

BTS SIO

Situation professionnelle numéro 1

Sélectionner un hyperviseur et effectuer un test de conversion P2V

Description :

La virtualisation fait partie intégrante des systèmes d'informations. Elle répond à des besoins de rationalisation de matériel et de simplification de l'administration.

Mots-clés :

Hyperviseur Samba
VMware HP Powershell
Eset Vconverter IBM TSE
Windows
nod32

Validation de la situation professionnelle

Nom	Date	Tampon
	26/05/2014	

Plan de la situation

Le cahier des charges.....	3
L'expression des besoins	3
La description de l'existant.....	3
Les offres du marché :.....	4
L'analyse des choix.....	5
Le choix : VMWare ESXi 5.1	5
Les nouveaux risques de l'hyperviseur.....	6
Préparation de la Migration vers Vmware ESXi :	6
Mise en œuvre	7
Préparation du serveur physique : Nettoyage	7
Préparation du serveur physique : Rôles et fonctionnalités	9
Installation de VMware ESXi 5.1.....	10
Conversion P2V de notre serveur	11
Lancement de la machine virtuelle dans ESXi:.....	12

Le cahier des charges

L'expression des besoins

La société es2com recherche un hyperviseur performant et stable. Elle souhaite faire une mise à niveau de ses serveurs actuels et aimerait élargir son champs de compétences afin de faire évoluer ses offres envers ses clients. Un de nos clients a justement besoin d'un hyperviseur et de convertir un serveur physique en VM.

La description de l'existant

Le serveur existant utilise le système d'exploitation : Microsoft Windows 2008 Standard.

Le licence est liée à la machine et le serveur est en production.

La configuration du matériel est exprimée ci-dessous :

	ml350
Processeurs-CPU	XEON E5504 @2Ghz (2CPU)
Mémoire-RAM	12Go
Stockages-DISQUES	150Go,300Go,1500Go
Puissance-ALIMENTATION	460W
PCI-EXPRESS-16X	CARTE RAID1
PCI-EXPRESS-X	CARTE RESEAU x2

Le serveur est de marque HP, avec un nom DNS correspondant à la gamme serveur (ml350).

Le serveur est capable de réaliser de la virtualisation, l'activation est présente dans le BIOS.

Un périphérique sur bande pour la sauvegarde est présent sur le serveur, voici notre solution :

Les cassettes pour revenir en arrière d'une semaine : C1.Lundi, C2.Mardi, C3.Mercredi, C4.Jeudi

Les cassette pour revenir en arrière de deux semaines : C5.pair vendredi, C5.impair vendredi.

Les cassette pour revenir en arriere d'un mois: C5DV.pair (dernier vendredi du mois) C5DV.impair

(Nous n'évoquons pas la sauvegarde , ceci est à titre indicatif)

Voici une vue de notre materiel (HP ProLiant ml350 G6)



Les offres du marché :

Actuellement, énormément d'hyperviseurs sont disponibles sur le marché et ils répondent à de nombreux problèmes posés dans le passé, pourtant ils ne sont pas tous égaux.

Voici un tableau comparatif des offres du marché existant en septembre 2012 :

	HYPER-V3	VMWARE ESX5.1	Citrix XenServer 6.1	Proxmox VE 2.2
CPU (logiques) par hôte	320	160	160	160
Mémoire physique maximale	4 To	32 Go	1 To (128 Go si au moins une VM paravirtualisée utilise un OS 32-bits)	2 To
Nombre maximal de VM par hôte	1024	512	150	?
vCPU par VM	64	8	16 (32 sous conditions)	?
vRAM par VM	1 To	32 Go	128 Go	?
Ajout à chaud	Non	Disques, NIC	Disques, NIC	Non
Taille maximale des disques virtuels	64 To (VHDX)	2 To (VMDK)	2 To	?
Thin Disk Provisioning	Oui	Oui	Limité	Non
SAN Multipath	Oui	Oui	Partiel	Oui
Gestion optimisée de la mémoire	Dynamic Memory	Dynamic Memory, Memory Ballooning, Transparent Page Sharing, Compression, Swapping	Non	KSM, Memory Ballooning, Swapping
Live Migration des VM	Oui	Non	Oui (XenMotion Live Migration)	Oui
Snpashot des VM	Oui	Oui	Oui (mais offline)	Oui
Live Storage Migration	Oui	Non	Non	Non
NIC Teaming	Oui	Oui	Oui	Oui
Outils d'administration à distance	Server Manager, RSAT	vSphere Client	XenCenter	Interface Web

L'analyse des choix

Hyper-V3 : Avec cette nouvelle version, Microsoft a clairement amélioré son produit et propose un hyperviseur natif performant et complet. Cependant par rapport aux autres systèmes du marché, l'architecture utilise une grande partie d'espace disque. Microsoft Hyper-V R3 reste très encombrant, notamment à cause du code Windows sans rapport avec la virtualisation intégrée au produit et avec l'ensemble des risques qu'il suppose.

Vmware ESXi5 : Vsphère Hyperviseur ne domine plus ses concurrents directs comme c'était le cas auparavant. Même si les limites de la version gratuite de l'hyperviseur ne devraient pas être gênantes pour une PME. Les analyses estiment que plus de 80 % de toutes les machines virtuelles utilisées dans le monde fonctionnent avec des logiciels VMware.

Citrix XenServer : Handicapé par des performances assez faibles du côté du stockage.

Citrix utilise des particularités lors de l'ajout des iso ainsi que le boot SSH qui rendent la mise en place d'une infrastructure difficile.

Domage que certaines fonctionnalités ne soient pas disponibles dans la version gratuite.

L'interface de gestion des VM semble difficile à prendre en main du premier abord par manque de simplicité.

Proxmox VE 2.2 : Proxmox VE souffre d'une prise en charge imparfaite des derniers processeurs d'Intel. Ajouter à cela une procédure d'installation des pilotes paravirtualisés un peu complexe et vous obtenez un système réservé à l'expert de la ligne de commande. Il faut connaître parfaitement le système linux avant de se lancer.

Le choix : VMWare ESXi 5.1

Nous avons opté pour l'hyperviseur de VMware qui est une solution éprouvée car c'est un des précurseurs dans le domaine. Aussi, il existe d'autres logiciels annexes tels que Workstation, Vcenter, Vsphere Web, Vcenter qui peuvent être utilisés de pair avec l'hyperviseur ESXi 5 de VMware, cela correspond à nos attentes. Les ressources matérielles qu'elle propose en version 5 sont suffisantes pour des petites entreprises.

Dans une autre mesure nous avons conscience que quelque soit l'hyperviseur utilisé, il n'est pas exempté de problèmes de sécurité, et qu'il amène un lot de nouveaux risques.

Nous prendrons conscience du fonctionnement globale de l'hyperviseur et de ses risques.

L'hyperviseur est une évolution dans le monde des serveurs. On ne parle plus que de VM et elles ne sont plus liées aux matériels et peuvent fonctionner ensemble sur un seul matériel physique. L'hyperviseur permet de centraliser tous les serveurs dans une même machine physique.

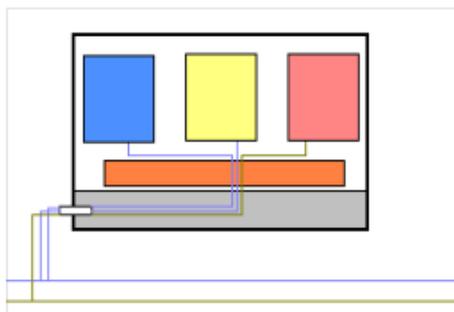
Juridiquement nous allons devoir posséder une clé d'activation valide pour utiliser librement et gratuitement notre hyperviseur. *La sécurité est plus sensible à cause de la couche d'abstraction.*



Les nouveaux risques de l'hyperviseur

- La couche d'abstraction peut être une faille si elle est compromise car c'est une couche basse
- Si la machine physique tombe en panne, tous les serveurs sont touchés.
- Vulnérabilité au niveau des instances partagées : exemple flux de carte réseau.

Les 3 rectangles de couleurs sont les VM, la zone grise est la machine physique, la zone orange est la zone d'abstraction. Pas de cloisonnement, le flux réseau E/S par la même carte.



Complexification de l'administration et de la mise en œuvre
Supervision et traçage des actions difficiles.
Prolifération des données non -souhaitées (VM copiée etc.)
Incapacité à comprendre les différentes erreurs hardware.
Investigation post incident plus difficile

Pour conclure, il nous faudra du temps pour maîtriser le fonctionnement global de notre hyperviseur.

Préparation de la Migration vers VMware ESXi :

Le passage d'un état existant d'un système d'information vers une cible définie est une étape critique. Convertir une machine physique en une machine virtuelle n'est pas un exercice très difficile, cependant nous devons être vigilant et nous devons minimiser les risques d'instabilité avant de la convertir.:

Etape 1 : Nettoyage ml350

- Suppression des logiciels et progiciels inutilisés.
- Récupération des différentes licences des postes avec le logiciel « nirsoft » par exemple.
- Vidages de tous les temporaires (IE, Windows...)
- Nettoyage de la corbeille de tous les comptes utilisateurs.
- Alléger les partages et nettoyer l'active directory (GPO, Scripts, Users)
- Faire un scan malwarebytes, anti-exploit, anti-rootkit, nod32 smart security et adwcleaner.

Etape 2 : Rôles et fonctionnalités ml350

- Suppression des rôles et fonctionnalités inutilisés.
- Analyse de l'observateur d'événement Windows.
- Enregistrement de la configuration matérielle du gestionnaire dans un fichier texte.
- Procédure de redémarrage de la machine.

Etape 3 : lancement de la migration

- Installation d'un ESX 5 en version d'essai de 60jours.
- Démarrage de la conversion à chaud de la machine vers ESXi 5.1

Mise en œuvre

Préparation du serveur physique : Nettoyage

Dans le but de favoriser des outils intégrés au système, nous allons utiliser « Powershell ».
L'outil de Scripting de Windows est orienté « objet » et est plus puissant que : « cmd.exe » en CLI.
Des logiciels tiers seront également utilisés pour la détection de menace :

- Eset Nod End File security
- Malwarebytes antimalware, anti-rootkit, et anti-exploit
- Adwcleaner, tskiller, et roguekiller

Le nettoyage s'effectue sur la machine de production le soir après les horaires de travail des employés.
Suivons ensemble les étapes énoncées plus haut avec la suppression des logiciels et progiciels obsolètes.

La commande suivante permet de faire la liste de tous les logiciels présents sur la machine.

```
GET-WMIOBJECT -CLASS WIN32_PRODUCT > PROGRAMMES.TXT
```

Le fichier « programmes.txt » contient l'ensemble des programmes installés sur la machine.
Puis, nous allons isoler un programme cible tel que "Eset" :

```
GET-WMIOBJECT -CLASS WIN32_PRODUCT | WHERE { $_.NAME -LIKE "*ESET*" }
```

Le résultat de la commande :

```
IDENTIFYINGNUMBER: {16307634-7BAE-4BB7-B88A-E220331C8AA4}  
NAME : ESET SMART SECURITY  
VENDOR : ESET, SPOL S R. O.  
VERSION : 6.0.316.1  
CAPTION : ESET SMART SECURITY
```

Nous avons aussi la possibilité de comparer notre liste des programmes actuels avec une autre.
Nous pouvons comparer notre liste avec celle de l'année dernière par exemple :

```
COMPARE-OBJECT -REFERENCEOBJECT (GET-CONTENT C:\PROGRAMMES13.TXT) -DIFFERENCEOBJECT (GET-CONTENT  
C:\PROGRAMMES12.TXT)
```

Continuons et procédons à l'appel de l'ensemble des formats disponibles :

```
GET-WMIOBJECT -CLASS WIN32_PRODUCT | WHERE { $_.NAME -LIKE "*WINZIP*" } | FORMAT-LIST*
```

La propriété "LocalPackage" apparaît, c'est celle qui nous intéresse.

On combine les commandes et on ajoute la variable choisi exemple : \$eset

- \$ESET = GET-WMIOBJECT -CLASS WIN32_PRODUCT | WHERE { \$_.NAME -LIKE "*ESET*" }
- \$ESET.LOCALPACKAGE

On lance la commande : « \$ESET.LOCALPACKAGE » ce qui nous renvoie à la source d'installation :

```
PS C:\> $Uzip = Get-WmiObject -Class win32_product | where { $_.Name -like "*Winzip*" }  
PS C:\> $Uzip.localPackage  
C:\Windows\Installer\203bbc.nsi  
PS C:\> _
```

Pour lancer la désinstallation, j'utilise la variable avec la commande localpackage.

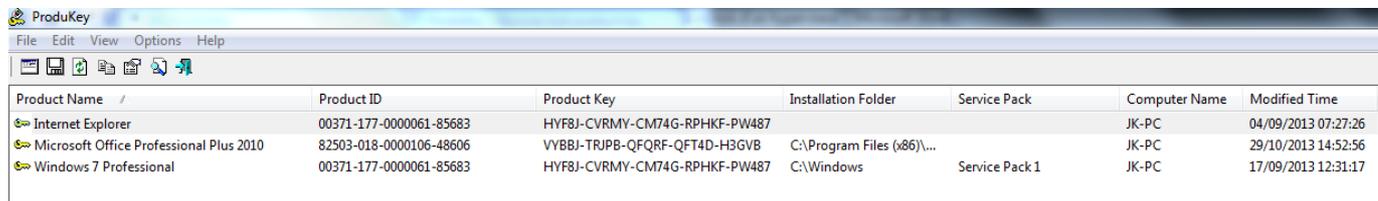
```
MSIEXEC /X $ESET.LOCALPACKAGE /PASSIVE
```

Continuons notre nettoyage du serveur avec un logiciel tiers : Nirsoft Produkey.

Le logiciel est disponible à cette adresse : http://www.nirsoft.net/utills/product_cd_key_viewer.html

Nous ne disposons pas de système de monitoring qui puisse centraliser nos licences.

Il nous permet de récupérer les clés des licences de notre système Windows 2008.



Product Name	Product ID	Product Key	Installation Folder	Service Pack	Computer Name	Modified Time
Internet Explorer	00371-177-0000061-85683	HYF8J-CVRMY-CM74G-RPHKF-PW487			JK-PC	04/09/2013 07:27:26
Microsoft Office Professional Plus 2010	82503-018-0000106-48606	VYBBJ-TRJPB-QFQRF-QFT4D-H3GVB	C:\Program Files (x86)\...		JK-PC	29/10/2013 14:52:56
Windows 7 Professional	00371-177-0000061-85683	HYF8J-CVRMY-CM74G-RPHKF-PW487	C:\Windows	Service Pack 1	JK-PC	17/09/2013 12:31:17

Le software, laisse une trace de son passage en tant que « Hacktool » Nod32 le détecte.

Une fois les licences stockées nous les sauvegardons dans une note sécurisée type Lastpass.

Les corbeilles des utilisateurs du domaine seront nettoyées avec la commande powershell suivante :

```
D /S C:\$RECYCLE.BIN
```

La suppression des fichiers obsolètes et des objets de l'AD peuvent être supprimés avec la commande :

```
DSRM CN=NOM_DU_PC,OU=COMPUTERS,OU=CONTAINER,DC=CHEMIN,DC=DE,DC=VOTRE,DC=DOMAINE,DC=COM -S  
SERVEUR_AD -NOPROMPT
```

Exemple : Domaine : es2com.fr ; PDC (contrôleur de domaine) : Zeus ; Machine à supprimer "es2com.old" (compte ordinateur)

Dans l'optique d'optimiser l'espace disque, un travail manuel doit être fait dans chaque partage.

On notera que l'ensemble des partages sont dans le disque C:/ et D:/

Je rédige une note de service à l'ensemble du personnel pour procéder à ce nettoyage :

Avis au utilisateurs du système informatique,

La société es2com travaille actuellement à la refonte du parc informatique et de l'ensemble des systèmes d'information. Une attention toute particulière doit être faite par chacun d'entre vous sur l'usage du stockage sur le serveur (ml350). En effet nous vous demandons un effort sur le nettoyage de vos dossiers et fichiers présents sur celui-ci et de ne garder présent que les documents à usage professionnel. Nous travaillons activement pour que ces contraintes de stockage ne soit plus une barrière à l'avenir.

Dans l'attente de voir une amélioration de l'espace de stockage disponible sur le serveur.

Jérémie

Notre dernière étape consiste à procéder aux différents scans avec des logiciels tiers :

- le Scan de Eset Nod End File security annonce aucune alerte de virus.

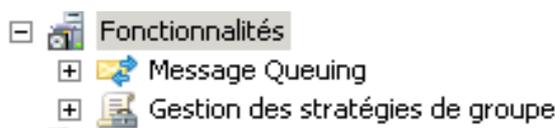
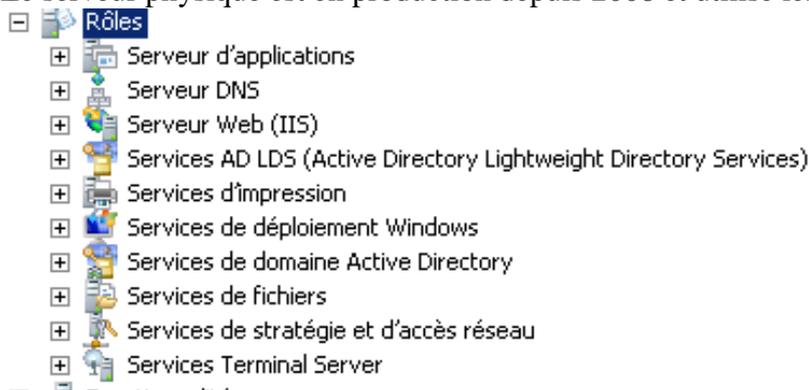
Parfois un email nous parvient, comme l'exemple ci-dessous : ESET File Security Alerte de Menace

```
10/04/2014 10:27:54 - MODULE PROTECTION EN TEMPS REEL DU SYSTEME DE FICHIERS - ALERTE DE MENACE DECLENCHEE  
SUR L'ORDINATEUR ML350 : L'OBJET C:\USERS\MRDUPON\AppData\Local\Temp\6\TEMP1_~1.ZIP\AVIS.DE.PAIEMENT.SCR  
CONTIENT LE VIRUS WIN32/TROJANDOWNLOADER.WASKI.A CHEVAL DE TROIE.
```

- Scan Malwarebytes antimalware, anti-rootkit, et adwcleaner n'on pas fait état d'une menace.

Préparation du serveur physique : Rôles et fonctionnalités

Le serveur physique est en production depuis 2008 et utilise les rôles suivants :



Les fonctionnalités suivantes sont aussi disponibles :

Les fonctionnalités sont bien utilisées mais actuellement nous n'y porterons aucune attention particulière. Cependant, nous décidons de supprimer les rôles inutilisés tels que :

- Serveur WEB (IIS)
- Service de déploiement windows
- Service de stratégie et d'accès reseau
- service tse

Le serveur ml350 se positionne en tant que contrôleur de domaine avec les services suivants : AD/DNS/Spooler/service fichier/Proiciel

Par défaut Windows ne permet pas de gérer le gestionnaire de périphérique autrement que graphiquement. Microsoft a développé un utilitaire appelé « devcon » qui permet de gérer l'ensemble des drivers et des périphériques installés sur nos serveurs.

Afficher l'ensemble des classes de périphérique :

```
DEVCON CLASSES
```

Afficher les périphériques présents localement sur l'ordinateur : `DEVCON FIND * > PERIPH.TXT`

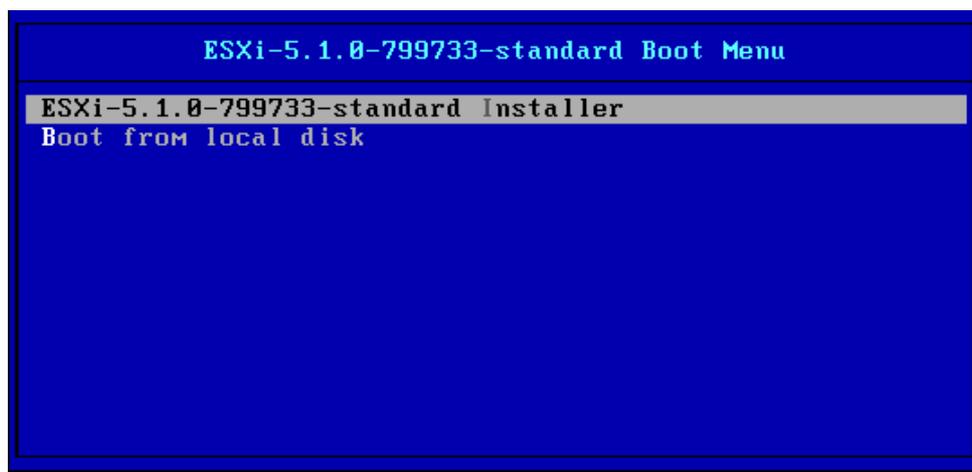
Nous allons supprimer le périphérique de la bande de sauvegarde par cassette : `DEVCON REMOVE @USB\`

L'expérience devcon est très intéressante notamment pour faire des scripts de contrôle de périphérique. Résoudre les problèmes récurrents de Windows sont importants afin de garantir une stabilité optimale du système. Voici comment exporter les événements avec powershell :

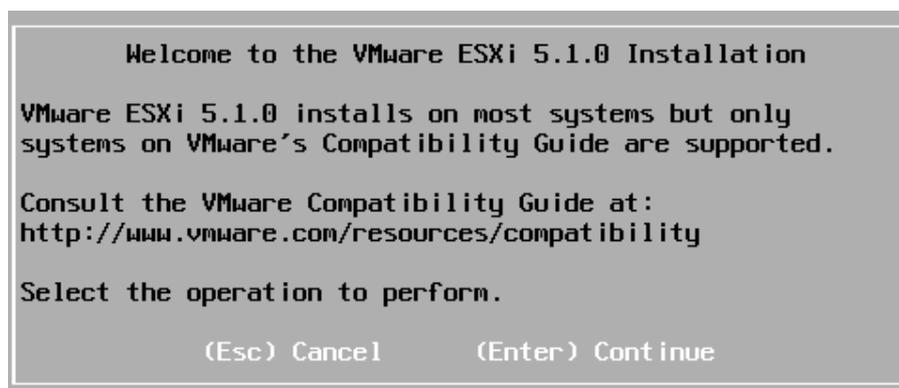
```
GET-EVENTLOG -LIST | %{ GET-EVENTLOG $_.LOG | EXPORT-CLIXML -PATH ($_.LOG + ".XML") } $EVENTS = GET-  
WINEVENT -LOGNAME "WINDOWS POWERSHELL  
$EVENTS.COUNT  
$EVENTS | GROUP-OBJECT ID -NOELEMENT | SORT-OBJECT COUNT -DESC  
COUNT NAME  
-----  
18 600 ; 3 400 ; 2 403  
$EVENTS | GROUP-OBJECT LEVELDISPLAYNAME -NOELEMENT  
COUNT NAME =  
-----  
23 INFORMATION // Uniquement des informations disponible //
```

Installation de VMware ESXi 5.1

Le passage de l'état physique vers la machine virtuelle se fera sur un serveur IBM compatible. Nous procéderons à la migration une fois ESXi5,1 et Vconverter installés.



Une fois les éléments de l'hyperviseur chargés, nous allons procéder à l'installation :

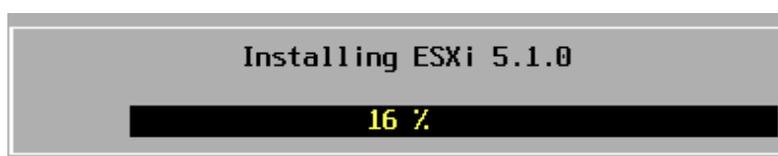
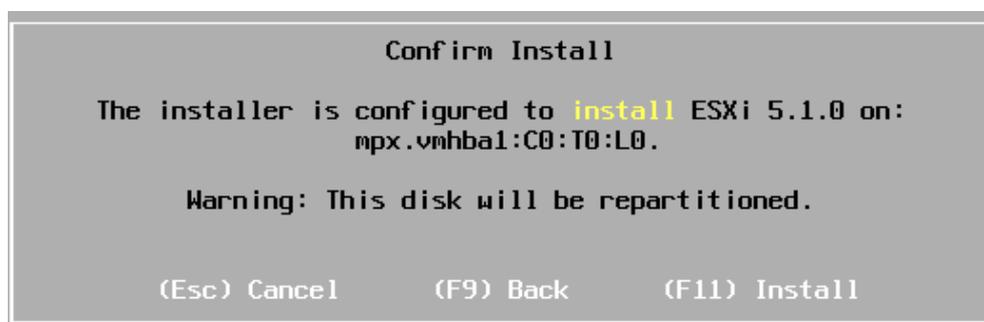


Une licence d'utilisation devra être acceptée en validant avec la touche : F11

Un scan du matériel aura lieu, puis l'hyperviseur nous présente le stockage disponible.

Il suffit de choisir le disque sur lequel l'hyperviseur sera installé, nous l'avons installé sur un SSD.

Pour la suite il nous faudra sélectionner notre disposition du clavier "french" et le mot de passe : root



L'installation se valide avec : F11, l'hyperviseur est ensuite installé sur la machine.

Conversion P2V de notre serveur

VMware vCenter Converter Standalone est un logiciel complet fournit par VMware dont le but est d'effectuer la conversion de machine, notamment **V2V** (Virtual to Virtual) et **P2V** (Physical to Virtual), afin de convertir une machine physique en machine virtuelle ou une machine virtuelle vers un type de machine virtuel différent.

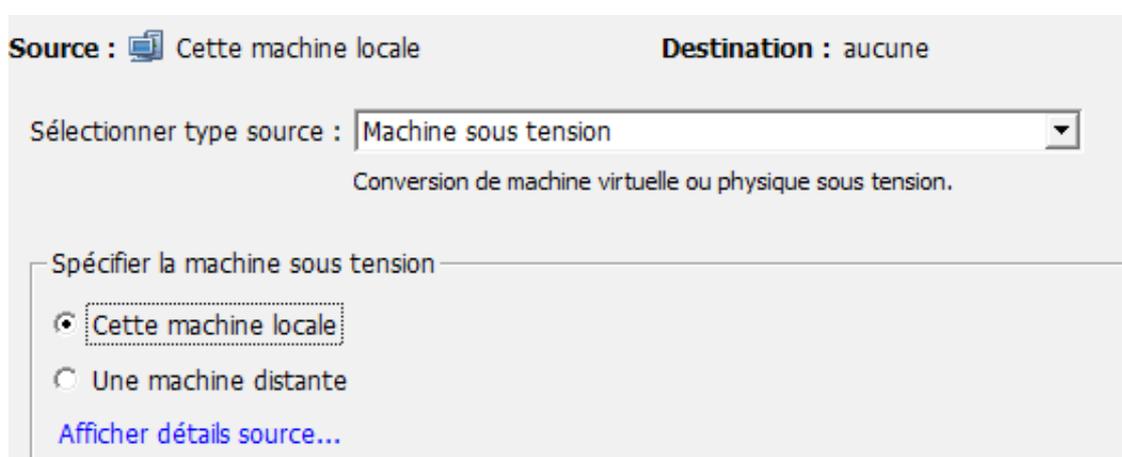
Pour obtenir le produit il faut se rendre sur le site de l'éditeur (vmware) ou bien nous avons VMware Workstation. En effet, il nous propose de télécharger le Vconverter très facilement.

Après l'installation du programme, nous lançons le programme en administrateur.

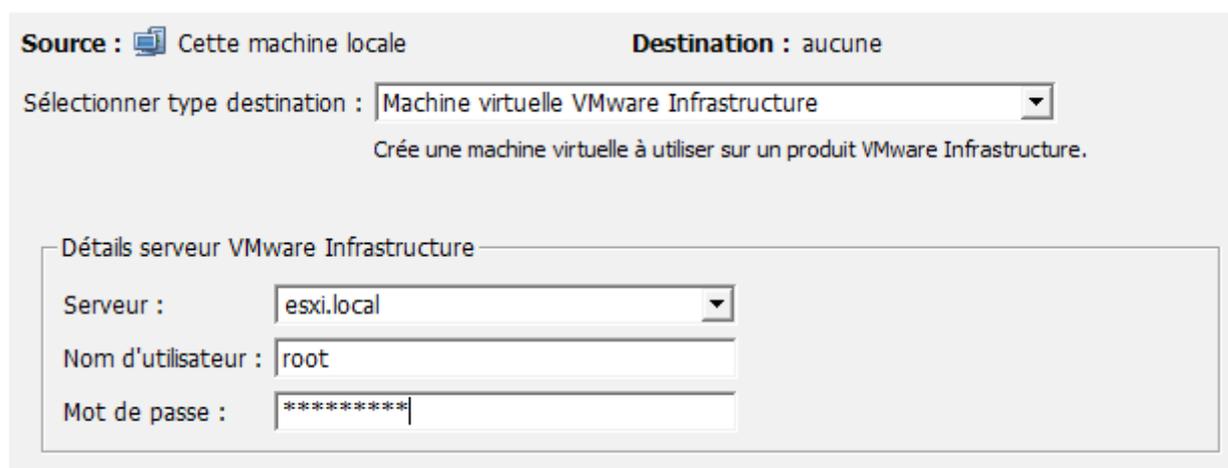
Nous choisissons naturellement « convertir une machine » :



La source sera la machine locale :



La destination sera notre hyperviseur sur notre réseau local :



Nous serons amenés ensuite à donner un nom à la machine virtuelle, choisir son datastore d'accueil ainsi que les options de conversion.

Un résumé de notre configuration s'affiche, puis la conversion démarre :

ID tâche	ID de travail	Source	Destination	État	Heure début	Heure fin
2	2	Cette machine...	esxi.local/...	1%	05/05/2014 1...	Temps restant estimé : 1 heures et 3 minutes

Le temps estimé est d'environ 1h03 minutes pour le disque C:

Lancement de la machine virtuelle dans ESXi:

La machine virtuelle se trouve maintenant sur notre hyperviseur, le logiciel client de l'hyperviseur est :
-Vmware Vsphere 5.1

Pour l'obtenir nous nous connectons à l'interface web de l'hyperviseur : <https://esxi.local.org/>
La connexion n'est pas certifiée, ensuite la page web apparaît :

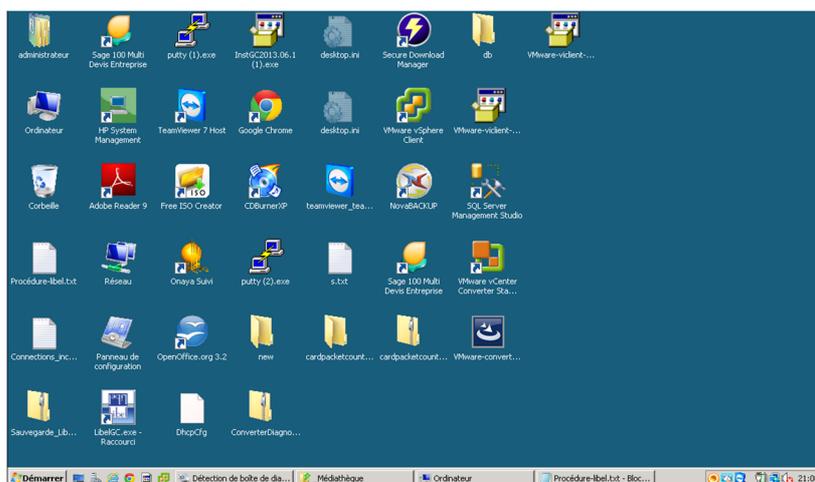


Il nous faut cliquer sur le lien suivant : Download Vsphere Client.

Après l'installation du logiciel sur un poste windows 7, nous nous connectons à l'hyperviseur.
Voici la machine virtuelle présente dans l'hyperviseur :



La machine est bien présente dans notre hyperviseur, vérifions son fonctionnement :



Le premier contact avec l'hyperviseur Vmware et les outils Vconverter a été un succès.
Nous avons désormais choisi notre hyperviseur et migré une machine physique vers notre hyperviseur.