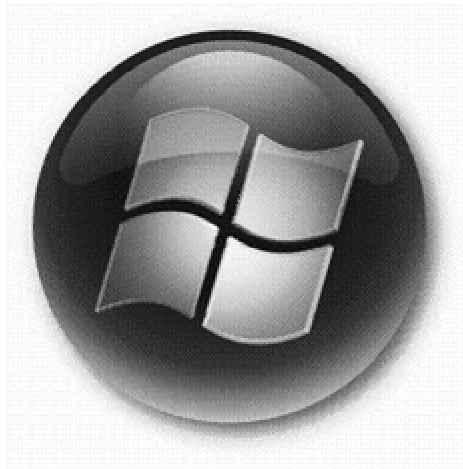


Gérer *Vista*



Étudiant : TAVARES José
Professeur responsable : LITZISTORF Gérald
En collaboration avec : CAU Lionel

Session: 2006

Plan de l'exposé

□ *Images Vista*
(7 semaines d'étude)

□ *PowerShell*
(2 semaines d'étude)

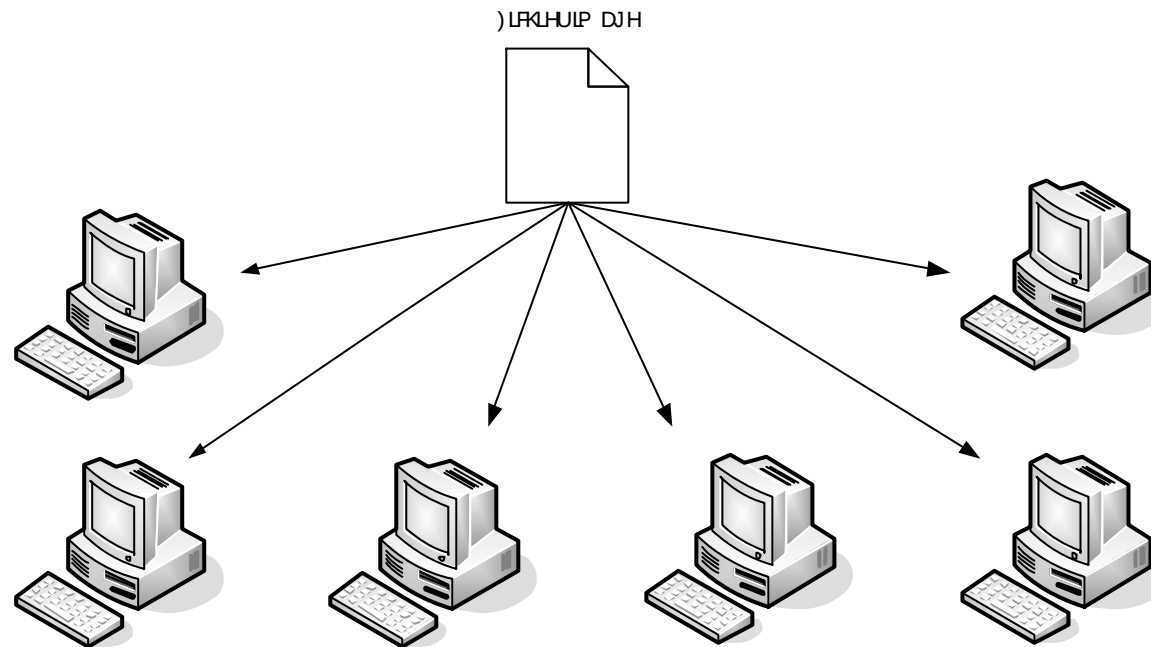
□ *Gestion des logs sous Vista*
(1 semaine d'étude)

Images *Vista* (7 semaines d'étude)

- Déploiement
- Qu'est ce qu'une image?
- Format d'image *WIM* dans *Windows Vista*
- *ImageX*
- *Windows PE 2.0*
- Fichiers de réponse (*Unattend.xml*)
- Phases de configuration
- *Windows System Image Manager*
- Serveur *WDS* (*Windows Deployment Services*)

Déploiement

Consiste à transmettre et installer une image sur plusieurs ordinateurs.



Qu'est ce qu'une image ?

Image au sens "image système" => Copie exacte (bit à bit) du disque/partition où le système d'exploitation a été installé



Utilités : Réinstallation rapide
Déploiement

Format d'image WIM

Windows Imaging Format (WIM)

- ☐ Indépendant du *Hardware*
- ☐ Basé sur les fichiers (plus sur les secteurs disque)
- ☐ Installation non destructive
- ☐ Compression (*XPress* ou *LZX*)
- ☐ Plusieurs images dans 1 seul fichier *WIM*
- ☐ Une seule instance par fichier
- ☐ Gérer une image en mode *Offline*
- ☐ API WIMGAPI

Compression *XPress* / *LZX*

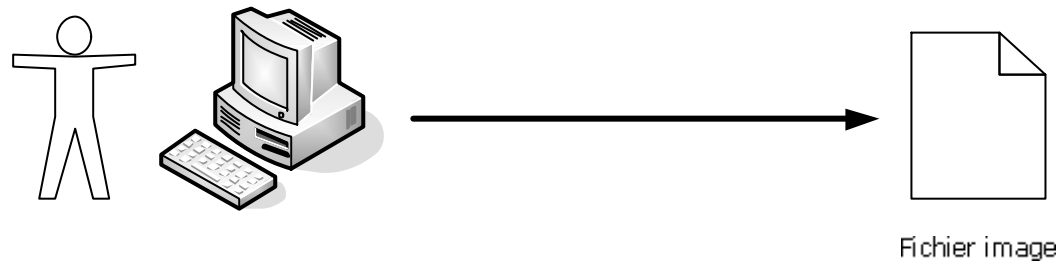
Tests : Taille obtenue / Temps de compression

Compression	Taille de base (partition)	Taille de l'image <i>WIM</i>	Temps nécessaire pour créer l'image <i>WIM</i>
none (<i>XPress</i>)	10.6 GB	5.55 GB	18 minutes
fast (<i>XPress</i>)	10.6 GB	3.34 GB	21 minutes
maximum (<i>LZX</i>)	10.6 GB	3.18 GB	50 minutes

La compression **none** ne veut pas dire qu'il n'y a pas de compression!

Scénario 1

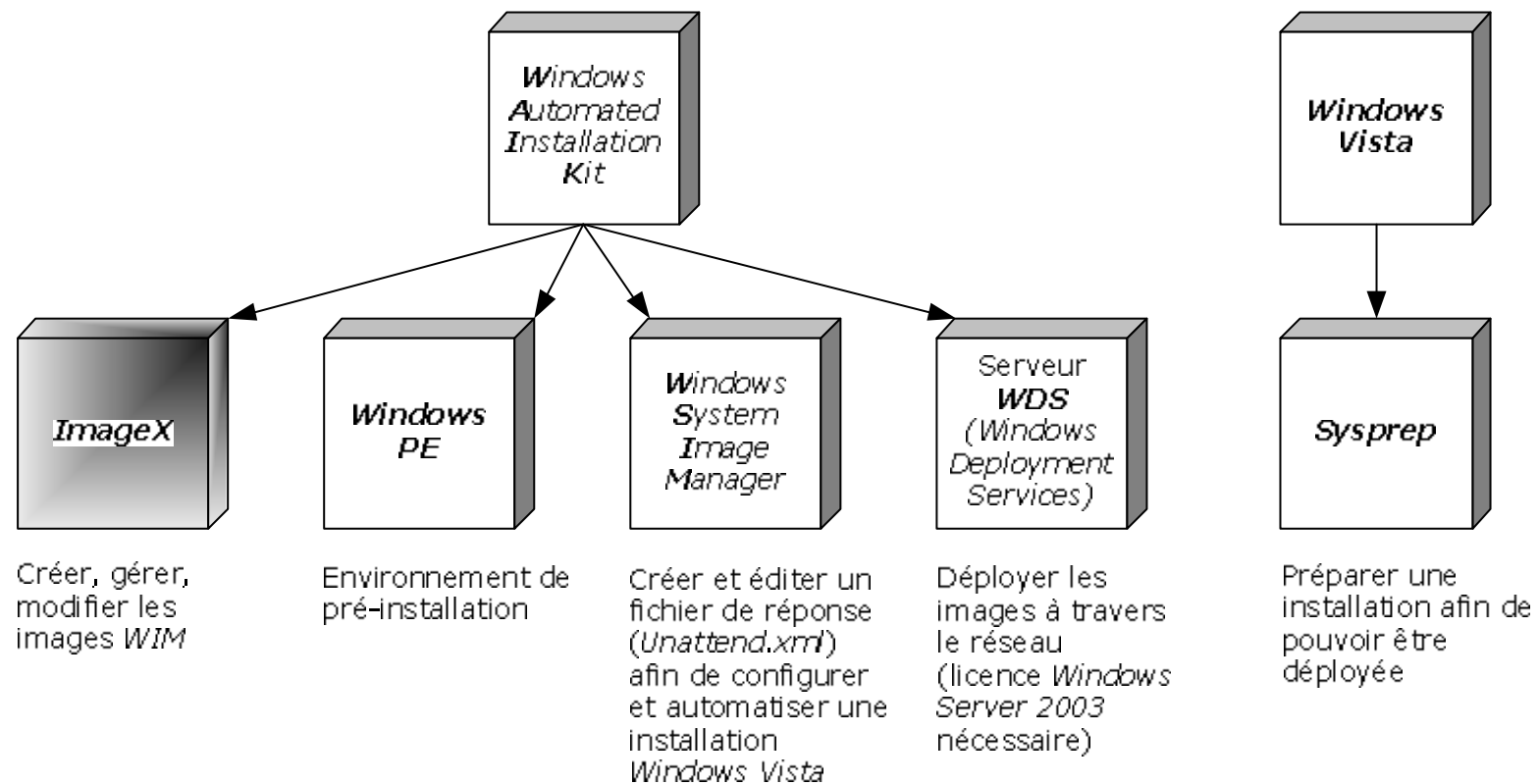
Un utilisateur à domicile souhaite effectuer une image de son pc



Questions ?

- Comment ?
- Avec quels outils ?

Outils disponibles



Outil *ImageX*

Outil en lignes de commandes (*CLI*), à exécuter sous *Windows PE*

Permet de :

- ☐ Capturer une image au format *WIM*

ImageX /capture

- ☐ Gérer les images

ImageX /append

/mount* ou */mountrw

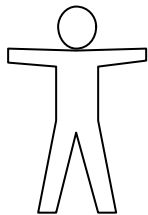
/commit

/split

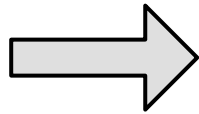
- ☐ Installer une image

ImageX /apply

Scénario 1 (suite)



Utilisateur

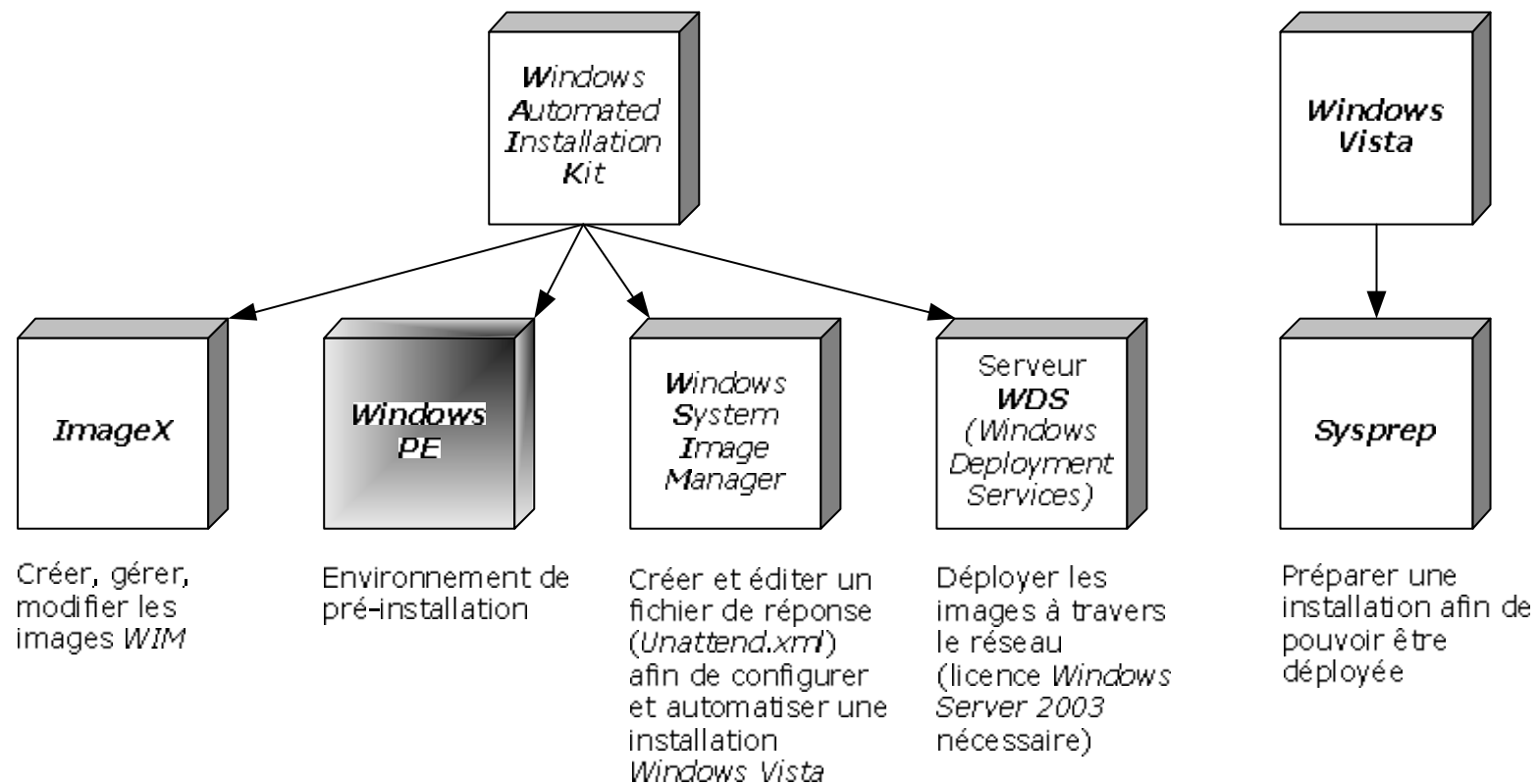


Ok, je sais comment créer une image
avec *ImageX*

Questions ?

- Depuis où j'effectue les commandes *ImageX* ?
- Lorsque mon *Vista* est en fonctionnement ?

Outils disponibles



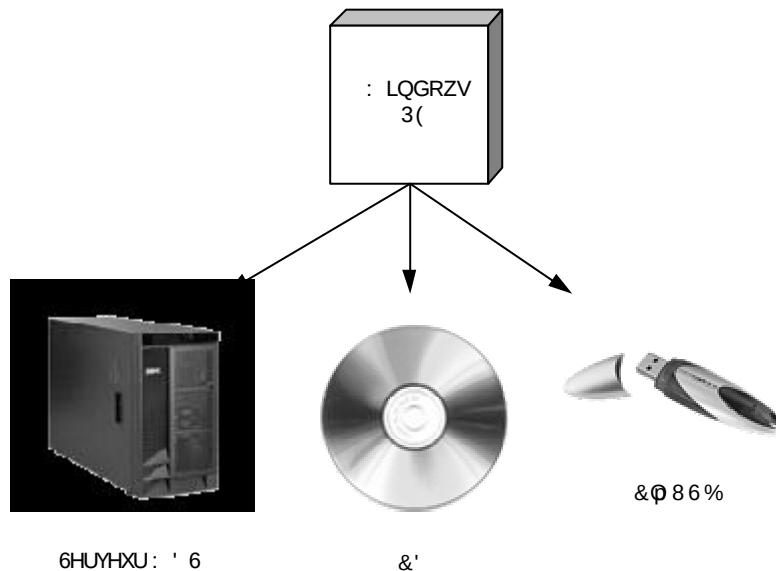
Windows PE 2.0

Windows Pre-Installation Environment

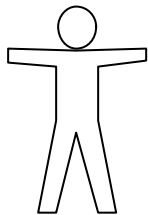
Exécution entièrement en mémoire RAM

Minimum de 256MB RAM nécessaire

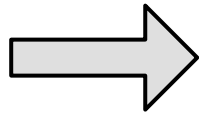
Taille de 154 MB



Scénario 1 (suite)



Utilisateur



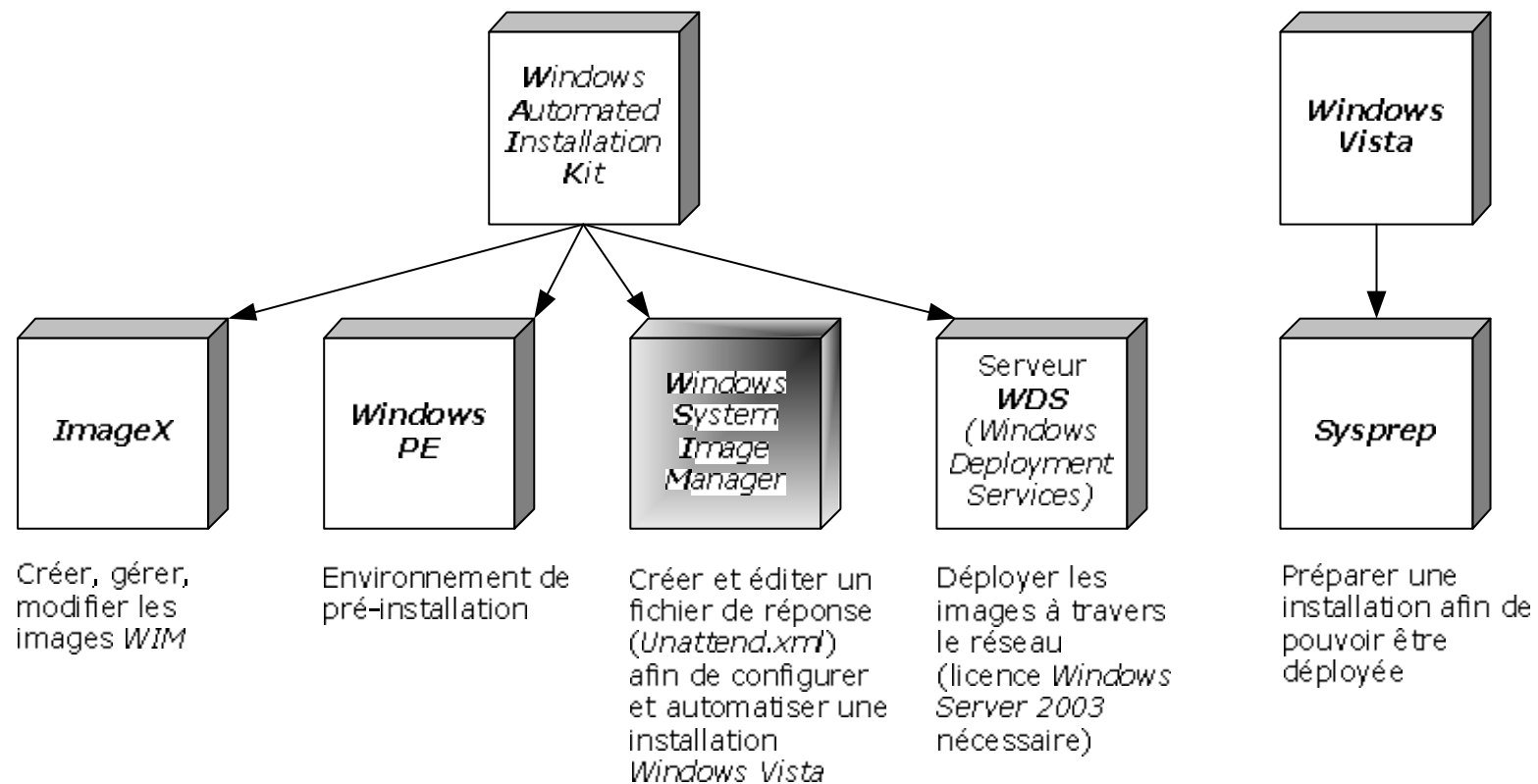
Ok, j'ai créé un CD de *boot Windows PE*

J'ai capturé mon installation avec *ImageX*

Questions ?

- Puis-je rajouter des fichiers ultérieurement à mon image ?
- Et lors d'un nouveau *service pack*, comment faire pour l'installer ?

Outils disponibles



Windows System Image Manager

Interface graphique (GUI)

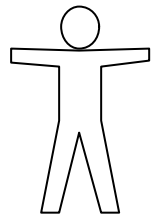
- ☐ Permet de créer entièrement un fichier *Unattend.xml*
 - Automatiser une installation
 - Personnaliser une installation
- ☐ Permet d'accéder à un dossier partagé
 - Ajouter des *service pack*, mises à jour (*hotfix*), langues
 - Ajouter des *drivers*

Windows System Image Manager

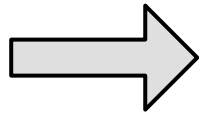
demo

Ajouter un service pack à une image

Scénario 1 (suite)



Utilisateur

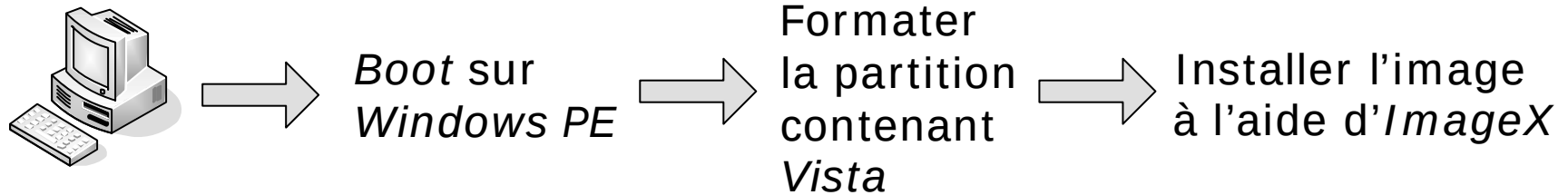


Mon *Vista* ne fonctionne plus correctement
Je souhaite réinstaller *Vista* à partir de
mon image

Questions ?

- Comment faire ?

Installation d'une image



Scénario 2

Une entreprise souhaite automatiser l'installation de *Windows Vista*, afin d'effectuer des déploiements sur leur réseau.

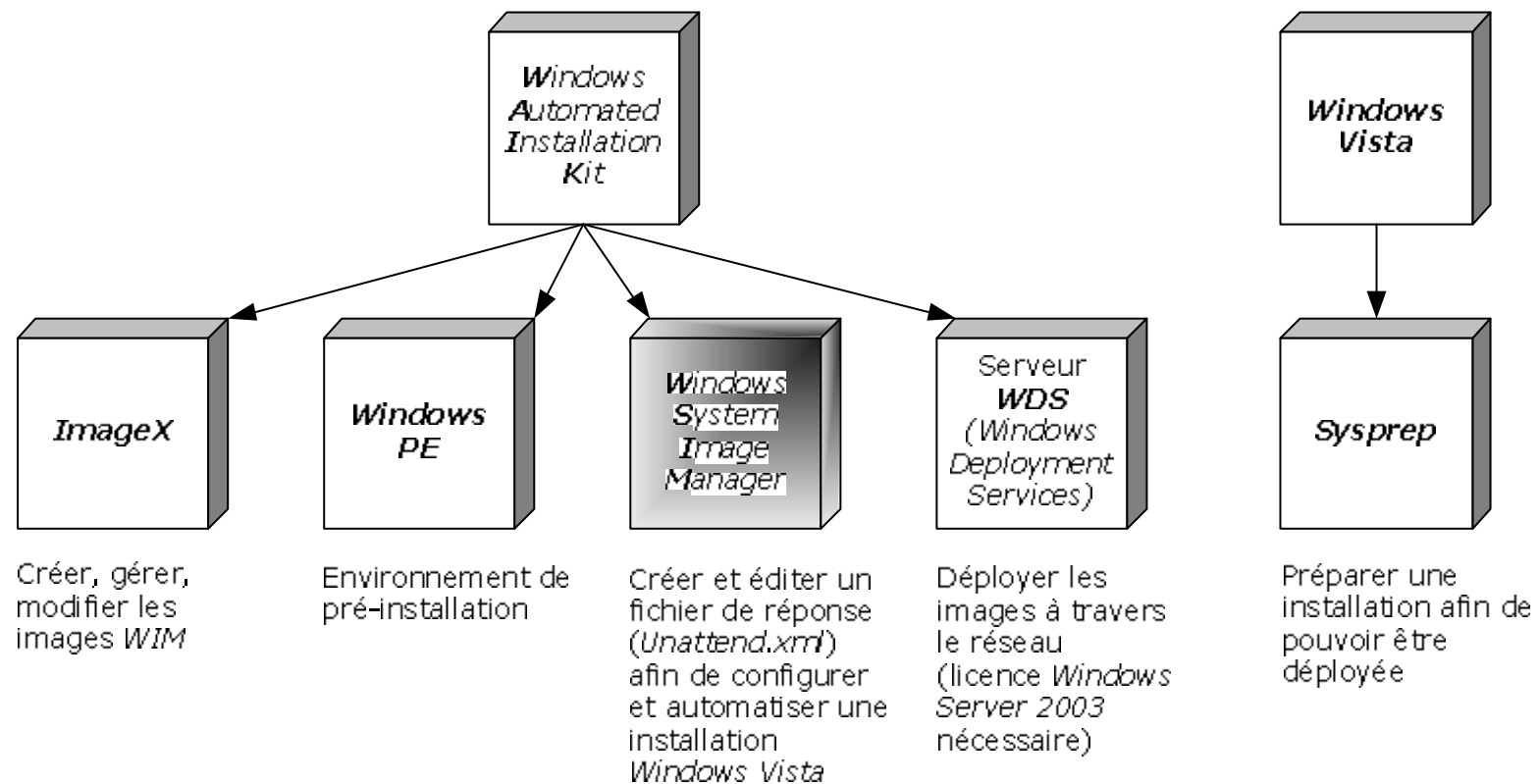
Cette entreprise désire

- Créer et formater des partitions
- Spécifier la partition sur laquelle installer *Vista*
- Entrer automatiquement la clef de licence *Vista*
- Définir un mot de passe administrateur

Questions ?

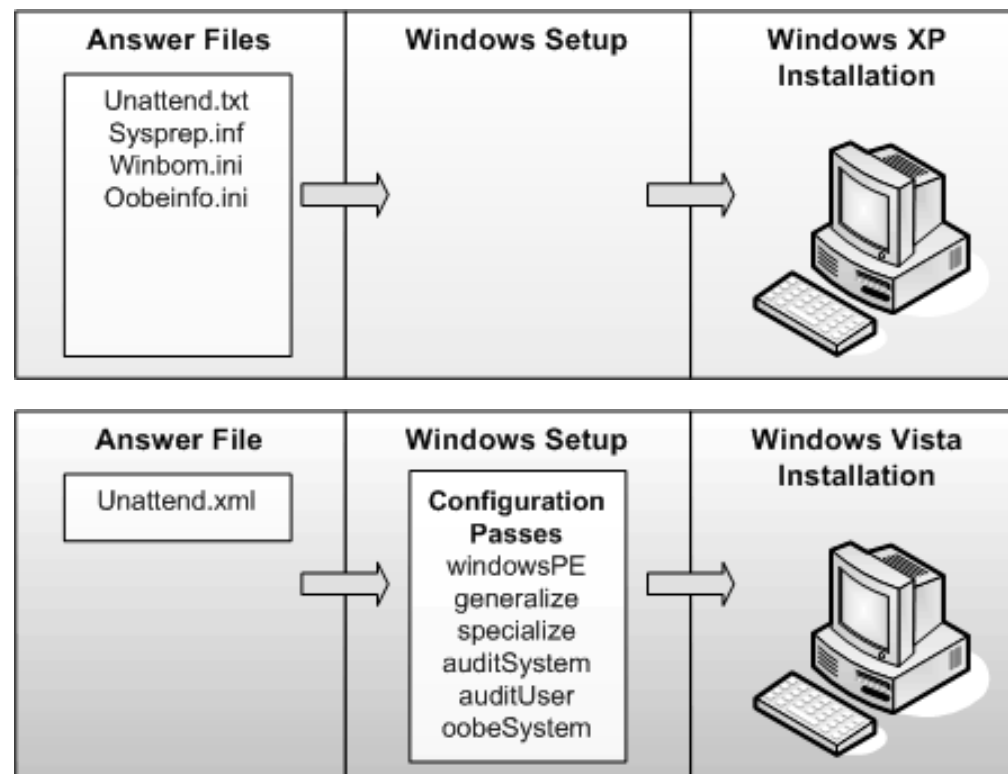
- Possible de faire ceci de manière automatisée ?
- Avec quels outils ?
- En termes de sécurité ? (mot de passe admin)

Outils disponibles

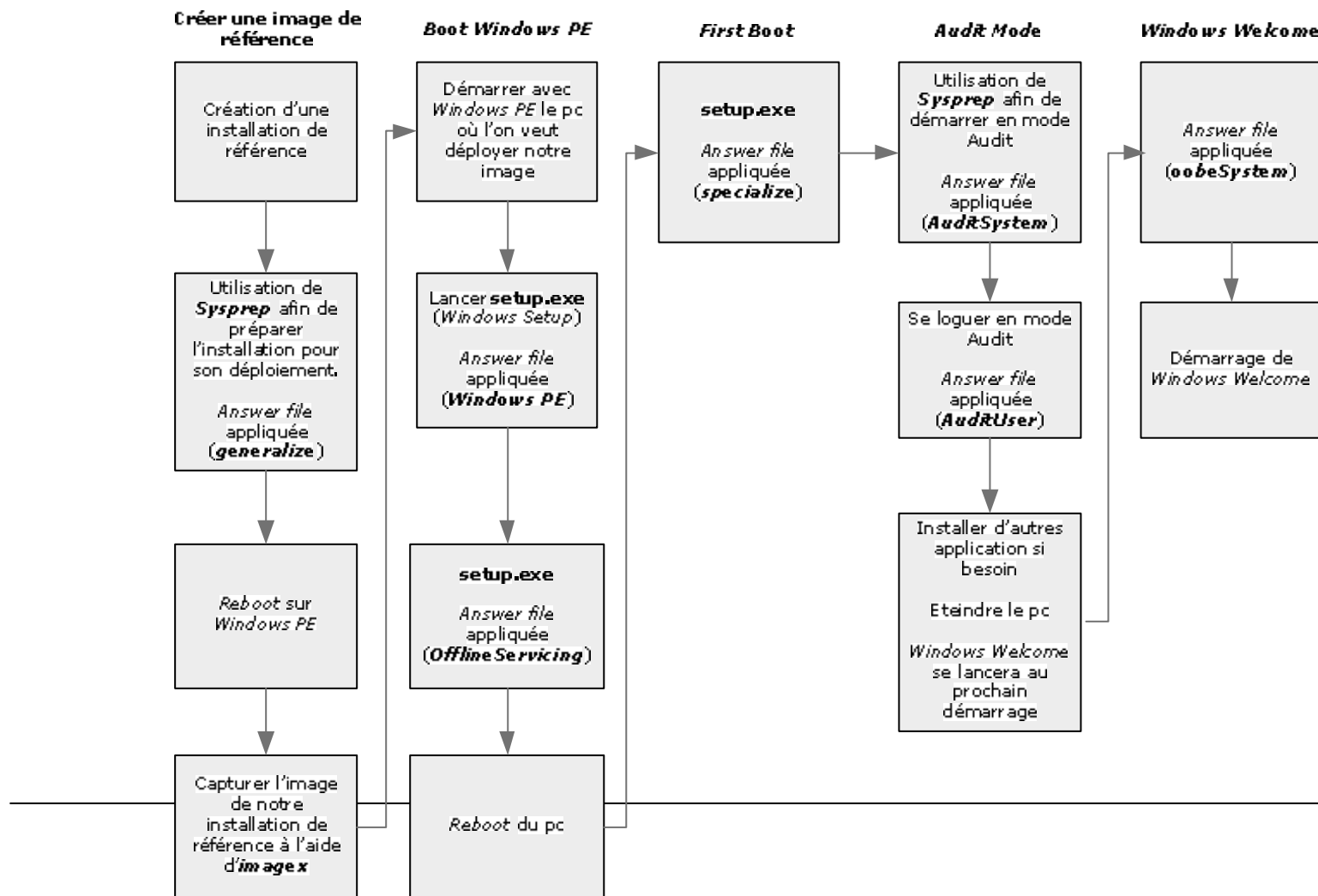


Fichier(s) de réponse (*Answer File*)

Automatiser et configurer une installation



Phases de configuration

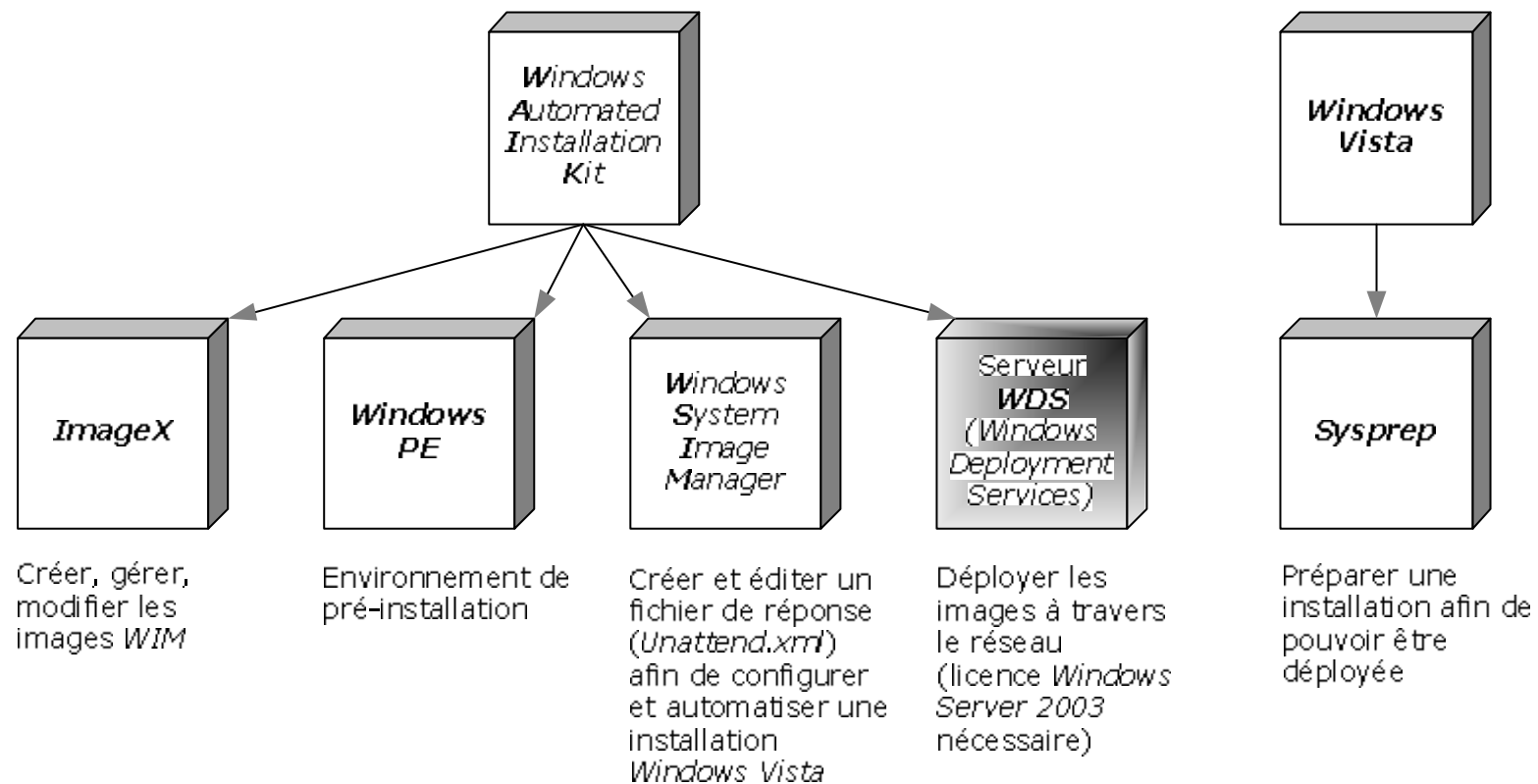


Windows System Image Manager

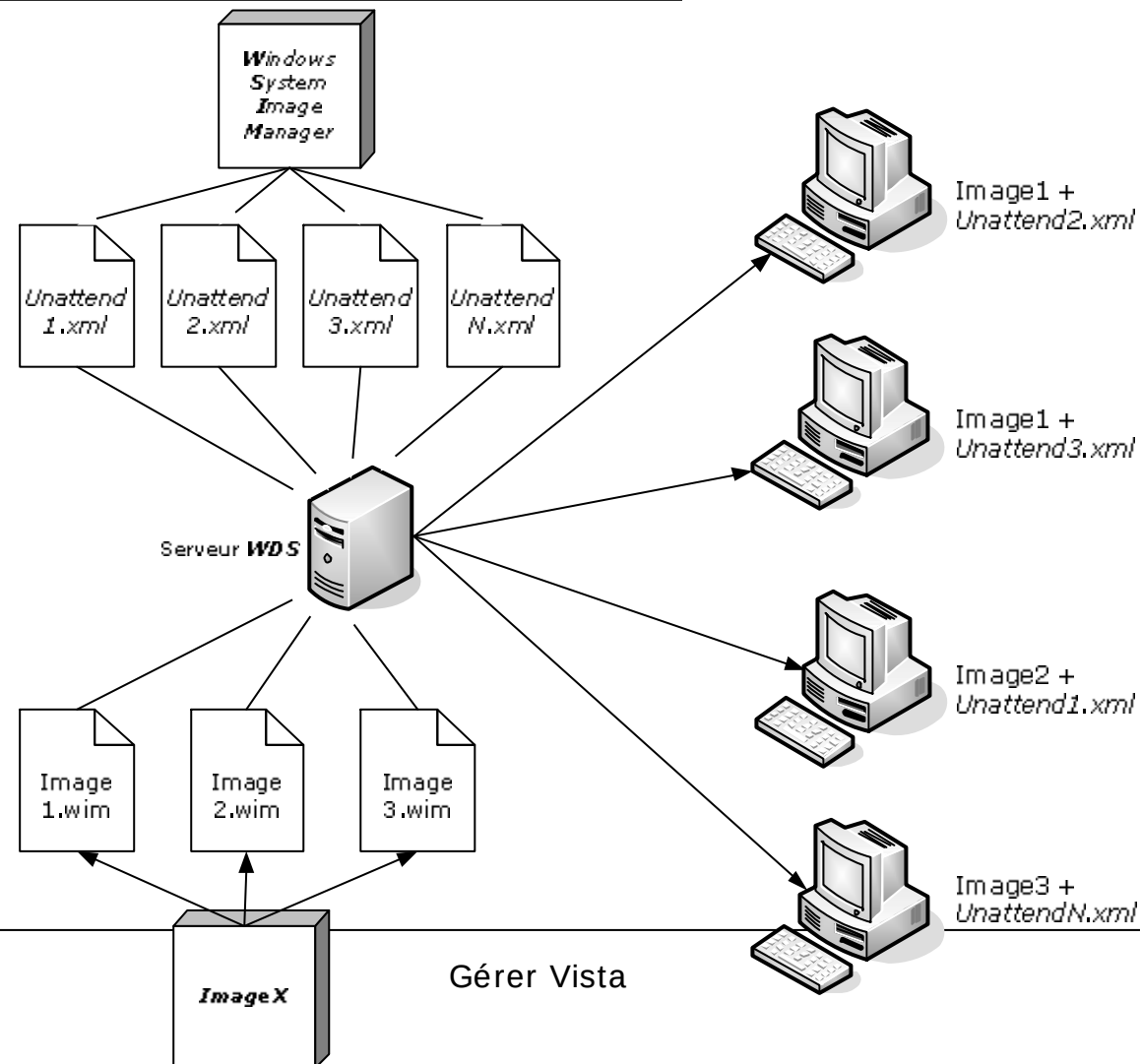
demo

Automatiser une installation

Outils disponibles



Serveur WDS (serveur d'images)



Pré-requis pour serveur WDS

- ☐ Licence *Windows Server 2003 SP1*
- ☐ Installation d'un serveur *RIS*
- ☐ Serveur DHCP
- ☐ Serveur DNS
- ☐ *Active Directory*
- ☐ Partitions NTFS

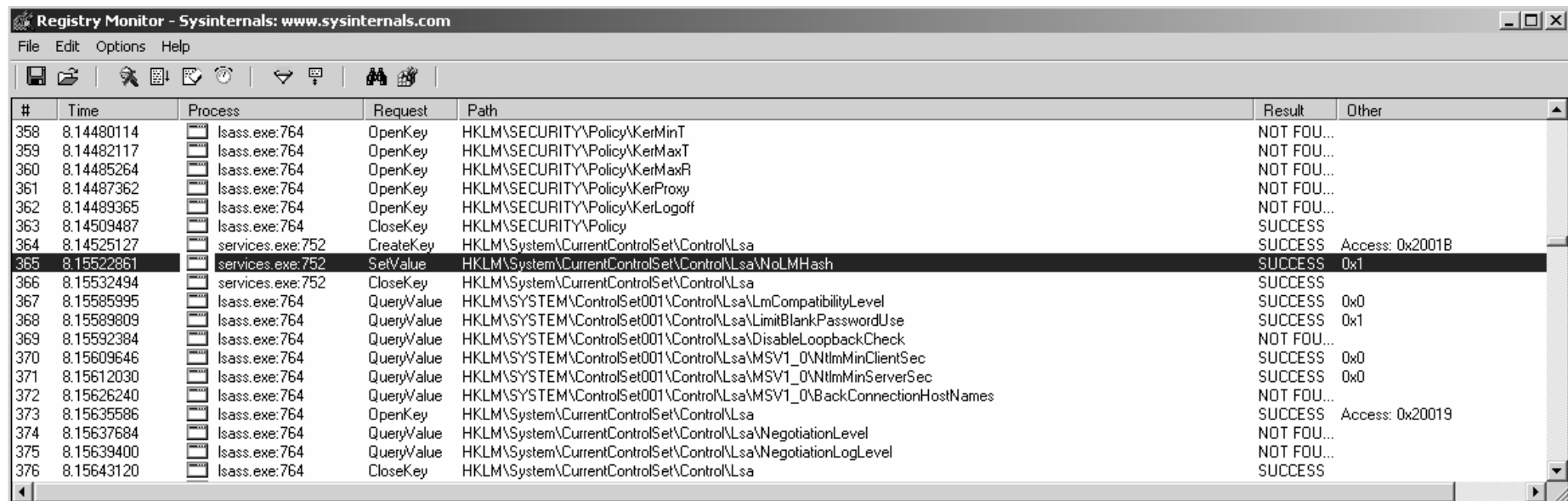
PowerShell (2 semaines d'étude)

- Qu'est ce que *PowerShell* ?
- Pourquoi avoir créé cet outil ?
- Que permet-il de faire ?
- Sécuriser un poste avec *PowerShell*
- Sécurité dans *PowerShell*

PowerShell

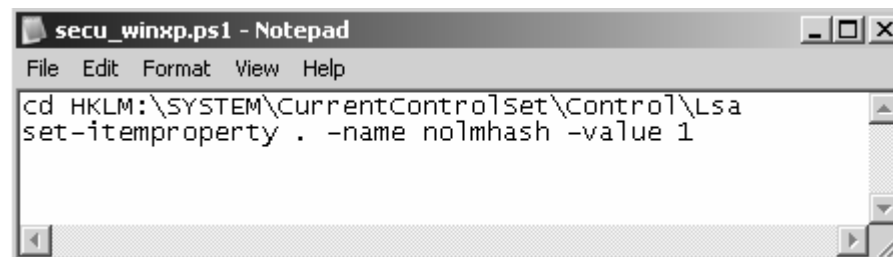
demo

Sécuriser un poste avec *PowerShell*



#	Time	Process	Request	Path	Result	Other
358	8.14480114	lsass.exe:764	OpenKey	HKLM\SECURITY\Policy\KerMinT	NOT FOU...	
359	8.14482117	lsass.exe:764	OpenKey	HKLM\SECURITY\Policy\KerMaxT	NOT FOU...	
360	8.14485264	lsass.exe:764	OpenKey	HKLM\SECURITY\Policy\KerMaxR	NOT FOU...	
361	8.14487362	lsass.exe:764	OpenKey	HKLM\SECURITY\Policy\KerProxy	NOT FOU...	
362	8.14489365	lsass.exe:764	OpenKey	HKLM\SECURITY\Policy\KerLogoff	NOT FOU...	
363	8.14509487	lsass.exe:764	CloseKey	HKLM\SECURITY\Policy	SUCCESS	
364	8.14525127	services.exe:752	CreateKey	HKLM\System\CurrentControlSet\Control\Lsa	SUCCESS	Access: 0x20018
365	8.15522861	services.exe:752	SetValue	HKLM\System\CurrentControlSet\Control\Lsa\NoLMHash	SUCCESS	0x1
366	8.15532494	services.exe:752	CloseKey	HKLM\System\CurrentControlSet\Control\Lsa	SUCCESS	
367	8.15585995	lsass.exe:764	QueryValue	HKLM\SYSTEM\ControlSet001\Control\Lsa\LmCompatibilityLevel	SUCCESS	0x0
368	8.15589809	lsass.exe:764	QueryValue	HKLM\SYSTEM\ControlSet001\Control\Lsa\LimitBlankPasswordUse	SUCCESS	0x1
369	8.15592384	lsass.exe:764	QueryValue	HKLM\SYSTEM\ControlSet001\Control\Lsa\DisableLoopbackCheck	NOT FOU...	
370	8.15609646	lsass.exe:764	QueryValue	HKLM\SYSTEM\ControlSet001\Control\Lsa\MSV1_0\NtlmMinClientSec	SUCCESS	0x0
371	8.15612030	lsass.exe:764	QueryValue	HKLM\SYSTEM\ControlSet001\Control\Lsa\MSV1_0\NtlmMinServerSec	SUCCESS	0x0
372	8.15626240	lsass.exe:764	QueryValue	HKLM\SYSTEM\ControlSet001\Control\Lsa\MSV1_0\BackConnectionHostNames	NOT FOU...	
373	8.15635586	lsass.exe:764	OpenKey	HKLM\System\CurrentControlSet\Control\Lsa	SUCCESS	Access: 0x20019
374	8.15637684	lsass.exe:764	QueryValue	HKLM\System\CurrentControlSet\Control\Lsa\NegotiationLevel	NOT FOU...	
375	8.15639400	lsass.exe:764	QueryValue	HKLM\System\CurrentControlSet\Control\Lsa\NegotiationLogLevel	NOT FOU...	
376	8.15643120	lsass.exe:764	CloseKey	HKLM\System\CurrentControlSet\Control\Lsa	SUCCESS	

Script PowerShell =>



```
secu_winxp.ps1 - Notepad
File Edit Format View Help
cd HKLM:\SYSTEM\CurrentControlSet\Control\Lsa
set-itemproperty . -name nolmhash -value 1
```

Sécurité dans *PowerShell*

Protection au niveau *scripts*

4 niveaux :

- *Restricted*
- *AllSigned*
- *RemoteSigned*
- *Unrestricted*

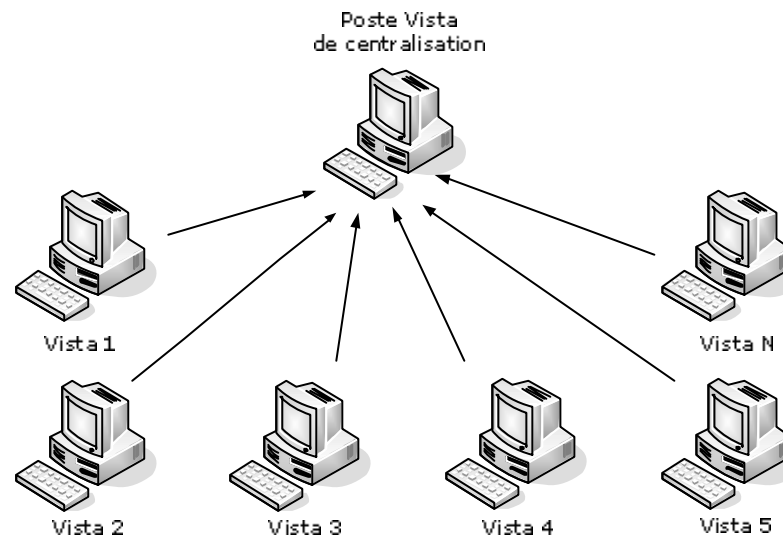
Pour signer un *script* => certificat nécessaire

De plus les extensions de *scripts PowerShell* ne sont pas associés au *shell* dans l'explorateur !

Gestion des *logs* sous *Vista*

(1 semaine d'étude)

- ❑ Nouvelle version d'*Event Viewer*
- ❑ Centralisation des *logs* de postes *Vista*



Event Viewer

Permet de :

- ☐ Consulter les logs (en local) du poste *Vista*
- ☐ Se connecter à un poste distant afin de consulter les *logs* qui y sont présents
- ☐ Filtrer les *logs*
- ☐ Associer une tâche à un événement spécifique (*Task Scheduler*)
- ☐ Centraliser les *logs* de postes *Vista*

Event Viewer

demo

Sécurité pour centraliser les *logs*

- ☐ Il faut être membre d'un domaine pour se connecter et centraliser les *logs*
- ☐ Possibilité d'envoi de *logs* avec le protocole HTTPS
- ☐ Effectuer un *backup* de l'ensemble des *logs*
- ☐ Statistiques
- ☐ *Troubleshooting*

Conclusion

- Images *Vista* et déploiement
- *PowerShell*
- Gestion des *logs* sous *Vista*

Questions

?