

PPE 1

Gestion de l'équipement informatique des visiteurs du laboratoire GSB

SOMMAIRE:

1. *Description*
2. *Propositions commerciales*
3. *Dispositions et solutions logicielles à installer*
4. *Éléments de configuration et de paramétrage à appliquer*
5. *Préconisations sur l'environnement de "masterisation"*
6. *Procédure à la préparation d'un poste antérieur à la délivrance au visiteur*
7. *Procédure à appliquer lors de la récupération d'un équipement*
8. *Charte*

1) Description:

Descriptif du laboratoire GSB:

L'industrie pharmaceutique est un secteur très lucratif au sein duquel le mouvement de fusion acquisition est très fort.

Le laboratoire Galaxy Swiss Bourdin (GSB) est le résultat d'une fusion entre le géant américain Galaxy (spécialisé dans le secteur des maladies virales dont le SIDA et les hépatites) et le conglomérat européen Swiss Bourdin (travaillant sur des médicaments plus conventionnels), lui même déjà union de trois autres laboratoires à taille plus réduite.

Descriptif du système informatique:

On trouve sur le site parisien toutes les fonctions administratives avec en plus un service labo-recherche, un service juridique et un service communication.

Le 6ème étage du bâtiment est entièrement occupé par la salle serveur et les accès y sont restreints.

Le domaine est très sécurisé, l'étage est accessible par ascenseur à l'aide d'une clé sécurisée, des portes d'accès par escalier sont munies d'un lecteur de badge et un sas d'entrée est contrôlé par un gardien présent 24h/24.

Les fonctions de base du réseau et les fonctions de communication sont assurées par les serveurs. Le réseau constitué autour de VLAN, permet la segmentation des services afin de fluidifier le trafic.

Les données de l'entreprise ne doivent en aucun cas fuiter car étant considérées comme stratégiques. Toutes les informations sont répliquées chaque jour aux Etats-Unis par le biais d'un lien dédié. Toutes les fonctions de redondances sont mises en oeuvre afin d'assurer un seuil de permission aux pannes maximales.

Du point de vue la gestion informatique, l'outil informatique et l'utilisation d'outils décisionnels pour améliorer la vision et la planification de l'activité ont toujours fait partie de la politique maison pour Swiss-Bourdin, et ce particulièrement en ce qui concerne la partie recherche, production, communication et juridique.

Pour ce qui est de l'équipement, l'informatique est fortement répandue sur le site. Tous les employés sont équipés chacun d'un poste fixe relié au système central. On compte plus de 350 équipements terminaux avec un nombre de serveurs physiques conséquent sur lesquels tournent

plus de 100 serveurs virtuels.

Dans la partie labo-recherche se trouve des stations de travail plus puissantes avec une multitude d'ordinateurs portables servant aux personnels de direction, service informatique, services commerciaux, etc.

Tous les employés possèdent une adresse de messagerie de la forme "*nomUtilisateur@swiss-galaxy.com*". Les anciennes adresses de chaque laboratoire ont été définitivement fermées à la date du premier Janvier 2011.



2) Propositions commerciales:

L'objectif est d'équiper 480 potentiels visiteurs à un tarif concurrentiel et le plus faible au regard du besoin. Les capacités de l'équipement ne seront pris en compte que dans le cadre des besoins professionnels.

L'ordinateur doit être facilement transportable, peu encombrant, avec une manipulation bureautique confortable et une connexion sans-fil. Comme les visiteurs sont mobiles, il faut mettre à disposition des ordinateurs portables et /ou tablettes.

Après avoir effectué des recherches et avoir comparé les prix des différents ordinateurs portables en vente sur le marché, un Asus X555la Xx3003t, un Asus Pc Portable L200ha Fd0072t ou bien un HP 15-af100nf sont les choix les plus intéressants.

L'usage personnel de l'équipement peut être envisagé, mais cela ne doit pas être fait depuis le profil professionnel. Aucune garantie ou dépannage relatifs aux outils personnels installés sur le matériel ne seront proposés.

Ordinateur /			
Caractéristiques	Asus X555la Xx3003t	Asus Portable L200ha Fd0072t	HP 15-af100nf
Prix (en euros)	399	499	282
Processeur	Intel Core i3-500 U Broadwell	Intel Quad-Core Atom	AMD E1-6015 1.4 GHz
Carte graphique	Intel HD 5500	Intel HD Graphics Gen8	AMD Radeon R2
Mémoire vive	4Go DDR3	2Go DDR3	4 Go DDR3L SDRAM
Espace de stockage	500 Go SATA II	32 Go EMMC	500 Go HDD
Dimension	38,2 x 25,6 x 2,58	28,6 x 19,3 x 1,75	38,4 x 25,5 x 2,43
Poids	2,3 Kg	0,98 Kg	2,19 Kg
Système d'exploitation	Windows 7 - 64 Bits	Windows 7 - 64 Bits	Windows 7 - 64 Bits

3) Solutions logicielles à installer:

Les visiteurs médicaux étant habitués aux systèmes d'exploitation Windows, nous installerons par conséquent Windows Seven et Windows 10 (plus récent). Avec une version 64 bits pour une plus grande partie de la mémoire allouée à l'exécution des tâches. Nous opterons sans doute pour le HP 15-af100nf qui semble être le plus rentable en terme de prix et performances.

Ils ont également des connaissances en informatique, nous utiliserons donc des logiciels simples et adéquat à utiliser comme par exemple la gamme OFFICE et l'anti-virus BitDefender ou bien Kasperski.

Pour choisir quel antivirus prendre entre les deux :

	BitDefender	Kaspersky
Points communs	Ils peuvent être téléchargé via Internet. ces deux antivirus accomplissent des scanners par-installation pour vérifier les éventuelles menaces possibles qui peuvent être présente dans les ordinateurs avant l'installation. Ils n'exigent pas à l'utilisateur de redémarrer son ordinateur après les mises-à-jours.	
Différences	<ul style="list-style-type: none">- Caractéristiques de networking sociales qui aident les utilisateurs à protéger les ordinateurs fixes et portables contre beaucoup d'adresses de web indésirables.- Possède un navigateur de paiement sécurisé utile pour les transactions.	<ul style="list-style-type: none">- Possède un Scanner de Vulnérabilité qui permet aux utilisateurs de scanner pour les vulnérabilités et les menaces qui peuvent être présentes dans les systèmes.- Est conçu dans une voie pour qu'il puisse contrôler et pénétrer différents programmes pour corriger des éditions de systèmes.

4) Eléments de configuration et de paramétrage à appliquer:

Afin de distinguer chacune des machines de notre entreprise en cas de problème passager ou sollicitation, il faut en premier lieu donner un nom à son ordinateur.

Le plus important est de donner un nom qui soit en rapport avec le contexte d'utilisation. Ensuite le nom de la machine ne doit pas être propre à la tâche qui lui est accordée, en effet l'ensemble des machines doivent être sous un nom générique qui englobe les différents domaines d'utilisation.

Il faut ensuite éviter de l'appeler par son propre nom ou par un nom trop long pour des raisons de confidentialité et de sécurité. Il faut également éviter les noms semblables à des noms de domaines ou bien difficile à prononcer pour des raisons de simplicité.

Certains logiciels ne reconnaissent pas tous les types de caractères, c'est pour cela que nous devons de préférence éviter aussi d'utiliser des termes alphanumériques ou bien des numéros en début de nom.

Une fois cela fait, nous devons aussi mettre en place des mots de passe sur les différents espace de stockages ainsi que sur l'accessibilité au réseau local afin de sécuriser l'accès aux données de l'entreprise.

Il faut faire en sorte ensuite que l'accès au réseau local se fasse automatiquement à chaque connexion afin de gagner un maximum de temps. Les espaces de stockages devront tous être ordonnés afin d'accélérer et de faciliter la recherche de ces dernier au sein de l'entreprise.

- Symantec Ghost Solution Suite
- Microsoft Deployment Toolkit 2010 (MDT)
- System Center Configuration Manager (ConfigMgr)

	MDT	ConfigMgr	Symantec Ghost Solution Suite
Avantage(s)	<ul style="list-style-type: none"> - A les mêmes fonctionnalités que ConfigMgr - Nécessite Windows AIK (pour W7) mais est téléchargeable gratuitement. - Propose des modèles intégrés pour l'actualisation, le remplacement, la mise à niveau et des installations complètes. - Compartimenter l'ensemble du déploiement. Facilite la gestion images, l'ajout ou suppression des pilotes et remplacement très simple du système d'exploitation souhaité. - Supports multimédias permettant de mettre une solution de déploiement complète sur un DVD (ou un ensemble de DVD selon la taille), sur un lecteur Flash USB (UFD) ou sur un disque dur externe - Créer un déploiement lié, partager et copier la solution de déploiement complète (ou simplement des parties) vers un bureau local afin que ces clients puissent réaliser localement leurs déploiements. 	<ul style="list-style-type: none"> - Possibilité de cibler des ordinateurs spécifiques (selon des critères voulus) - Gestion des correctifs - Fonctionnalités de création de rapports détaillés qui permettent de suivre chaque étape d'un OSD. - S'adapte à la taille de l'entreprise, peu importe le nombre de bureau ou l'emplacement géographique. 	<ul style="list-style-type: none"> - Réduction des coûts associés à la migration et au déploiement des systèmes d'exploitation, ainsi qu'au dimensionnement des ordinateurs de bureau, des portables et des serveurs dans l'ensemble de l'entreprise - Gain de temps et réduction du risque d'erreur humaine par rapport aux déploiements de PC classiques - Réduction des temps d'arrêt pour l'utilisateur final grâce à l'automatisation du processus de déploiement des systèmes d'exploitation - Efficacité accrue des ressources informatiques grâce à des tâches de déploiement automatisées et répétitives - Outils de migration de systèmes d'exploitation sans intervention permettant de réduire les coûts de passage à un nouveau système d'exploitation
Inconvénient(s)	<ul style="list-style-type: none"> - Il y a une limite dans le nombre d'utilisateur. 	<ul style="list-style-type: none"> - Difficile à installer et à configurer. - SQL Server est nécessaire. - Obligation de configurer plusieurs rôles de serveurs de site. 	<ul style="list-style-type: none"> - Parc homogène - Configuration réseau pouvant poser problème sur certaine topologie

5) Préconisations sur l'environnement de "masteurisation":

Avant de commencer la masteurisation, il faut tout d'abord que certaines conditions soient remplies pour optimiser l'environnement :

- Pour le déploiement du Masteur, il faut que l'entreprise possèdent des machines identiques pour éviter tout problèmes de drivers.
- Il faut des partitions pour le système d'exploitation car les problèmes proviennent la plupart du temps des logiciels. Mais on effectuera la masteurisation que pour la partition seulement.
- Il faut des licences de volumes (Pour Microsoft, les programmes de licences en volume, conçus pour les entreprises, s'avèrent une façon économique d'acquérir entre 5 à 1000 licences logicielles à la fois.)
- Faire un guide d'utilisation pour les utilisateurs ou former des équipes support à l'utilisation du logiciel de Masteur pour le respect des procédures.

Ensuite, plusieurs conditions seront également nécessaire afin de pouvoir faire la masteurisation :

- Sauvegarde sur une partition : Pour que le visiteur puisse lui-même effectuer une restauration.
- Sauvegarde sur un serveur : Pour faciliter la préparation et le reconditionnement des machines en cas de problèmes.
- Fonctions de clonage : afin de créer des postes identiques.
- Possibilité de crypter la sauvegarde : afin de sécuriser les données de l'entreprise.
- Restauration Pré-OS : pour pouvoir reconditionner les machines même si Windows 7 ne démarre pas.

Nous avons donc choisis trois solutions qui répondent à ces critères :

remarque : L'utilisation de Symantec Ghost Solution Suite semble est un choix plus judicieux pour la masterisation.

a) Préparation de la machine mère

Nous allons faire une machine-mère. C'est celle qui servira de modèle pour les 479 autres machines. Premièrement, nous allons supprimer la partition de restauration propriétaire.

Nous installerons 3 partitions :

- OS : il contiendra Windows Seven ainsi que les logiciels :

On installe Windows Seven sur une clé de volume sur une partition NTFS de 20 Go.

Puis on crée deux sessions : Une sessions administrateur nommée "professionnel" avec un mot de passe que le visiteur devra changer (ex : "Aremlacer"), ainsi qu'une session utilisateur nommée "personnelle". Le groupe de travail sera défini comme "GSB" et le mot de passe root (ex : "123456").

Il faudra ensuite installer :

- 1) l'antivirus, le firewall etc... avec la même clef de volume utilisé pour Windows Seven.
 - 2) La suite OFFICE (Excel, Word, Outlook et PowerPoint). On prendra cette fois-ci une autre clé de volume.
 - 3) Un logiciel de Masteur tout en activant le module de restauration Pré-OS
 - 4) Un logiciel de cryptage où on activera le module bitlocker de windows.
- DATA Professionnelles : On y stockera les données professionnelles.
 - DATA Personnelles : Le visiteur pourra y stocker ses données dedans.

Deuxièmement on cryptera OS, DATA professionnelles avec une même clef. On fait ceci pour que l'entreprise ne puisse pas accéder aux données personnelles. Le visiteur n'aura plus qu'à utiliser une autre clef.

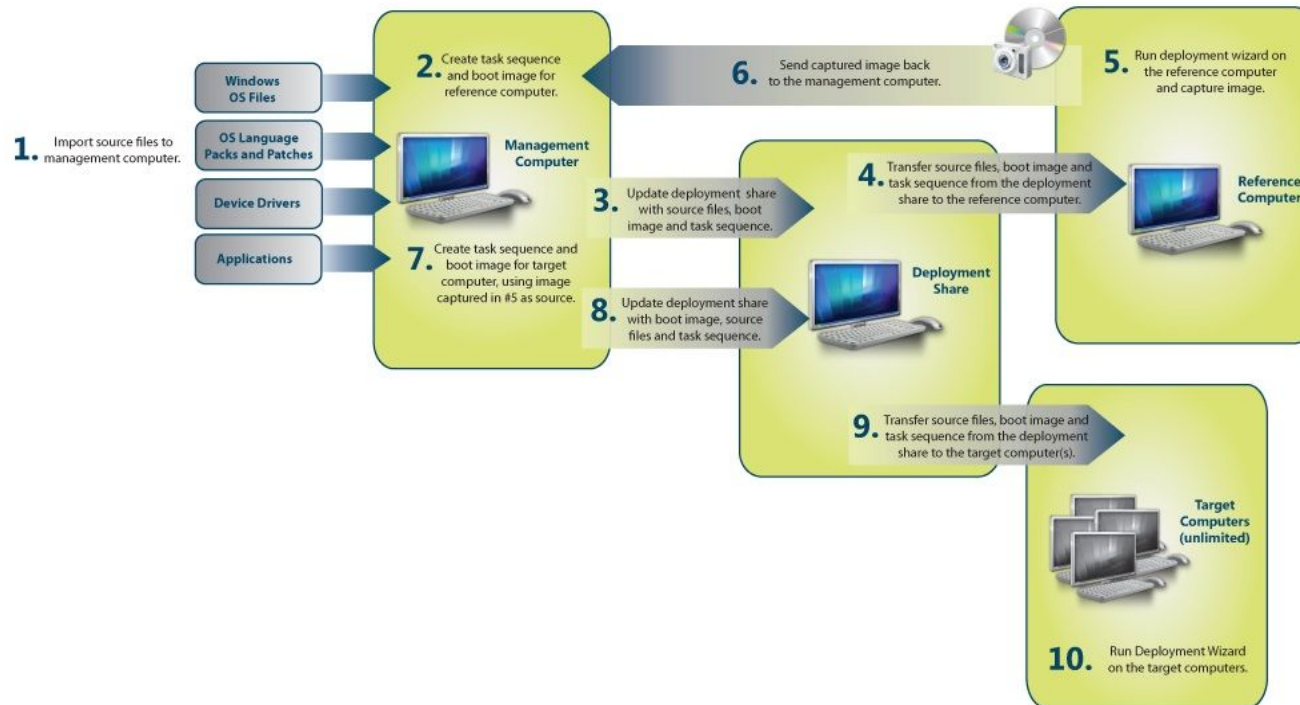
Troisièmement et enfin on désactive la suite de protection afin de pouvoir créer les Masteur. On crée alors un masteur du disque entier que l'on placera sur le serveur PXE.

Nous pouvons ainsi déployé les Masteurs sur l'ensemble des machines.

b) Installation du Masteur sur les autres machines

Il faut activer le bios la ROM de boot sur le réseau. On paramètre le serveur pour chacune des machines. On démarre ensuite les machines sur le serveur PXE de déploiement en sélectionnant l'image GLOBAL xx-mm-yy. Et après la procédure finie, il faut contrôler la présence du cryptage, des différentes partitions et logiciels

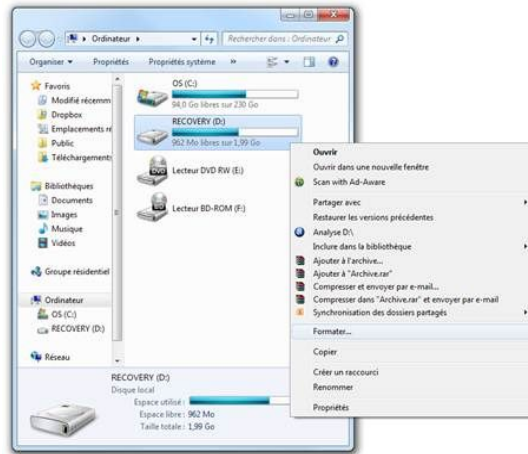
Et seulement après ça, on réactive la suite de protection.



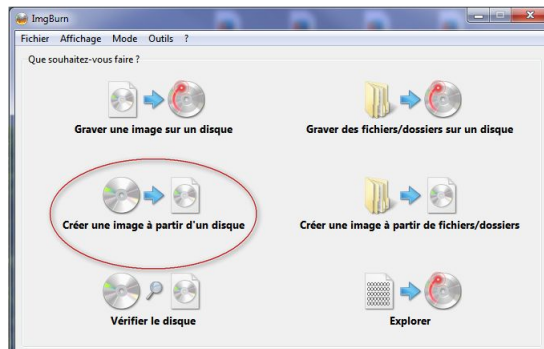
6) Procédure à la préparation d'un poste antérieur à la délivrance au visiteur:

Deux étapes sont nécessaires au reconditionnement d'un poste visiteur.

Il faut tout d'abord formater le disque dur du poste visiteur.



Puis lancer l'image disque, soit à partir du serveur, soit par le CD contenant l'image disque.



7) Procédure à appliquer lors de la récupération d'un équipement:

Toutes les données professionnelles seront sauvegardées sur le serveur à chaque nouvelle connexion au serveur de l'entreprise. Les données personnelles seront gérées par l'utilisateur et non par l'entreprise.

En cas de panne l'utilisateur rendra l'ordinateur à l'entreprise avec une fiche expliquant les problèmes rencontrés. En fonction de cela une réparation ou un reconditionnement de la machine sera effectué selon le problème. En cas de reconditionnement seuls les données et les logiciels relatifs à l'entreprise seront réinstallés sur la machine.

8) Charte:

1) PRÉAMBULE

Ce texte disposant d'un aspect réglementaire est avant tout un code de bonne conduite à l'attention de l'ensemble des salariés et collaborateurs de l'entreprise. Il a pour objectif d'informer chaque utilisateur du réseau aux risques encourus suite à un usage abusif des ressources informatiques de l'entreprise.

La charte fait partie intégrante du règlement intérieur et présente les conditions d'utilisation et d'accès du parc informatique.

Cette charte est destinée à un usage informatif et ne remplace en aucun cas les lois en vigueur.

2) DÉFINITION DES TERMES

Les ressources informatiques de l'entreprise sont constituées de l'ensemble des outils informatiques : logiciels, serveurs... ainsi que des services destinés à un professionnel : messagerie, connexion internet...

Tout salarié et collaborateur est autorisé à utiliser les ressources informatiques de la société.

3) CONDITIONS GÉNÉRALES D'UTILISATION

L'utilisation des moyens informatiques n'est pas strictement réservée aux seuls besoins de l'activité de l'entreprise mais les données professionnelles et personnelles doivent être séparées. L'utilisateur est le seul responsable en cas de perte des ses données personnelles et ne pourra pas réclamer à l'entreprise la restitution de celles-ci.

L'utilisateur ne doit pas mettre en péril et de manière volontaire la sécurité et l'intégrité du parc informatique.

Il est d'ailleurs invité à respecter les règles de sécurité définies ci-dessous afin d'éviter toute mise en danger de la sécurité de manière involontaire.

Toutes les utilisations allant à l'encontre des lois et règlements en vigueur sont interdites, et notamment celle portant atteinte aux mœurs, à l'honneur, à la vie privée, ou à l'intégrité morale d'une personne.

4) REGLES DE SECURITE

Chaque collaborateur est responsable de l'usage qu'il fait des ressources informatiques de la société. Les recommandations fournies par la direction des systèmes d'information sont les suivantes :

- L'utilisateur doit choisir son mot de passe en mélangeant caractères alphanumériques et chiffres.
- Le mot de passe doit être minimum de 8 caractères
- Si possible, l'utilisateur est prié de changer régulièrement son mot de passe afin d'éviter d'éventuel vol de mot de passe
- Les mots de passe sont personnels et ne doivent pas être communiqués à un tiers
- L'utilisateur ne doit pas accéder à des ressources (Site Internet ou autres) qui n'ont aucun rapport avec son activité professionnelle au sein de l'entreprise
- Les collaborateurs sont invités à respecter l'ensemble des directives fournies par les administrateurs systèmes et les responsables informatiques
- Dans le cadre de son activité professionnel le, le collaborateur doit garder une attention particulière à l'utilisation de sa messagerie. Il doit signaler tout comportement suspect à la direction du système d'information qui prendra les décisions nécessaires.

5) SANCTIONS DISCIPLINAIRES

Les utilisateurs ne respectant pas les règles de sécurité peuvent être passibles de plusieurs avertissements avant d'être définitivement remerciés par l'entreprise. Dans le cas d'une mise en danger volontaire de la sécurité du système informatique, l'entreprise se donne le droit de poursuivre l'employé pour fautes graves afin d'obtenir le licenciement et des dommages et intérêts proportionnels à la faute commise. Il s'expose donc à des poursuites civiles et/ou pénales conformément aux textes en vigueur (articles 323-1 à 323-7 du code pénal)

6) INFORMATIQUE ET LIBERTÉS

Conformément à la loi du 22 juillet 1992 sur le respect de la vie privée, l'entreprise est tenue de respecter les informations concernant ses salariés. Ainsi, « toute création d'un fichier contenant des informations nominatives doit faire l'objet de formalités préalables à sa mise en œuvre auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL). Toute personne sur laquelle des informations figurent dans un tel fichier doit être informée de l'existence de ce fichier, de sa finalité, de l'existence d'un droit d'accès et des modalités de mise en œuvre

de celui-ci, dès la collecte des informations la concernant. »

Je soussigné(e) ,reconnait avoir pris connaissance du règlement ci-dessus et en accepte les conditions:

Signature, lu et approuvé :

Bon usage de l'équipement:

- L'utilisation des ressources informatiques et l'usage des services Internet ainsi que du réseau pour y accéder ne sont autorisés que dans le cadre exclusif de l'activité professionnelle des personnels
- La connexion d'un équipement au réseau de l'université ne peut être effectuée que par les personnels habilités.
- L'accès aux différentes ressources informatiques est soumis à une réglementation.
- Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement à un tiers.
- Ces autorisations peuvent être retirées à tout moment en cas de non respect de la réglementation.
- Toute autorisation prend fin lors de la cessation, même provisoire de l'activité professionnelle ou d'études qui l'a justifiée.

Les risques liés au vol et à la gestion de la sécurité:

- La perte des données informatiques ne constituent pas un dommage matériel, il faut les couvrir en option.
- Il est interdit de divulguer toutes informations relatives à l'utilisateur et à son poste de travail, tel que le mot de passe ou les données confidentielles.
- L'utilisateur doit s'assurer de la sécurité de toutes les données liés à son propre poste et à l'entreprise.

Rappel de l'usage personnel d'un outil professionnel:

- L'utilisation des postes doit se faire uniquement dans le cadre de l'activité professionnel.
- L'utilisateur se doit de respecter l'ensemble du matériel mis à sa disposition.
- L'utilisateur est responsable de son poste et des outils informatiques qu'il exploite.

Sources:

<http://lemeilleurantivirus.fr/bitdefender-vs-kaspersky-qui-est-mieux/>

[https://fr.wikipedia.org/wiki/NTFS_\(informatique\)](https://fr.wikipedia.org/wiki/NTFS_(informatique))

https://fr.wikipedia.org/wiki/Preboot_Execution_Environment

https://fr.wikipedia.org/wiki/Windows_7

https://fr.wikipedia.org/wiki/Kaspersky_Anti-Virus

<https://www.symantec.com/fr/fr/ghost-solution-suite/>

<https://technet.microsoft.com/fr-fr/windows/hh147630.aspx>

<https://technet.microsoft.com/fr-fr/windows/dn475741.aspx>

http://labo-microsoft.supinfo.com/articles/Windows7_Disk_Management