Benjamin FORTE

Université de la Méditerranée
INSTITUT UNIVERSITAIRE DE TECHNOLOGIE
Réseaux et Télécommunications

RAPPORT DE STAGE
Diplôme Universitaire de Technologie

Infrastructure informatique virtuelle dans un environnement hospitalier.

Benjamin FORTE

Service Informatique du centre Hospitalier

Edmond Garcin d'Aubagne.

Responsable en entreprise : M. Gilbert Casanova

Responsable académique : M. Nadir Boussoukaia

Juin - 2011

Table des Matières

III/ Retours d'expériences & Tâches réalisées

III/ Conclusions

Remerciements & Ambition du rapport.

Je tiens à remercier l'équipe du service informatique de l'hôpital, et particulièrement M. Casanova, responsable du service, ainsi que les personnes qui ont fait tout leur possible pour me transmettre leurs savoirs et leurs compétences :

M. Gilbert Casanova, mon tuteur de stage, qui a su m'intégrer au sein de son équipe dès le premier jour. Notamment lors des transmissions de compétences entre les ingénieurs des entreprises externes (*IT-med*[1], *Trend France*[2]) sous-traitant le projet, et les ingénieurs du service informatique. J'ai pu avoir accès à l'ensemble des documents officiels du projet comme l'appel d'offre de l'hôpital et la réponse de *Systemat*[3].

M. Pierre Sun, ingénieur du service informatique, qui m'a fourni toutes les informations relatives au cœur de réseau de l'hôpital, et qui a fait preuve de beaucoup de pédagogie dans ses explications notamment sur le *packaging*[4] des applications des divers services de l'hôpital sous *Thinapp*[5].

M. Marc Sarkissian, également ingénieur du service informatique, que je tiens tout particulièrement à remercier pour sa constante disponibilité et ses explications abouties.

Enfin, je souhaite remercier M. Raphaël Julmy, ingénieur à IT-med, pour n'avoir fait aucune différence entre le statut des ingénieurs du service informatique et mon statut d'étudiant stagiaire lors des transmissions de compétences.

Sans oublier, l'équipe de Trend Micro France, pour avoir répondu à mes questions pendant leurs interventions au sein du service.

Ambition du Rapport.

L'objectif de mon compte-rendu est de rendre accessible la compréhension du fonctionnement d'une architecture virtuelle, via une étude théorique graduelle ainsi qu'un retour d'expérience sur la mise en production de celle-ci, dans un environnement critique.

1 Entreprise (maître d'œuvre) de 6 personnes ayant récupérée le projet, suite au dépôt de bilan de Systemat.

2 Editeur du logiciel Anti-Virus Trend-Micro.

3 Systemat est l'entreprise qui a été retenu au lancement de l'appel d'offre de l'hôpital.

4 Consiste à générer un exécutable (fichier.exe, ou .dat) à partir du programme d'origine, isolant l'application encapsulée, du système d'exploitation.

5 Logiciel de packaging propriétaire VMware.

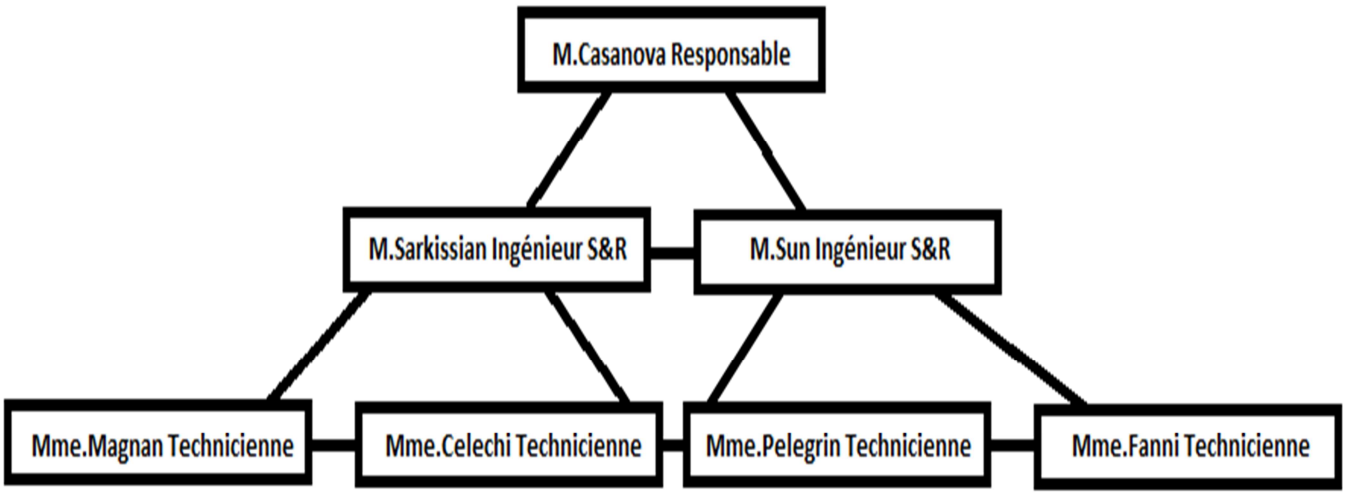
Avant-propos.

Présentation de l'hôpital et de son service informatique.

En 1965 Edmond Garcin, Député, Conseiller Général, entame son premier mandat de maire d'Aubagne. Le chantier de l'hôpital est lancé. Le 14 décembre 1971 l'ensemble hospitalier est inauguré.
Grace à une action permanente d'Edmond Garcin, l'hôpital voit sa superficie augmentée et ses équipements se trouvent à la pointe de la technologie moderne. Depuis le Centre Hospitalier a été régulièrement entretenu et modernisé.

Le service informatique de l'hôpital est responsable de l'exploitation du réseau, du commutateur principal situé au local technique, jusqu'au poste de l'utilisateur final situé dans les services hospitaliers (pédiatrie, urgence, maternité, accueil, laboratoire…).

Voici l'équipe qui constitue le service informatique :



Organigramme du service informatique du C.H.A (Centre Hospitalier d'Aubagne)

Depuis 3 années, les restrictions budgétaires ne cessent d'augmenter pour le service public, (gels des salaires, départs non remplacés, manque de personnels, matériel vieillissant).

C'est pourquoi en 2009, le C.H.A a lancé un appel d'offre pour le renouvellement de son infrastructure informatique vieillissante et onéreuse, vers la technologie qui répond à l'ensemble de ces problèmes : La virtualisation des serveurs et des postes de travail, avec à terme un nouveau cœur de réseaux totalement redondé.

Les Logiciels utilisés au CHA sont décrits dans le détail en Annexe 1

Objet du stage.

Ma présence au sein de ce service reflète une volonté de mettre en place un certain nombre de dispositifs liés aux nouvelles technologies d'infrastructures informatiques, notamment la virtualisation du parc informatique de l'hôpital. Pour moi, il s'agissait dans un premier temps d'être aux côtés de Pierre et de Marc, et de participer à la mise en place des *clients légers*[6] en test, aux urgences et à l'accueil. Ensuite, mon objectif a été de faire une étude concrète du choix et de la mise en œuvre d'une telle infrastructure dans un milieu hospitalier, sachant que l'objectif final pour l'hôpital est une virtualisation totale de son parc. Soit 440 postes clients légers, 950 utilisateurs dont 900 profils uniques, et 50 groupes de travail globaux *Active-Directory*[7] sur 4 années.

Les objectifs communs.

L'objectif principal, pour le service informatique du C.H.A par rapport à mon stage, est d'épauler Marc et Pierre dans le déploiement et la gestion, via *VMware View*[8], des clients légers dans tous les services.

Pour ma part, l'objectif est de mettre en application les compétences en systèmes et réseaux, acquises durant les deux années d'études au sein de l'IUT. Cette mise en application passe par une capacité à appréhender les problèmes et les transmissions de compétences effectuées entre les ingénieurs de la société sous-traitante et ceux du service informatique. Puis dans la connaissance du fonctionnement d'une architecture réseaux d'entreprise.

Il est également important de mettre en avant le caractère bénéfique de ce stage pour ma *future poursuite d'étude et mon projet professionnel**, ceux-ci seront directement liés avec l'objet de ce stage. Cette expérience m'a permis d'acquérir une connaissance théorique solide dans la mise en œuvre d'une *infrastructure virtuelle*[9], et des notions pratiques.

* *Voir conclusion page 31.*

[6] Au sens matériel, un client léger est un ordinateur qui, dans une architecture client-serveur, n'a presque pas de logique d'application. Il dépend donc surtout du serveur central pour le traitement.

[7] Annuaire propriétaire Microsoft, répertoriant les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés et les imprimantes.

[8] VMware, Inc. est une société, fondée en 1998, qui propose plusieurs produits propriétaires liés à la virtualisation d'architectures x86. C'est aussi par extension le nom d'une gamme de logiciels de virtualisation.

[9] Ensemble de ressources informatiques potentiellement partagées, distribuées, hétérogènes, délocalisées et autonomes.

I/ Présentation fondamentale.

Qu'est-ce que la virtualisation ?

1°) Définition.

De manière générale, la virtualisation : C'est l'ensemble des techniques matérielles et/ou logicielles qui permettent de faire fonctionner sur une seule machine plusieurs systèmes d'exploitation et/ou plusieurs applications, séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes.

2°) Historique.

La virtualisation est une technologie qui suscite beaucoup d'intérêt depuis quelques années au sein des entreprises et depuis peu chez un public de particuliers. Cependant cette technologie n'est pas nouvelle comme nous nous prêtons à le croire, celle-ci remonte au début de l'informatique. En effet l'idée de faire fonctionner plusieurs programmes simultanément sur une même machine date des années 50. Ce concept innovant avait pour but de partager les ressources matérielles de la machine entre toutes les applications. Cette notion de partage de ressources se nomme le « time sharing » ou temps partagé et se rapproche du concept de virtualisation que l'on connait aujourd'hui. C'est Christopher Strachey qui est le premier à introduire le principe de Time Sharing, en Juin 1959, dans une conférence internationale sur le traitement de l'information à l'UNESCO.

En 1965, le centre de recherche d'IBM développe un projet nommé M44/44X. Le but de ce projet était d'étudier le concept novateur du « time-sharing ». En 1967, l'idée de virtualisation matérielle est développée. Ce modèle virtualise toutes les interfaces matérielles via la Virtual Machine Monitor (VMM). Le système d'exploitation est le TSS (Time-Sharing System) aussi appelé le superviseur. C'est le premier système de virtualisation complète.

Au début des années 2000, la société VMware développe et popularise un système propriétaire de virtualisation logicielle des architectures du type. Cependant l'architecture *IA-32 (x86[10])* posait quelques problèmes de gestion des instructions en fonction du niveau de privilège utilisé par le système hôte. C'est pour cette raison qu'en 2006 AMD et Intel, les deux fondateurs-leader du marché du processeur x86, ont repensé l'architecture de leurs puces pour une meilleure prise en charge des instructions liées à la virtualisation. C'est ce que l'on nomme la « virtualisation matérielle ».

[10] La norme x86 regroupe les microprocesseurs compatibles avec le jeu d'instructions de l'Intel « 8086 ». Cette série est nommée IA-32 (pour Intel architecture 32 bits) par Intel pour ses processeurs à partir du Pentium.

3°) Fonctionnement d'un système d'exploitation (Operating System).

Le système d'exploitation est un ensemble complexe faisant office de *couche d'abstraction*[11] entre le matériel (hardware, niveau physique) et le logiciel (software, niveau logique).

Il est composé de multiples composants, chacun ayant un rôle bien spécifique. Parmi les tâches dévolues au système d'exploitation, on retrouve notamment la gestion de la mémoire vive (RAM) et des périphériques (stockage, carte réseau, imprimante, écran, clavier, etc.). La gestion de la RAM est l'une des tâches les plus complexes du système d'exploitation. En effet, tous les programmes (que ce soit au niveau de l'utilisateur ou du système d'exploitation) ont besoin de mémoire pour fonctionner. C'est dans la RAM que seront stockés :

- Le code des programmes en cours d'exécution,
- Les données des programmes en cours d'exécution,
- Le code du système d'exploitation,
- Les données du système d'exploitation.

Le gestionnaire de la mémoire est un composant fondamental appartenant au *noyau*[12] du système d'exploitation. Sa tâche, est d'allouer et libérer de la mémoire à des processus lorsqu'ils en ont besoin (applications et système d'exploitation).

Quand la RAM vient à manquer, le système peut utiliser une partie du disque dur comme extension de mémoire (le « swap »). Le disque dur est toutefois beaucoup plus lent que la RAM, aussi le gestionnaire de mémoire essaie d'en limiter l'usage.

Toutefois, le système d'exploitation n'a pas le contrôle direct sur la gestion de la mémoire au niveau physique. Ce rôle est dévolu au processeur. C'est donc par le jeu d'une interaction complexe entre le système d'exploitation (qui gère la RAM au niveau logique) et le processeur (niveau physique) que se déroule l'exécution d'un programme.
Le programme est interprété par le processeur, puis composé d'une suite d'opérations élémentaires nommées « instructions ». Ces instructions consistent principalement en des demandes d'accès à la RAM, des opérations mathématiques et des appels spécifiques au matériel (carte graphique, carte réseau, clavier, écran, disque dur, etc.). Cette suite d'instructions élémentaires exécutées dans l'ordre donne au final le programme, qui peut être un programme du système d'exploitation ou un programme utilisateur.

[11] La couche d'abstraction matérielle une couche logicielle accédant au matériel informatique.

[12] En tant que partie du système d'exploitation, le noyau fournit des mécanismes d'abstraction du matériel, notamment de la mémoire, du (ou des) processeur(s), et des échanges d'informations entre logiciels et périphériques matériels.

Le système d'exploitation a aussi pour rôle de faire abstraction du matériel pour les programmes utilisateurs. Ainsi, un programme doit se comporter de la même manière quel que soit le modèle de carte réseau utilisé pour communiquer, de même pour la marque ou le type de disque dur contenant les fichiers.

Cette abstraction est réalisée par les pilotes des périphériques. Ces pilotes sont en général destinés à un type de matériel particulier et offrent au système d'exploitation un ensemble cohérent d'opérations.

Par exemple, tous les pilotes de disque dur permettent de lire le contenu du disque à un endroit donné et tous les pilotes de la carte réseau permettent d'envoyer et de recevoir des données. Le système d'exploitation se repose sur les pilotes de périphérique pour apporter des couches d'abstraction supplémentaires, accessibles aux programmes utilisateurs, par exemple pour la gestion des fichiers, des protocoles réseaux.

Les programmes utilisateurs ne peuvent accéder au matériel qu'à travers les couches d'abstractions, assurant ainsi la cohérence du système. Le système d'exploitation doit, pour assurer cette abstraction, avoir un accès exclusif au matériel afin de le contrôler. Les systèmes d'exploitation sont donc conçus comme s'ils étaient les seuls à accéder au matériel. Il est important de retenir cette notion d'exclusivité, pour mieux appréhender la notion de virtualisation.

Le système virtualisé ne pourra pas accéder au matériel directement, comme s'il était le seul, car c'est le système hôte qui a ce rôle. Il y a donc des solutions de contournement mises en place, qui varient selon les produits et les technologies utilisés. La séparation en couches du système d'exploitation fait qu'une grande partie du code est indépendante du matériel.

4°) Les différents types de virtualisation.

Tout d'abord, il est important de savoir qu'il n'existe pas qu'un seul type de virtualisation. A l'heure actuelle, il existe plusieurs technologies de virtualisation et nous pouvons les séparer en deux groupes distincts :

- « Virtualisation matérielle », nous pouvons citer les virtualisations complètes, la paravirtualisation, le système à hyperviseur et le cloisonnement, que nous détaillons dans les pages suivantes.
- « Virtualisation logicielle », notamment la virtualisation d'applications. Le principe de fonctionnement, ainsi que les spécificités de chaque solution étant différentes, nous étudierons dans ce rapport, la solution proposée par VMware grâce au logiciel ThinApp.

4°) A/ Virtualisation complète.

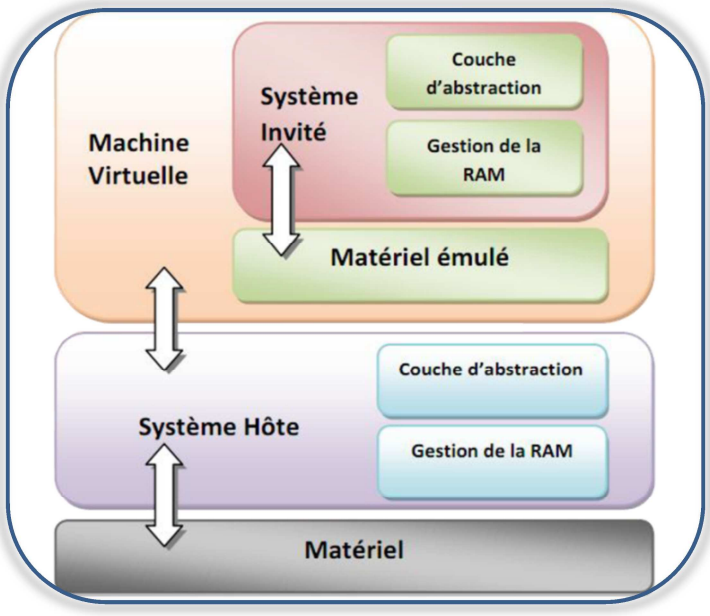
La virtualisation complète a pour principe *d'émuler*[13] la globalité d'une machine physique. Le système invité (système virtualisé, en surcouche du système d'exploitation natif) a l'illusion de s'exécuter sur une machine physique à part entière.

Le système invité est alors considéré comme une application standard par le système hôte. Or nous avons vu précédemment que le système d'exploitation a une interaction très forte avec le matériel ce qui n'est pas le cas avec une application classique tel qu'un éditeur de texte par exemple.

Nous pouvons alors nous demander comment est géré, dans un système de virtualisation complet, les échanges que doit avoir l'OS avec le matériel ?

Pour que le système invité puisse être émulé il est nécessaire qu'une couche applicative comprenne les instructions du système invité et que celles-ci soient relayées au système hôte puis transmises aux matériels et inversement. Ce mécanisme de transcription d'instructions est réalisé par la « machine virtuelle». Elle émule également pour le système invité, le matériel standard de base nécessaire (souris, clavier, interfaces réseaux, carte graphique, etc.…)

La particularité de la virtualisation complète est que le système invité n'est pas modifié lors de son installation. Ce qui n'est pas le cas avec d'autres solutions de virtualisation que nous verrons plus tard dans le document. Il est important de noter que le matériel émulé ne pourra jamais être plus performant que le matériel disponible sur le système hôte. Seule une catégorie limitée de matériel standard est proposé à l'émulation par les machines virtuelles. Ceci pour limiter le nombre d'instructions devant être traduites pour passer de la machine virtuelle au matériel, afin d'éviter des dégradations de performance trop importantes.



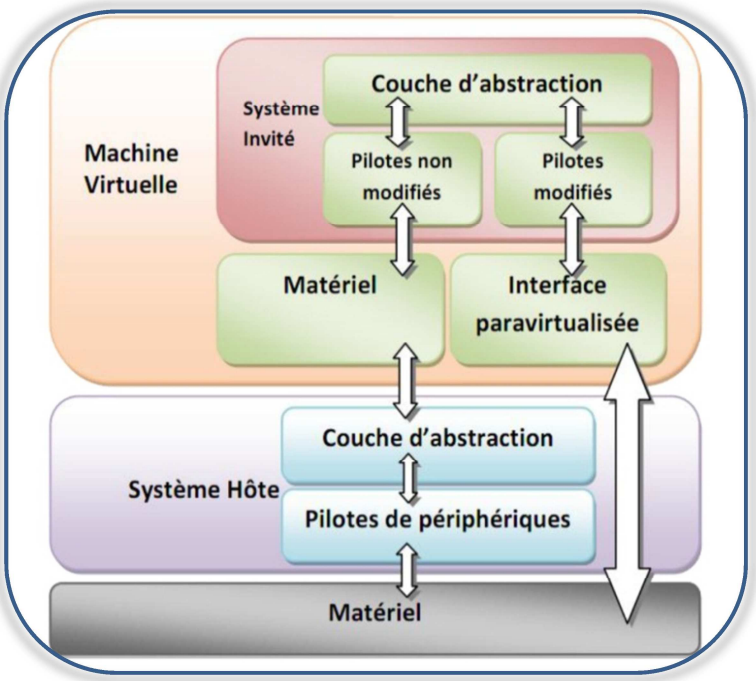
[13] Substitution ou imitation d'un élément matériel informatique, par un logiciel.

4°) B/ Paravirtualisation.

Ce système est proche de la virtualisation complète car seul le système hôte à un accès directe au matériel. Mais contrairement au précédent système, le système invité est amélioré pour traduire à la machine virtuelle les actions à réaliser. Le système a « conscience » qu'il s'exécute dans une machine virtuelle.

Cela évite à la machine virtuelle de traduire tous les appels aux matériels effectués par l'OS invité. Certaines sont traduites directement grâce à des pilotes paravirtualisés, notamment en ce qui concerne la gestion de la mémoire et des Entrées/Sorties. La paravirtualisation apporte donc un gain de performance et de réactivité grâce au contournement de couche d'abstraction.

Cette solution implique des modifications dans les systèmes invités pour que ces dernières soient supportées par la machine virtuelle. Pour cela, il est donc nécessaire d'avoir un accès au code source et les permissions de le modifier ce qui limite son utilisation à seulement quelques systèmes d'exploitation.

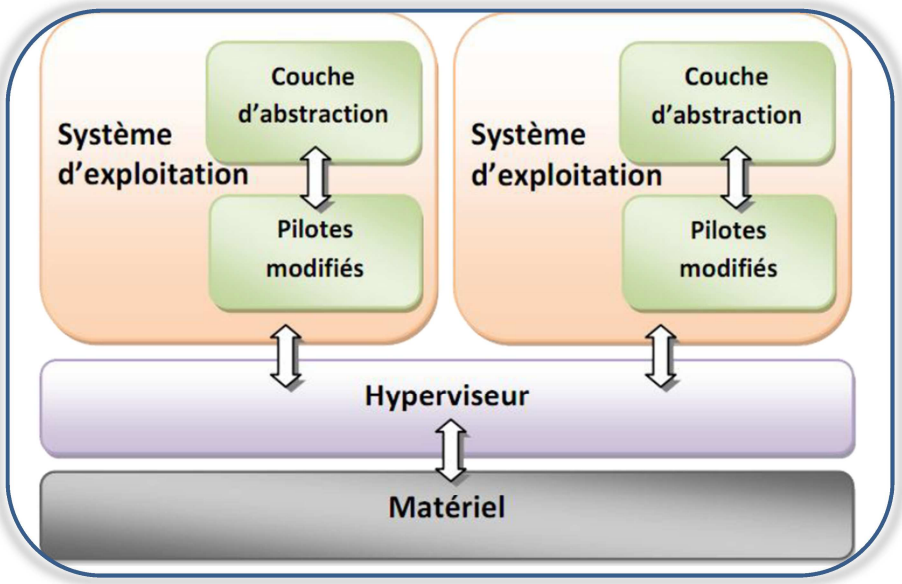


4°) C/ Les systèmes à Hyperviseur.

C'est l'évolution logique de la paravirtualisation compte tenu des améliorations de performance. L'hyperviseur est un système minimaliste qui sera l'interlocuteur unique du matériel dès le démarrage du système. C'est lui qui régule l'utilisation des ressources matérielles entre les systèmes d'exploitation installés en surcouche. Le système hôte complet installé au-dessus de cette couche ne peut accéder au matériel que via celui-ci. Il est donc simple *d'instancier*[14] un ou plusieurs OS.

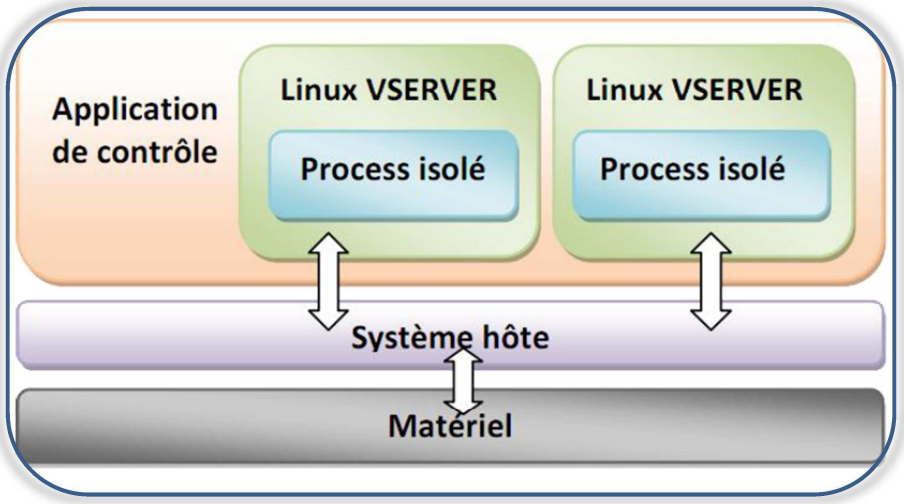
[14] L'instanciation consiste à créer un nouvel objet à partir d'un objet existant. Dans ce cas, installer des nouveaux OS, à partir d'un original (ici, l'hyperviseur).

Ce système permet d'assurer une répartition efficace des ressources entre les systèmes de façon à ce qu'aucun d'entre eux n'influe sur les performances de l'autre. Pour modifier les paramètres de l'hyperviseur, il est nécessaire d'élire un système privilégié qui en aura la charge. Il permettra également d'instancier de nouveaux systèmes invités.



5°) D/ Le cloisonnement.

Une autre pratique répandue dans le domaine de la virtualisation est le cloisonnement. Derrière ce nom se cachent plusieurs technologies visant à séparer fortement les processus s'exécutant sur un même système d'exploitation. Le cloisonnement vise à isoler chaque processus dans un conteneur dont il est théoriquement impossible de sortir. Un processus isolé de la sorte ne saura pas quels autres processus s'exécutent sur le même système, et n'aura qu'une vision limitée de son environnement. Le but principal de cette technologie est d'améliorer la sécurité du système d'exploitation et des applications.



6°) Pourquoi virtualiser ?

Aujourd'hui les services informatiques sont toujours en quête de compétitivité, ils essaient continuellement d'améliorer leurs productivités mais aussi de diminuer leurs coûts. Cette recherche de performance se traduit souvent chez les *DSI*[15] par l'adoption de nouvelles technologies matérielles et/ou logiciels. Une des technologies qui suscite un intérêt grandissant est la « virtualisation ».

Ce n'est pas un concept nouveau, mais son omniprésence qui est plus récente. On l'attribue ainsi à tout processus touchant à la virtualisation dans sa définition la plus élémentaire, à savoir tout processus d'abstraction des ressources informatiques de leur couche matérielle sous-jacente. Bien des projets de virtualisation ont ainsi pour motivation première de redéfinir le parc matériel comme un ensemble de ressources partagées, qui pourront alors être gérées de façon centralisée via une interface unique. Il existe de nombreuses définitions du terme « virtualisation », lequel est utilisé pour l'infrastructure dans son ensemble ou toute composante de celle-ci.

Avant de considérer la virtualisation du centre de données, il est capital pour une entreprise de définir quelle technologie ou catégorie de service elle souhaite virtualiser. Globalement, il existe trois domaines de virtualisation : le système d'exploitation, le système de stockage et les applications. Très vastes, ces domaines ne délimitent pas clairement les aspects parfois les plus pertinents de la virtualisation du centre de données.

Dans ce rapport de stage, la virtualisation sera d'une part abordée dans son ensemble, et d'autre part un focus sera effectué sur la virtualisation applicative, (également connu sous le nom de « portabilité d'applications » ou « virtualisation de services applicatifs »).

Cette procédure consiste à exécuter le logiciel sur un serveur distant plutôt que sur l'ordinateur de l'utilisateur. Les *DLL*[16] des programmes redirigent tous les appels de l'application virtualisée vers le système de fichiers du serveur. Lorsque le logiciel est exécuté à partir du serveur, aucune modification n'est apportée au système d'exploitation de l'ordinateur local (*OS*[17]), au système de fichiers ou au *registre*[18].

---

[15] Le Directeur des Systèmes d'Information d'une organisation (entreprise, association, etc.), est responsable de l'ensemble des composants matériels (postes de travail, serveurs, équipements de réseau, systèmes de stockage, de sauvegarde et d'impression, etc.) et logiciels du système d'informations.

[16] Dynamic Link Library, librairie de routines utilisées par différents programmes.

[17] Un système d'exploitation (SE ou OS en anglais pour Operating System) est un ensemble cohérent de logiciels permettant d'utiliser un ordinateur et tous ses éléments (ou périphériques).

[18] Le base de registre, est une base de données utilisée par le système d'exploitation Windows. Elle contient les données de configuration du système d'exploitation et des autres logiciels installés désirant s'en servir.

Les avantages de la virtualisation sont nombreux :

- Augmenter l'espace de stockage disponible.
- Accès unifié aux données.
- Fiabiliser des connexions.
- Faciliter de gestion pour les administrateurs, centralisation des postes de travail pour les mises à jour.
- Faciliter la gestion du parc matériel.
- S'inscrire dans une politique de développement durable.
- Exemple plus spécifique : Support informatique aisé du *projet DPI*[19] qui entraine de nombreuses contraintes sur les infrastructures des systèmes de communications tels que la *haute-disponibilité*[20] des postes de travail. En effet les données du patient étant complètements dématérialisées, un agent hospitalier se doit d'accéder à ces informations en 24h/24 et 7j/7 sur son poste.

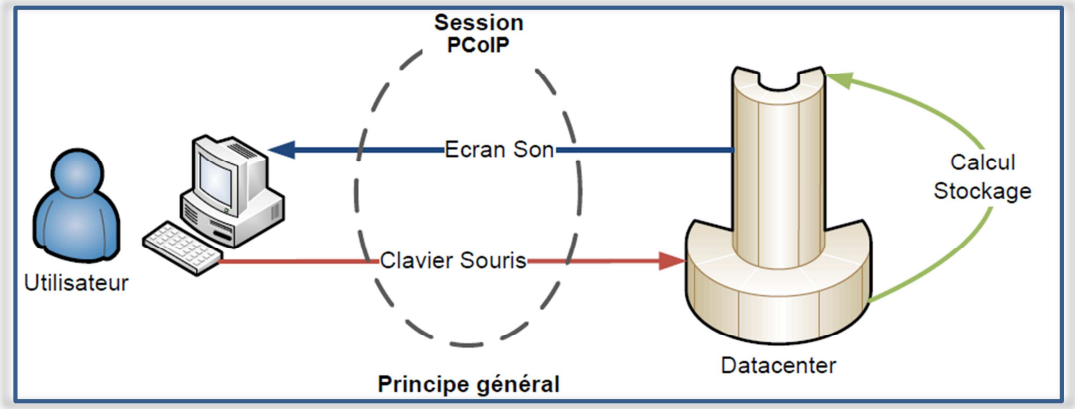
[19] Projet public lancé par le ministère français de la Santé visant à ce que chaque français dispose d'un dossier médical informatisé reprenant tout son passé et son actualité médicale. Le projet est lancé par la loi n°2004-810 du 13 août 2004 relative à l'assurance maladie. Son but est de fournir au médecin traitant l'information la plus complète pour qu'il puisse proposer le traitement ou les examens les plus adaptés et également d'éviter des redondances inutiles d'examens ou de prescriptions. Les principaux obstacles à son emploi sont la sécurisation des accès et la mise en œuvre.

[20] La haute disponibilité désigne une architecture informatique, ou un service, disposant d'un taux de disponibilité convenable. On entend par disponible le fait d'être accessible et rendre le service demandé. La disponibilité est aujourd'hui un enjeu très important en cas d'indisponibilité, les répercussions en termes de coûts et de productions peuvent avoir un effet catastrophique.

II/ Étude théorique et comparative.

1°) Principe.

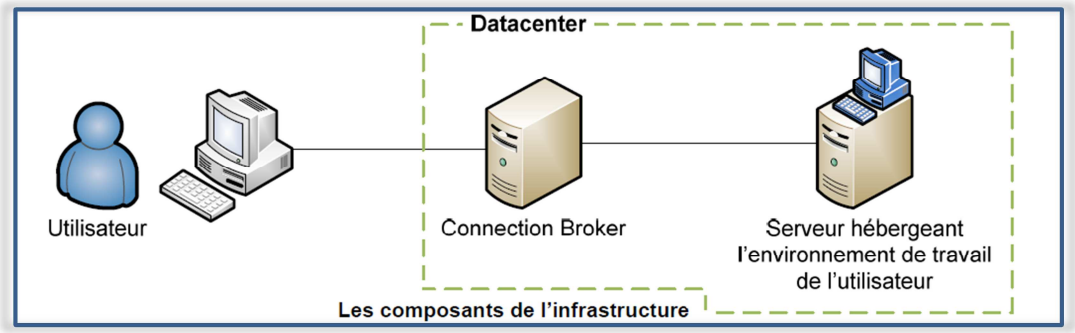
La virtualisation du poste de travail peut se comparer aux systèmes centralisés des années 70 avant l'arrivée de la micro-informatique. On va fournir à un utilisateur un environnement de travail utilisant les ressources (CPU, mémoire…) du Datacenter de la société. De ce fait, on désolidarise la partie interface homme machine (écran, clavier et souris), de la partie calcul et stockage. Il circule donc sur le réseau entre le client et le Datacenter : le déport d'affichage, le son, les déplacements de la souris et les frappes clavier. Toutes ces données sont transportées à travers une session *RDP*[21] ou ici *PCoIP*[22]



L'architecture comporte deux couches distinctes :

- Le *connection broker*[23] attribuant une session à l'utilisateur.
- Le serveur hébergeant l'environnement de travail des utilisateurs.

Ces deux parties seront abordées dans l'analyse des solutions du marché. Une architecture de virtualisation du poste client peut se schématiser de la manière suivante :



[21] Remote Desktop Protocol, défini par Microsoft. C'est le protocole standard de connexion de terminaux graphiques sur un serveur Windows distant.

[22] PC-Over-IP a été développé par la société Teradici, ce protocole a la particularité d'être auto-adaptative en fonction du besoin du contenu et de la quantité de bande passante disponible sur le réseau.

[23] Intermédiaire entre les utilisateurs et le service final. Il identifie les machines virtuelles pour les utilisateurs afin d'initier la connexion à distance (ici, c'est le View Manager).

Ce type d'infrastructure apporte les avantages suivants :

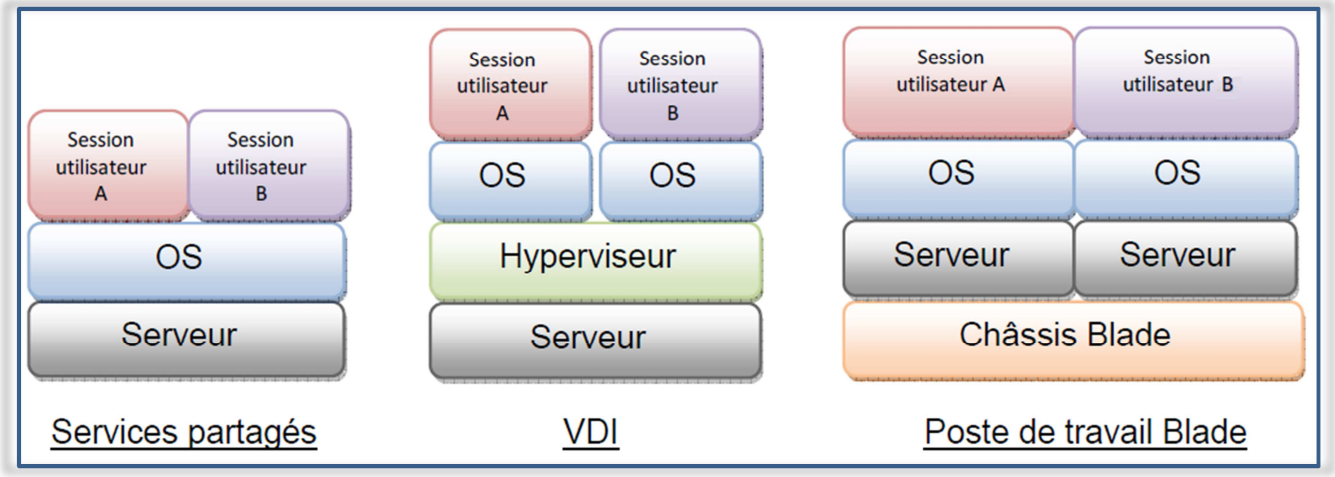
- Administration centralisée des postes de travail.
- Haute disponibilité
- Mise à jour des systèmes et applications facilitées
- Stockage centralisé des données

2°) Modèles existants.

Aujourd'hui, 3 modèles de consolidation de poste de travail existent sur le marché :

- Services partagés.
- VDI (Virtual Desktop Infrastructure).
- Poste de travail Blade.

Ces différents types d'infrastructure se différencient de la manière suivante :



Services partagés : Il s'agit de la technologie de consolidation la plus implantée du marché grâce à la solution « MetaFrame » de Citrix. Le principe est que, le même OS est partagé par plusieurs utilisateurs, grâce à l'utilisation des sessions Windows. Soit un serveur pour un OS pour plusieurs utilisateurs.

VDI : Cette technique s'inscrit dans la continuité de la virtualisation de serveur. Elle se base donc sur le même *hyperviseur*[24] que pour les serveurs. Le principe est qu'un utilisateur accède à son propre poste de travail mais que celui-ci est virtualisé et partage ainsi les ressources du serveur avec d'autres postes virtuels. Soit un serveur pour plusieurs OS pour plusieurs utilisateurs.

Poste de travail Blade : Il s'agit de la technologie la moins répandue du marché car c'est la plus onéreuse. Le principe est qu'un serveur de type Blade soit dédié à un utilisateur. Soit un serveur pour un OS par utilisateur.

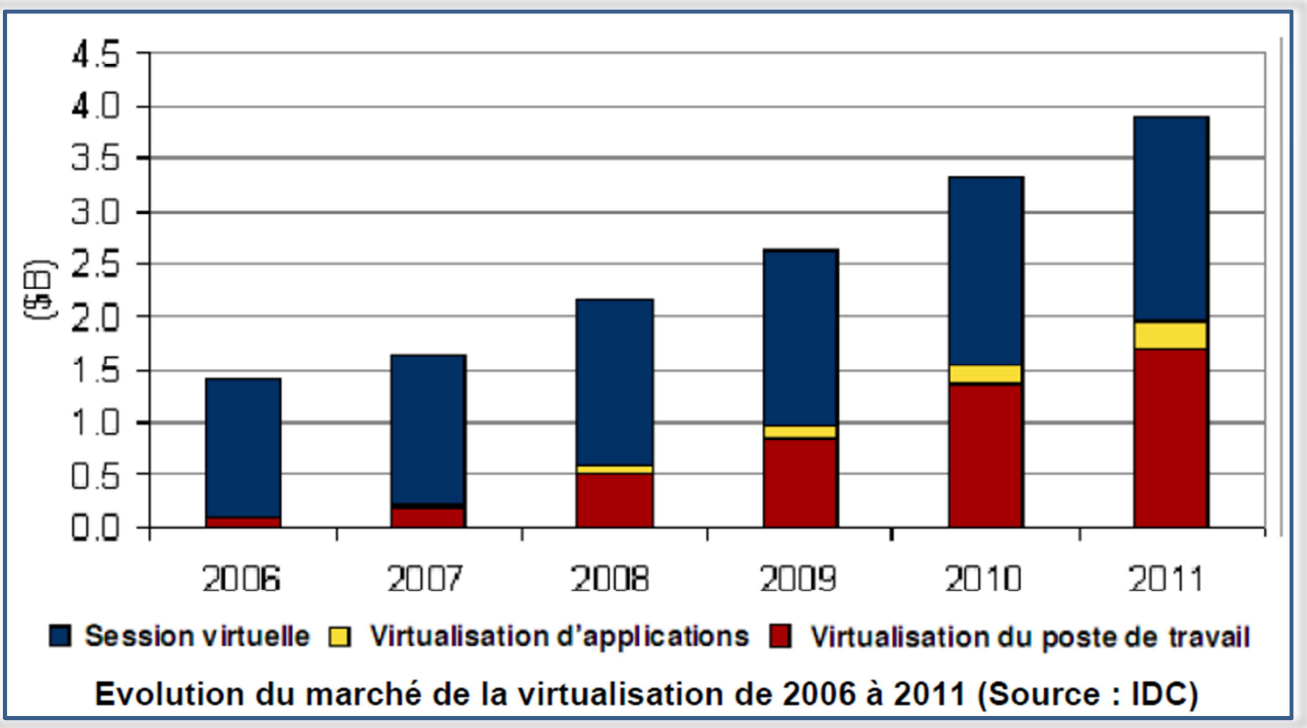
[24] Cat°1 : s'exécute directement sur une plateforme matérielle donnée (Noyau hôte). Un système d'exploitation secondaire peut de ce fait être exécuté au-dessus (OS invité). (VMware ESX, Xen de Citrix).
Cat°2 : logiciel qui s'exécute à l'intérieur d'un autre système d'exploitation. (VMware Workstation, VirtualBox).

	Services partagés	VDI	Blade
Utilisateurs supportés par machine	Plus d'une centaine	Plusieurs dizaines	Un seul
Environnement utilisateur	Windows 2003 Server	Divers OS	Windows XP
Isolation de l'environnement	Faible puisque les utilisateurs partagent le même OS	Maximal	Maximal
Compatibilité des applications	Certaines ne fonctionnent pas sous l'environnement Windows Server	Les mêmes que sur un poste de travail classique	Les mêmes que sur un poste de travail classique

3°) Étude du marché et évolutions.

Aujourd'hui la virtualisation, des serveurs et des postes de travail, est la technologie la plus en vogue dans les *départements IT*[25]. Le marché de la virtualisation de poste de travail a connu une très forte croissance entre 2006 et 2011.

Cette technologie est un bon compromis entre les postes de travail trop onéreux et les services partagés trop limités du point de vue des applications. Et même en consolidant, les environnements de travail sont parfaitement isolés grâce à la virtualisation.



Evolution du marché de la virtualisation de 2006 à 2011 (Source : IDC)

[25] Administrer, gérer, maintenir l'utilisation des technologies d'Information et de Communication, (l'informatique).

Comme nous l'avons vu précédemment, la consolidation du poste de travail comporte deux couches distinctes :

- Le connection broker attribuant une session à l'utilisateur.
- Le serveur hébergeant les sessions utilisateurs.

Nous allons d'abord commencer à traiter cette dernière partie en comparant les principaux hyperviseurs du marché.

4°) Virtualisation du poste de travail.

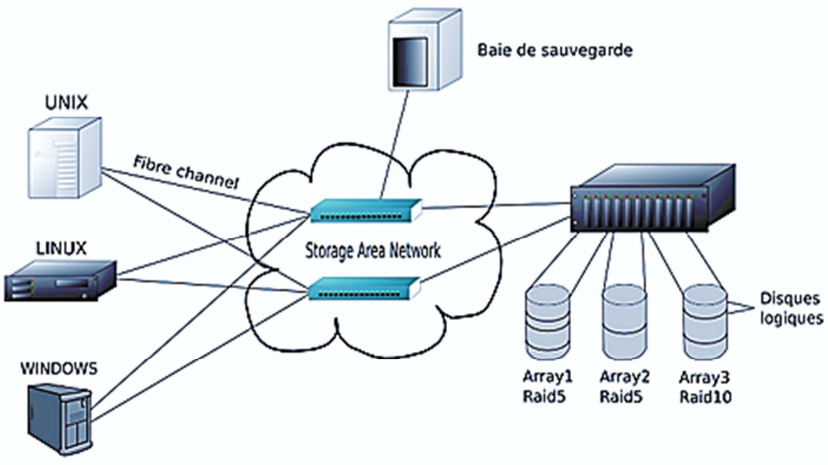
Le précurseur de la virtualisation est VMware, qui a su ces cinq dernières années démocratiser la virtualisation des serveurs grâce à son hyperviseur nommé ESX. Citrix a été quant à lui le premier à démocratiser la consolidation du poste client avec son offre MetaFrame. La virtualisation prenant de plus en plus de part sur ce marché, cette compagnie a fait l'acquisition de la société XenSource en Aout 2007. Ainsi, elle a pu proposer une solution avec l'hyperviseur Xen. D'autres, se sont lancés dans cette technologie, tant bien que mal, comme Microsoft avec l'hyperviseur Hyper-V lancé difficilement en Juin 2008 pour la sortie de Windows Server 2008.

À ce jour, seules les solutions de VMware et Citrix sont arrivées à maturité. C'est pour cela que nous ne comparerons que ces deux produits.

Pour le choix de l'hyperviseur, le C.H.A a plusieurs contraintes, il faut qu'il soit compatible et optimisé avec le réseau *SAN*[26] du C.H.A existant. Puis que le système de packaging d'applications, fonctionne avec toutes les plates-formes spécifiques aux divers services (« Urqual » pour la gestion des urgences, et « Pharma » qui est une plate-forme de suivi, commande et gestion des médicaments, utilisée par l'ensemble du personnel soignant).

[26] Storage Area Network, est un réseau spécialisé permettant de mutualiser des ressources de stockage.

- Assure la redondance du stockage, c'est-à-dire l'accessibilité au système de stockage en cas de panne de l'un de ses éléments, en doublant au minimum chacun des éléments du système (haute disponibilité).
- Fonctionne dans un environnement complètement hétérogène : serveurs Unix, Windows.
- Agrégation de liens (fibre channel), et assure le fait que la requête envoyée par un serveur a bien été reçue et prise en compte par les systèmes de stockage.



5°) Comparatif de ESX et XEN.

ESX effectue une virtualisation complète, c'est-à-dire que les machines virtuelles ne sont pas conscientes d'être exécutées au-dessus d'un système hôte et qu'elles n'ont pas directement accès aux ressources matérielles du serveur. Au contraire, les machines virtuelles sous Xen en sont conscientes puisque les ressources ne sont pas virtualisées comme sur VMware, seul l'accès à celles-ci l'est. Cette para-virtualisation oblige la machine hôte à avoir un processeur de type VT (*Intel VT ou AMD-V*[27]) pour faire tourner des systèmes hétérogènes de Windows XP à Ubuntu.

	ESX	XEN
Surdimensionnement de la mémoire RAM	Oui	Non
Compatibilité de Windows XP	Oui	Oui, en utilisant un processeur VT
Console de gestion multi-serveurs	Avec VirtualCenter	Avec XenCenter
Migration à chaud des machines virtuelles	Avec Vmotion	Avec XenMotion
Partage transparent des emplacements mémoires	Oui	Non

Dans ce comparatif, on s'aperçoit qu'ESX est en avance sur XEN. Cela est dû au fait que la solution de VMware existe depuis plusieurs années.

Les deux fonctionnalités qui mettent en défaut l'hyperviseur de Citrix sont importantes. En effet, le partage transparent des emplacements mémoires permet de réduire considérablement l'utilisation mémoire. Par exemple, si plusieurs machines virtuelles exécutent Windows XP, elles posséderont de nombreuses pages identiques. Dans ce cas, les pages identiques seront stockées dans le même emplacement mémoire.

Le *surdimensionnement*[28] de la mémoire RAM permet quant à lui d'exécuter plus de machines virtuelles simultanément sur le même serveur. Par exemple, la quantité de mémoire cumulée des machines virtuelles qui s'exécutent sur un serveur disposant de 8 Go de mémoire physique peut être de 16 Go. Concrètement si l'on cumule ces deux fonctionnalités, on pourra démarrer beaucoup plus de machines virtuelles sur ESX que sur XEN.
La solution de VMware a donc été retenue par le C.H.A pour virtualiser les postes de travail et les serveurs.

---

[27] Jeu d'instruction processeur visant à résoudre de manière matérielle les difficultés liées à la virtualisation du CPU, à la virtualisation de la mémoire, et à la virtualisation des périphériques du système. (Technologie présente chez les 2 principaux leaders des micro-processeurs Intel© et AMD©).

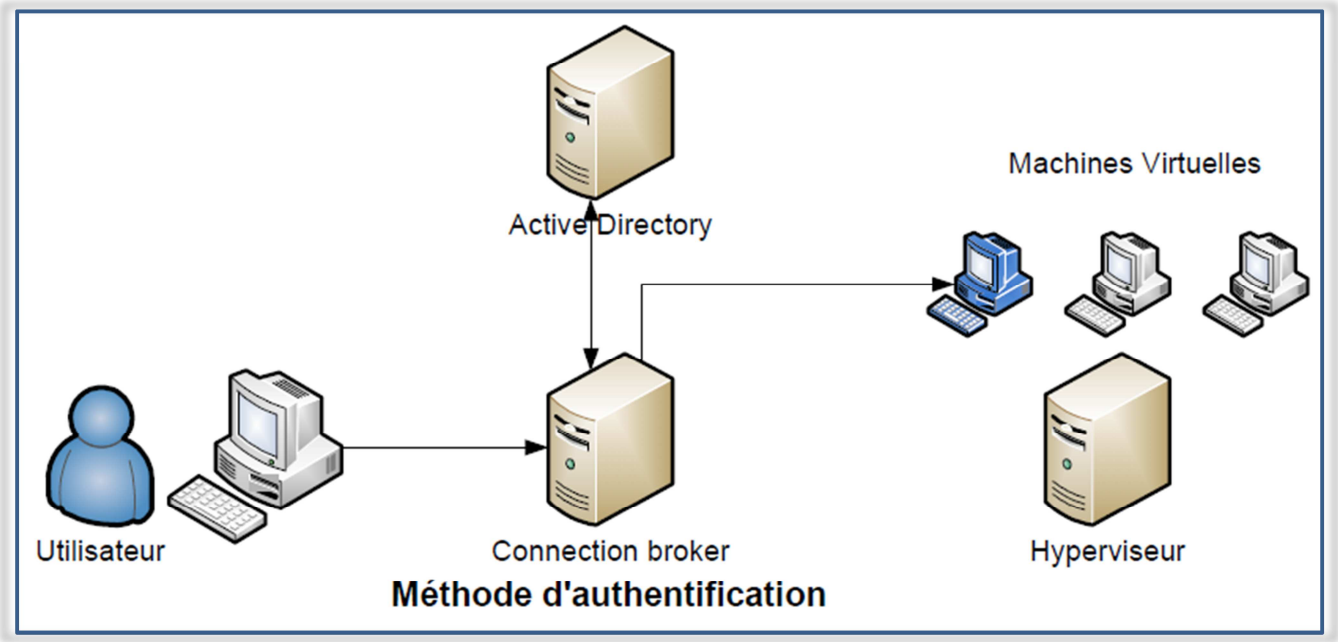
[28] Ressources systèmes de la machine virtuelle dépassant celle du serveur physique. Exemple : la quantité de mémoire cumulée des machines virtuelles qui s'exécutent sur un serveur disposant de 8 Go de mémoire physique peut être de 16 Go grâce à une attribution intelligente et dynamique des ressources physiques aux VM.

6°) Connection broker.

On peut considérer le « connection broker » comme le point central d'une architecture de consolidation de poste de travail. En effet, c'est le serveur qui va mettre à disposition de l'utilisateur un environnement de travail.

7°) Authentification de l'utilisateur.

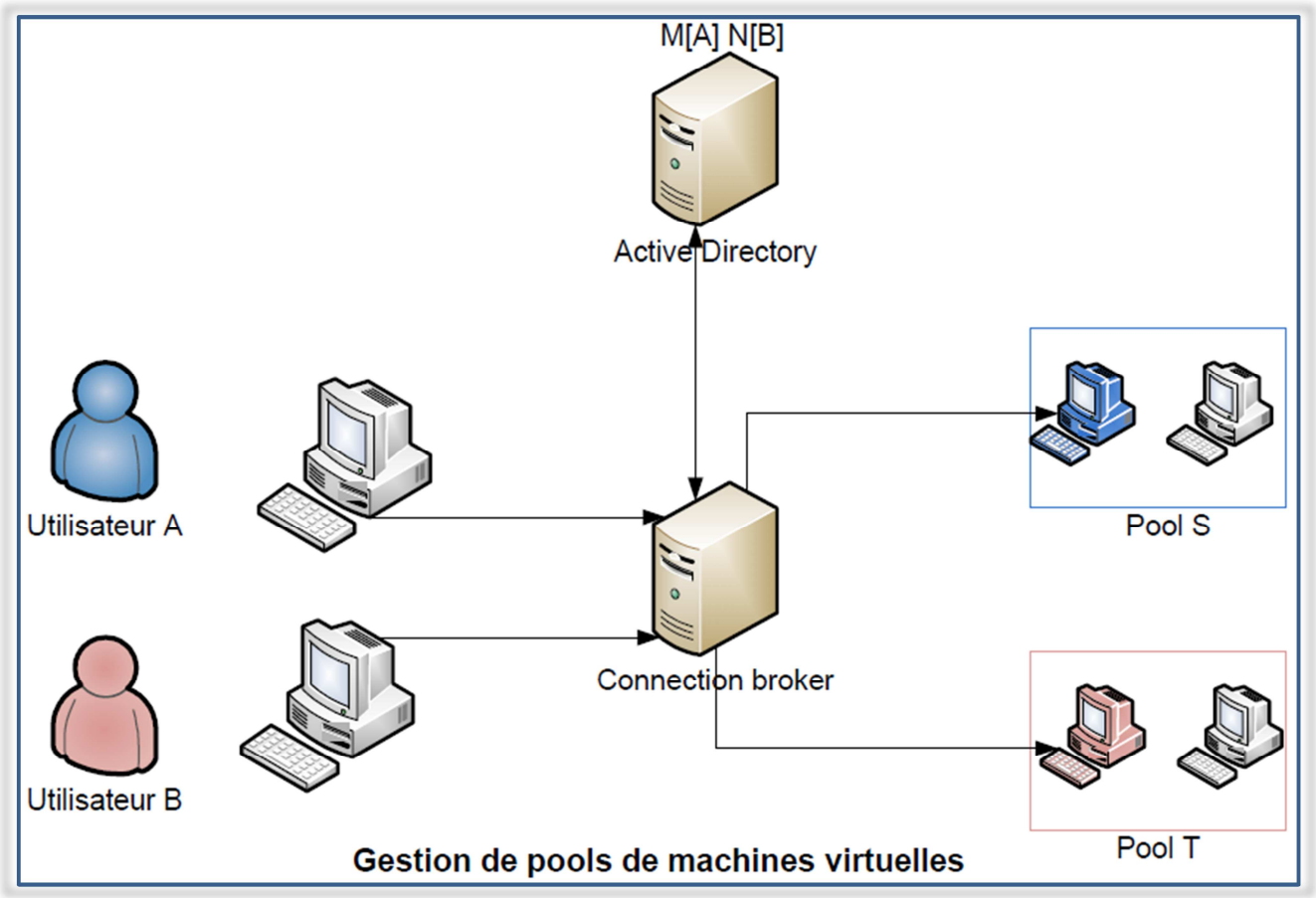
Le « connection broker » est interfacé avec un annuaire de type *LDAP*[29] (Active Directory de Windows) contenant les paramètres d'authentification de chaque utilisateur.



[29] Protocole permettant l'interrogation et la modification des services d'annuaire. Ce protocole repose sur TCP/IP. Il a cependant évolué pour représenter une norme pour les systèmes d'annuaires, incluant un modèle de données, un modèle de nommage. C'est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leurs valeurs. Le nommage des éléments constituant l'arbre (racine, branches, feuilles) reflète souvent le modèle politique, géographique ou organisationnel de la structure représentée par l'annuaire.

8°) Gestion des pools de machines virtuelles.

Un utilisateur A, faisant parti du groupe M dans l'annuaire, a accès à une machine virtuelle du pool S. Alors qu'un utilisateur B, faisant parti du groupe N, a accès à une machine virtuelle du pool T. Dans ce cas, le *profil itinérant de Windows*[30] doit être mise en place car l'utilisateur n'aura jamais la même machine virtuelle attribuée.



[30] Le profil itinérant de Windows est une fonction de l'Active Directory. C'est la définition d'un profil qui est disponible sur l'ensemble des postes de travail référencés dans l'AD. Ainsi l'utilisateur du profil itinérant n'est pas dépendant de son poste pour s'authentifier et accéder à son environnement de travail. L'ensemble de l'architecture VMware View (notamment la gestion des pools) est interfacée avec le(s) domaine(s) AD existant.

9°) Allocation automatique des machines virtuelles (Provisionning).

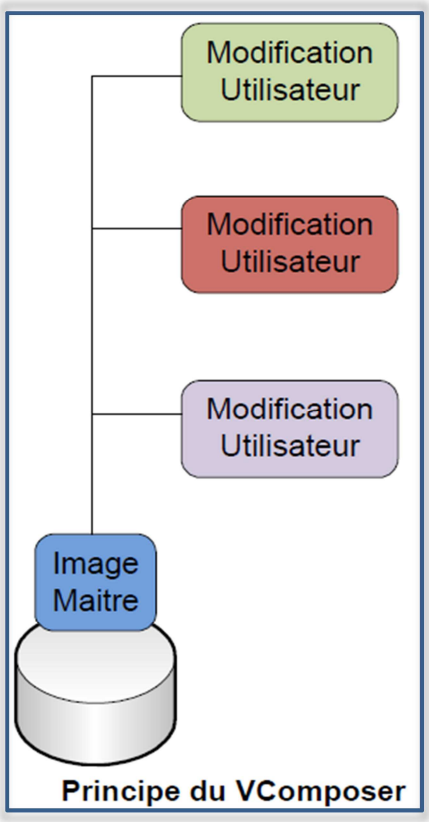
Un poste de travail virtuel peut être créé à la connexion d'un utilisateur ou de manière préventive pour éviter des périodes de surcharge.

Nous allons comparer maintenant les principaux « connection broker » du marché à l'aide d'un tableau :

	Quest Software Provision VAS Network 5.9	Leostream CB 5.0	Vmware View 3	Citrix Xen Desktop
Support d'ESX	Oui	Oui	Oui	Oui
Support de XEN	Oui	Non	Non	Oui
Bureau assigné temporairement	Oui	Oui	Oui	Oui
Bureau assigné en permanence	Oui	Oui	Oui	Oui
Gestion de pools	Oui	Oui	Oui	Oui
Provisioning de VMs	Oui	Non	Oui	Non
SSO	Oui	Oui	Oui	Oui

Comparatif des connexions brokers

SSO : « Single Sign-On » est une méthode permettant à un utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs applications.



Principe du VComposer

Les brokers choisis offrent pratiquement les mêmes fonctionnalités. Seules les solutions de « Quest Software » et « VMware » se démarquent grâce au « provisioning » de machines virtuelles. Il reste une fonction que seul VMware propose aujourd'hui à savoir le « View Composer ».

Ce composant permet de créer des images virtuelles partageants le disque virtuel d'une image maitre (*clones-liés*[31]). Cela permet ainsi de réduire jusqu'à 90% le stockage des postes de travail virtuels.

Grâce à cette dernière fonctionnalité, VMware a pris une avance non négligeable sur la concurrence.

[31] Provisionner des postes de travail virtuel à partir d'une seule machine virtuelle (c'est une VM qui fait 15 Go et qui permet de déployer jusqu'à 64 VM de 2Go). Ainsi une image maitresse (Réplica) sera la source de plusieurs VM. On sépare donc les données systèmes (maintenant communes), des données utilisateurs.

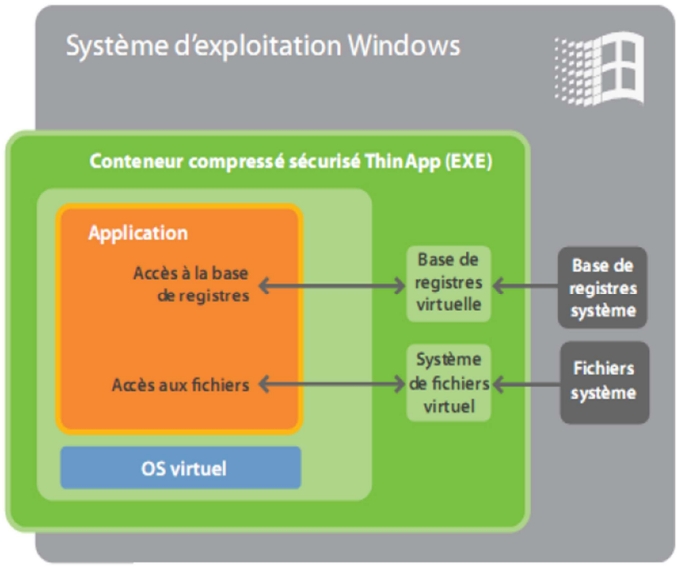
10°) A/ La virtualisation d'application.

Cette technologie est un complément de la virtualisation du poste de travail. La virtualisation d'application permet d'exécuter différentes applications, sous différentes versions, sans conflit car elles sont isolées du système.

Cet outil de création de package d'application permet d'avoir une isolation complète de l'application. Cela permet d'être complètement indépendant des droits de l'utilisateur sur sa machine.

La création d'un package se déroule selon les étapes suivante :

- Démarrage de la capture avec ThinApp
- Installation complète de l'application
- Finir la capture ThinApp après l'installation
- Création du package en *.exe*[32]
- Utilisation du package



Conteneur d'application virtualisée

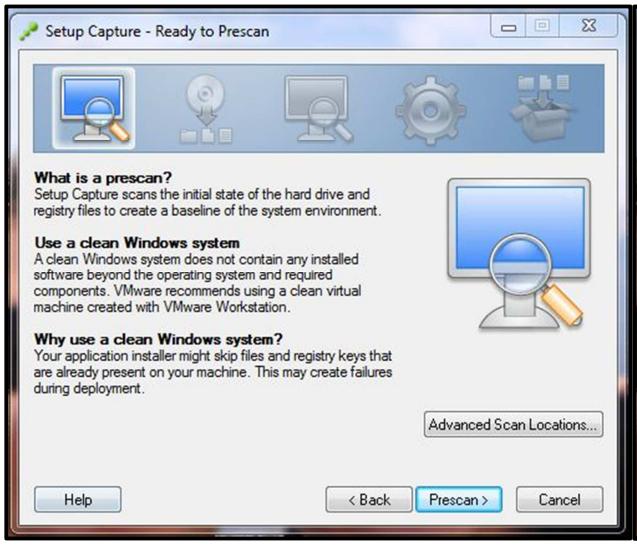
Cette technologie permet de maintenir les versions des applications à jour sans réinstaller complètement les logiciels sur les postes. Ainsi, placer un tel « package » sur un partage réseau permet à un ensemble d'utilisateurs d'exécuter le même package et donc la même application.

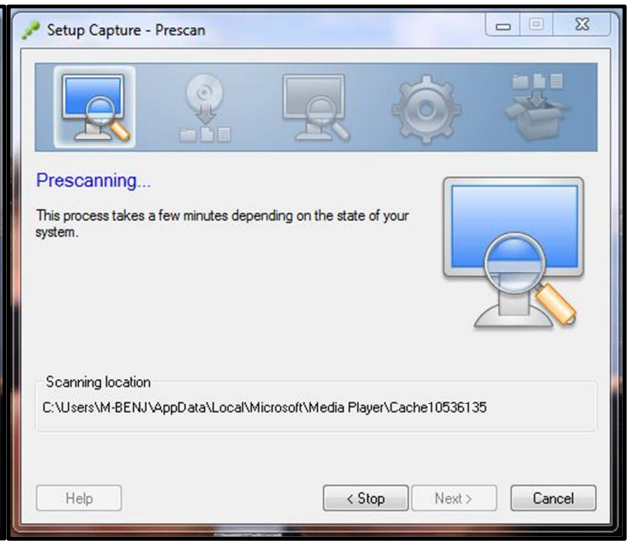
Exemple : Il est possible d'avoir plusieurs versions de client « *Oracle*[33] », exécutées sur le même poste. Plutôt que de rajouter des serveurs (en rack) autonomes, l'architecture prévoit l'utilisation de tous les serveurs d'infrastructure :
Serveur active directory, supervision, administration, sauvegarde, à travers des machines virtuelles (VM) VMware.

[32] Un Fichier exécutable est un fichier contenant un programme et identifié par le système d'exploitation en tant que tel. Le chargement d'un tel fichier entraîne la création d'un processus dans le système, et l'exécution du programme.

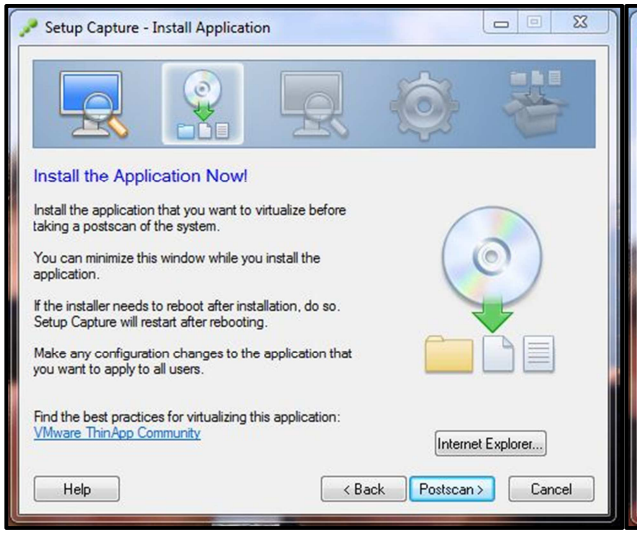
[33] Système de gestion de base de données relationnelles (SGBDR) qui, depuis l'introduction du support du modèle objet dans sa version 8, peut être aussi qualifié de système de gestion de base de données relationnel-objet (SGBDRO).

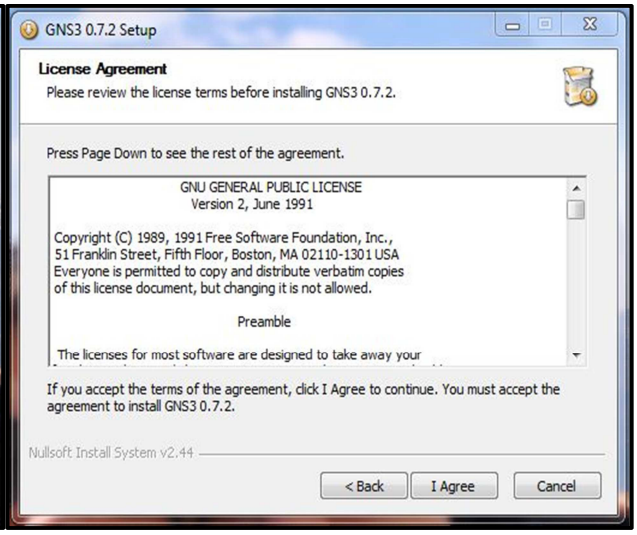
10°) B/ Virtualisation du logiciel « GNS3 » sous ThinApp 4.6.



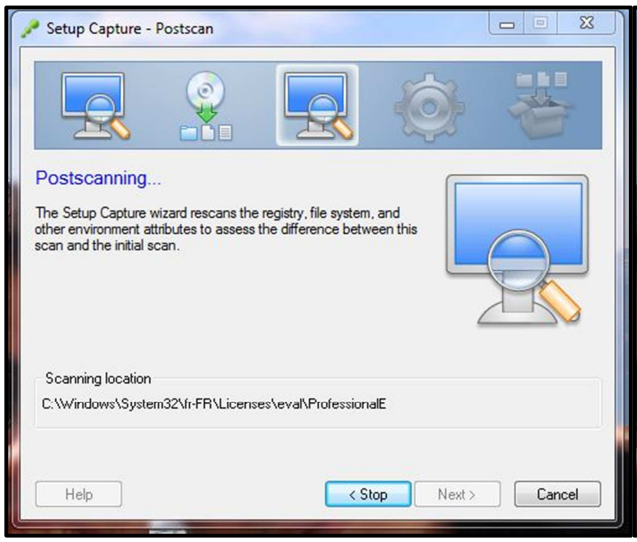


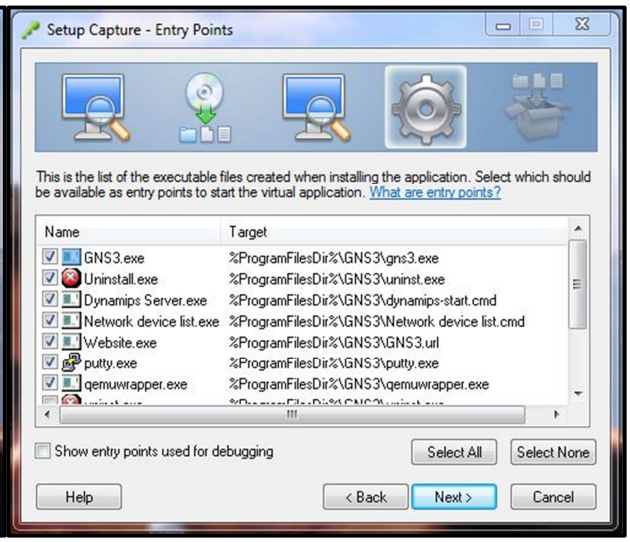
Scannage du système (Prescan). Registres, dossiers d'installations.



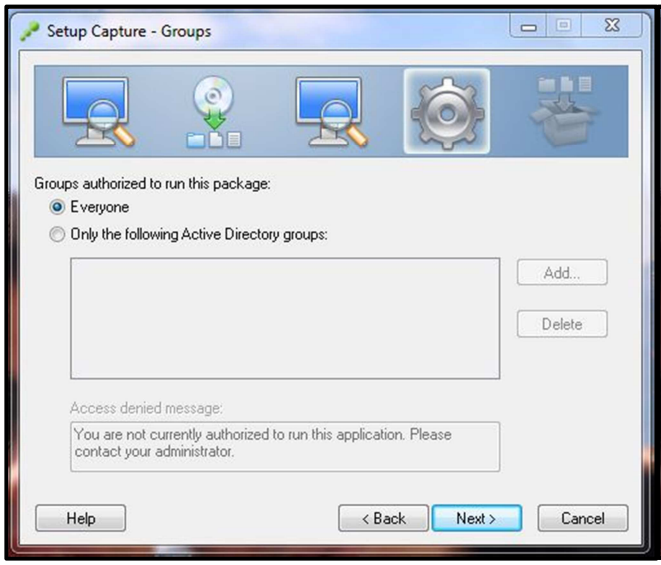


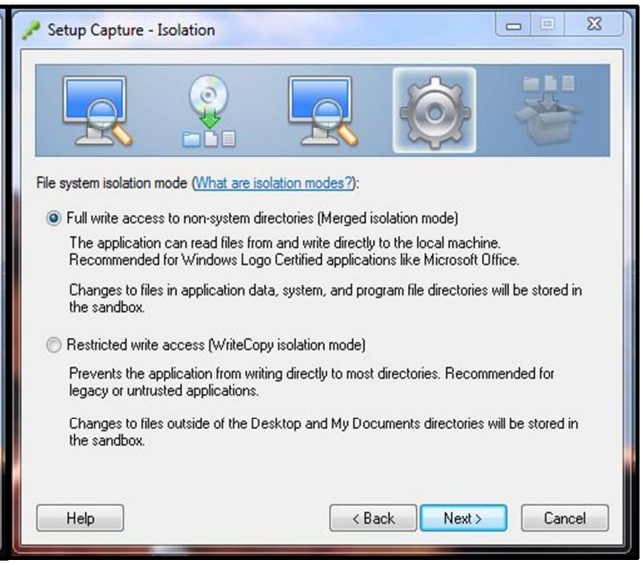
Attente d'une nouvelle installation. Installation de « GNS 3 ».





Nouveau Scannage (Postcan). Composants de GNS3 à « packager ».

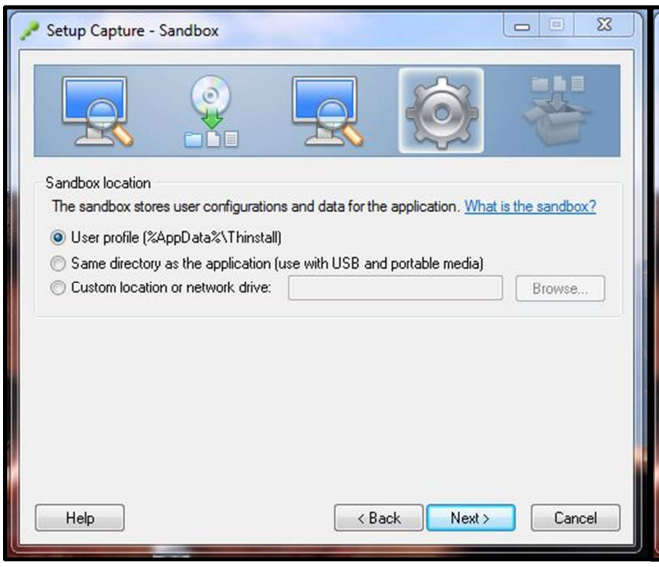


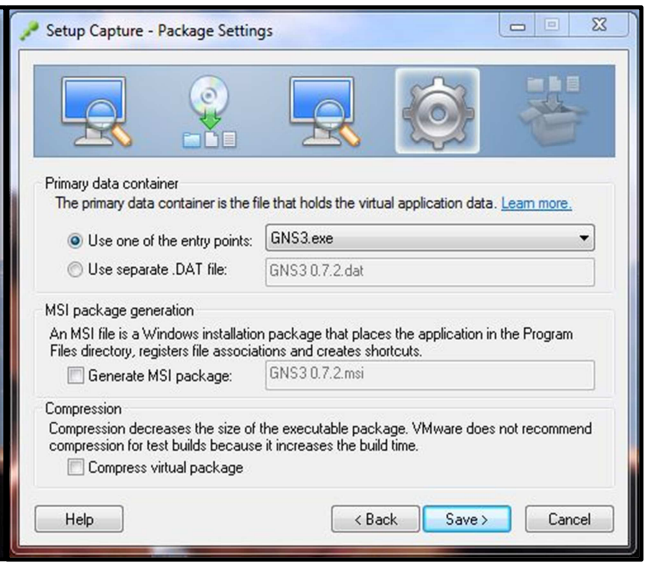


Sélection du type de profil d'utilisateur, autorisé à exécuter le « package », ou non d'après l'AD.

«Merged Isolation mode» : Le logiciel ne peut pas écrire dans les répertoires du système d'exploitation.

«WriteCopy Isolation Mode» : Le logiciel peut écrire partout sur le disque.



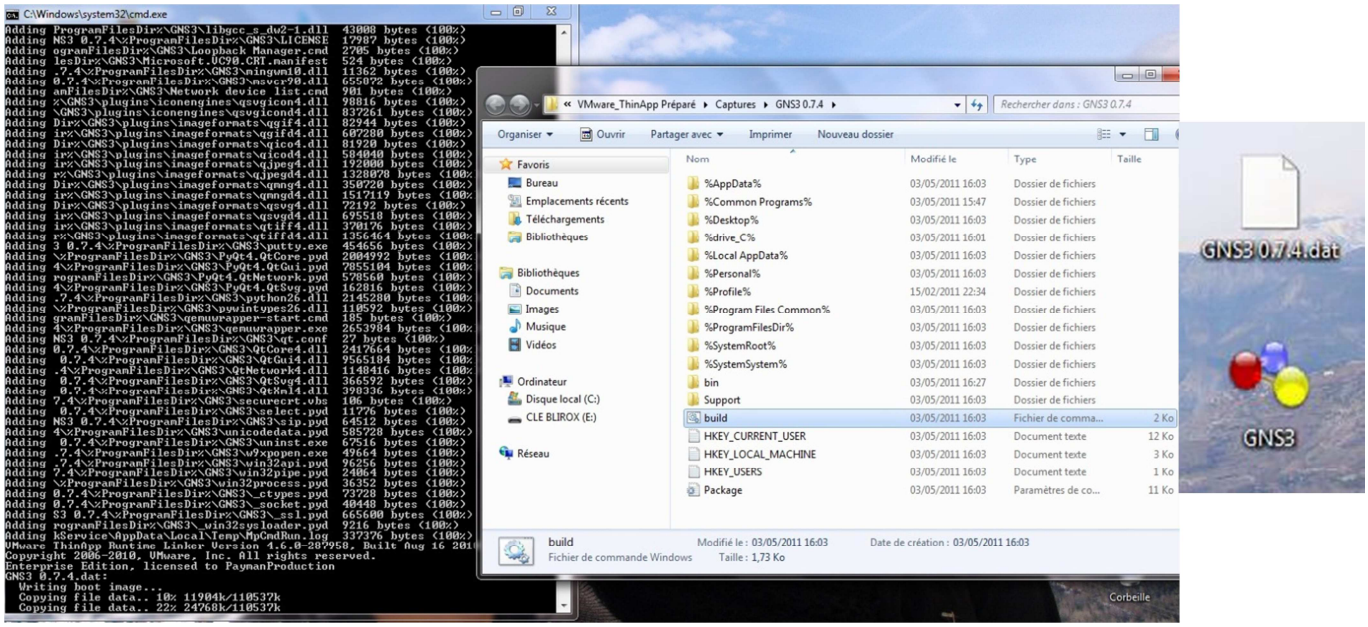


Dossier où sont stockées les modifications de l'application (Delta). Exemple : Lors d'une mise à jour d'un logiciel « packagé », cette modification sera stockée dans la sendbox. Celle-ci se trouve par défaut, dans %users%\AppData\Thinstall\ et sous Windows Seven dans C:\Users\\AppData\Roaming\Thinstall\, ou sur un partage réseau spécifique.

1°) Package « .exe » seulement : de très grande taille, le package ralenti considérablement l'analyse anti-virus, et fait perdre des performances au système.
2°) Package « .exe » et « .dat » : ici, le « .exe » joue le rôle de point d'entrée dans le « .dat » contenant les données.
3°) Package « .msi » : permettant une intégration conventionnelle dans l'environnement Windows (visible dans ajout/supp programme, indexation…)

10°) B/(1) Compilation du package.

Une fois la procédure de ThinApp terminée, nous pouvons voir l'ensemble des fichiers systèmes (DDL, base de registres, dépendances du logiciel packagé) dans le dossier du projet. Pour finaliser la procédure, il suffit d'effectuer le rassemblement de cet ensemble de fichiers via un script « build.bat » en un «.exe » qui sera un point d'accès de quelques Kilos/octets vers un «.dat » qui contient l'ensemble des données du programme packagé.



10°) B/(2) Utilisation de cette méthode au C.H.A .

Aujourd'hui, uniquement deux applications packagées sont en production, « Urqual » (Logiciel de gestion des urgences en temps réel), et « pharma » (Logiciel de commande et de gestion des médicaments). Elles transitent via l'infrastructure virtuelle précédemment étudiée. La démarche de « packaging » de ces applications est identique à celle de GNS3, détaillée ci-dessus.

À terme, l'ensemble des applications des services de l'hôpital seront ainsi packagées. Hormis *Microsoft Office et Convergence*[34] qui sont directement intégrés au *master*[35] des VM. Voir en **Annexe 2,** la création d'un master optimisé.

[34] Convergence (Logiciel administratif du C.H.A détaillé en annexe 1 utilisé par l'ensemble du personnel) est dépendant d'un module de Microsoft Word nommé « Word fusion » pour l'impression des documents administratifs, notamment pour la prise en charge des macros=> (*exécution automatique d'une suite de taches toujours dans le même ordre et de façon répétitive*). D'où l'intérêt d'inclure la suite Microsoft Office et Convergence dans les masters des VM.

[35] Image d'origine du système d'exploitation (Ici Windows XP) servant de base aux clones-liés des VM créent dynamiquement.

III/ Retours d'expériences & Tâches réalisées.

1°) Phase de mise en production des clients légers.

Durant le mois de Mai et Juin, j'ai participé avec Marc et Pierre au début de la mise en production des clients légers. Nous avons réalisé les contraintes et les difficultés qu'une telle infrastructure engendre à divers niveaux.

2°) L'environnement informatique du CHA.

Au sein de l'hôpital, l'outil informatique est omniprésent et doit être disponible 24h/24 et 7j/7 (*voir les logiciels du C.H.A en* **Annexe 1)**. Il existe deux types d'utilisateurs relativement différents : les utilisateurs polyvalents ayant une expérience basique, et ceux qui se limitent exclusivement au(x) logiciel(s) indispensable(s) à leur travail, avec une certaine forme de « contrainte ». Le défi de l'équipe du C.H.A est d'implanter une telle architecture, mais aussi de faire en sorte que celle-ci soit la plus transparente possible vis-à-vis des différents types d'utilisateurs (*habitudes, aucun login/mot de passe personnel, besoins ciblés).*

3°) Engagement financier et rentabilité.

Pour obtenir les ressources budgétaires nécessaires au financement du projet (avoisinant les *un million deux-cent mille euros*), M. Casanova a dû démontrer les réels gains et économies permises par ce type d'architecture (*énergies, non remplacement des machines, augmentation de la productivité, facilité d'administration*). Aucun retour n'est donc possible, le projet doit arriver à terme.

4°) Mise en production : déploiement initial ciblé.

La haute disponibilité et la diversité des utilisateurs, rendent le déploiement et les essais difficiles. L'équipe du C.H.A a dans un premier temps privilégié un déploiement limité dans deux services contrastés :

- Urgences : quatre clients-légers, exploitation du logiciel « Urqual » packagé, utilisation continue, utilisateurs peu coopératifs.
- Bureau des entrées : huit clients-légers, exploitation du logiciel « Noyau Convergence » packagé/non-packagé, utilisation journalière, utilisateurs coopératifs.

Ce type de démarche permet de faire des essais d'intégration et de fonctionnement de manière transparente dans diverses situations avant de répandre le déploiement à l'ensemble du centre hospitalier.

5°) Problème rencontré et raisonnements dialectiques associés.

Les douze utilisateurs concernés par le déploiement ont fait part à l'équipe du C.H.A d'un phénomène de latences durant l'utilisation de leur poste virtuel. Ces latences se traduisent par des gels d'images et/ou du système de quelques secondes, de manière aléatoire, et notamment lors de l'utilisation des logiciels « Urqual » et « Convergence ». Suite à ce phénomène avéré, une large investigation va être amorcée sur l'architecture virtuelle, de la première couche jusqu'à la septième.

Les domaines d'essais réalisés étant vastes, je vais m'appuyer sur le modèle TCP/IP ci-dessous, pour répertorier ainsi chaque essai à une couche de l'architecture (la couche « transport » n'entre pas dans l'étude). J'effectue par la suite un focus sur les essais qui ont majoritairement influencés notre vision du problème.

Applications	Réseau	hôte réseau
1°) Packaging/non-packaging. 2°) Version Client/serveur VMWare View 3°) Vérification des Masters 4°) Clones-liés/Non clones-liés 5°) Paramétrage PCoIP et RDP 6°) Base de Données Oracle	7°) Adressage 8°) VLSM 9°) Sous-répartiteurs 10°) Routage	11°) Client-légers 12°) Câblage 13°) Débit 14°) Switchs 15°) ESX 16°) Stockage (SAN)

Hôte réseau : Les essais au niveau client sont : changement client légers par une configuration plus onéreuse (puce Teradici spéciale PCoIP). Essais avec différents raccordements à divers points du réseau. Au niveau serveur : statistiques des performances des ESX et de la baie de stockage.

Réseau : Le réseau local du C.H.A est relativement vaste et peu optimisé : absence de *VLANs*[36], commutation exclusivement de *niveaux 1 et 2*[37], *domaines de diffusions*[38] importants, vision et administration du réseau perfectibles, câblage du bâtiment en rénovation. Ces faiblesses du réseau laissent aisément à penser que le phénomène de latence provient de celles-ci. Nous avons donc directement raccordé un client léger sur la baie des serveurs virtuels, de manière à être indépendant du réseau, et nous avons constaté le même phénomène de latence.

[36] Un réseau local virtuel, communément appelé VLAN (pour Virtual LAN) est un réseau informatique logique indépendant. De nombreux VLAN peuvent coexister sur un même commutateur réseau. Avantages : réduire la taille d'un domaine de diffusion permet de créer un ensemble logique isolé, pour améliorer la sécurité.

[37] Désigne, dans le modèle en couche OSI d'un réseau, la couche physique et liaison de données. La commutation est uniquement effectué grâce à l'adresse MAC (physique) des machines, il n'y a donc pas de routage.

[38] Zone du réseau composée de tous les ordinateurs et équipements de communication qui peuvent être contactés en envoyant une trame à l'adresse de diffusion de la couche liaison de données (nombreuses collisions possibles).

Applications : Nous avons testé plusieurs configurations : Logiciels installés sur le master et packagés ; nous avons constaté un gain de performances avec le logiciel « Urqual » uniquement, une fois celui-ci installé sur le master. Nous avons approfondi les paramétrages du protocole PCoiP.

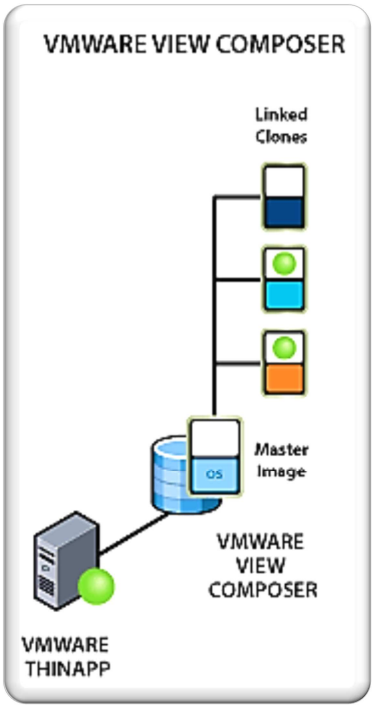
Origine des latences.

Comme nous l'avons précisé en introduction, la protection anti-virus est assurée par Trend Micro. Initialement, la solution OfficeScan 10.5 a été mise en place dans l'infrastructure virtuelle de manière conventionnelle, à savoir : serveur virtuel dédié à l'application, ainsi qu'un *agent*[39] sur chaque VM (intégré au master de chaque *pool*[40] de VM). Nous avons désactivé l'agent anti-virus sur les VM et constaté une absence totale de latences, ainsi qu'une réactivité digne d'un PC conventionnel sur l'OS, comme sur les applications métiers du C.H.A .

La solution.

VMware vShield Endpoint[41] déporte l'analyse anti-virus vers une machine virtuelle renforcée et dédiée sur laquelle une base virale d'un éditeur antivirus est installée.

Grace à cette *API*[42] VMware vShield Endpoint, Trend Micro propose une protection anti-virus, nommée Deep Security 7.5, qui fournit une protection complète aux VM sans agents tiers installés. Réduisant ainsi de manière significative, la charge mémoire et CPU de l'ensemble des VM. Une protection qui minimise l'impact de ses ressources sur l'ESX, et qui participe à une plus grande *banalisation*[43] du poste de travail virtuel.



39 Programme résident qui accomplit des tâches à la manière d'un automate en arrière-plan/ou non du système d'exploitation, qui est souvent installé sur une machine cliente qui exécute un service installé sur un serveur distant. Exemples : le passage de messages, l'appel de procédure à distance, l'évaluation à distance…etc.

40 Le pool est à la base de la notion de « clones-liés ». 1°) Créer un pool correspondant à un groupe d'utilisateur précis. 2°) Créer un master, à savoir une image d'un OS ou vont pointer, l'ensemble des VM. 3°) Créer les VM (clones-liés au master du pool correspondant), qui représentent en terme de taille, le delta des modifications de l'utilisateur, du master, par rapport à la VM *(Voir le schéma ci-contre illustrant le principe, avec un serveur ThinApp)*.

41 Module de sécurité s'intégrant dans vSphère. *(Détaillé en page 29).*

42 Interface permettant l'interaction des programmes les uns avec les autres, de manière analogue à une interface homme-machine, qui rend possible l'interaction entre un homme et une machine.

43 Postes de travail identiques, sans dépendances et simpliste.

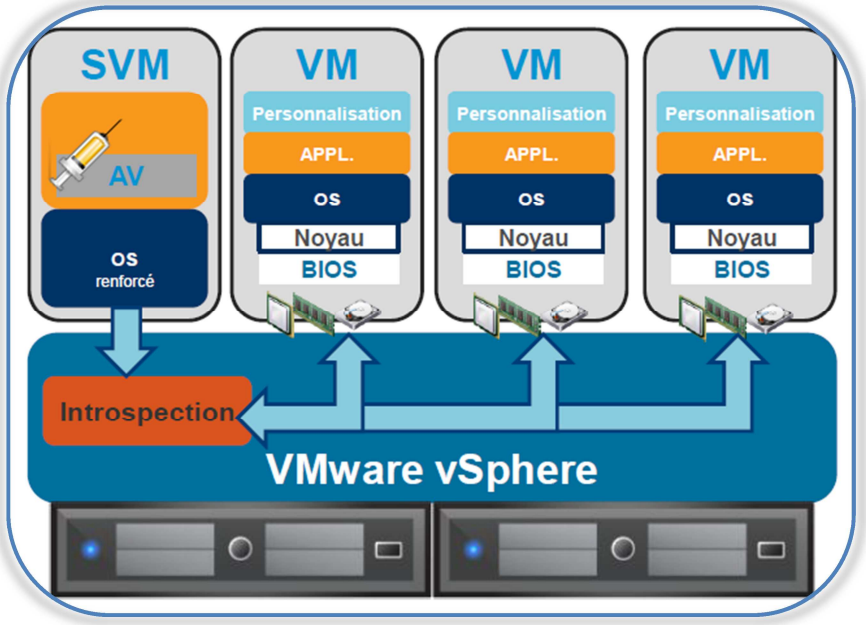
Présentation et Principe de VMware vShield.

Voici, une présentation succincte des modules existant de VMware vShield :

- vShield Manager est l'outil centralisé permettant d'activer et d'installer les différents éléments que compose la famille vShield.

1. vShield zone : vAPI de sécurisation, délivré par VMware, permettant d'intégrer un pare-feu directement dans l'infrastructure VMware et de segmenter les réseaux à l'intérieur de l'Hyperviseur.
2. vShield Edge : Permet la sécurisation périmétrique de l'infrastructure virtuelle intégrant du VPN, du DHCP, de la journalisation et de l'audit.
3. vShield app : sécurisation au niveau des applications hébergées par les VM. Il analyse les applications et les paquets échangés (firewalling).

4. vShield Endpoint : Solution utilisée par le C.H.A, avec Trend Micro.



Afin d'analyser les flux réseau, CPU et mémoire, vShield Endpoint s'intègre directement à l'environnement vSphère et se compose d'une *machine virtuelle dédiée à la sécurité (SVM voir schéma ci-dessus*). C'est les API VMsafe de VMware, qui permettent à ses partenaires (ici Trend Micro avec Deep Security 10.5), de développer une solution de sécurité orientée virtualisation. Sous la forme d'une machine virtuelle de sécurité capable d'accéder, de rapprocher et de modifier les informations en fonction des matériels virtuels suivants :

- Exécution des processus (gestion des clients) : API clients et processus qui surveillent et contrôlent entièrement l'exécution des processus sur la VM.

- Stockage : les fichiers de disque de la machine virtuelle (VMDK) peuvent être installés, manipulés et modifiés lorsqu'ils sont conservés sur des périphériques de stockage.

- Mémoire et processeur **:** VMsafe permet *l'introspection*[44] des pages de mémoire et de l'état des processeurs de la machine virtuelle cliente.
  VMsafe Memory & CPU API (VMsafe-Mem/CPU).

- Mise en réseau **:** filtrage des paquets réseau sur l'hyperviseur et sur une machine virtuelle de sécurité.
  VMsafe Network Packet Inspection API (VMsafe-Net).

Tous ces composants renvoient les flux directement à la SVM de sécurité qui a toutes les paternes *(définition de virus, comportements, prises de décisions…etc).* L'avantage, est que l'on ne conserve qu'un seul paterne par serveur ESX. Cela soulage le réseau lors des mises à jour, et concerne seulement la SVM.

6°) Maquette d'un environnement client-serveur, de type VMware vSphère.

Comme nous pouvons le constater d'après les chapitres précédents, la compréhension de cette infrastructure et de ses composants n'est pas aisée. C'est pourquoi j'ai réalisé une maquette de principe, modélisant un environnement client-serveur vSphère, de manière à ce que le principe de base soit probant.

6°) (1)\ Qu'est-ce que VMware vSphère ?

La plateforme vSphère, est une suite d'une quinzaine de modules permettant : la virtualisation, la mise en production, et l'administration des serveurs d'entreprises. Ces modules, (que nous ne détaillons pas ici) interviennent dans tous les domaines : stockages, réseaux, ressources systèmes, sécurité, maintenance, administration et applicatif. La maquette concerne uniquement les ressources systèmes (ESXi, qui est l'hyperviseur **voir les pages 9 et 10** de VMware dans sa version gratuite), et l'administration (client vSphère permettant le management de l'ESXi).

[44] Adjectif signifiant une analyse du sujet par lui-même. Dans la lutte que se livrent virus et antivirus, c'est aujourd'hui en effet à celui qui exécute son programme le premier : si un code malveillant parvient à démarrer avant l'antivirus, il sera particulièrement difficile pour ce dernier d'avoir confiance dans les données qu'il pourra lire sur la machine. Le parasite contrôlant le système, il pourra lui présenter des lectures erronées et laisser voir un système sain. Et jusqu'à aujourd'hui, le code malveillant et l'antivirus partaient sur un pied d'égalité dans cette course, car ils sont tous les deux de simples applications hébergées sur le même système. L'API VMsafe permet aux éditeurs de solutions de sécurité, d'exécuter leur code au même niveau que l'hyperviseur, c'est à dire à l'extérieur des machines, totalement intouchable et jouissant surtout d'une vue imprenable sur le système : contrôler la mémoire, les entrées/sorties, le processeur et les unités de stockage. Cela signifie qu'en dehors de toute vulnérabilité propre à VMware, un code malveillant s'imaginera seul au monde et n'aura aucun moyen de se savoir observé par la solution de sécurité, d'où le terme d'introspection.

6°) (2)\ Virtualisation complète d'un système d'exploitation Hyperviseur.

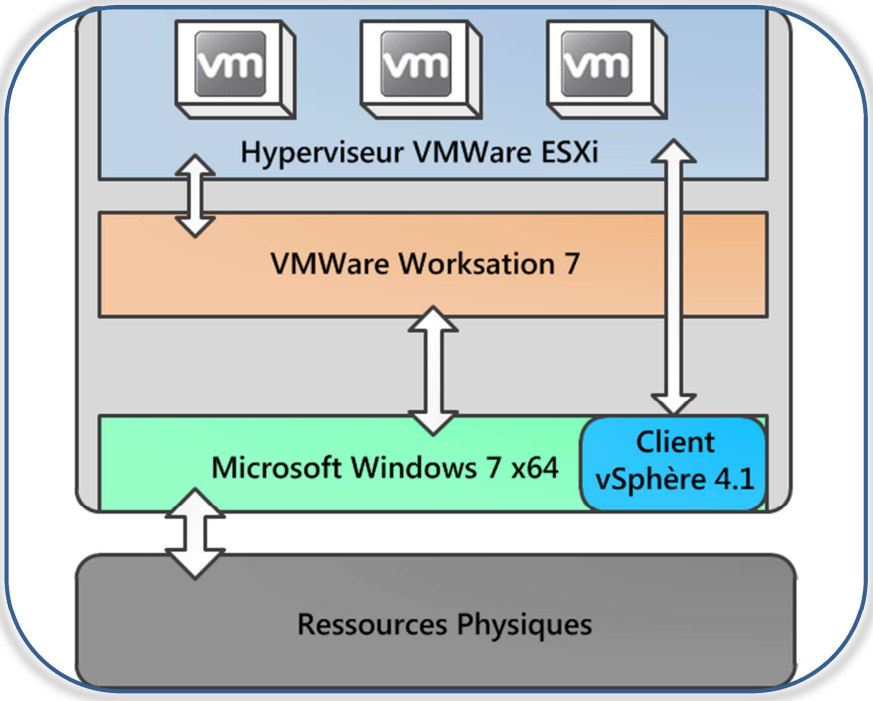


Schéma de principe d'une maquette client-serveur de type vSphère

Le système d'exploitation hôte est « Windows Seven Professional Edition 64 Bits ». La virtualisation complète page 8 de l'hyperviseur ESXi est réalisée grâce au logiciel « VMware Workstation », installé en tant que programme utilisateur sur l'OS hôte. Les ressources physiques émulées correspondent au minimum requis d'un serveur ESX physique en production, à savoir : *4 Go de mémoire vive, un minimum de 60 Go de disque dur (cela dépend du nombre de VM), d'un processeur quadruple cœurs supportant les instructions, intel VT ou AMD-V*. Ainsi, les ressources de la machine physique sont totalement émulées et mises à la disposition de la maquette.

7°) Points importants non-abordés.

Il est important de préciser que techniquement, une infrastructure virtuelle de cette envergure est extrêmement dense en domaines de compétences. C'est pourquoi, je souhaite énumérer les composantes de l'architecture non-abordées dans ce rapport.

- Mise en place et fonctionnement du PRA (Plan de reprise d'activité)
- Mise en place et fonctionnement du réseau SAN, des backups, de la gestion des bandes magnétiques LTO.
- Etudes d'avant-projet réalisées par l'équipe du C.H.A (études et essais des technologies existantes, choix de la technologie, enquêtes sur la compatibilité des logiciels métiers par rapport à l'environnement virtuel).
- Etude concrète des capacités du réseau local, avant le renouvellement du cœur du réseau prévu pour septembre 2012.

IV/ Conclusions.

Pourquoi ce choix de stage ?

" «Virtualisation», «dématérialisation», «plateforme», «en ligne», autant de termes étroitement liés à «l'informatique dans les nuages». De façon quasi unanime, les fournisseurs de solutions de virtualisation estiment que le décollage du marché aura lieu début 2012, notamment sous l'impulsion du secteur public en France. La montée en puissance de la virtualisation précipitera le recul des ventes de micro-ordinateurs, notamment pour les PC de bureau et les serveurs. Les seuls formats épargnés seraient ainsi les ordinateurs portables. Selon ce scénario très probable, on ne verra plus sur les bureaux des entreprises que des configurations « écran-clavier-souris », le cerveau des « clients légers » logeant dans le socle de l'écran ou dans la structure du bâtiment, au même titre qu'une prise électrique. "

Extrait d'un article du journal « Le Monde » Février 2011.

Pour être compétent en tant qu'intégrateur de ce type d'architecture, les domaines de compétences requis, dépendants des uns des autres, sont : réseaux, administrations des systèmes Windows/Unix, stockage, sécurité et maitrise des technologies VMware et Citrix. Durant ces 12 semaines au sein du C.H.A, j'ai pu me rendre compte, que ce métier est pluridisciplinaire et son domaine émergeant, où l'expérience est une forte valeur ajoutée. Aujourd'hui, le C.H.A est une véritable vitrine technologique, représentant actuellement une des rares architectures virtuelles en production, d'une telle envergure en France. Ce stage m'a permis de me rendre compte, de manière concrète, du potentiel de ce métier vers lequel je prétends me diriger (licence professionnelle IRI orientée virtualisation, alternée par un contrat d'apprentissage, avec un intégrateur spécialisé qui est NEXTO. www.nexto.fr). Et au-delà, ce stage a révélé une passion pour cette technologie, autant sur la technique que sur la morale. En effet, l'aspect de participation à une démarche de développement durable, liée aux économies d'énergies, me comble.

Bilan.

Mon stage, au sein du service informatique du C.H.A, fut complet et considérablement formateur, tant sur le plan technique que théorique. Mes recherches de documentations techniques furent importantes afin d'être capable de suivre les transmissions de compétences et réaliser les taches qui m'ont été confiées. Il était également intéressant de constater les similitudes entre certaines problématiques rencontrées durant le stage et celles soumises durant les TP/TD de réseaux. Je pense particulièrement à M. Roland Depeyre, pour ses explications et exemples extrêmement concrets. Que j'ai pu retrouver lors de réflexions techniques que j'ai pu avoir durant le stage concernant les caractéristiques d'un réseau local. Je souhaite également souligner l'impact majeur qu'a pu avoir l'épreuve du TCS (http://jeuxj.free.fr/cisco_acacia_2011/), sur ma motivation et mon intérêt concernant les réseaux et ses applications.