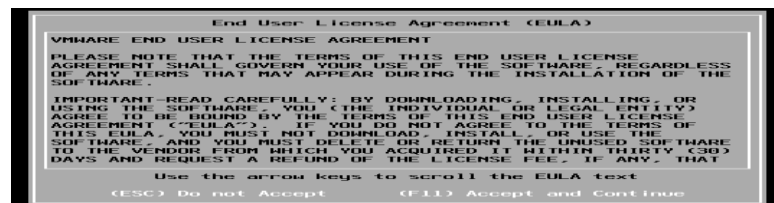


Capture 2: Interface d'installation de VMware ESXI 5



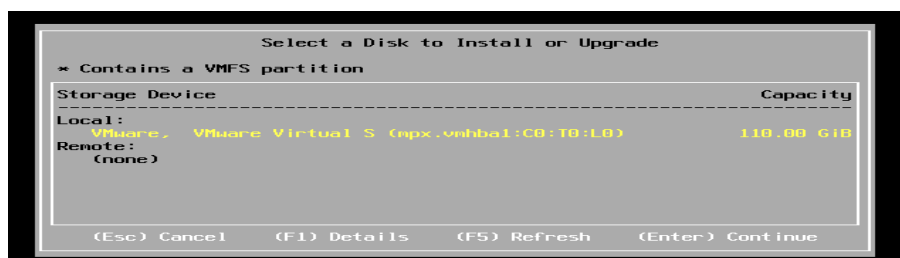
Capture 3:Interface de lecture de VMware ESX

Démarrage du boot System



Capture 4: Etape de l'installation

Ici nous acceptons la licence d'ESXi.

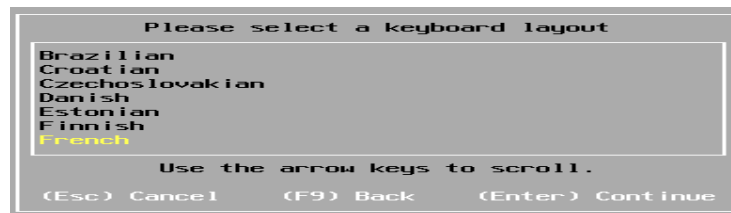


Capture 5:Espace de stockage de VMware ESXI5

Ici nous avons la possibilité de choisir la langue d'entrée sur la console de configuration (pour notre cas nous avons choisi la langue Française) et le mot de passe root « Entrer »



Capture 6: Interface de configuration du mot de passe

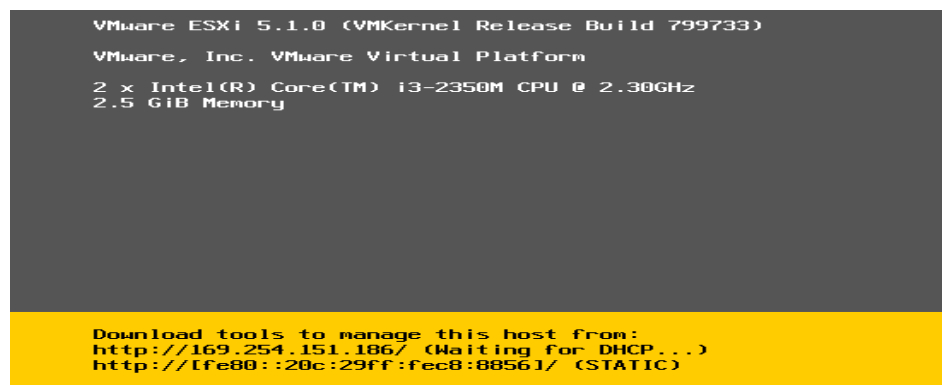


Capture 7: Interface de configuration de la langue



Capture 8: Début de l'installation

Après cette interface nous arrivons à interface de couleur gris-jaune appelée console directe où nous effectuerons nos différentes configurations.

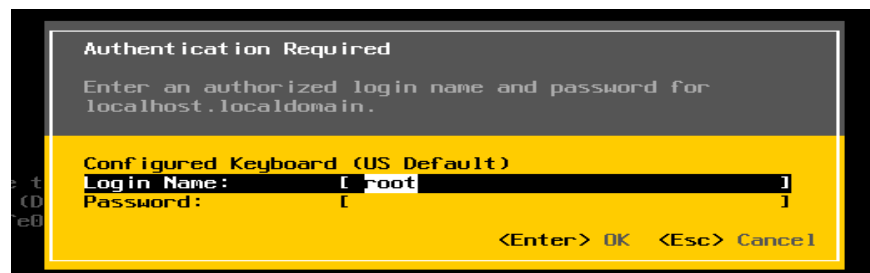


Capture 9: Fin de l'installation

1.1.2. Configuration du serveur ESXI

La configuration de l'ESXi se fait sur une interface de couleur gris-jaune appelée console directe. À la fin de l'installation, nous avons notre interface gris-jaune stable qui présente un URL avec une adresse IP obtenue dynamiquement du serveur DHCP.

Avec la touche F2, après authentification, nous accédons à l'interface de configuration d'ESXi où nous allons juste nous intéresser à la configuration réseau et au test de cette dernière.



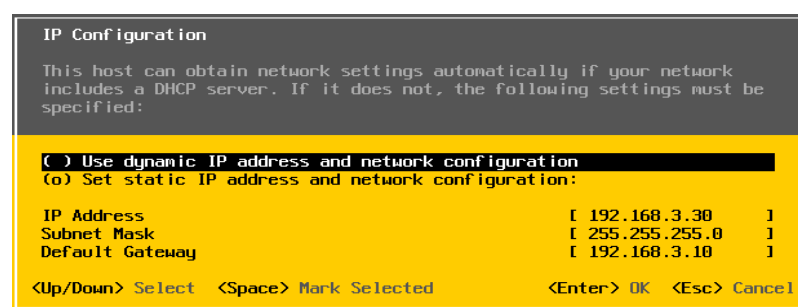
Capture 10:Interface d'authentification

On renseigne le nom de l'utilisateur et le mot de passe pour se connecter à l'interface de configuration.



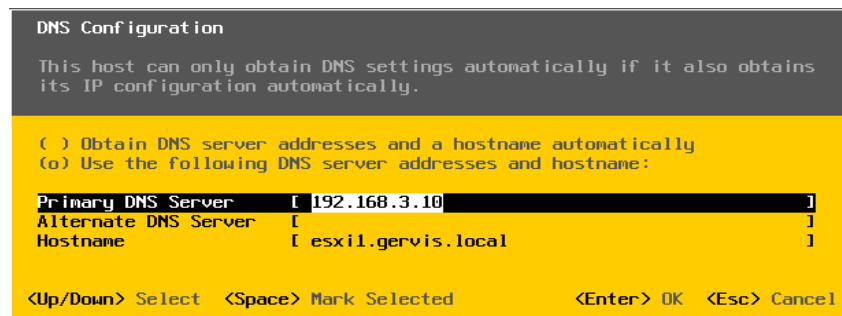
Capture 11:Interface de configuration

Pour configurer on va a « configure Management Network puis Entrer » on sélectionne le mode statique en fixant une adresse IP statique

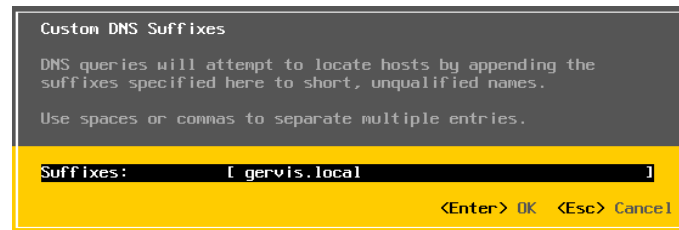


Capture 12:Configuration paramètres IP

Ici on nomme le serveur et on lui attribue de façon statique les paramètres réseau à savoir l'adresse IP, le masque de sous-réseau, l'adresse du serveur DNS et le suffixe DNS.

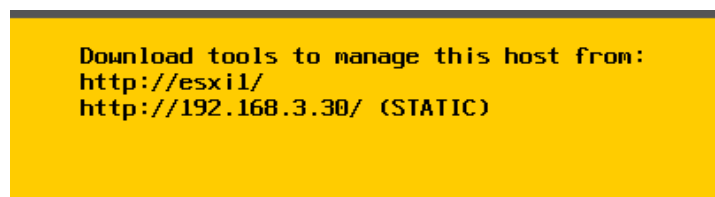


Capture 13 : Configuration de du nom et de l'adresse IP



Capture 14 : Configurations paramètres DNS

Une fois la configuration terminée, on fait **Esc** et **Yes** pour confirmer les modifications faites et notre serveur ESXi est opérationnel. Le test réalisé à la capture de l'annexe 3 confirme que l'hôte ESXi est bien paramétré.



Capture 15 : Interface stable

1.2. Installation et configuration de view client

✓ Installation sur une machine Windows 7

L'installation du logiciel client VMware Sphere client téléchargeable sur le site officiel de VMware avec un enregistrement au préalable pour télécharger.

Exécuter le logiciel client. C'est la console pour entrer dans l'interface d'administration d'ESXI.

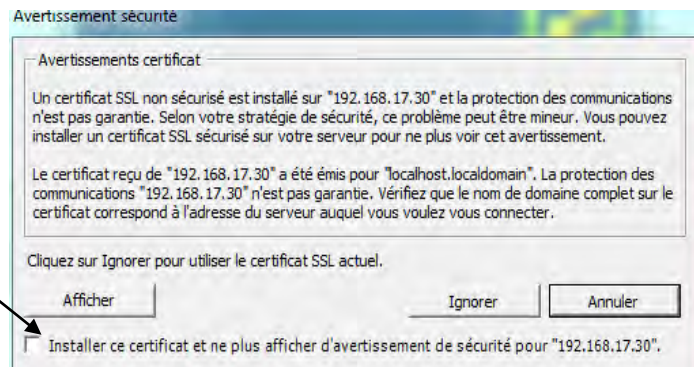
✓ Connexion au serveur ESXI



Capture 16: Interconnexion à ESXi

Dans cette interface on coche le certificat et on ignore.

Dans cette interface on coche sur installer le certificat et on ignore



Capture 17: Certificat SSL

C'est dans cette interface qu'on effectue les différentes tâches d'administration (création des VM) tout en pointant sur le serveur



Capture 18: Interface d'administration de VMware ESXi 5

1.3. installation et configuration de VMware vCenter Server

Comme nous le savons déjà, le serveur vCenter nous permettra de gérer de façon centralisée plusieurs ESXi et de débloquer les fonctionnalités avancées (vMotion, DRS, HA).

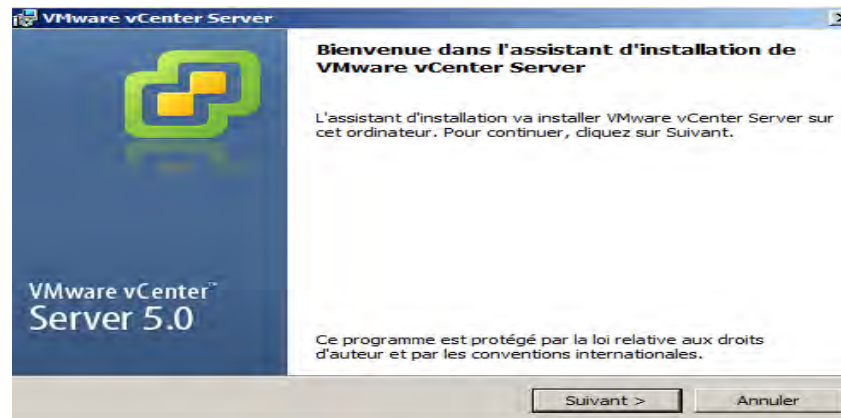
1.3.1. Installation

Il faut, au préalable, télécharger le fichier ISO de vCenter Server sur le site de VMware. Ce fichier ISO est alors monté comme un DVD et nous avons l'interface d'installation ci-dessous :



Capture 19: Interface d'installation de vSphere

Nous choisissons vCenter Server et on clique sur **Install** pour avoir l'assistant d'installation de vCenter Server après avoir choisis la langue d'installation.

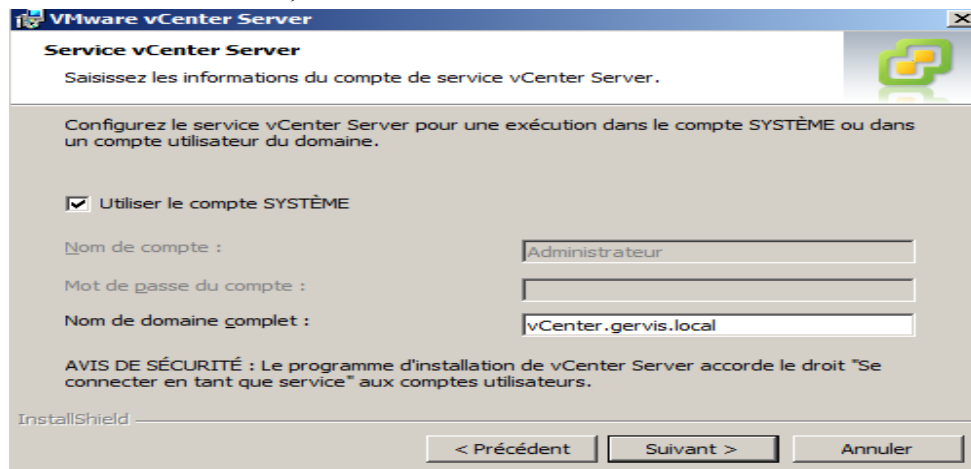


Capture 20:Assistant d'installation de vCenter Server

Viennent ensuite les actions à exécuter suivantes :

- on lit le contrat du brevet d'utilisateur final et on fait **Suivant**
- on accepte le contrat de licence et on fait **Suivant**
- on renseigne les informations sur le client c'est-à-dire le Nom d'utilisateur, l'organisation et la clé de licence de vCenter Server et on fait **Suivant**
- On choisit une option de base de données. Dans notre cas, c'est **Installer une instance de Microsoft SQL Server 2008 Express** et on fait **Suivant**

- On saisit les informations du compte de service vCenter Server, c'est-à-dire le nom d'utilisateur, le mot de passe et le nom complet du vCenter Server et on fait **Suivant** ;

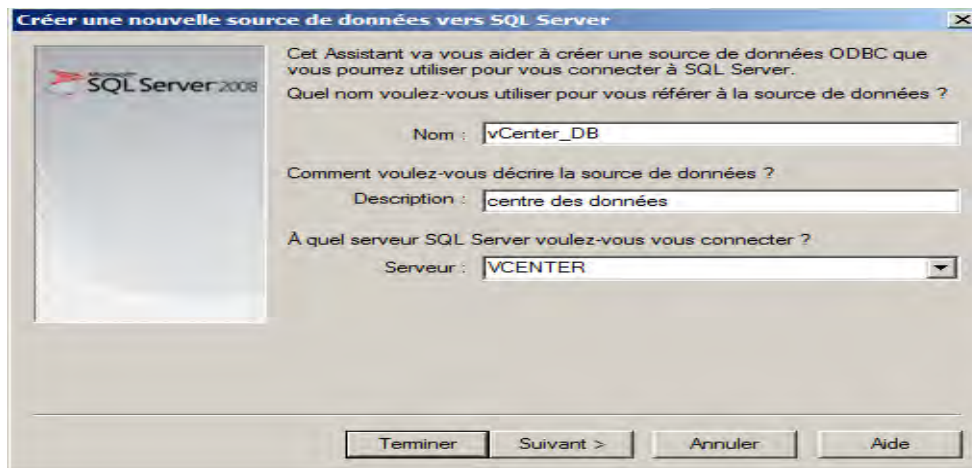


Capture 21: Informations sur le compte utilisateur vCenter

- On choisit une option Linked mode vCenter Server. Dans notre cas nous avons choisi **Créer une instance VMware vCenter Server autonome** et on fait **Suivant** ;
- On configure les ports en indiquant les ports de communication du vCenter Server et on fait **Suivant** ;
- On sélectionne une mémoire JVM vCenter Server qui décrit le mieux notre installation et on fait **Suivant** ;
- Ensuite on clique sur **Install** pour débuter l'installation proprement dite
- Enfin on termine l'installation en cliquant sur **Terminer**.

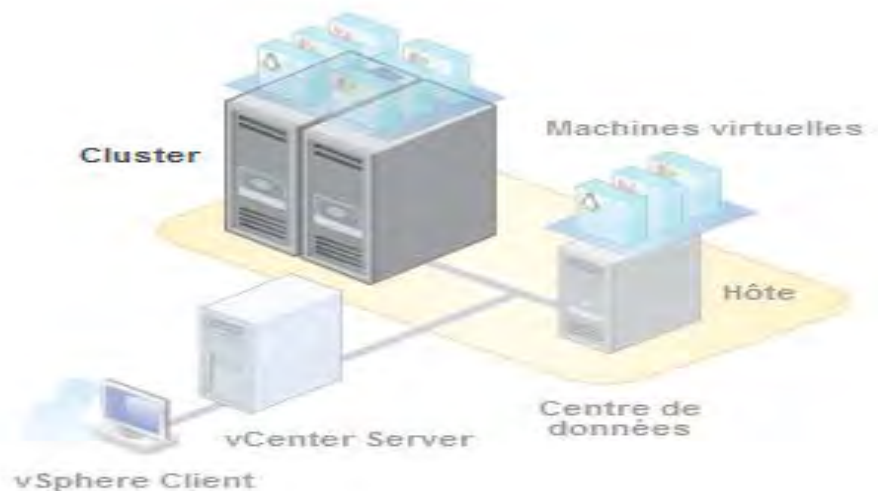
1.3.2. Configuration

Dans un premier temps la configuration du vCenter Server consiste à créer une source de données ODBC. Un ODBC est un service Windows créé spécialement pour l'échange de données. Il est question pour nous ici d'indiquer au vCenter qu'il doit aller chercher la base de données dont il a besoin sur le serveur SQL installé sur la VM faisant office de contrôleur de domaine.



Capture 22:Création d'un ODBC

La configuration la plus importante du vCenter Server consiste en la création de centres de données (Datacenter). Un Datacenter est le conteneur principal d'objets d'inventaire tels que des hôtes et des machines virtuelles. A partir du Datacenter, nous pouvons ajouter et organiser des objets d'inventaire. Habituellement, on ajoute des hôtes, des dossiers et des clusters (groupes d'hôtes) à un Datacenter. Un vCenter Server peut contenir plusieurs Datacenter (Dakar, Kaolack, Thiès,...). Les grandes entreprises en emploient plusieurs pour représenter leurs unités d'organisations.

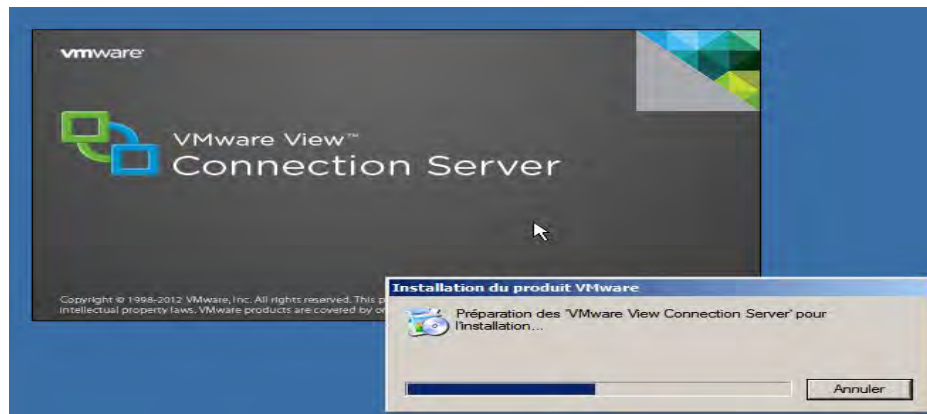


Capture 23:Organisation d'un Datacenter

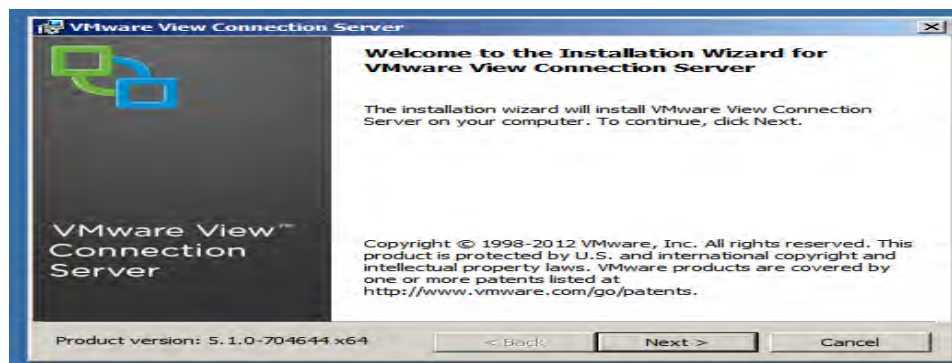
2. Installation et configuration de l'architecture VMware View

2.1. Installation de Connection server

ViewConnection Server s'installe avec un fichier exécutable téléchargeable sur le site de VMware. L'exécution dudit fichier lance l'extraction d'un certain nombre de fichiers nécessaires à l'installation du serveur.

**Capture 24:Extraction de fichiers nécessaires**

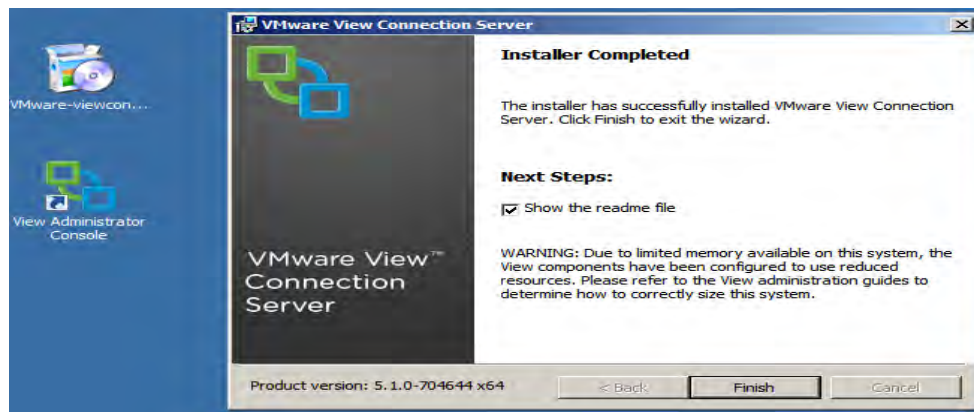
Une fois l'extraction terminée nous avons l'assistant d'installation qui s'affiche.

**Capture 25:Assistant d'installation**

Une suite de clic sur Next nous amène successivement à :

- Accepter le contrat de licence
- Choisir le dossier de destination de l'installation
- Choisir l'option d'installation (View Standard Server)
- Choisir le type de configuration du firewall (Configuration automatique)

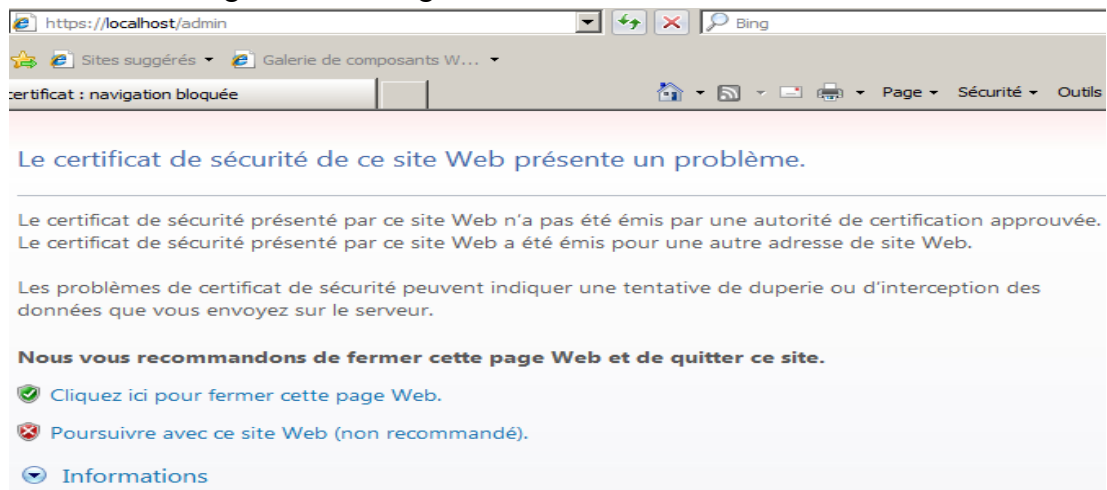
Nous arrivons alors à la boîte de dialogue où nous aurons à lancer l'installation proprement dite en cliquant sur **Install**. A la fin de l'installation, nous cliquons sur **Terminer** pour achever l'installation.



Capture 26:Fin installation

2.2. Configuration de Connexion au serveur view

La configuration du serveur de connexion suggère que nous nous connectons au serveur. Pour cela, un double-clic sur le raccourci de la console de gestion du serveur nous dirige vers un navigateur comme ci-dessous.



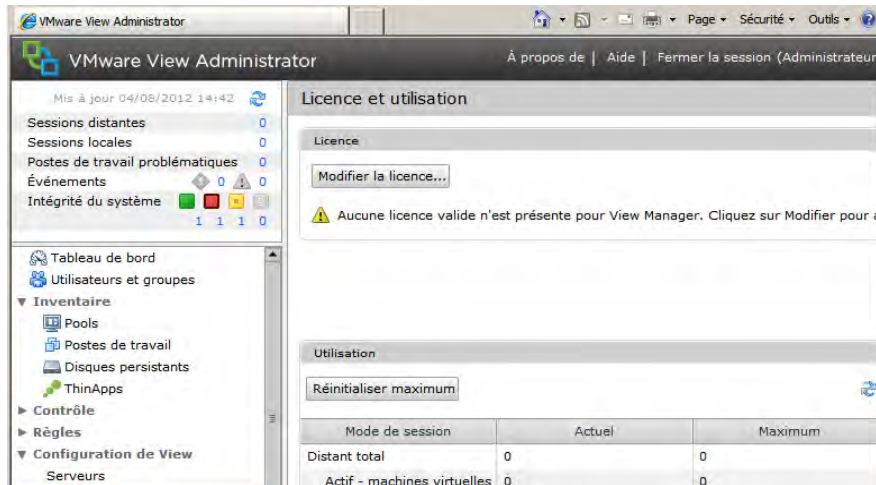
Capture 27:Ouverture de vConnection Server

Lorsque nous cliquons sur **Poursuivre avec ce Web**, nous obtenons l'interface d'authentification à la connexion au serveur. On se « logge » avec les paramètres de l'administrateur local.



Capture 28:Interface de logging de View administrateur

Une fois la connexion authentifiée, nous avons l'interface de configuration du serveur de connexion. Ici nous allons mener une série d'actions.

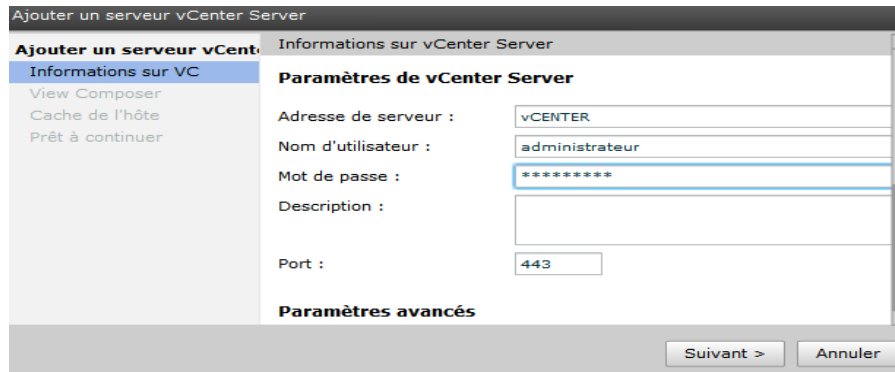


Capture 29:Tableau de bord de view Administrateur

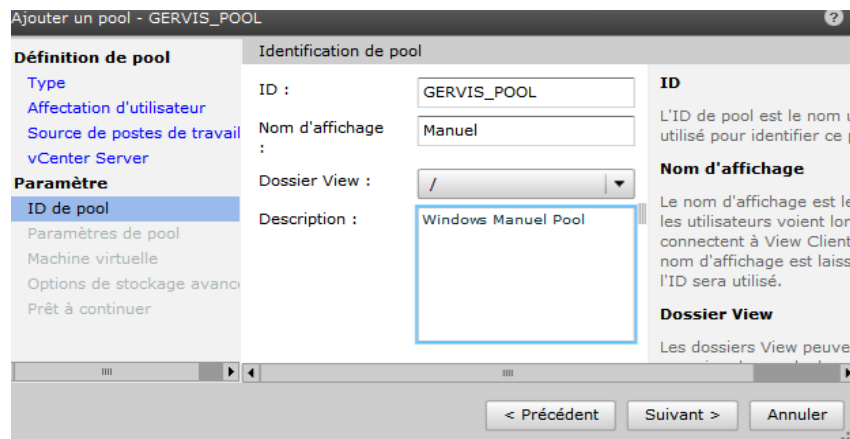
- Activation de la licence : elle consiste à faire un clic sur **Modifier la licence** et à rentrer la clé de licence fournie pour l'évaluation.
- Ajout du vCenter Server : Au niveau du tableau, on clique sur **Serveur** puis **Ajouter**. Dans le formulaire qui s'ouvre, on renseigne les paramètres du vCenter Server à savoir l'adresse du serveur (VC), le nom d'utilisateur de la VM sur laquelle le serveur est installé et son mot de passe. En faisant **Suivant** on est invité à accepter le certificat auto-signé qui a été installé avec vCenter. Et puis on termine l'ajout du serveur en cliquant sur **Terminer** ;
- **Création et activation du pool manuel** : un pool manuel fournit un accès à un jeu existant de machines qui exécute View Agent. Au niveau du tableau de bord, on clique sur **Pools** → **Ajouter** → **Pool manuel** et on fait **Suivant**. On choisit successivement le type d'affectation d'utilisateur, la source de poste de travail, le vCenter Server et les paramètres d'identification du pool qui contiennent notamment le nom du pool et la VM modèle et enfin on clique sur **Terminer** pour finir la création du pool manuel. A cette étape nous sommes invités par un formulaire à renseigner le groupe des utilisateurs autorisés à accéder aux postes de travail. Pour rappel, nous avons au préalable créé ce groupe au niveau d'Active Directory ;



Capture 30:Utilisateur du domaine



Capture 31: Ajout d'un serveur vCenter sur le coursier de connexion



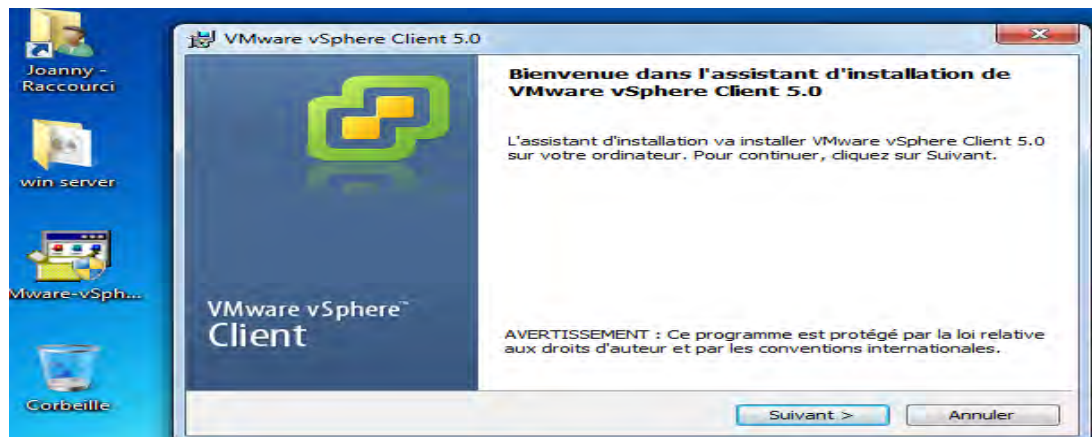
Capture 32: Configuration du Pool

2.3. Composants clients

✓ Installation de vSphere client

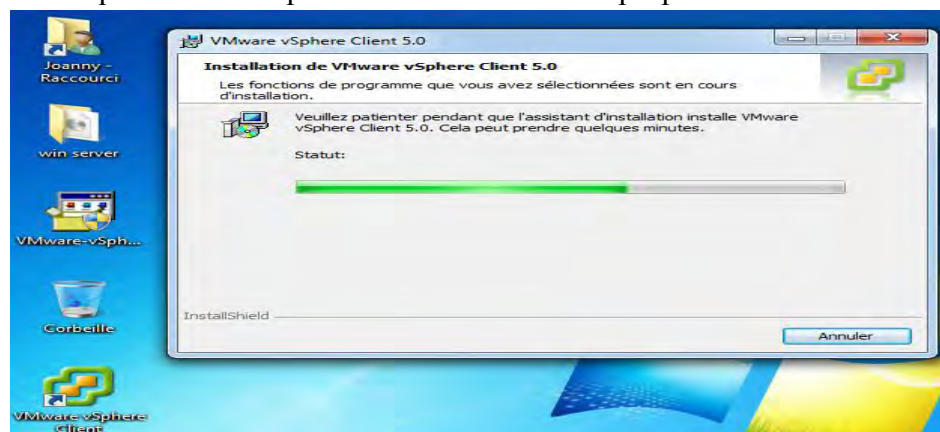
vSphere Client s'installe sur un OS Windows. Dans notre cas, nous l'avons installé sur une VM Windows 7 Edition Intégrale 32bits. Ici c'est donc un fichier ayant l'extension exe que nous allons exécuter pour installation de vSphere Client. A l'exécution, l'installateur VMware vSphere Client prépare l'assistant d'installation. Une fois l'extraction terminée, viennent les étapes suivantes :

- on choisit la langue, l'assistant d'installation apparaît et on fait **Suivant**.



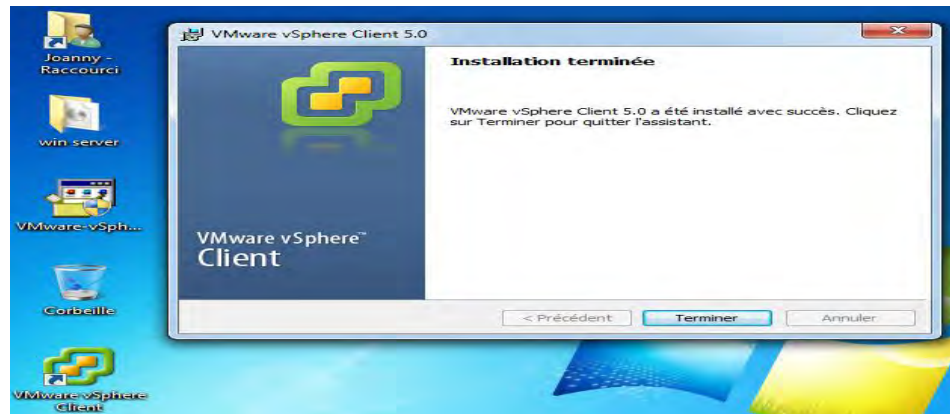
Capture 33:Assistant d'installation de vSphere Client

- on lit le contrat du brevet d'utilisateur final et on fait **Suivant**
- on accepte le contrat de licence et on fait **Suivant**
- on renseigne les informations sur le client c'est-à-dire le Nom d'utilisateur et l'organisation et on fait **Suivant**
- On choisit le dossier de destination d'installation et on fait **Suivant**
- On clique sur **Install** pour débuter l'installation proprement dite.



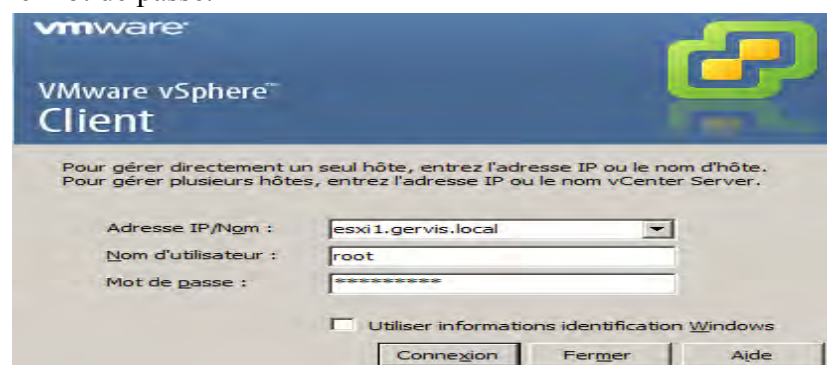
Capture 34:Début installation

- On termine l'installation en cliquant sur **Terminer**.

**Capture 35:Fin installation**

Nous pouvons désormais ouvrir une session sur l'hôte ESXi en faisant un double-clic sur le raccourci de vSphere Client sur le bureau. On obtient alors la boîte de dialogue de VMware vSphere Client pour nous logger. On renseigne :

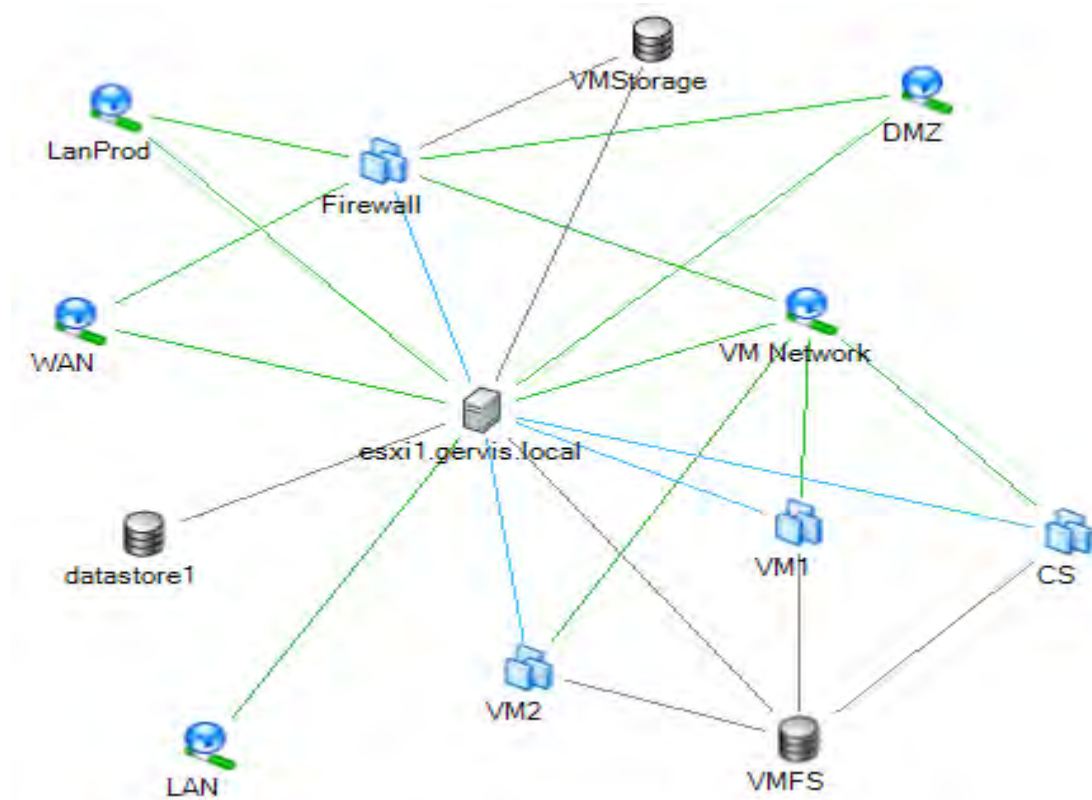
- ✓ Le nom ou l'adresse IP de l'hôte ESXi
- ✓ Le nom d'utilisateur ;
- ✓ Et le mot de passe.

**Capture 36:Interface de login de vSphereClient**

Une fois connecté au serveur ESXi, nous avons créé cinq machines virtuelles à savoir :

- Une VM Windows Server 2008 R2 Standard 64bits nommée DC qui fait office de contrôleur de domaine et sur laquelle nous installerons le serveur SQL pour le vCenter Server;
- Une VM Windows Server 2008 R2 Standard 64bits nommée CS sur laquelle nous installerons le ViewConnection Server ;
- Une VM Windows Server 2008 R2 Standard 64bits nommée VC sur laquelle nous installerons le vCenter Server ;
- Une VM Windows Seven 64bits nommée VM2 sur laquelle nous installerons le View Agent ;
- Une VM Windows XP Pro SP3 32bits nommée VM1 sur laquelle nous installerons View Client;

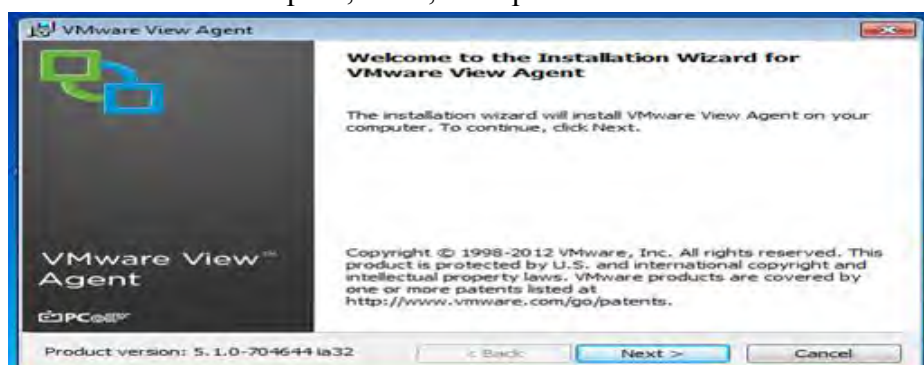
Notre infrastructure ressemblera donc à ceci :



Capture 37:Architecture du Mappage Réseau View

✓ Installation de view agent

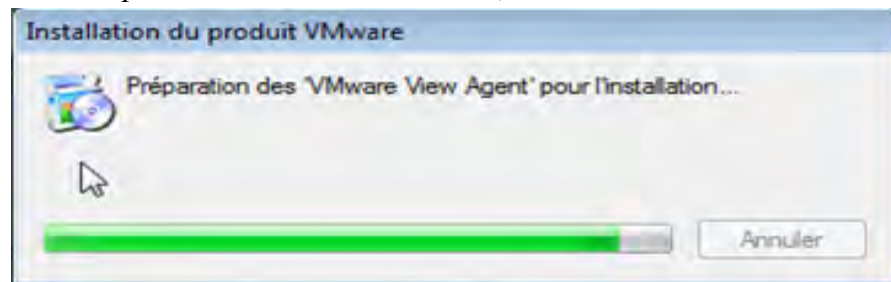
La machine virtuelle View Agent doit être à jour. Pour cela, nous avons téléchargé et installé les mises à jour (voir annexe 4). L'installation de View Agent se fait grâce à un fichier exécutable téléchargeable sur le site de VMware. Une fois exécuté, l'installateur Windows procède à l'extraction des fichiers nécessaires à l'installation pour, enfin, nous présenter l'assistant d'installation.



Capture 38:Assistant d'installation de view Agent

- On clique sur **Next** ;
- On accepte le contrat de licence et on fait **Next** ;

- Un choix automatique des fonctionnalités à installer est faite et on fait **Installe** puis on débute l'installation ;



Capture 39:Assistant d'installation de view Agent en cours

- Enfin on termine l'installation en cliquant sur **Finish**.

2.4. Installation de view Client et connexion à ViewConnection Server

✓ Installation de view Client

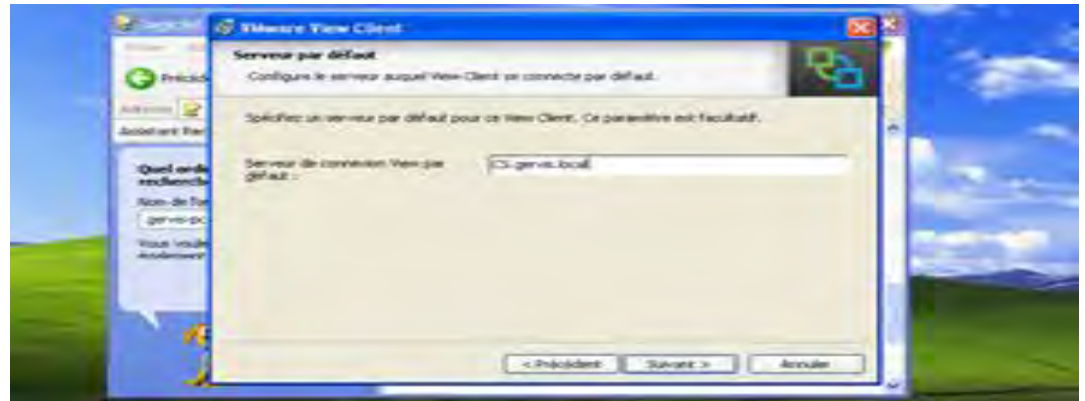
Tout comme le serveur de connexion et le view Agent, view Client aussi s'installe avec un fichier exécutable téléchargeable sur le site de VMware. L'exécution dudit fichier lance l'extraction d'un certain nombre de fichiers nécessaire à l'installation.



Capture 40 : Extraction de fichiers nécessaires à l'installation

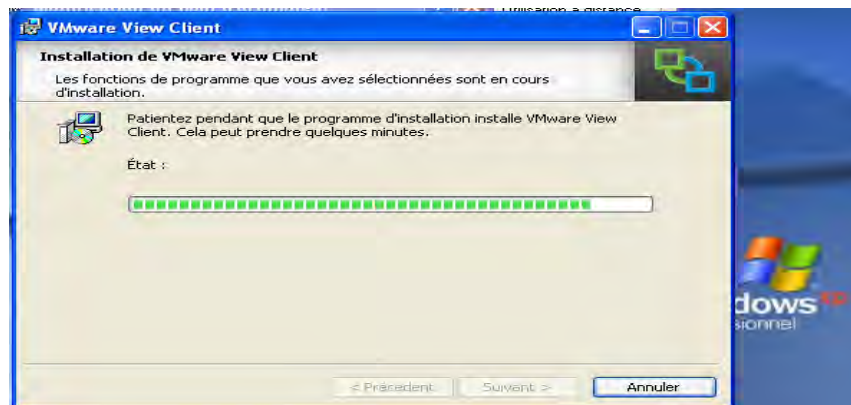
De même de View Agent, l'installation de View Client se fait grâce à un fichier exécutable téléchargeable sur le site de VMware. Une fois le fichier exécuté l'installateur Windows procède à l'extraction des fichiers nécessaires à l'installation pour enfin nous présenter l'assistant d'installation.

- On fait **Suivant** ;
- on accepte le contrat de licence et on fait **Suivant** ;
- on est invité à sélectionner les fonctions du programme à installer et on fait **Suivant** ;
- On renseigne le serveur de connexion auquel View Client se connectera et on fait **Suivant** ;



Capture 41: Indication du Broker par défaut

- On spécifie le répertoire d'installation et on clique sur **Install** pour débuter l'installation proprement dite.



Capture 42: Installation de view Client en cours

- Enfin on fait **Terminer** pour finir complètement l'installation.

2.5. Connexion à ViewConnection Server

➤ Cas d'un PC portable

Lorsque nous faisons un double-clic sur le raccourcis de VMware View Client la boîte de dialogue ci-dessous apparaît avec déjà l'adresse du serveur de connexion que nous avons renseignée plus haut.



Capture 43: Connexion au serveur de connexion

Un clic sur **Configurer SSL...** nous permet de choisir un mode de vérification du certificat. Nous choisissons donc l'option **Autoriser la connexion non vérifiable** parce que nous utilisons un certificat auto-signé c'est-à-dire un certificat qui n'est pas approuvé par un Public Key Infrastructure PKI.



Capture 44: Configuration du ssl

Nous cliquons successivement sur **OK** et **Se connecter** pour avoir la boîte de dialogue d'authentification ci-dessous.

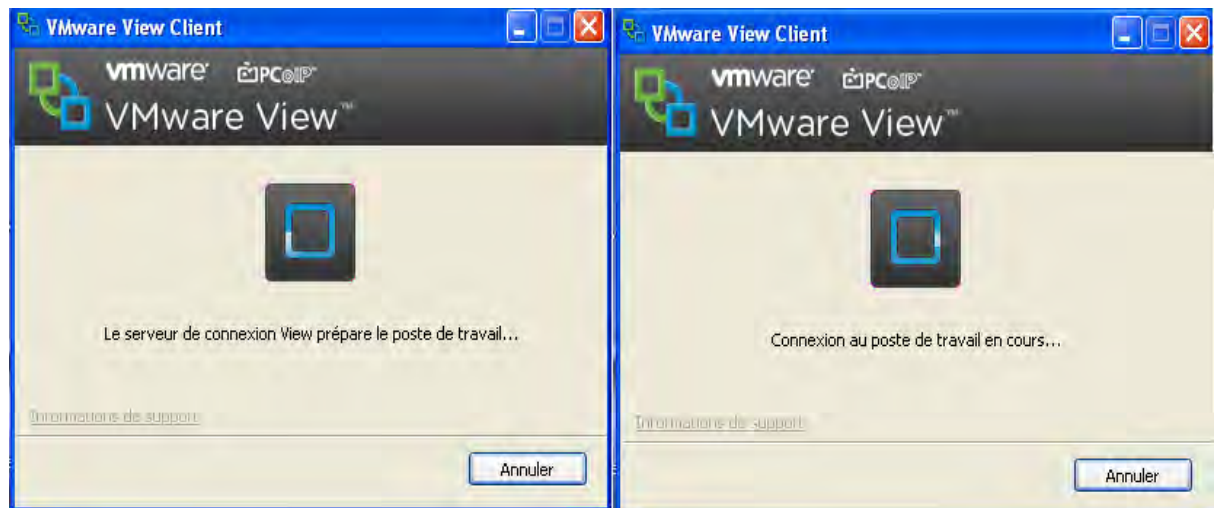


Capture 45: Login de connexion à un bureau virtuel

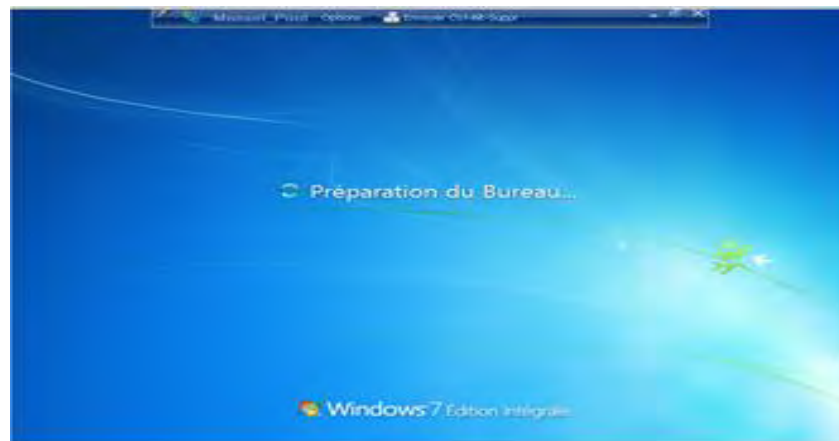
Un clic sur **Connexion** nous présente la boîte de dialogue ci-dessous avec comme information une invitation à se connecter à un poste de travail via le pool que nous avons créé au niveau du viewConnection Server.

**Capture 46: Pool d'accès au bureau virtuel**

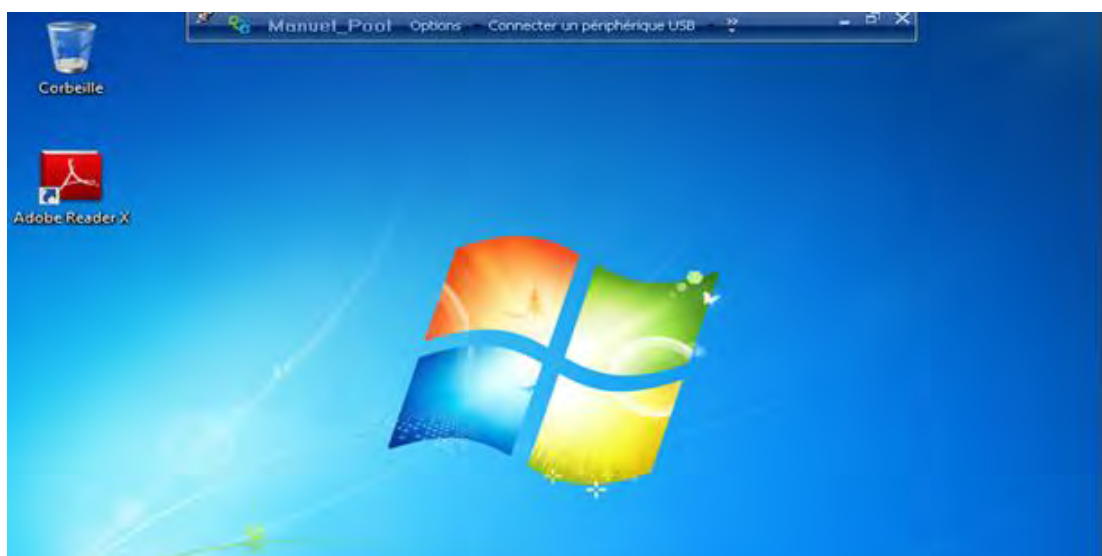
Lorsque nous cliquons sur **Se connecter** nous avons successivement les captures ci-après avant d'avoir notre poste de travail :

**Capture 47: Tentative de connexion au bureau virtuel**

Et nous voilà connecté à notre poste de travail virtuel via un PC physique



Capture 48: Image bureau sur pc



Capture 49: Image du bureau virtuel sur PC physique



Capture 50: Interface View agent

NB : Pour que la connexion au poste de travail virtuel réussisse, ce dernier doit être dans l'état de cette figure.

3. INSTALLATION ET CONFIGURATION D'UN CLUSTER VMWARE VCENTER HA, DRS et DPM

Cette partie traite de l'installation et la configuration d'un Vcenter Cluster de type HA (High Availability) DRS (Distributed Resource Scheduler) et DPM (Dynamic Power Management).

✓ Déblocage des fonctionnalités de vSphere DRS VMotion

Il est question de mettre en place un cluster VMware d'ESXi. Trois fonctionnalités seront activées telles que :

- **HA (High Availability)** : Haute disponibilité des VM en cas de dysfonctionnement/panne d'un ESXi, les VM seront redémarrées sur un autre hôte du cluster.



Figure 18: Architecture HA (High Availability)

- **DRS (Distributed Resource Scheduler)** : Répartition de la charge des VM sur les ESXi afin d'éviter une surcharge d'un hôte, les VM sont déplacées à chaud sur les hôtes du cluster.

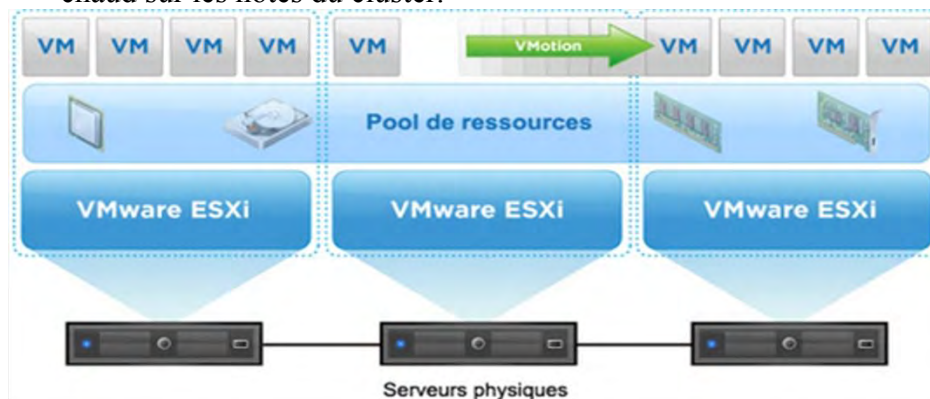


Figure 19: Architecture DRS (Distributed Resource Scheduler)

- **DPM (Dynamic Power Management)** : Permet l'arrêt ou le redémarrage des ESXi à la demande en fonction des besoins en ressources (CPU, RAM) d'un cluster DRS.

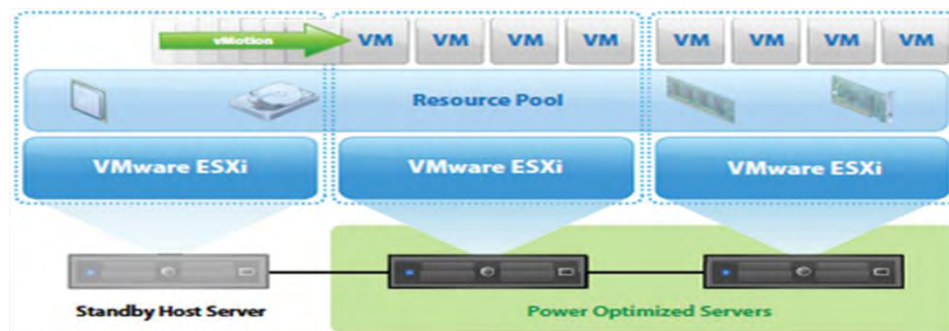


Figure 20: Architecture DPM (Dynamic Power Management)

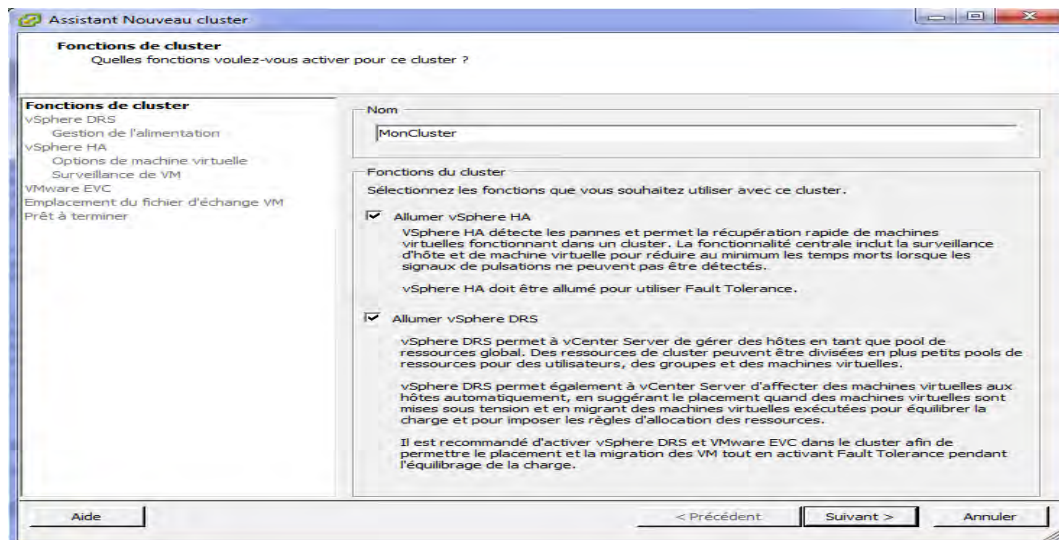
Dans un premier temps, vous devez vous connecter au VCenter via une console Vsphere et créer un centre de donnée: Un centre de données contient les ESXi ou les VM.



Capture 51:Interface de création d'un centre des données

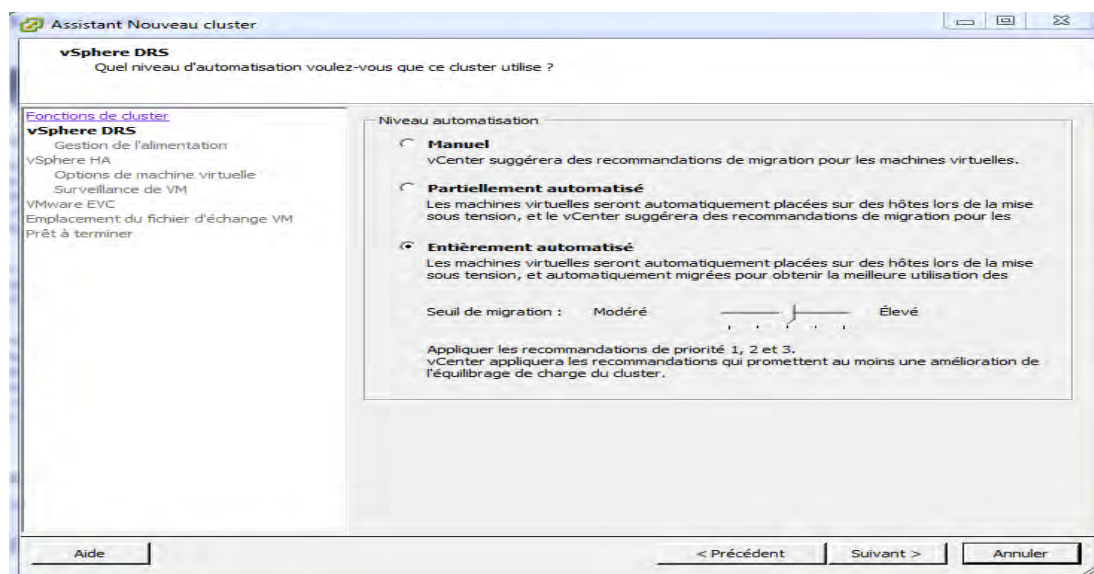
Ensuite faire un clic droit sur le centre de données que vous venez de créer et faire nouveau cluster.

L'assistant de cluster se lance, attribuer un nom au cluster puis sélectionner les fonctions HA et DRS du cluster.



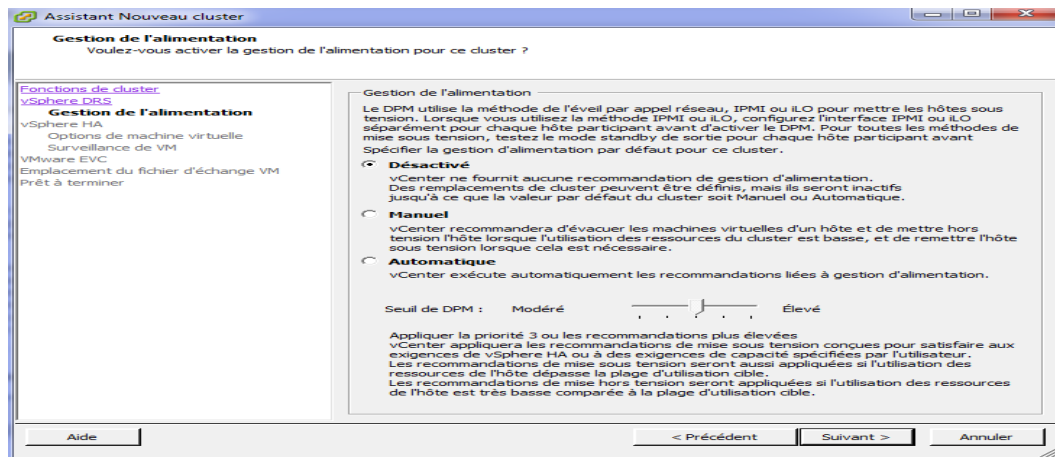
Capture 52: Interface de fonctions HA et DRS du cluster

L'assistant nous propose de paramétrer le DRS, trois modes sont présents, nous optons pour une automatisation entièrement automatisée pour une amélioration de la répartition de la charge au sein du cluster.



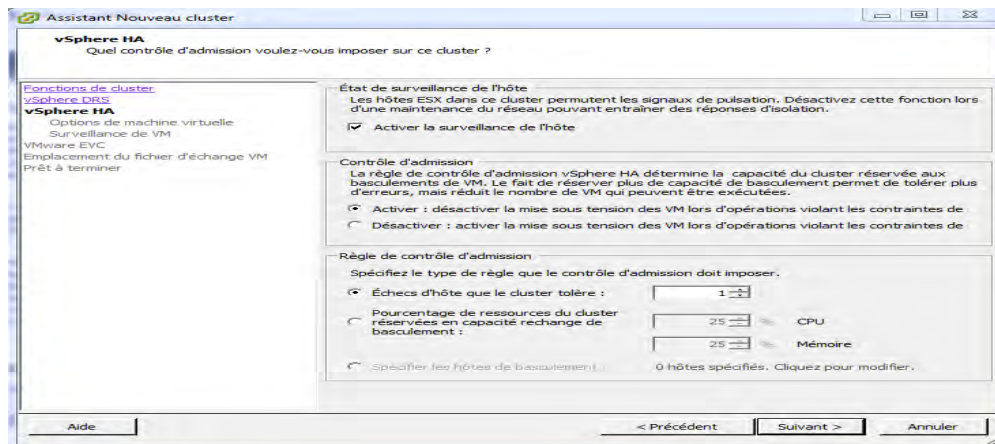
Capture 53: Interface DRS

Ensuite nous passons à la configuration du HA et la partie état de surveillance de l'hôte. Il faut activer la surveillance d'hôte de façon à ce que VMware HA puisse surveiller les pulsations émises par l'agent VMware HA sur chaque hôte dans le cluster. Quand cette option est sélectionnée, chaque hôte du cluster est surveillé pour s'assurer de son bon fonctionnement. En cas de défaillance d'un hôte, les machines virtuelles sont redémarrées sur un autre hôte.



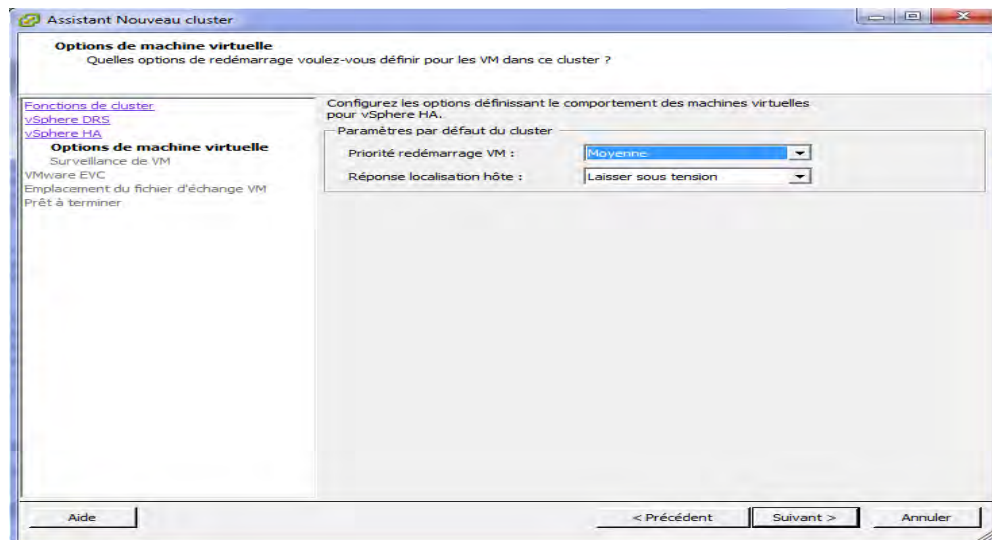
Capture 54:Interface VMware HA

L'assistant permet d'activer ou de mettre hors tension le contrôle d'admission pour le cluster VMware HA et de choisir les règles d'application, nous laissons par défaut.



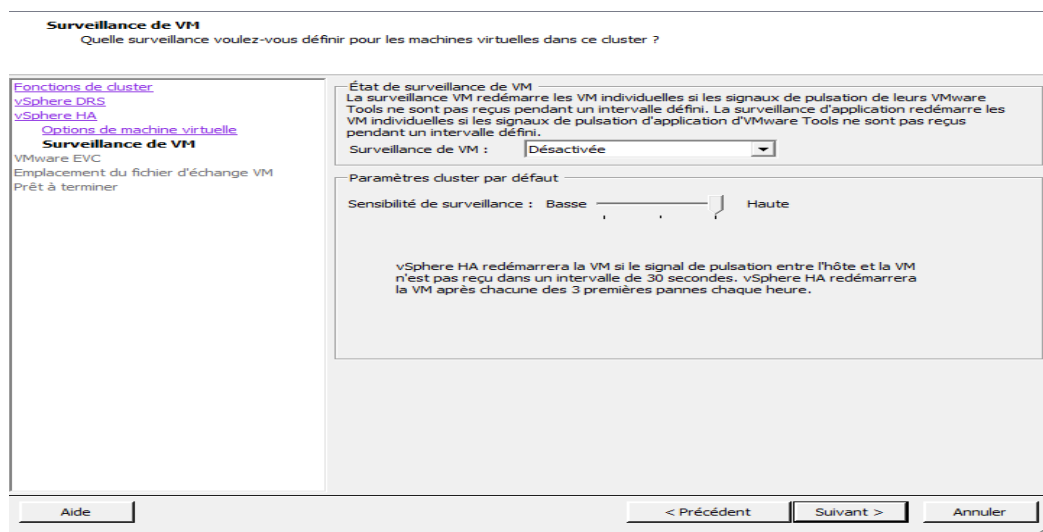
Capture 55 : Interface des règles d'applications du cluster VMware HA

Il faut ensuite définir le type d'ordre dans lequel les machines virtuelles sont redémarrées (priorité de redémarrage VM), ainsi que l'action à effectuer sur les VM en cas de reconnexion de celles-ci sur un autre ESXi.



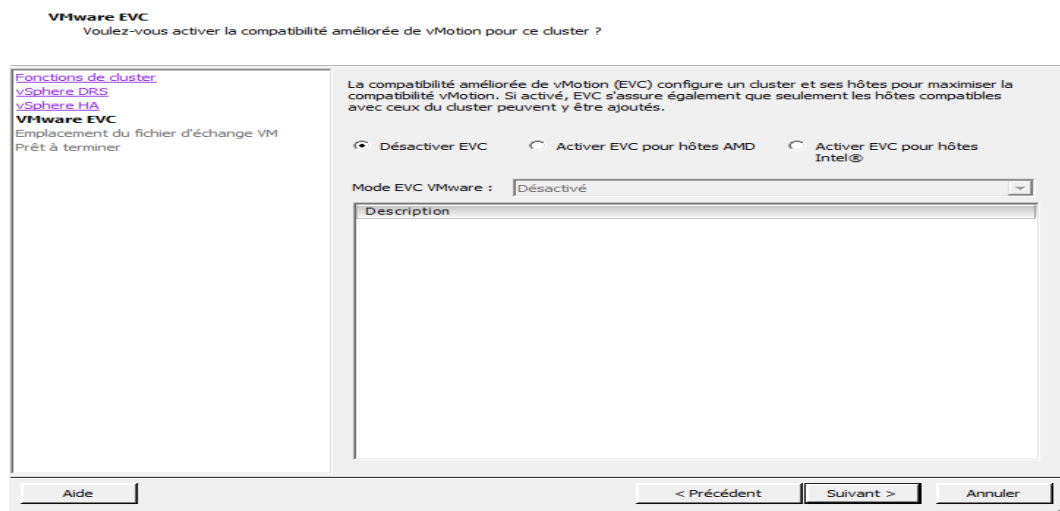
Capture 56:Interface sur fixation de priorité de redémarrage

Vous pouvez ensuite choisir d'activer la surveillance de VM, si vous activez ce monitoring, VMware HA redémarrera automatiquement les VM dont il ne reçoit plus de battement de cœur. Les battements de cœur sont envoyés automatiquement au serveur par les VMware Tools chaque secondes.



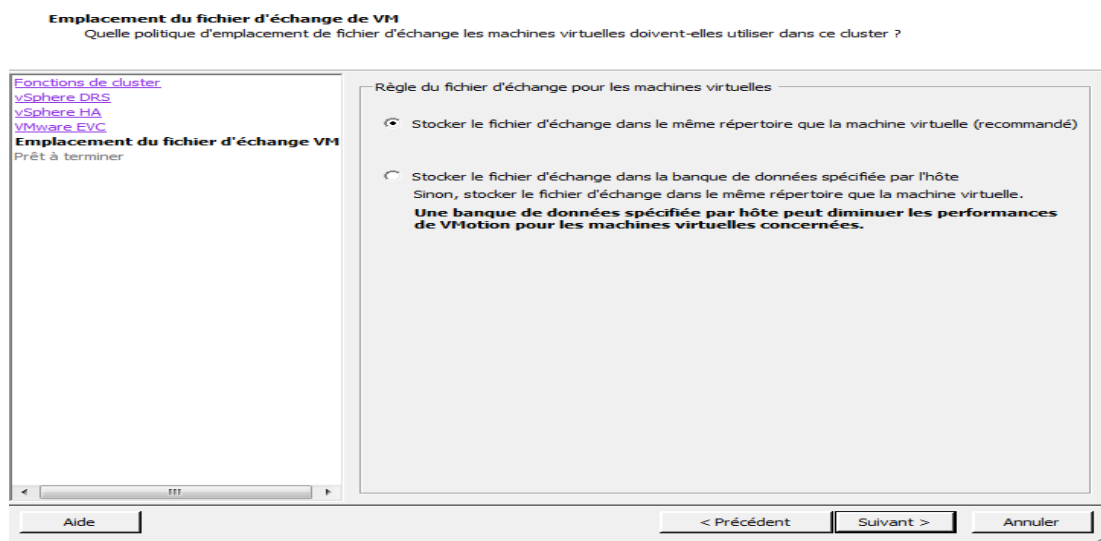
Capture 57:Capture sur VMware HA

Ensuite vient l'activation ou non d'EVC.



Capture 58:Interface d'activation ou non d'EVC

Choisir ensuite où stocker les fichiers Swap des VM, dans le même dossier que les VM (recommandé) ou dans un datastore sélectionné.



Capture 59:Interface permettant de spécifier l'emplacement des fichiers

Pour finir, un récapitulatif de la configuration du cluster.

Prêt à terminer
Vérifiez les options sélectionnées pour ce cluster et cliquez sur Terminer.

Fonctions de cluster	Le cluster sera créé avec les options suivantes :
vSphere DRS	Nom de cluster : MonCluster
vSphere HA	vSphere DRS : Actifé
VMware EVC	Niveau d'automatisation vSphere DRS : Entièrement automatisé
Emplacement du fichier d'échange VM	Seuil de migration vSphere DRS : Appliquer les recommandations de priorité 1, 2 et 3.
Prêt à terminer	Surveillance d'hôte vSphere HA : Exécution
	Contrôle admission : Actifé
	Règle de contrôle d'admission : Nombre de défaillances de l'hôte tolérées par le cluster 1
	Pannes d'hôte autorisées : 1
	Priorité redémarrage VM : Moyenne
	Réponse d'isolement d'hôte : Laisser sous tension
	Surveillance VM vSphere HA : Désactivée
	Sensibilité de surveillance : Haute
	Mode EVC VMware : Désactivé
	Emplacement du fichier d'échange de VM : Même répertoire que la machine virtuelle

Aide < Précédent Terminer Annuler

Capture 60:interface récapitulatif de la configuration du cluster

Une fois que le cluster est créé, il ne reste plus qu'à ajouter des machines hôtes ESXi au cluster du VCenter.

Vous devez faire un clic droit et ajouter un hôte pour introduire votre premier ESXi au cluster. Spécifier le nom d'hôte ou l'IP ainsi que le compte root.

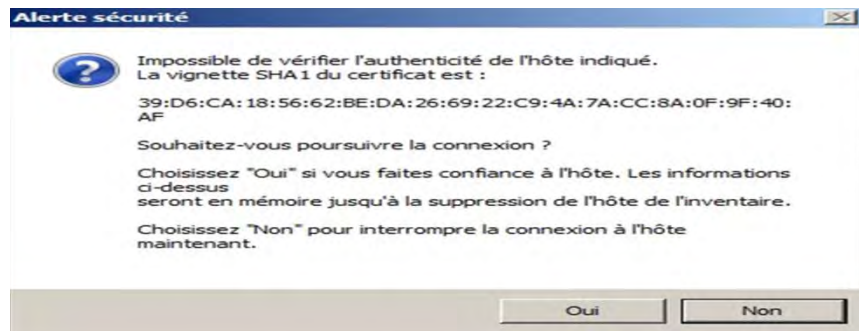
Spécifier paramètres connexion
Entrez les informations utilisées pour se connecter à cet hôte.

Paramètres de connexion	Connexion
Résumé hôte	Entrez le nom ou l'adresse IP de l'hôte à ajouter au vCenter.
Prêt à terminer	Hôte : esxi1
	Autorisation
	Entrez les informations de compte d'administration de l'hôte. vSphere Client utilisera ces informations pour se connecter à l'hôte et établir un compte permanent pour ses opérations.
	Nom d'utilisateur : root
	Mot de passe : *****

Aide ≤ Précédent Suivant ≥ Annuler

Capture 61:Interface d'administration de l'hôte

Faites oui pour poursuivre.

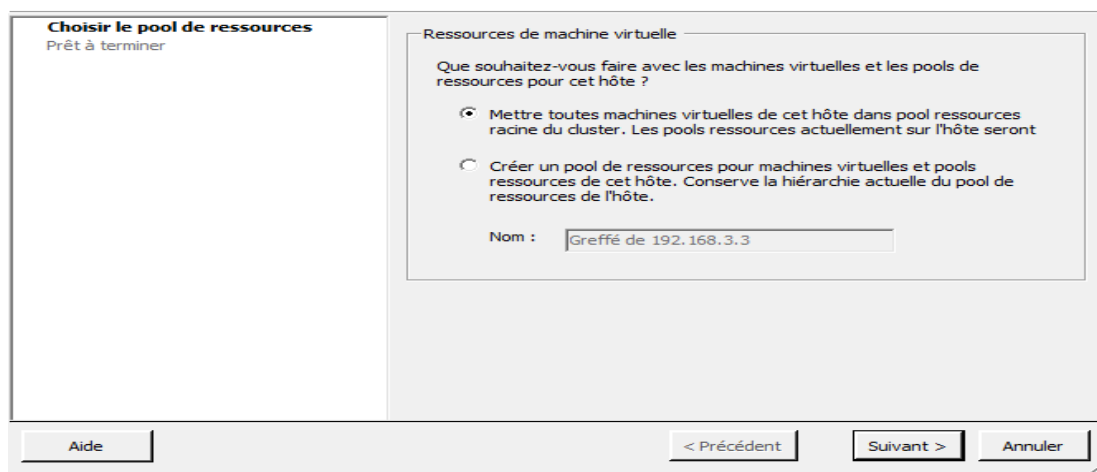
**Capture 62: Certificat non identifié SHA1**

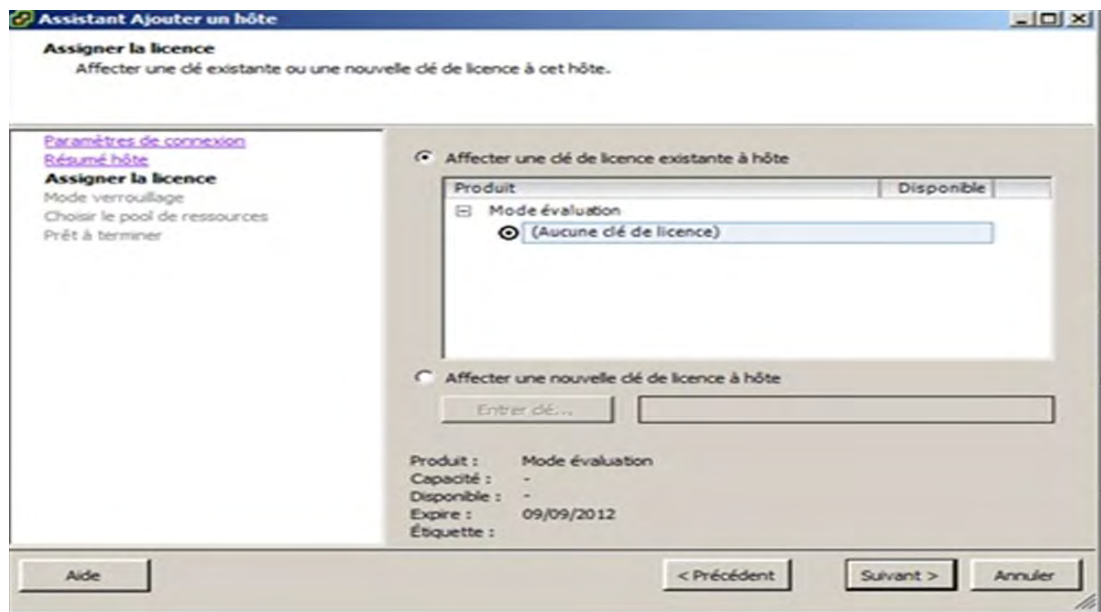
Un récapitulatif des objets de l'ESXi vous sont présentés, ici qu'une VM est présente.

Introduire une licence adéquate pour le cluster si vous en avez (Advanced, entreprise plus...).

Choisir le pool de ressources de destination

Choisir où placer les machines virtuelles de cet hôte dans la hiérarchie du pool de ressources.

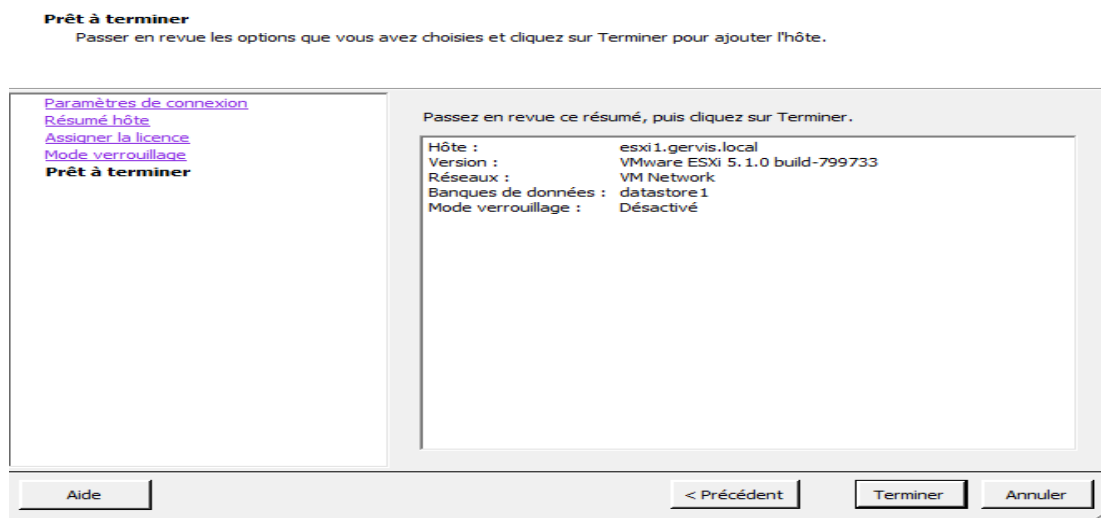
**Capture 63:Interface Pool Ressources de destination**



Capture 64:Interface d'assignation de la licence

L'assistant vous propose de placer les VM dans un pool de ressources particuliers, cette fonction permet de limiter les performances d'un nombre de VM.

Un récapitulatif de l'ESXi vous sont présentés, nous pouvons apercevoir les datastores, les réseaux ainsi que la destination cluster.



Capture 65:Interface d'assignation de la licence



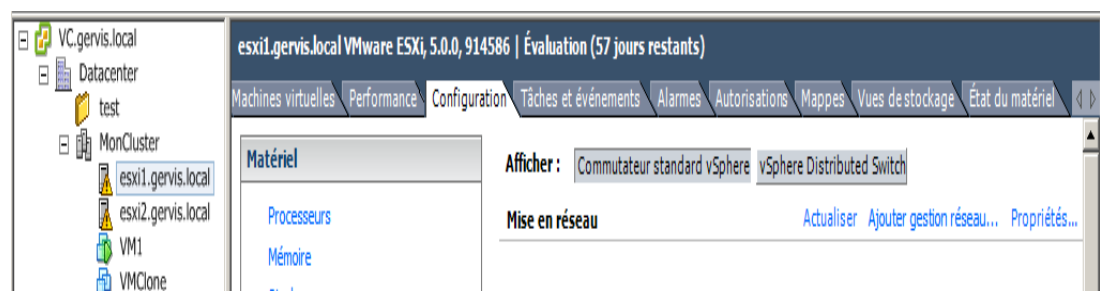
Capture 66: Interface récapitulatif

Une fois terminé, vous pouvez voir l'avancement de la configuration de l'hôte dans le cluster, cette opération prend quelques minutes

Tâches récentes								
Nom, Cible ou Statut contient :								
Nom	Cible	Statut	Détails	Lancé par	vCenter Server	Heure de début de...	Heure de début	Heure de fin
Ajouter hôte	Haute Digo	En cours		admin	VCENTERS	11/07/2012 15:20:14	11/07/2012 15:20:16	
Ajouter hôte	Haute Digo	85%		admin	VCENTERS	11/07/2012 15:19:37	11/07/2012 15:19:37	

Capture 67: Interface d'avancement de la configuration

Et voilà votre cluster est installé et vos VM sont normalement répartis, à noter que dans notre cas ci-dessous le DPM n'a pas mis en veille un des ESXi puisqu'il considère qu'il n'aura pas assez de ressource pour satisfaire le besoin des VM.



Capture 68: Vue générale des hôtes esxi dans un cluster

4. Création et attribution des droits des utilisateurs et de groupes

IP adresse de ESX est : 192.168.3.30 et VCenter est : 192.168.3.15

✓ Création des utilisateurs et groupes dans ESX/ESXI

▪ Créer un groupe sur l'hôte ESX:

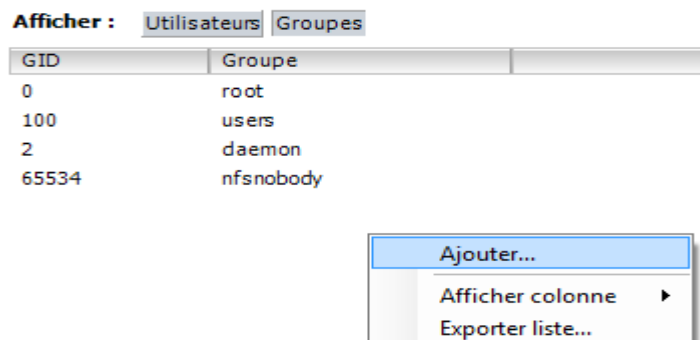
Pour créer un groupe sur l'hôte ESX il faut se connecter avec le vSphere Client sur l'hôte ESX est non sur le vCenter.



S'authentifier sur le Serveur ESXi

Capture 69:Connexion sur vClient

- Allons dans l'onglet "Utilisateurs et groupes locaux".
- Affichons les "Groupes"
- Faisons un clic droit puis "Ajouter..."



Capture 70:Création d'un Groupe sur ESX

Saisissons un nom pour notre groupe et éventuellement un ID. Dans notre cas nous appelons le groupe "Madgatdsi".

Capture 71:Création d'un Groupe sur ESX

Le groupe est désormais créé, nous allons maintenant créer un utilisateur et l'ajouter à ce groupe.

○ **Créer un utilisateur sur l'hôte ESX :**

Allons dans l'onglet "Utilisateurs et groupes locaux". Affichons les "Utilisateurs" et faisons clic droit puis "Ajouter..."

Afficher : Utilisateurs Groupes

UID	Utilisateur	Nom
65534	nfsnobody	Anonymous NFS User
501	btsig	ESXi User
2	daemon	System daemons
0	root	Administrator
500	vpuser	VMware VirtualCenter administration account
100	dcui	DCUI User

Ajouter...
 Afficher colonne ▶
 Exporter liste...

Capture 72:Création d'un utilisateur d'hôte

Ensuite, saisissons le nom de connexion dans "**Connexion**" ainsi qu'un mot de passe (qui est obligatoire et qui doit être **complexe** sinon il y aura une erreur lors de la création), le "Nom" et le "UID" sont facultatifs. Affecter l'utilisateur à un groupe en sélectionnant le groupe et en cliquant sur "**Ajouter**". Un utilisateur peut appartenir à plusieurs groupes.

Capture 73:Interface d'ajout d'un utilisateur

- Attribuer un rôle au groupe ou à l'utilisateur pour lui donner des autorisations sur l'hôte ESX

Il faut attribuer un rôle au groupe ou à l'utilisateur, un rôle qui correspondra à ce qu'il a le droit de faire et ne pas faire sur l'hôte ESX à partir du clientvSphere.

Pour cela :

- Accédons à l'onglet "**Autorisations**" et un Clic droit sur "**Ajouter autorisation**"

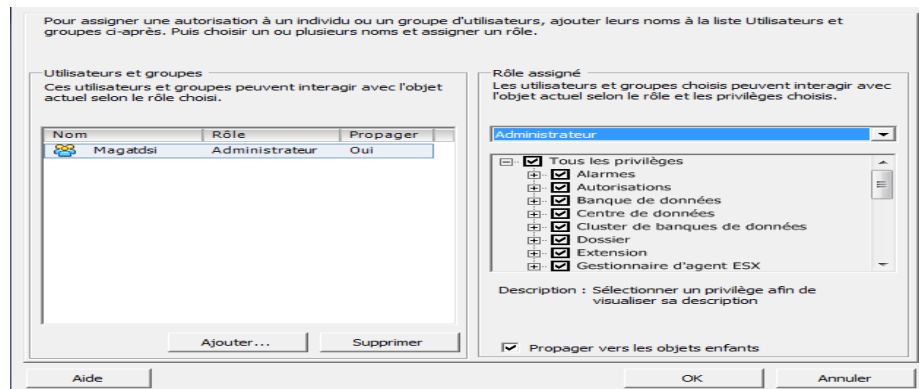
Capture 74:Ajout d'un utilisateur dans un groupe

- Cliquez sur "**Ajouter**"

Sélectionnez le groupe ou l'utilisateur que auquel vous souhaitez attribuer un rôle puis cliquant sur "**Ajouter**" et sur "**OK**".

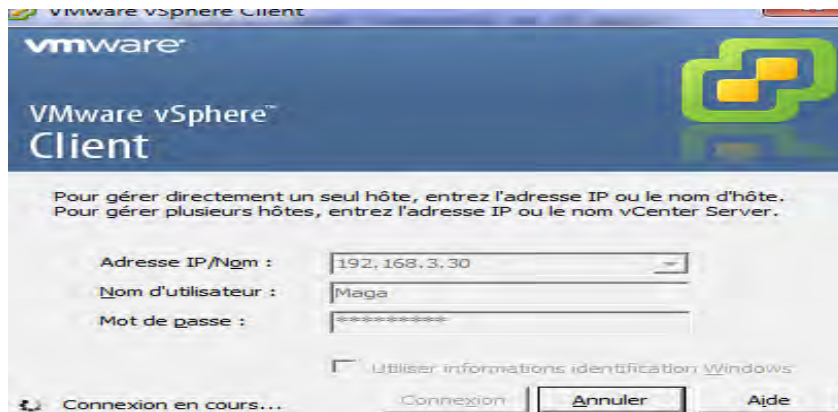
Ensuite, dans le champ "**Rôle assigné**" vous devez sélectionner le rôle que vous souhaitez attribuer à cet utilisateur ou ce groupe d'utilisateurs, puis confirmez en

cliquant sur "OK".



Capture 75:Attribution d'un rôle

Il est désormais possible de se connecter à l'hôte ESX (**pas au vCenter**) avec les utilisateurs du groupe Magatdsi avec.



- S'authentifier sur le Serveur ESXi avec l'utilisateur.
 - ✓ **Les utilisateurs et les groupes pour le vCenter**

Cela ne se fait pas à partir du client vSphere mais vous devez créer un utilisateur ou un groupe directement avec le serveur sur lequel est installé le vCenter, cela revient à créer des utilisateurs et groupes Windows. Vous ne verrez pas les utilisateurs créés sur l'hôte ESX et les autorisations effectuées avec le vSphere client directement sur l'hôte ESX ne seront pas répliquées dans la base de données du vCenter, c'est pour cela qu'il vaut mieux faire tout à partir du vCenter si vous l'utilisez. Au cas où vous avez seulement un hôte ESX, autant tout gérer avec les groupes et utilisateurs Linux.

○ **Sur Windows:**

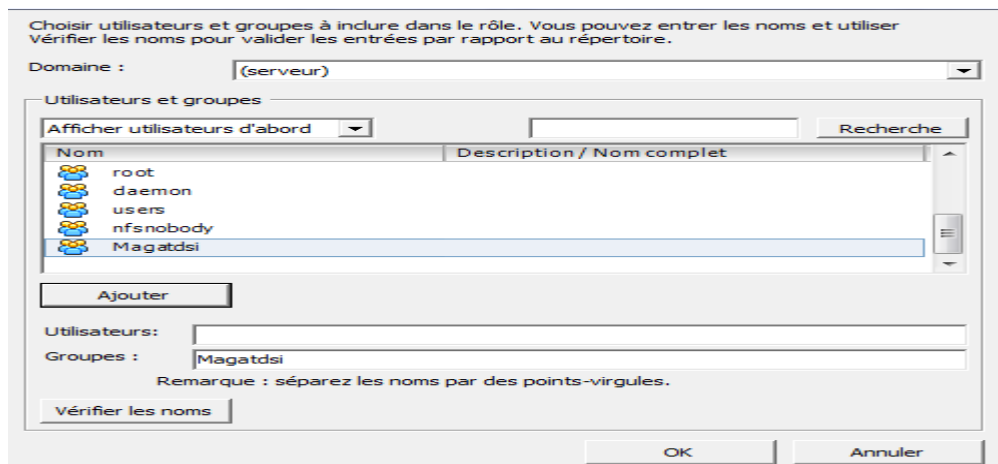
Créez un compte Windows sur le serveur vCenter et définissez lui un mot de passe.

- ✓ **Avec le vSphere client (connecté au vCenter) :**

Sélectionnez l'objet sur lequel vous souhaitez ajouter une autorisation (cela peut être l'intégralité du vCenter, uniquement sur un centre de données, un pool de ressources ou un hôte ESX).

N.B: les autorisations appliquées sur un objet parent peuvent être répliquées sur les objets enfants.

- Accédons à l'onglet "**Autorisations**" puis un Clic droit "**Ajouter autorisation**"

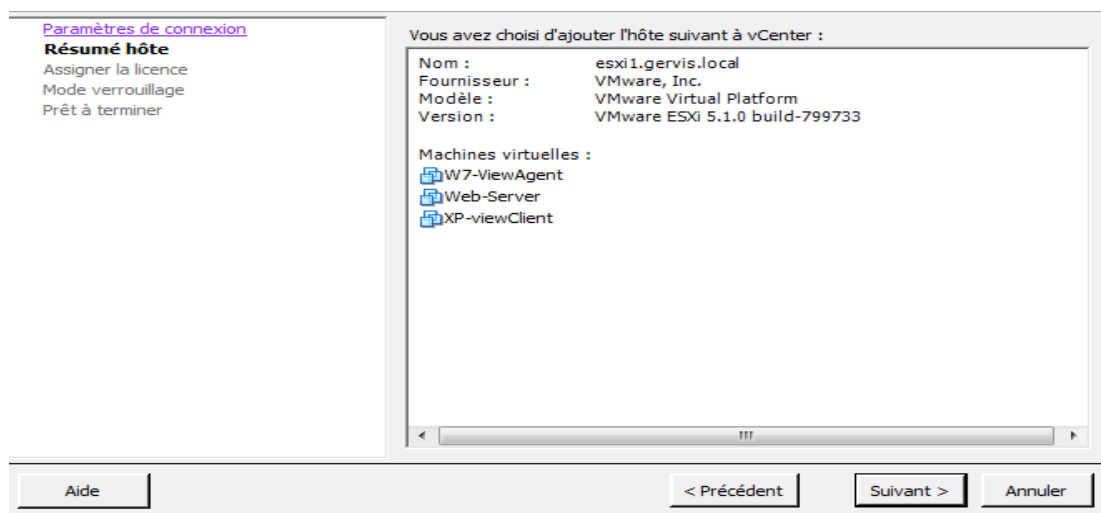


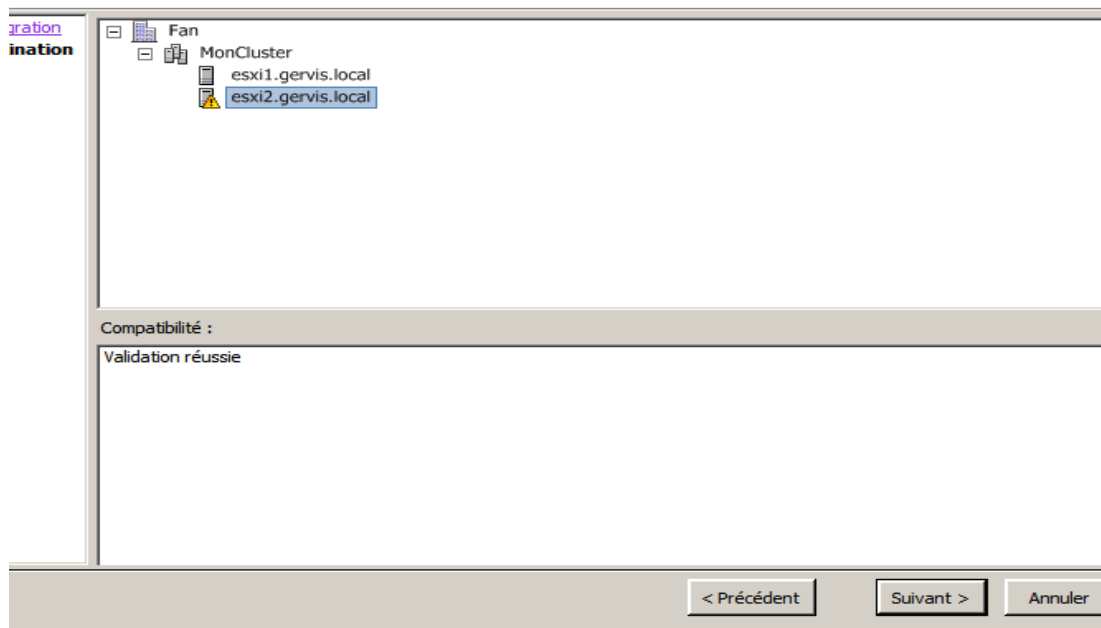
Capture 76: Ajout d'une autorisation

Pour ajouter une autorisation c'est le même principe qu'avec les utilisateurs Linux. Pour que les autorisations appliquées à un objet parent s'applique sur les objets enfants il faut cocher la case "**Propager vers les objets enfants**".

Informations hôte

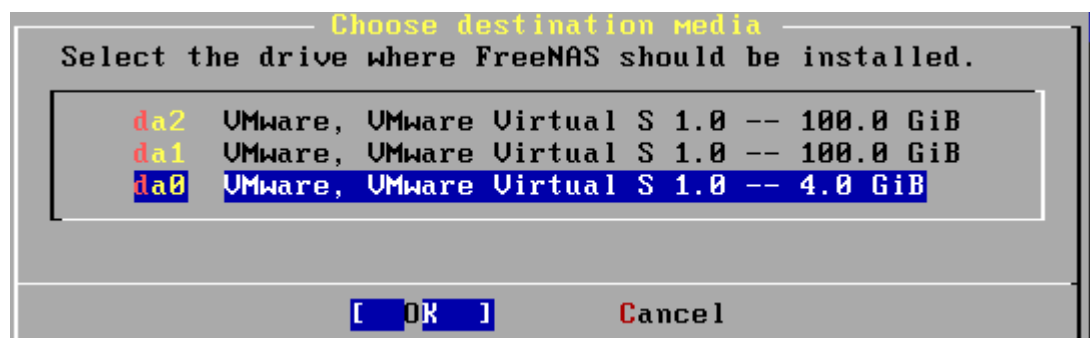
Examiner les informations produit pour l'hôte spécifié.



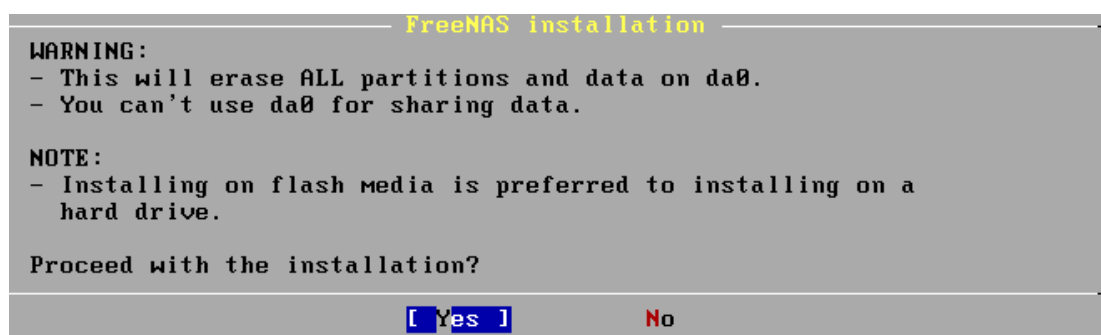


5. Installation et configuration de l'architecture de stockage (FreeNas)

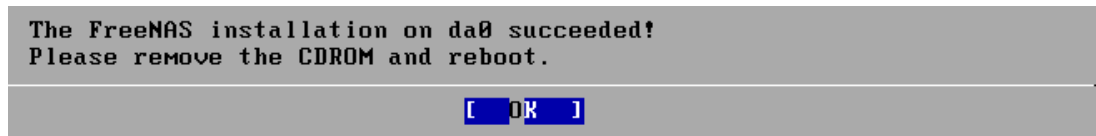
Télécharger l'image iso sur la page Téléchargements du site <http://www.freenas.org/> et gravez un cdérom à l'aide de cette image.



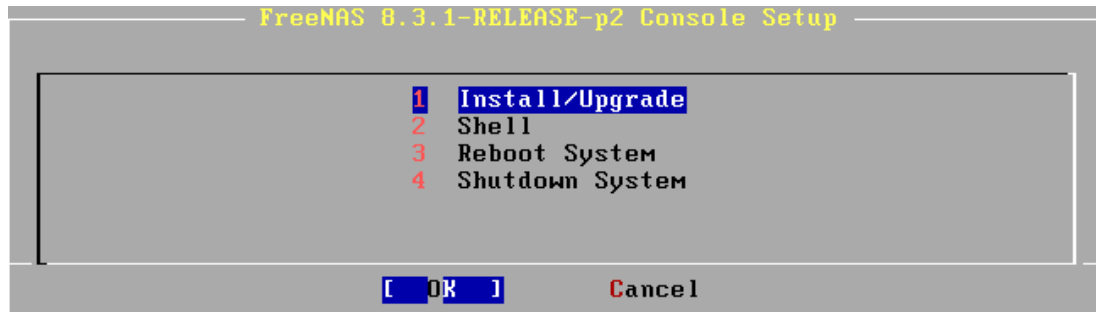
Capture 77: Choix de l'espace du stockage de l'os de FreeNAS



Capture 78: Début de l'installation

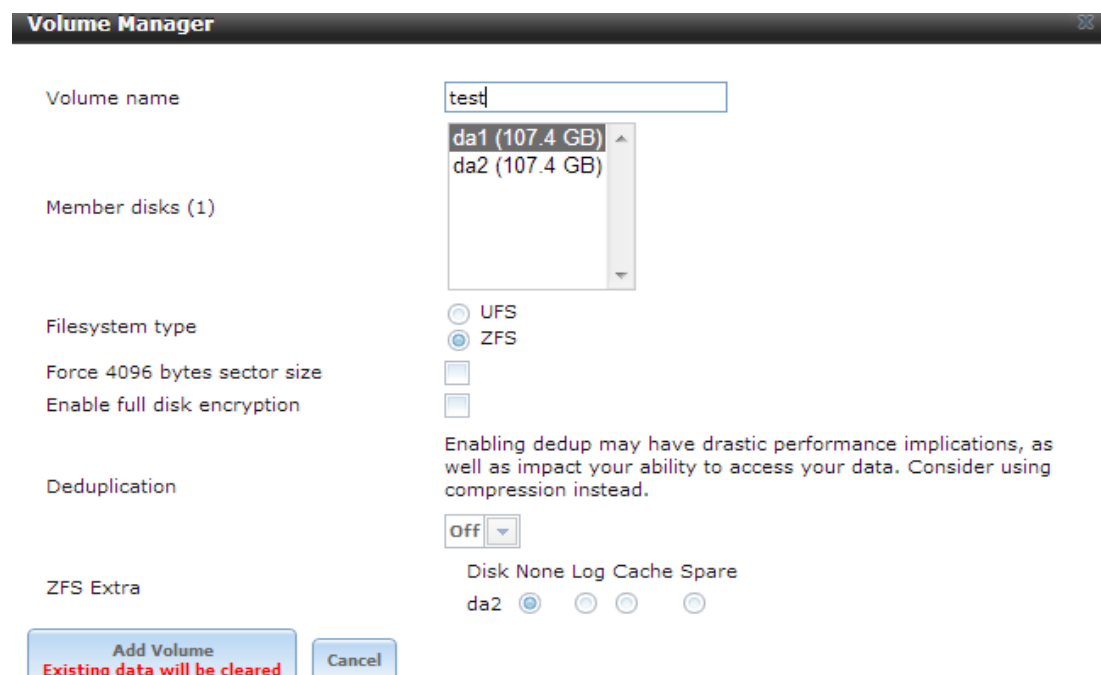


Capture 79:Fin de l'installation



Si vous avez des disques non formatés ou si vous souhaitez écraser le système de fichiers (et données) sur vos disques, utilisez l'écran Créer un volume pour formater les disquettes désiré comme un volume UFS ou un pool ZFS.

Si vous cliquez sur le stockage -> Volumes -> Créer un volume



Capture 80:Configuration de l'espace de stockage (RAID)

Un volume ZFS existant peut être divisé en groupes de données. Cela vous permet de créer un ensemble de données par action, permettant plus de granularité sur laquelle les utilisateurs ont accès à quelles données. Un ensemble de données est similaire à un dossier en ce que vous pouvez définir des autorisations s'il est

aussi semblable à un système de fichiers en ce que vous pouvez définir des quotas et la compression.

- **REMARQUE:** si votre but est de partager un volume entier de ZFS, vous n'avez pas à créer des ensembles de données. Si vous souhaitez diviser les données d'un volume ZFS en actions différentes, de créer un dataset pour chaque action.

Si vous cliquez sur Volumes -> Créer ZFS DataSet, vous verrez l'écran de la figure suivante. Notez que cette option de menu n'est pas disponible qu'après que vous avez créé un volume ZFS.

Change Permissions

Change permission

Change permission on /mnt/test/Backup to:

Owner (user)	root																
Owner (group)	wheel																
Mode	<table border="1"> <thead> <tr> <th></th> <th>Owner</th> <th>Group</th> <th>Other</th> </tr> </thead> <tbody> <tr> <td>Read</td> <td>☒</td> <td>☒</td> <td>☒</td> </tr> <tr> <td>Write</td> <td>☒</td> <td>☐</td> <td>☐</td> </tr> <tr> <td>Execute</td> <td>☒</td> <td>☒</td> <td>☒</td> </tr> </tbody> </table>		Owner	Group	Other	Read	☒	☒	☒	Write	☒	☐	☐	Execute	☒	☒	☒
	Owner	Group	Other														
Read	☒	☒	☒														
Write	☒	☐	☐														
Execute	☒	☒	☒														
Type of ACL	☒ Unix ☐ Windows																
Set permission recursively	☐																

Change **Cancel**

Capture 81:Permission pour les groupes d'utilisateurs

Add Dataset

Dataset Name: Backup

Compression level: Inherit

Enable atime:

- ☒ Inherit
- ☐ On
- ☐ Off

Quota for this dataset: 0

Quota for this dataset and all children: 0

Reserved space for this dataset: 0

Reserved space for this dataset and all children: 0

ZFS Deduplication:

Enabling dedup may have drastic performance implications, as well as impact your ability to access your data. Consider using compression instead.

Inherit

Add Dataset **Cancel**

Add Unix (NFS) Share

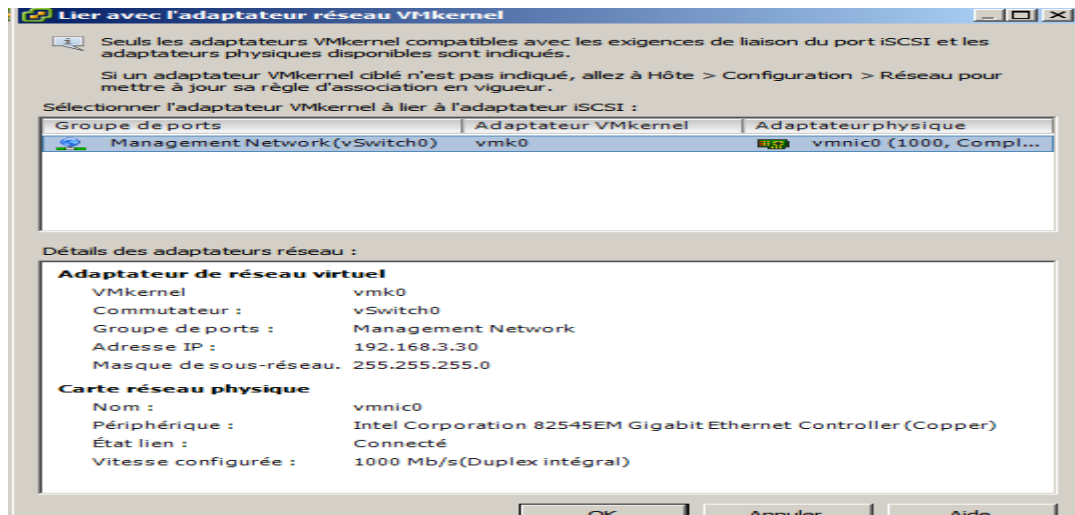
Comment	NFS
Authorized networks	
Authorized IP addresses or hosts	192.168.3.0/24
All Directories	☐ <i>i</i>
Read Only	☐ <i>i</i>
Quiet	☐ <i>i</i>
Maproot User	root <i>i</i>
Maproot Group	N/A <i>i</i>

Capture 82: Configuration du réseau

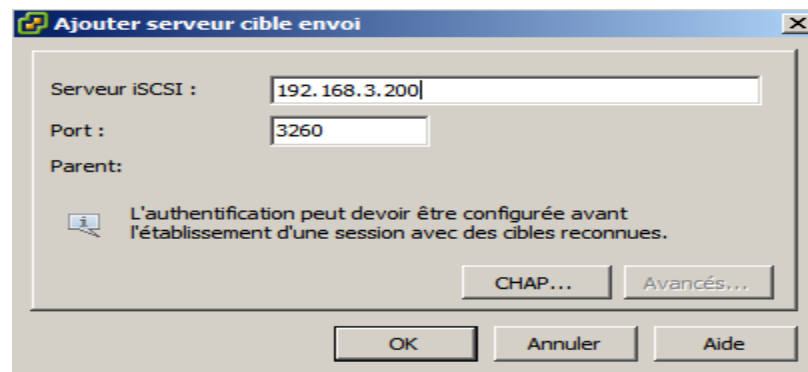
Target Name	100GB <i>i</i>
Target Alias	100G <i>i</i>
Serial	000c299bf5fd00 <i>i</i>
Target Flags	read-write
Portal Group ID	1 (testPortal)
Initiator Group ID	1 (iSCSinit)
Auth Method	Auto <i>i</i>
Authentication Group number	None
Queue Depth	32 <i>i</i>
Logical Block Size	512 <i>i</i>

OK Cancel

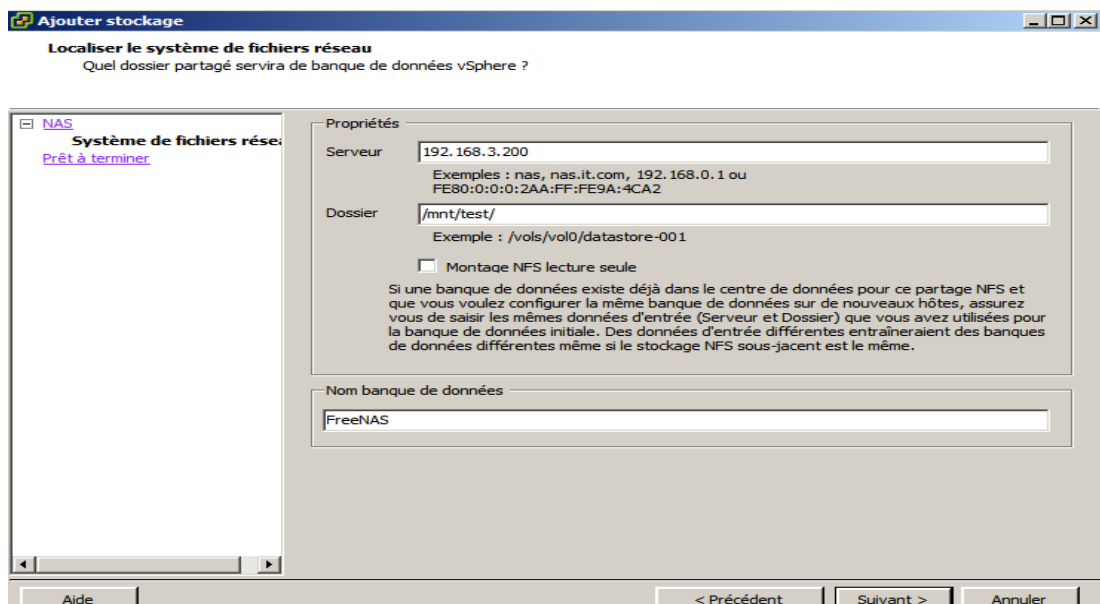
Capture 83: Configuration de l'espace de partage



Capture 84: Liaison de l'adaptateur réseau



Capture 85: Ajout du Stockage FreeNAS dans ESXi



Capture 86: Montage de FreeNas dans Esxi

CONCLUSION

En définitive le Datacenter répond à des besoins de plus en plus croissants dans l'univers de l'informatique : sauvegarde à distance, externalisation de sa salle serveur, virtualisation des applications. La sauvegarde à distance qui pourrait devenir un premier levier pour intéresser les chefs d'entreprise. Le nombre d'applications transférables sur un Datacenter est conséquent. Pour des PME voulant externaliser une partie de son SI, ou louer des services à la consommation des solutions **Cloud Computing** existent avec un maillon des services (*Paas : Platform as a service ; Iaas : infrastructure as a service ; Saas Software as services*).

La multiplication des données, le nombre croissant d'informations à conserver sur support magnétique, la complexité des applications, les ressources matérielles en constante progression sont des raisons qui nous ont orientées vers la mise en place d'un DATACENTER. La réalisation de ce travail a été très fastidieux dans la mesure où nous n'avons pas d'équipements ayant les capacités requises pour implémenter cette technologie en mode réelle de production car elles coutent excessivement chers. Mais nous avons néanmoins pu contourner la situation en utilisant la version d'évaluation de 60 jours proposés par VMware qui fournit des fonctionnalités réduites en mode de production. Ce projet m'aura également permis de me familiariser avec du matériel professionnel grâce à une visite effectuée au sein de la douane et aux différents échanges avec le personnel technique, que je tiens encore à remercier. Ainsi, mes connaissances, des produits VMware et de matériels professionnels se sont vues enrichies. Mais comme dans toute œuvre humaine il y'a toujours des imperfections ; ainsi les difficultés rencontrées et les implémentations non réalisées ont été mis en perspectives fautes d'acquisition de licence dont cout est extrêmement élevés. Comme perspectives nous avons :

- ✓ La Mise en place d'une DMZ avec VMware VShield
- ✓ Déploiement d'un PKI sur les sites WEB et le serveur de messagerie

Enfin le Datacenter offre une fonctionnalité nommée VMotion qui permet de migrer à chaud des machines virtuelles d'un cluster d'un hôte ESXi à un autre. La migration à chaud d'une machine virtuelle peut se faire sans interruption de service, ce qui rend le processus totalement transparent. La migration à chaud peut être utilisée pour mettre en œuvre l'équilibrage de charge, afin d'optimiser l'utilisation des ressources et de mieux gérer et économiser l'énergie. Elle est susceptible d'être très utile pour la maintenance d'infrastructures physiques. Elle permet également d'améliorer la tolérance aux fautes : si une défaillance imminente est suspectée, le problème peut être résolu avant d'interrompre le service.

BIBLIOGRAPHIES

- ✓ Livre blanc « Cloud Computing et confidentialité » Microsoft, Novembre 2009
- ✓ Livre blanc « La protection de la vie privée à l'ère du Cloud Computing - Le point de vue de Microsoft », Microsoft, Novembre 2009
- ✓ Livre blanc « Windows Azure™ Security Overview » par Charlie Kaufman et Ramanathan Venkatapathy.
- ✓ Livre blanc « Le Cloud en toute confiance » Septembre 2010
- ✓ Regards sur le numérique, hors-série, « Le Cloud Computing, qu'est que ça va changer ».
- ✓ Syntec Informatique, « Le livre blanc du Cloud Computing »
- ✓ Livre blanc de François Tonic « Cloud Computing » Septembre 2009.
- ✓ Cloud Computing & SaaS de Guillaume Plouin, éditions Dunod, mars 2009.

WEBOGRAPHIE

[1]<http://www.vmware.com/fr>

Pour accéder aux supports et téléchargement [Juin-Juillet 2012]

[2]https://my.vmware.com/fr/web/vmware/info/slug/desktop_end_user_computing/vmware_view/5_1

Téléchargement de vmwareview (view client, view agent, viewThinApp,) et vmwareworkstation [Juin-Juillet 2012]

[3]<https://play.google.com/store/search?q=vmware+view&c=apps&rdid=com.vmware.view.client.android&rdot=1>

Téléchargement de vmwareview client for android [19 Août 2012]

[4]https://my.vmware.com/fr/web/vmware/info/slug/datacenter_cloud_infrastructure/vmware_vsphere/5_0

Téléchargement de vSphere et vCenter [Juillet 2012]

[5]http://www.vmware.com/files/fr/pdf/UsingVMwareViewClientforAndroid_fr.pdf

Guide d'installation et d'utilisation de vmwareview client for android [19 Août 2012]

[6]<http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-50-basics-guide.pdf>

Documentation sur vSphere [Juillet 2012]

[7]<http://fr.wikipedia.org/wiki/Hyperviseur>

différents types d'hyperviseur [10 Juillet 2012]

[8]<http://www.youtube.com/watch?v=sQ9v5525bBk>

videos de formation du vmwarevSphere 5.0 [Juillet 2012]

[9]http://www.petenetlive.com/Top_Level/techmain.html#VMWARE

Tutoriel de déploiement sur les produits VMware [Juillet 2012]

[10]http://www.novatim.com/newsletters/avril_2010/virtualisationpdt.html

Comment virtualiser un PC [Juillet 2013]

[11]<http://www.virtualisationwindows.com/avantages-faiblesses-virtualisation.html>

Avantages et faiblesses de la virtualisation de poste de travail [Juillet 2013]

[12]<http://www.virtualisationwindows.com/virtualisation-poste-travail-hyper-v.html>

la virtualisation de poste de travail [Juillet 2013]

[13]<http://www.virtualisation-news.com/2008/06/dossier-comparatif-xenserver-hyper-v-vmware-infrastructure.html>

[Comparaison XenServer-Hyper-V-V](#)

http://solutions.journaldunet.com/0210/021004_san_nas.shtml<http://www.silicon.fr> Thierry Bloch, chargé de cours

http://fr.wikipedia.org/wiki/Storage_Area_Network

http://www.dataligence.com/storage_survey_nassan.htm

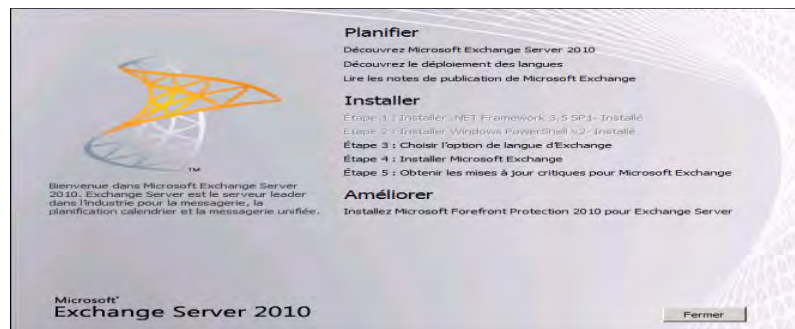
http://www.zdnet.fr/entreprise/service-informatique/serveurs_stockage/0,50007198,2108230,00.htm

ANNEXES

Pre-requis pour L'installation de Exchange 2010 sur une machine Windows Serveur 2008 R2

Installation et configuration de Exchange 2010

Commençons par lancer l'installation. Sur Windows 2008 R2, Windows Installer 4.5 est installé par défaut et si vous avez suivi l'installation des pré-requis, .NET 3.5 SP1 devrait déjà être installé. On commence donc à l'étape 3.



Capture : Début d'installation

Lancez l'autorun du DVD, vous constatez que vous ne pouvez pas cliquer sur les deux premières étapes de l'installation car nous les avons déjà réalisées lors des étapes précédentes. Cliquez sur l'Etape 3 : choisir l'option langue d'Exchange puis sélectionnez Installer uniquement les langues à partir du DVD.



Capture : Etapes de l'installation

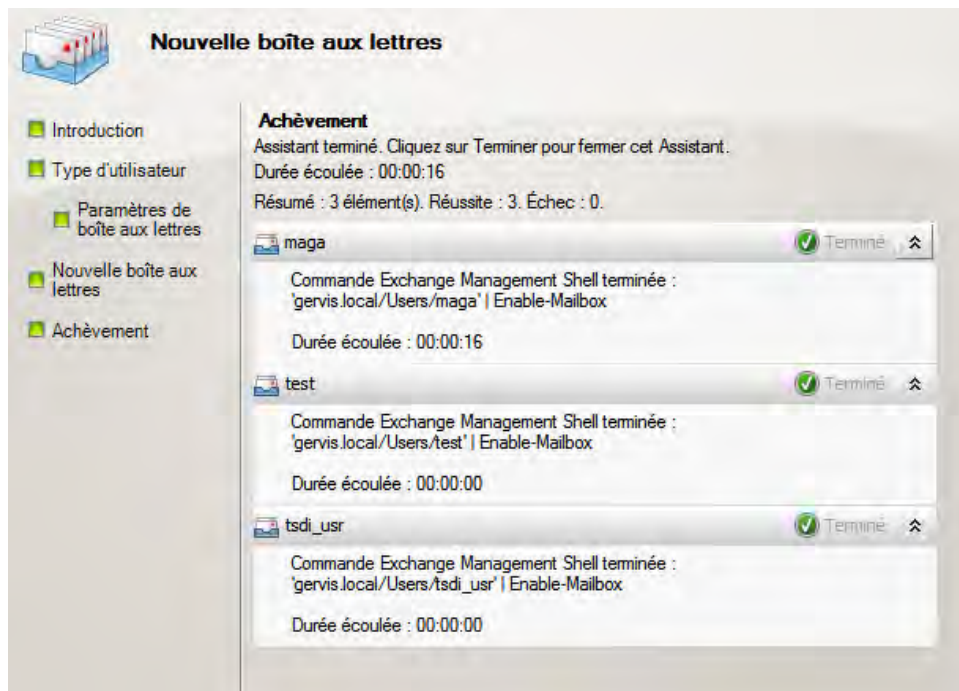
Une fois cela nous pouvons passer à l'étape suivante, et enfin Installer Microsoft Exchange (étape 4).

ANNEXES

Nous passerons certaines étapes qui sont communes à d'autres installations pour nous concentrer sur ce que l'on doit faire pour bien installer notre serveur de messagerie.

On vous demandera ensuite, si votre réseau contient des clients Outlook 2003, afin d'en assurer la compatibilité.

Si vous voulez autoriser les clients à se



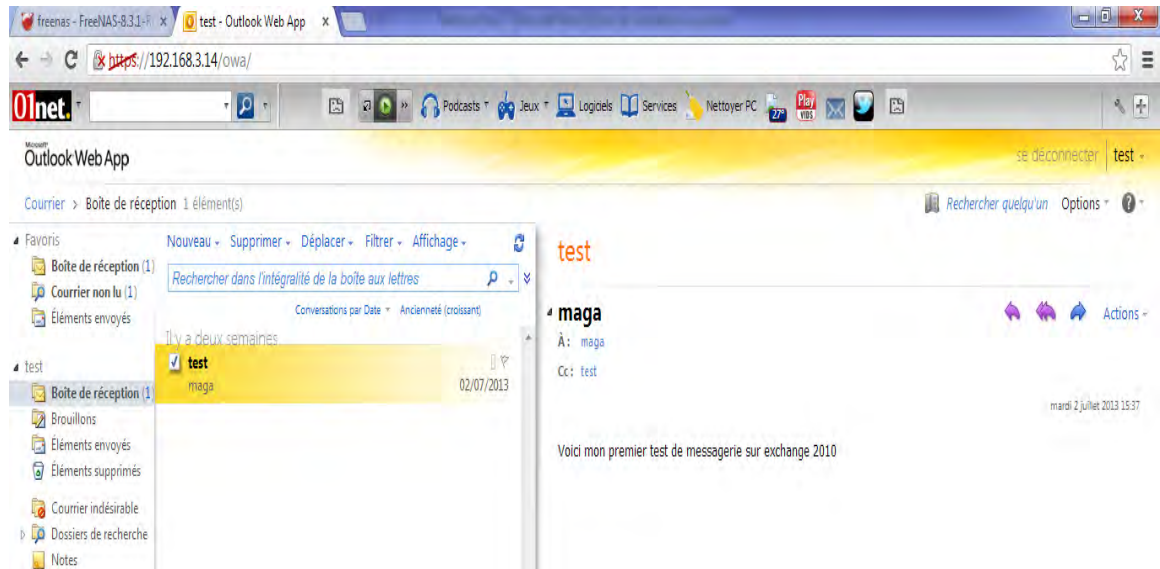
Capture : Fin Installation d'exchange



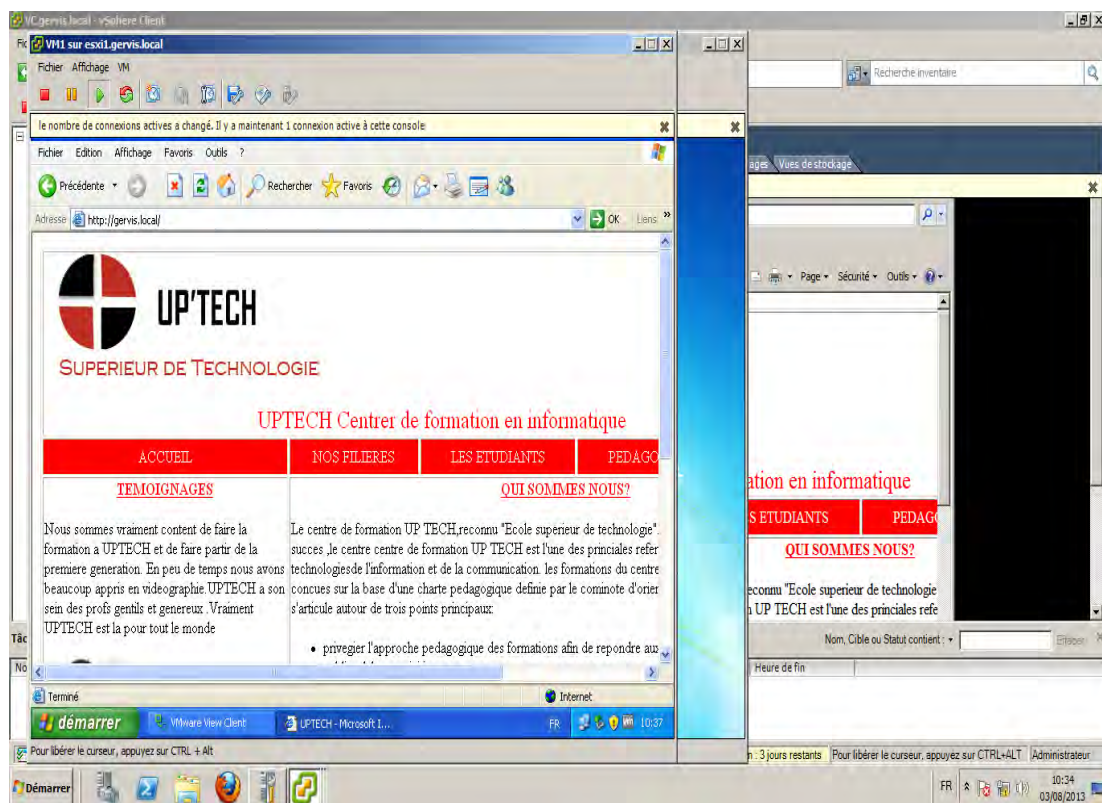
Connexion avec un compte utilisateur

ANNEXES

Maintenant, connectez-vous à CLIENT1 avec maga et envoyer a test un e-mail. Pour créer et envoyer un message e-mail

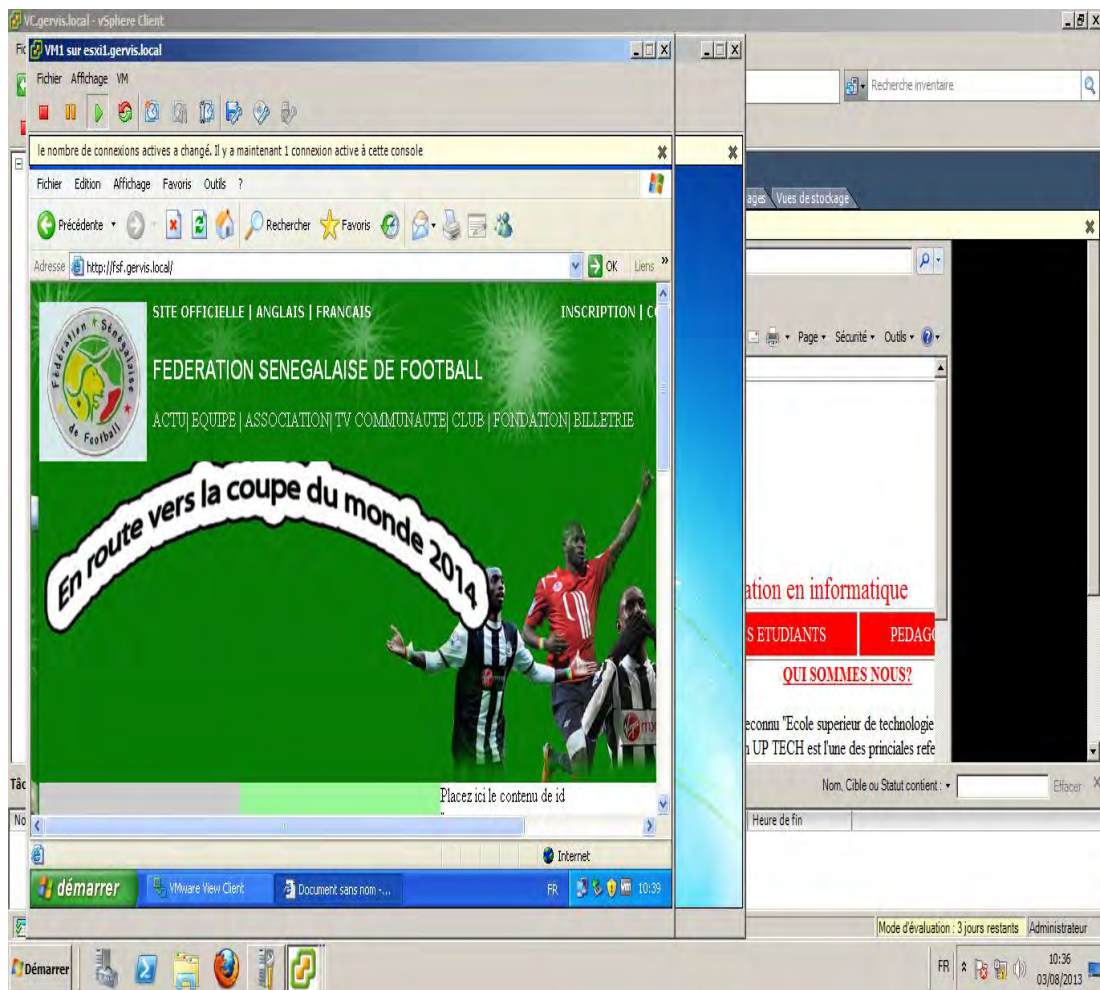


Capture du test d'envoi d'un mail sur outlook



Capture : Connexion au site 1

ANNEXES



Capture : Connexion au site2