# Windows Vista : Complément de cours

1	Présenta	ation de ce document :	3
	1.1 Où t	rouver ce document :	3
	1.2 Obje	ectifs de ce document	3
2	Commer	nt tester Windows Vista :	4
3	Commer	nt déployer Windows Vista en entreprise :	5
	3.1 Len	ouveau format d'image WIM :	5
	3.2 Win	dows PE :	5
	3.2.1	Principe de fonctionnement :	5
	3.2.2	Pour générer une image ISO à partir d'un répertoire d'installation Windows P	E :
		6	_
	3.2.3	Capture avec ImageX :	6
	3.2.4	Gestion des disques avec Windows PE :	6
	3.3 Con	nment déployer en masse Windows Vista:	7
	3.4 Win	dows Assessment :	8
	3.5 ACI	5.0 : Application Compatibilité ToolKit 5.0 :	8
	3.5.1	Pourquoi certains programmes ne sont pas compatibles avec Windows Vista	.:8
	3.5.2	Principe de fonctionnement d'ACT :	9
	3.5.3		9
	3.5.4	Prise en main de l'interface :	10
	3.5.5	Creation du paquetage :	10
	3.5.6	Synchroniser avec la communaute ACT:	11
	3.5.7		12
	3.6 USI	// I :	12
	3.6.1	Principe general :	12
	3.0.2	Queiques exemples de commande :	12
	3.0.3	Deur plue d'informatione aur LISMT :	10
	3.0.4	Pour télécharger LISMT 2.0 :	12
	3.0.5		13
	371	Génération du fichier unattend vml :	13
	372	Pour plus d'informations sur le WAIK :	16
	373	Pour télécharger le WAIK :	16
	3.7.5 3.8 Win	dows Deployement Service :	16
	3.8.1	Principe de fonctionnement :	16
	382	Installation sans assistance avec WDS -	17
	39 Prés	sentation de Windows DEployment ToolKIt ·	17
	3.9.1	Principe de fonctionnement :	17
	3.9.2	Problème rencontré avec le Windows Deployment Toolkit :	19
	3.9.3	Pour plus d'informations sur Window Deployment Toolkit :	19
	3.9.4	Pour télécharger Microsoft Deployment Toolkit	19
4	Les autre	es nouveautés de Windows Vista :	20
	4.1 Lap	ossibilité de filtrer l'application de GPO local :	20
	4.2 Len	ouveau pare feu de Windows Vista :	20
	4.2.1	Principe de fonctionnement :	20
	4.2.2	Pour plus d'informations sur la pare feu de Windows Vista :	22
	4.3 I'UA	C :	22
	4.3.1	Le but :	22
	4.3.2	Le principe :	22
	4.4 EFS	s : nouveaux assistants :	23
	4.5 Pris	e en charge du MUI dans Windows Vista :	24
5	Se forme	er rapidement avec Windows Vista :	25

#### 1 PRESENTATION DE CE DOCUMENT :

#### 1.1 OU TROUVER CE DOCUMENT :

Ce document a été écrit par M. Guillaume MATHIEU. Une version HTML est disponible sur <u>http://msreport.free.fr</u>.

Une version au format PDF peut être téléchargée à l'adresse suivante : <u>http://msreport.free.fr/articles/WindowsVista</u>

#### 1.2 OBJECTIFS DE CE DOCUMENT

Ce document a pour but de vous présenter Windows Vista du point de vue de l'entreprise. Nous verrons donc dans ce document les avancées de Windows Vista pour le monde de l'entreprise.

Nous verrons dans ce document :

- Comment tester Windows Vista.
- Comment déployer Windows Vista en entreprise.
- Certaines nouveautés de Windows Vista.
- Comment se former rapidement sur Vista.

#### 2 COMMENT TESTER WINDOWS VISTA :

Vous pouvez installer Windows Vista de nombreuses machines physiques pourvu que celles-ci disposent d'au moins 512 Mo de mémoire vive et d'un processeur 800 Mhz et environ 15 Go de libre sur le disque.

Pour pouvoir activer la nouvelle interface AERO, vous devez disposer d'une carte graphique DIRECTX 9.0 qui supporte les PIXEL Shaders 2.0, les drivers WDDM, 32 bits par pixel et disposant d'au minimum 64 Mo de mémoire vidéo

Windows Vista peut être testé sur les plates formes de virtualisation suivante :

- Virtual PC 2007 (en tant que machine hôte et machine invité).
- Vmware 6.0 (en tant que machine hôte et machine invité).
- Vmware ESX 3.5.
- Virtual Server 2005 R2 SP1.

Si vous souhaitez pouvoir monter des maquettes intéressantes (1 serveur 2008 et 1 ou 2 machines Vista), prévoir la configuration suivante pour la machine Virtual PC / Vmware.

- Au moins 2 Go de mémoire vive (512 pour chacun des 3 systèmes) :
- 2 disques durs (un pour le système et un pour les machines virtuelles). Vmware écrit de nombreuses informations sur le disque système même si les machines virtuelles sont sur un second disque dur.
- Afin d'optimiser les performances, penser à activer les instructions d'accélérations de la virtualisation AMD-V ou INTEL-VT. Le gain est d'environ 100%. Par défaut elles sont désactivées. Pour plus d'informations sur IntelVT, voir <u>http://www.intel.com/technology/virtualization/</u>

#### Remarque :

- Attention, il n'est pas possible d'activer l'interface AERO sur ces machines virtuelles car la carte graphique émulée ne respecte pas les contraintes AERO.
- BITLOCKER n'est pas supporté avec un Vista installé dans une machine virtuelle et ne peut donc pas être testé dans cette configuration.

#### 3 COMMENT DEPLOYER WINDOWS VISTA EN ENTREPRISE :

Windows Vista intègre un nouveau format de d'image d'installation (image WIM) et s'appuie sur Windows PE.

Cette partie consistera à vous présenter les principales nouveautés en termes de déploiement proposée par Windows Vista.

#### 3.1 LE NOUVEAU FORMAT D'IMAGE WIM :

#### **3.1.1 Principe de fonctionnement :**

Le format d'image WIM (Windows Installation Manager) est apparu avec « *Windows Deployment Services* ».

Pour rappel « Windows Deployment Services » est le remplacement de RIS (« Remote Installation Services »).

Il existe deux types d'image WIM :

- Les images WIM de BOOT : ce sont en fait des images WIM qui contiennent un système d'exploitation de type WINPE. Ce type d'image permet :
  - ✓ D'installer Windows Vista, XP, 2003 ou 2008 sur l'ordinateur.
  - De démarrer l'ordinateur sur un système Windows PE (un dérivé allégé de Windows Vista).
  - De capturer un système le contenu d'une machine pour créer une image d'installation (on parle d'image de capture).
- Les images WIM d'installation : ces images WIM contiennent les fichiers systèmes nécessaires à l'installation de Windows XP, Vista, 2003 ou Windows 2008. Il est important de noter que l'on peut déployer une image WIM Windows Vista et Windows 2008 sur une architecture matérielle différente.

Pour générer une image WIM, on utilise un outil de WAIK appelé « IMAGEX ».

#### 3.1.2

#### 3.1.3 Pour plus d'informations sur le format d'image WIM :

Voir article ci-dessous : <u>http://technet.microsoft.com/fr-fr/library/cc507842(TechNet.10).aspx</u>

#### 3.2 WINDOWS PE :

#### **3.2.1** Principe de fonctionnement :

Il s'agit d'un système d'exploitation dérivé de Windows XP / Vista / 2003 / 2008. Il a pour but de remplacer MSDOS comme outil de démarrage pour l'installation de Windows. Le grand avantage de Windows PE est qu'il est indépendant du matériel. Windows PE sert aussi :

- Pour faire du dépannage (« Windows Recovery Environnement » est basé sur Windows PE). Certains éditeurs (comme l'éditeur d'ERD Commander) ont développés des addon à Windows PE qui permettent de disposer d'une interface graphique et des principaux logiciels de maintenance.
- Pour capturer une image système, on utilise une image de Windows PE avec l'utilitaire « IMAGEX ».

Microsoft fournit une procédure pour créer une image Windows PE à partir du CD d'installation de Windows XP, Vista, 2003 et Windows 2008.

Pour plus d'informations sur Windows PE voir articles ci-dessous :

- <u>http://technet.microsoft.com/fr-fr/library/cc507857(TechNet.10).aspx</u>
- http://www.clubic.com/article-75377-1-creer-cd-disque-secours-microsoft-windows-pe-2.html

Attention, au biut de 24 heures, un système WinPE redémarre automatiquement.

## **3.2.2** Pour générer une image ISO à partir d'un répertoire d'installation Windows PE :

Oscdimg -n c:\winpe\_x86\ISO c:\winpe\_x86\winpe\_x86.iso -n -bc:\winpe\_x86\etfsboot.com Voir l'article ci-dessous pour plus d'informations : https://forums.microsoft.com/TechNet/ShowPost.aspx2PostID=1286533&SiteID=17

https://forums.microsoft.com/TechNet/ShowPost.aspx?PostID=1286533&SiteID=17

#### 3.2.3 Capture avec ImageX :

d:\>d:\imagex.exe /compress fast /capture c: y:\image.wim "Installation perso Vi sta" ImageX Tool for Windows Copyright (C) Microsoft Corp. All rights reserved. Files/folders excluded from image capture by default: \WINDOWS\CSC \RECYCLER \\$Recycle.Bin\\* \\$ystem Volume Information \pagefile.sys \hiberfil.sys \\$ntfs.log Turning on VERIFY option for network share Scanning: 4517 files in 1332 directories

#### 3.2.4 Gestion des disques avec Windows PE :

Voir article http://support.microsoft.com/kb/947441/fr.



#### 3.3 COMMENT DEPLOYER EN MASSE WINDOWS VISTA:

Il existe de très nombreux outils qui permettent le déploiement de masse de Windows Vista (on s'y perd même un peu).

On peut cependant classifier ces outils en 3 catégories :

- Les outils de d'analyse de parc : ils permettent de faire un inventaire de votre parc informatique. Windows Vista étant une version majeure de Windows, de nombreuses applications ne fonctionnent plus correctement sous Windows Vista. Microsoft propose trois outils pour faire cela :
  - ✓ « Windows Advisor » : cet outil est présent sur le CD d'installation. Il va permettre de valider la compatibilité logiciel et matériel de votre ordinateur dans le vue d'une migration vers Windows Vista (de Windows 2000 / XP vers Windows Vista). Cet outil n'est pas adapté au monde de l'entreprise.
  - « Windows Assessment » : cet outil permet de scanner l'ensemble de votre réseau et de détecter le matériel et les logiciels qui supporteront la migration vers Windows Vista.
  - *« Windows ACT 5.0 »* (Application Compatibility Check) : cet outil vous permettra d'analyser la compatibilité de vos applications avec Windows Vista. Cet outil intègre une base de connaissance et permet de se synchroniser avec la communauté ACT pour bénéficier du retour des autres personnes qui ont basculés vers Windows Vista. Attention cet outil nécessite le déploiement d'un agent sur les machines sur lesquelles les tests de compatibilité applicatifs sont effectués.
- Les outils de transfert des données des utilisateurs: ces outils permettent de sauvegarder / restaurer les données des utilisateurs présentes en local sur les stations de travail en vue d'une migration de Windows Vista. En effet de nombreuses entreprises préfèrent ne pas migrer le système d'exploitation existant vers Windows Vista car on obtient souvent des comportements inattendues de la part des applications. Ainsi les entreprises préfèrent réinstaller complètement le système d'exploitation. Cela pose le problème de la récupération des données des utilisateurs. Microsoft propose deux outils pour cela :
  - « Outil de transfert de fichiers et de paramètres » : cet outil est disponible dans le menu démarrer dans la section Outils systèmes. Il permet à un utilisateur de transférer individuellement les données d'une machine source vers un ordinateur cible via une interface graphique conviviale. Cet outil n'est pas adapté au monde de l'entreprise.
  - ✓ USMT : cet outil se présente sous forme de deux outils en lignes de commande (SCANSTATE et LOADSTATE). Il permet de scripter le transfert des données et est entièrement personnalisable à l'aide de fichiers XML.
- Les outils de déploiement de masse :
  - « WAIK (« Windows Automated Installation KIT ») » : cet outil se présente sous la forme d'une console et d'une invite de commande. Depuis la console il est possible de générer des fichiers de réponses pour automatiser le déploiement d'une image d'installation WIM. L'invite de commande permet de disposer de commandes pour effectuer des actions sur une image WIM (montage d'une image Wim sous forme d'un lecteur en lecture / écriture pour copier des sources d'installation par exemple).
  - « Windows Deployment Services » : cet outil va nous permettre de déployer Windows Vista via le réseau à l'aide du protocole PXE. On amorce sur une image de boot WIM qui nous permet de déployer une image d'installation WIM. Avec le WAIK, on peut générer des fichiers de réponse pour automatiser le démarrage de l'image WIM de boot et le choix et le déploiement d'une image WIM d'installation.
  - « Windows Deployment Toolkit » (remplacement de « Business Desktop Deployment » alias BDD 2007) : il s'agit en fait d'une suite d'outil qui se base sur tous les outils précédemment présentés. Il existe deux types de déploiement :
    - Lite Touch: Cela permet de déployer Windows Vista via WDS ou un partage de fichiers.

✓ Zero Touch: Cela permet de déployer le système et des logiciels via une infrastructure SMS / System Center.

#### 3.4 WINDOWS ASSESSMENT :

Téléchargement de Windows Vista Assessment : <u>http://www.microsoft.com/downloads/details.aspx?FamilyID=67240b76-3148-4e49-943d-4d9ea7f77730&displaylang=en</u>

#### 3.5 ACT 5.0 : APPLICATION COMPATIBILITE TOOLKIT 5.0 :

Cette application permet de valider le fonctionnement de vos programmes avec Windows Vista.

Nous allons voir dans cette partie :

- Pourquoi certaines applications ne sont pas compatibles avec Windows Vista.
- Le principe de fonctionnement d'ACT 5.0.

#### **3.5.1** Pourquoi certains programmes ne sont pas compatibles avec Windows Vista :

Avec Windows Vista, les sources de problèmes sont :

- Les nouveaux mécanismes de sécurité d'Internet Explorer 7.0.
- L'abandon de certains composants systèmes.
- Le pare feu.
- L'UAC.

Internet Explorer 7.0 propose un nouveau mode de fonctionnement appelé « mode protégée ».

Avec le mode protégé, dans Internet Explorer, une application web ne peut écrire que dans les dossiers suivants :

- Fichiers Internet temporaires.
- Le dossier Historique
- Le dossier Cookies
- Le dossier Favoris
- Les fichiers temporaires de Windows.

Pour plus d'informations sur le mode protégé de Windows Vista :

- http://technet2.microsoft.com/WindowsVista/fr/Library/dfc3160b-0578-427d-8a48-6b63a8e917b81036.mspx
- http://windowshelp.microsoft.com/Windows/fr-FR/help/95211ecc-19b5-439a-b6c5e2aefd8013031036.mspx

Avec Windows Vista, certains composants intégrés dans Windows XP ont disparus. C'est en autre le cas pour :

- Les Extension FRONT Pages
- Le service de fichiers pour MAC
- D3DRM
- Netmeeting.
- L'assistant publication de sites web

Il faut donc réécrire les applications basées sur ces composants.

Avec une version 64 bits de Windows Vista,

- Plus aucun pilote ne peut s'exécuter en mode noyau.
- Par défaut, les pilotes non signés en version 64 bits refusent de s'installer.

L'UAC et le pare feu de Windows Vista sont aussi des vecteurs de problèmes (voir plus loin dans ce document pour plus d'informations).

Pour contourner ce problème, utiliser :

- Assistant compatibilité de Windows Vista
- Autoriser sites web dans Internet Explorer en tant que site de confiance (désactive le mode protégé pour Internet Explorer).
- Désactiver ou reconfigurer l'UAC.
- Ouvrir les ports sur le pare feu. Avec le pare feu de Windows Vista, vous pouvez autoriser tous les flux d'une application en entrée ou sortie.

#### **3.5.2** Principe de fonctionnement d'ACT :

Nous venons de voir qu'il y a de nombreuses sources d'incompatibilités applicatives avec Windows Vista.

ACT va donc nous permettre de fait un inventaire de votre parc informatique. Il est important de noter qu'ACT :

- S'appuie sur une base de données SQL Server (Standard ou Express).
- Nécessite l'installation d'un agent sur les stations de travail que l'on intègre dans l'inventaire.
- ACT s'appuie sur 3 modules :
  - ✓ Module de test UAC
  - ✓ Module de test Internet Explorer
  - ✓ Module de test des problèmes avec le WRP (*Windows Ressource Protection*) et les nouvelles contraintes pour la non prise en charge des pilotes en mode noyau.

ACT nécessite principalement d'effectuer 3 tâches :

- Créer le paquetage de données (agent ACT 5.0) et le déployer sur les stations de travail à l'aide d'une GPO par exemple.
- Configurer les applications par niveau de priorité
- Analyser données collectés

#### 3.5.3 Installation d'ACT :

Avant de commencer l'installation, penser à installer une base de données sur votre serveur (SQL Server ou SQL Server 2005 Express).

Une fois installé (suivre le pas à pas du setup), vient le moment de la configuration de la base de données.

oplication Compatil	bility Toolkit (ACT) Configuration Wizard	Application Compatibility Toolkit (ACT) Configuration Wizard	<
	Welcome to the ACT Configuration Wizard	Select the Configuration Option	
	<ul> <li>This wizard will enable you to configure:</li> <li>ACT database - A SQL Server database that stores your application inventory and issue data.</li> <li>ACT log share - A share into which the log files collected from your client computers are written.</li> <li>ACT Log Processing Service account - A user account with read and write access for the ACT Log Processing Service. This service processes the log files collected from your client computers, storing the data in your ACT database.</li> </ul>	<ul> <li>Enterprise configuration (Configure this computer to process log files and view reports.)</li> <li>Wew and manage reports only (Only view and manage reports from an existing database.)</li> </ul>	
	< Back Next > Cancel	Help Cancel	_

Application Compatibil	lity Toolkit (ACT) Configuratio	n Wizard		×				
Configure Your ACT Database Settings NOTE: You must have read/write permissions to configure these settings. Contact your SQL administrator if you do not have permissions.								
Specify a SQL Serv	er and Database to store compatibi	lity data						
SQL Server:	(local)\MAPS	<b>.</b>	Connect Bro	owse				
Database:		<b>v</b>	Create					
		_						
Help		< Back	Next >	Cancel				
Application Compatibi	lity Toolkit (ACT) Configuratio	n Wizard		×				
NOTE: You must have n do not have permissions	ACT Database Settings ead/write permissions to configure t	hese settings. C	ontact your SQL a	administrator if you				
Specify a SQL Serv	er and Database to store compatibi	lity data						
SQL Server:	WIN-CH1Y9QPIKWY\SQLEXPF	RESS 💌	Refresh Bro	owse				
Database:	ACT	- -	Create					
	,							

#### 3.5.4 Prise en main de l'interface :

Une fois que l'on a fait un inventaire, la liste des programmes apparaît. Attention, pour voir si l'application est compatible ou nous vous pouvez synchroniser avec la communauté ACT ou filtrer les programmes sur le champ « issue » (problème). Les applications incompatibles n'apparaissent pas avec un code de couleur donc attention !

#### 3.5.5 Création du paquetage :

Lorsque l'on crée le paquetage de l'agent ACT, on peut sélectionner les modules d'analyse que l'on veut utiliser.

Dans le jargon ACT, l'agent ACT est appelé DCP (« Database Compatibility package ».

Compatibili	ty Evaluators includ	led in the Data (	Collection Packa	ige ——					
Select the compatibility evaluators to include.									
Name     Settings       ✓     Internet Explorer Compatibility Evaluator       ✓     Inventory Collector       ✓     User Account Control Compatibility Evaluator       ✓     Windows Mata Compatibility Evaluator									
Collect	t <b>ory Collector</b> s system data for co	mpatibility evalua	tion.						
Prompt for restart Prompt users to restart if required by the installation (Microsoft Windows 2000 only).									
Prom	estart	equired by the in	stallation (Micros	oft Windows 20 Cancel	00 only). Apply				
dows2000-Atket	estart ot users to restart if n UA - Application Compatibilit	equired by the in y Manager	stallation (Micros	oft Windows 20	00 only).				
dows2000/ARKel Indow Help	ot users to restart if n VA - Application Compatibilit	equired by the in y Manager	stallation (Micros	oft Windows 20	00 only).				
Adows2000-ARKef Andow Help Adows	A Application Compatibilit Windows2000-ARKEMA when v Operating System or Service Pr w v version of Internet Explorer (y v of Updates	equired by the in y Hanager	Stallation (Micros	oft Windows 20	00 only).				
Anys2000-ARKET      Andow Help      Andow Help      Andow Help      Comparison      Anys2000-ARKET      Anys200-ARKET	Application Compatibilit     Windows2000-ARKEMA     Windows2000-ARKEMA     when     v Operating System or Service Pa     we supdates     ation usage     As soon as possible after inst     Jacome	equired by the in y Hanager ack (for example, Microsoft ou must test with Internet E allation	Stallation (Micros	oft Windows 20 Cancel	00 only).				
dows2000-ARKet indow Help	A polication Compatibilit     Windows2000-ARKEMA     Windows2000-ARKEMA     when     v Operating System or Service PR     we version of Internet Explorer (y     we use of Internet Explorer (y     we use of Internet Explorer (y     as oon as possible after inst     3	equired by the in  V Hanager  Kck (for example, Microsoft ou must test with Internet E  allation	Stallation (Micros	oft Windows 20 Cancel	00 only).				
Applying Windo     Applying Windo     Applying Windo     hen to monitor apple     Starting:     Juration:     Jpload data every:     here to output collect	Application Compatibilit     Windows2000-AFICEMA     Windows2000-AFICEMA     when     Operating System or Service PI     we supdates     ation usage     [3	equired by the in y Hanager ack (for example, Microsoft ou must test with Internet E allation I1/90PKWYVACTFLES)	stallation (Micros	oft Windows 20 Cancel	00 only). Apply Advanced ↓ 008 ▼ 00.28				

#### 3.5.6 Synchroniser avec la communauté ACT:

Avec le bouton « Send and receive », on peut synchroniser sa base avec la base ACT communautaire pour avoir le retour des autres utilisateurs d'ACT.

ACT Send/Receive	<u> </u>
Synchronizing	Cancel
	Details >>
Don't show this dialog box during Send/Receive	

#### 3.5.7 Problèmes rencontrées :

Attention les logs qui ne remontent pas pour les stations de travail qui ne sont pas sur le même domaine par défaut. En effet ces machines n'ont pas les droits d'accès aux partages où les logs sont déposés.

#### 3.6 USMT :

#### 3.6.1 Principe général :

USMT permet de sauvegarder et de restaurer automatiquement les données des utilisateurs, et les comptes utilisateurs locaux des machines.

Cet outil est complètement intégré à « Windows Deployment Toolkit ».

Cet outil est basé sur deux commandes :

- SCANSTATE.
- LOADSTATE.

Le fonctionnement de ces deux outils peut être paramétré à l'aide des fichiers XML suivants :

- Config.xml : fichier facultatif mais nécessaire avec Vista car remplace Migsys.xml.
- MigApp.xml : contient les paramètres des applications à migrer
- MigSys.xml : utilisé que pour Windows XP, pas pour Vista
- MigUser.xml : contrôle les dossiers utilisateurs à migrer
- Fichiers xml personnalisés pour migrer dossier et fichier sur ordinateur

#### Remarque :

- Il est à noter que l'USMT permet de migrer automatiquement les fichiers chiffrés et les certificats associés (si l'on arrive à déchiffrer les données).
- USMT crée un fichier usmt3.mig.
- Attention USMT ne supporte pas le changement de version des logiciels autres qu'Office. Donc vous oubliez le passage d'un applicatif de la version 2.0 à la version 5.0, cela risque de marcher fort mal.
- Attention l'USMT nécessite Windows 2000 service pack 4, le ROOLUP 1 post SP4 et Windows Installer 3.1 sinon on obtient le message d'erreur ci-dessous :

Windows	Installer			X
⚠	Ce package d' service Windo service pack V récente du ser	nstallation ne p vs Installer. Vo /indows conter vice Windows I	beut pas être install us devez installer u nant une version pl Installer.	é par le in us
		ОК		

#### **3.6.2** Quelques exemples de commande :

Scanstate [StorePath] [/i:[path\]FileName] [Options]

```
scanstate /i:migapp.xmi /i:miguser.xmi
/genconfig:config.xml
```

C:\Documents and Settings\administrateur.ARKEMA>"C:\Program Files\USMT301\ScanSt ate.exe" \\WIN-CH1Y9QPIKWY.arkema.lan\usmt\w2ktest /i:migapp.xml /i:miguser.xml /config:config.xml /o /all /efs:copyraw Log messages are being sent to 'C:\Program Files\USMT301\ScanState.log' Scanning the computer for files and settings... Collecting files and settings for: This Computer 'ARKEMA\administrateur' (user 1 of 2) '2000PROA\Administrateur' (user 2 of 2) Saving files and settings -ScanState has successfully collected the files and settings.

g:\>LoadState \\WIN-CH1Y9QPIKWY.arkema.lan\USMT\w2ktest\ /i:migapp.xml /i:miguse r.xml /ui:administrateur@arkema.lan

Log messages are being sent to 'g:\LoadState.log' Scanning the computer for files and settings... Applying files and settings - 1 minute(s) remaining... 4 g:\>rename dir Unassigned\$dir Le fichier spécifié est introuvable.

LoadState has successfully restored the files and settings.

#### 3.6.3 Les bonnes pratiques :

- Migrer par vague pour éviter de saturer le réseau.
- Chiffrer le magasin temporaire (résultat de la commande SCANSTATE).

#### 3.6.4 Pour plus d'informations sur USMT :

- http://www.microsoft.com/downloads/details.aspx?familyid=799AB28C-691B-4B36-B7AD-6C604BE4C595&displaylang=en
- Lire le fichier d'aide installé avec USMT, il est très bien fait.

#### 3.6.5 Pour télécharger USMT 3.0 :

http://www.microsoft.com/downloads/details.aspx?familyid=799AB28C-691B-4B36-B7AD-6C604BE4C595&displaylang=en

#### 3.7 LE WAIK :

Le WAIK intègre les outils suivants :

- WINPE
- IMAGEX
- Le « Windows System Image Manager ».

Nous allons voir dans cette partie comment générer un fichier de réponse pour automatiser une installation de Windows Vista.

#### 3.7.1 Génération du fichier unattend.xml :

Tout d'abord, il faut comprendre que l'installation de Windows Vista se fait en 7 étapes :

- Windows PE
- OfflineServicing
- Généralize
- Specialise
- AuditSystem
- AuditUser

OobeSystem : il s'agit de l'assistant qui vous demande de saisir votre nom d'utilisateur.
 Chaque étape de l'installation peut être paramétrée et automatisée. On peut même définir certains paramètres à l'aide du fichier de réponse qui ne nous sont pas proposé par
 'l'installation de Windows Vista par défaut ou exécuter des scripts à l'aide de fichier de réponse.

Pou plus d'informations pour personnaliser l'Out Of Box, consulter l'article ci-dessous : <u>http://windowshelp.microsoft.com/Windows/fr-FR/help/6ae38832-f98d-4e0c-8b48-</u> <u>2f27cfd18f851036.mspx</u>



En bas à gauche, on a toutes les variables disponibles.

A droite, on a notre fichier de réponse avec toutes les variables que l'on a ajoutées. Il est à noter que pour savoir les valeurs que l'on doit rentrer, on peut faire un clic doit sur le paramètre et sélectionner F1. On sait alors ce que l'on peut rentrer (pratique pour les codes régionaux par exemple).

Untitled* - Windows System Image Manager		_63
1918년 - 2018년 1918년 - 2018년 17 월 🕞 🔀 🕞 🔏 🍈 🗡 🔎 🞯 🔁 🗐		К
Partage Fichier de réponses	Propriétés de Microsoft-Windows-	International-Core-WinPE
Selecti Components Components Components Components Components Components Components Components Components Components Components Components Constant Cons	Propriétés     AppledConfigurationPass     Enabled     Id     Paramètres     InpuLocale     LayereDriver     SystemIocale     UlLanguage     UlLanguage     UlLanguage     UlLanguage     UlLanguage     UlLanguage     Ulanguage     Ulang	1 windowsPE True x86_Microsoft-Windows-International-Core-WinPE_neutral_31bf3856ad364ei fr-FR fr-FR fr-FR fr-FR fr-FR fr-FR

Fichier de réponses		Propriétés de Microsoft-Windows-International-Core-WinPE					
E- 🕑 Untitled		Propriétés					
E Components		AppliedConfiguratio	on	Pass	1 windowsPE		
🖻 🦣 1 windowsPE		Enabled			True		
x86_Microsoft-Windows-International-Core-WinPE_neut	Œ	ld			x86_Microsoft-Windows-International-Core-WinPEneutral_31bf3856ad364e3		
SetupUILanguage	E	2 Paramètres					
x86_Microsoft-Windows-Setup_neutral		InputLocale	Г	Annu dan la sua differentian	FR		
DiskConfiguration		LayeredDriver	Annuler la modification	Annuler la modification			
⊡		SystemLocale		Écrire une chaîne vide			
CreatePartitions		UlLanguage		Écrire la valeur de l'image	FR		
ModifyPartitions		UILanguageFa			FR		
		UserLocale		Aide F1	FR		
🖹 🗇 🦳 OSImage							

La capture ci-dessous montre comment configurer un script dans un fichier de réponse : La commande se rentre dans le « PATH » :

- cmd /c net user Administrator\_ploc /active:yes
   cmd /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v FilterAdministratorToken /t REG\_DWORD /d 0 /f

Toujours taper cmd / c + la ligne de commande.

Fichier de réponses	Propriétés de RunSynchronousCommand[Order="2"]			
🖃 🖭 Unattend		Propriétés		
Components		AppliedConfiguration Pass	4 specialize	
🖃 🖣 1 windowsPE		Component	Microsoft-Windows-Deployment	
- x86_Microsoft-Windows-International-Core-Win		KeyName	Order	
Setup UILanguage		Path	Run Synchronous/Run SynchronousCommand[Order="2"]	
ianter in the second s		Paramètres		
		Action	AddListItem	
		Description	EnableAdmin_ploc	
🖃 🗐 ImageInstall		Order	2	
🖻 🗂 OSImage		Path	cmd /c net user Administrator_ploc /active:yes	
installFrom		WillReboot	Never	
MetaData[Key="/image/index"				
Install To				
🖻 🗂 UserData				
ProductKey				
2 offlineServicing				
x86_Microsoft-Windows-PnpCustomizationsNor				
⊡ DriverPaths				
PathAndCredentials[Key="1"]				
PathAndCredentials[Key="2"]				
PathAndCredentials[Key="3"]				
PathAndCredentials[Key="4"]				
PathAndCredentials[Key="5"]				
E 4 3 generalize				
x86_Microsoft-Windows-Shell-Setup_neutral				
E X86_Microsoft-vvindows-Deployment_neutral				
Run SynchronousCommand[Order= 1]				
Purioynchronouscommand[Urder= 2]	A	ppliedConfigurationPass		
Nurisynchronouscommand[Urder= 3]				
ter windows-iE-internetExplorer_net ♥				

#### Problèmes rencontrées avec les fichiers de réponse :

 Attention à l'ordre pour les disques. Dans le fichier XML, la création doit être avant la modification du disque. Pour être sur il faut faire à la fin un fichier enregistrer sous pour recréer un nouveau fichier XML.

#### 3.7.2 Pour plus d'informations sur le WAIK :

 Lire le fichier « C:\Program Files\Windows AIK\Docs\Whitepapers\getting\_started\_itpro.htm » présent une fois que l'on a installé le WAIK.

#### 3.7.3 Pour télécharger le WAIK :

http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08

#### 3.8 WINDOWS DEPLOYEMENT SERVICE :

#### 3.8.1 Principe de fonctionnement :

Il s'agit du système d'un système de déploiement de Windows via le réseau.

C'est le remplaçant de « Remote Installation Service »

- « Windows Deployment Services » :
- S'appuie sur le format d'image WIM pour les images de boot WIM comme pour les images d'installation WIM.
- Gère le multicast pour un déploiement simultanée de plusieurs machines.

#### 3.8.2 Ce qu'il faut retenir de WDS :

- Il existe 2 types d'image WIM de BOOT /
  - ✓ Les images de boot : utiliser pour installer Windows.
  - Les images de capture : utiliser pour capturer un système d'exploitation (nécessite que l'exécution de SYSPREP sur le postes avant dernier redémarrage / arrêt).
- Attention ne pas utiliser l'image WIM boot.wim du cd de Windows Vista sp0 car celui-ci ne gère pas le multicast.
- Suite à un changement de la configuration réseau multicast, il faut redémarrer le service d'installation à distance Windows Vista.
- On peut repasser un client d'une communication en multicast à une communication en unicast en cliquant sur « Déconnecter un client d'une transmission multicast ».
- Pas de support d'IPV6 pour WDS.
- Il faut une image WIM de boot (image Win PE) et une image d'installation (master).
- La vitesse en multicast s'effectue à la vitesse du client le plus lent.
- Les machines X64 supportent le boot PXE sur une image de boot 32 bits et sur une image de boot 64 bits mais pas l'inverse.
- Pas plus de 13 images de boots avec WDS.
- Pas d'espace dans le nom du fichier WIM.
- Si l'on boot sur une image de boot X64, on ne voit que les images WIM d'installation X64.
- Les images WIM Vista n'ont pas de couche d'abstraction matérielle (HAL). Il est donc possible de déployer une image WIM Vista sur des architectures matérielles différentes (voir page 14 du WDS\_STEP BY STEP).
- Avec l'utilitaire de capture IMAGEX, on ne voit que les partitions préparer à l'aide de SYSPREP.

Pour créer une image d'installation :

- Installer le système et les applications.
- Mettre à jour le système et les images.
- Configurer les paramètres par défaut de votre système et de vos applications (Default User...).

Msreport - Guillaume MATHIEU http://msreport.free.fr

La connaissance s'accroît quand on la partage.

 Lancer l'utilitaire SYSPREP en mode OOBE et activant la case à cocher « GENERALYSE ».

#### 3.8.3 Installation sans assistance avec WDS :

Vous pouvez automatiser l'installation d'un système via WDS : Il existe deux types de fichier de réponse avec WDS :

- Un pour automatiser toutes les tâches WDS (connexion à une image avec tel ou tel compte utilisateur).
- Un pour automatiser l'installation du système (associé à l'image WIM).

Pour automatiser les tâches WDS, aller dans les propriétés de votre serveur dans la console « Service de déploiement Windows » puis dans l'onglet Client.

Pour automatiser l'installation du système, aller au niveau de l'image WIM puis faire un clic droit propriétés. Au niveau de l'onglet « *Général* », cocher « *Autoriser l'image à s'installer en mode sans assistance* ».

Propriétés de WIN-CH1Y9QPIKWY	×	P	ropriétés de Image	×
Général       Paramètres de réponse PXE       Services d'annuaire         Démarrer       Client       DHCP       Paramètres réseau       Avancé         Le client des services de déploiement       Windows peut être configuré pour s'exécuter en mode sans assistance. En mode sans assistance, les pages d'interface utilisateur sont traitées sans l'intervention de l'utilisateur en fonction des paramètres définits dans le fichier d'installation sans assistance du client des services de déploiement Windows.         Image: Activer l'installation sans assistance       Activer l'installation sans assistance         Fichier d'installation sans assistance       Architecture x86 :         WdsClient Unattend\Unattend xm       Parcourir         Architecture ia64 :       Parcourir			Général Version Sé Windows Type d'image : État : Architecture : Description : Groupe d'images : Nom du fichier :	Image d'installation En ligne x86 Windows Vista BUSINESS Windows Vista install.wim
Architecture x64 :       Parcourir         Création des comptes clients       Image: Création du client WDS         Informations complémentaires sur l'installation sans assistance       OK         OK       Annuler			Taille : Créé(e) : Modifié(e) : Type de couche HAL	7395 Mo (7755000465 octets) lundi 21 janvier 2008 03:49:37 mardi 24 juin 2008 06:03:24 .: acpiapic à s'installer en mode sans assistance Sélectionner un fichier

#### **3.8.4** Pour plus d'informations WDS :

http://technet2.microsoft.com/windowsserver2008/en/library/8866a02e-dd26-4c11-b29af9988b6797f51033.mspx?mfr=true

#### Lire le STEP BY STEP de WDS, il est très bine écrit !

http://technet2.microsoft.com/WindowsServer2008/en/library/7d837d88-6d8e-420c-b68fa5b4baeb52481033.mspx

#### 3.9 PRESENTATION DE WINDOWS DEPLOYMENT TOOLKIT :

Cet outil est le remplaçant de BDD (Business Desktop Deployment).

#### 3.9.1 Principe de fonctionnement :

- Intègre le WAIK, USMT, ACT 5.0.
- Pour bénéficier du multicast avec WDS, il faut installer sur Windows Server 2008
- Pour fonctionner avec Windows 2000, nécessite le sp4, MSXML 3.0, Microsoft Visual C++ Runtime, Internet Explorer 5.0 et Windows Script version 5.6.

- Windows Deployment Toolkit va en fait paramétrer le fichier de réponse unattend.xml et définir dans ce fichier de réponse le lancement de nombreux scripts. Ces scripts se trouvent dans le répertoire d'installation de « Windows Deployment Toolkit »
- Lors création des tâches, on peut éditer le fichier de réponse et donc ajouter d'autres scripts de connexion.
- Il existe un fichier bootstrap.ini qui permet de personnaliser l'assistant qui se lance quand vous démarrer depuis l'image « Lite Touch » de WDT. Exemple de fichier bootstrap.ini :

[Settings] Priority=Default Properties=MyCustomProperty [Default] OSInstall=Y UserDataLocation=NETWORK SkipAppsOnUpgrade=YES SkipCapture=NO SkipAdminPassword=YES SkipProductKey=YES

			di Unattendoxml* - Win	dows System Image Hana	ger
			Fichier Edition Inst	irer Outls ??	
			1 🔁 🏓 🛅 🔛 1 🔏 1	9 🛛 🗶 I 🏷 I 🕹 I	0
			Partage de distribu	tion	Fichier de réponses
			9 a C'Untroution		Invatend     Corponents     Corponents     InvidowsPE     SoftmasProto     SoftmasProt
métés de VISTAIRSULT eneral OS Info Task Sequ	ence				
Operating system description:	Windows Vista ULTIMATE		E S Windows Vista UL	TIMATE(Catalogue)	•
Build:	6.0.6001.18000		Components     Packages		
Platform:	x86				
	Please wait while the catalog is being generated.	Edit Unattend.emi			Messages XML (0) Valdation (0) Jeu Description
chier de réponses		Propriétés d	le InstallFrom		
Unattend		Propriétés			
Components		AppliedConfig	urationPass	1 windowsPE	
1 windowsPE	oft.Windowe.International.Core.WinPE	Component		Microsoft-Windows-Setu	ip natall Canaz
1 windowsPE	oft-Windows-International-Core-WinPE_neutral ILanguage	Component Path		Microsoft-Windows-Setu ImageInstall/OSImage/I	ıp nstallFrom

Msreport - Guillaume MATHIEU <u>http://msreport.free.fr</u> La connaissance s'accroît quand on la partage.

taData[Key="/image/index"]

allFrom

tallTo

#### 3.9.2 Problème rencontré avec le Windows Deployment Toolkit :

Lorsque vous importer la première image d'installation, il est nécessaire de définir une importation complète du CD et non pas uniquement de l'image WIM. Sinon on obtient ce message au moment du chargement de l'image Lite Touch.



#### 3.9.3 Pour plus d'informations sur Windows Deployment Toolkit :

- http://technet.microsoft.com/en-us/library/bb977913.aspx
- http://www.microsoft.com/downloads/details.aspx?familyid=3bd8561f-77ac-4400-a0c1fe871c461a89&displaylang=en&Hash=DAl05Mr2BLY7d6jFjYZPzC6h4TlfmaxaiyH7sDY2X V3T5tiVYLoShLSFkCwK8CWJ4dRRjA4jgKc4UMahmUNulA%3d%3d
- http://technet2.microsoft.com/windowsserver2008/en/library/fbd2d37b-4127-43fd-a079f78bbd44b7601033.mspx?mfr=true

#### 3.9.4 Pour télécharger Microsoft Deployment Toolkit :

http://www.microsoft.com/downloads/details.aspx?FamilyID=3bd8561f-77ac-4400-a0c1fe871c461a89&DisplayLang=en

#### 4 LES AUTRES NOUVEAUTES DE WINDOWS VISTA :

#### 4.1 LA POSSIBILITE DE FILTRER L'APPLICATION DE GPO LOCAL :

On peut appliquer une **GPO local** sur une station Windows Vista à un seul utilisateur. En effet avec Windows 2000 / XP, quand on définissait localement une stratégie de groupe, elle s'appliquait à tout les utilisateurs de la machine.

Cette possibilité n'est intéressante que pour des stations de travail en groupe de travail. Si vous êtes en domaine, utiliser une GPO de domaine.

Pour faire cela, ajouter le composant « *Group Policy Object* » et cliquer sur « *Browse* ». Aller ensuite dans l'onglet « *Utilisateurs* » et sélectionner l'utilisateur pour lequel vous voulez configurer les paramètres de stratégies de groupe.

Select Group Policy Object	×		
Welcome to the Group Policy W	izard		
		Rechercher un objet Stratégie de groupe	<u>? ×</u>
ľ	Local Group Policy Objects are stored on the local computer. Use the Browse button to select one of the Group Policy Objects	Ordinateurs Utilisateurs Utilisateurs et groupes locaux compatibles avec la stratégie Nom	e de groupe locale : Il existe des objets de stratégie.
	Group Policy Object:	Se Administrateur Se Arkema Enfant	Non Non Non
	Local Computer Browse	<ul> <li>Formation</li> <li>Formation2</li> <li>Guillaume</li> </ul>	Non Non Non
	Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This only applies if you save the console.	Manin instrateous	Non
	< <u>₿</u> ack <b>Finish Cancel</b>	·	OK Annuler



#### 4.2 LE NOUVEAU PARE FEU DE WINDOWS VISTA :

#### 4.2.1 Principe de fonctionnement :

- Le pare feu de Windows Vista est un pare feu entrant et sortant à état Pou plus d'informations ce qu'est un pare feu avec état (statefull) et les différences avec les pare feu sans état (stateless), voir articles ci-dessous : <u>http://fr.wikipedia.org/wiki/Pare-feu</u>
- Le pare feu de Windows Vista permet de faire des règles de filtrage basées sur des ports, des adresses IP, des types de protocoles et des applications. Si l'on met en place de

l'IPSEC (mécanisme d'isolation), on peut aussi filtrer selon la machine source et destination et selon des utilisateurs et des groupes utilisateurs.

- Le pare feu de Windows Vista se configure deux manières différentes :
  - ✓ A l'aide d'une interface simplifiée depuis le panneau de configuration (Pare feu).
  - ✓ Depuis la console MMC « Pare feu avec prise en charge avancée de la sécurité »
- Il est possible de gérer le pare feu à l'aide de la commande « Netsh advfirewall »
- L'ordre d'application des règles dépend de leurs spécificité (nombres de paramètres).
   Plus une règle est précise, plus elle est évaluée en premier. Les différents types de règles dans le pare feu de Windows Vista sont :
  - ✓ Sur des services
  - ✓ Sur des connexions sécurisées (IPSEC).
  - ✓ Sur des règles d'authentification d'outrepassement
  - ✓ Sur des règles refusées
  - ✓ Sur des règles acceptées
  - ✓ Sur des règles par défauts
- Le service pare feu s'appelle MpsSVC.
- Le pare feu est entièrement administrable par GPO (avec Windows Server 2008). On retrouve sous forme de GPO les mêmes options que dans la console « Pare feu avec prise en charge avancée de la sécurité »
- Une des grandes nouveautés du pare feu est l'amélioration de la prise en charge du protocole RPC. Pour plus d'informations sur le protocole RPC, voir article <u>http://technet2.microsoft.com/WindowsServer/en/library/4dbc4c95-935b-4617-b4f8-</u> <u>20fc947c72881033.mspx</u>. Avec le pare feu de Windows Vista, il faut créer deux règles :
  - ✓ Une pour permettre l'accès aux services RPC
  - ✓ L'autre spécifiant comme protocole dynamic RPC pour permettre l'accès aux services qui tournent su port RPC.
- Il est possible de journaliser les connexions (refusées ou acceptés du pare feu). Voir capture ci-dessous.

#### Remarque :

 Sous Vista, la console Jeu de stratégie résultant ne prend pas en charge l'affichage des options du pare feu avec filtrage avancées. Ces derniers apparaissent sous forme de Les paramètres de registre supplémentaires.





#### Extrait des fichiers de log du pare feu :

2000-00-25	17.09.19	ALLOW TC	A TAS'TOO'A'2T	192.100.0.200	495J4 00 V -	UUUSEND	
2008-06-23	12:09:35	ALLOW TO	P 192.168.0.31	192.168.0.200	49355 135 0	- 0 0 0 SEND	
2008-06-23	12:09:35	ALLOW TO	P 192.168.0.31	192,168,0,200	49356 135 0	- 0 0 0 SEND	
2008-06-23	12.00.35	ALLOW TO	p 102 168 0 31	102 168 0 200	49357 49156	0 - 0 0 0 SEN	n
2000-00-25	12.09.55	ALLOW ICI	F 192.100.0.91	192.100.0.200	49337 49130	0 - 0 0 0 JEN	
2008-06-23	12:09:35	ALLOW TC	P 192.168.0.31	192.168.0.200	49358 389 0	- 0 0 0 SEND	
2008-06-23	12:09:36	ALLOW TC	P 192.168.0.31	192.168.0.200	49359 389 0	- 0 0 0 SEND	
2008-06-23	12:10:34	ALLOW TO	P 192.168.0.20	0 192.168.0.31	56626 135 0	- 0 0 0 RECEL	VE
2000 06 22	12.10.24	DROD TOD	100 100 0 000	100 100 0 01	FCC37 40153 5		
2008-06-23	12:10:34	DROP ICP	192.108.0.200	192.108.0.31	<b>3002/ 49133 3</b>	2 5 4025323203 0 81	92 RECEIVE
2008-06-23	12:10:37	DROP TCP	192.168.0.200	192.168.0.31	56627 49153 5	2 5 4025323203 0 81	92 RECEIVE
2008-06-23	12:10:43	DROP TCP	192.168.0.200	192.168.0.31	56627 49153 4	8 5 4025323203 0 81	92 RECEIVE
2008-06-23	12.10.55	ALLOW TO	p 102 168 0 20	0 102 168 0 31	56629 445 0	- 0 0 0 PECET	/E
2000-00-25	12.10.55	ALLOW ICI	- 132.100.0.20	0 192.100.0.51	J0023 44J 0	- 0 0 0 KECEI	V E
2008-06-23	12:10:55	ALLOW TC	P 192.168.0.31	192.168.0.200	49360 88 0 -	000SEND	
2008-06-23	12:10:55	ALLOW TC	P 192.168.0.31	192.168.0.200	49361 88 0 -	000SEND	
2008-06-23	12:11:34	ALLOW UD	P 192.168.0.31	192.168.0.255	137 137 0 -	SEND	
2008 06 22	12.11.24	ALLOW TO	0 100 169 0 01	102 168 0 201	40262 120 0	0.0.0 CEND	
2008-00-23	12:11:34	ALLOW IC	P 192.108.0.31	192.108.0.201	49502 139 0	- 0 0 0 SEND	
2008-06-23	12:11:36	ALLOW UD	P 192.168.0.20	1 192.168.0.25	5 138 138 0 -	RECEIV	E

#### 4.2.2 Pour plus d'informations sur la pare feu de Windows Vista :

http://go.microsoft.com/fwlink/?LinkId=64343 http://go.microsoft.com/fwlink/?LinkID=102503 http://go.microsoft.com/fwlink/?LinkId=64382 http://go.microsoft.com/fwlink/?LinkId=64344

#### 4.3 L'UAC :

#### 4.3.1 Le but :

Le but de l'UAC est double :

- Empêcher qu'un programme malveillant s'exécute avec des droits administrateur. Je vous rappelle que quand vous vous loguez en administrateur du domaine sur une station de travail, vous êtes administrateur de toutes les machines du domaine. Gare à un virus qui ferait un scan du réseau et exécuterait des commandes sur toutes les machines du réseau. Avec l'UAC ce script ne pourrait pas s'exécuter.
- Permettre de configurer le comportement à l'installation d'un programme. Vous pouvez configurer le fait qu'une fenêtre POPUP va s'afficher permettant à l'utilisateur de se loguer avec un compte administrateur ou définir que l'installation de l'application va échouer avec un message « Accès refusé ».
- Dans le même principe, vous pouvez définir si une fenêtre d'authentification ou un message « Accès refusé » apparaît lorsqu'un utilisateur standard essaie d'effectuer une tâche d'administration.

#### 4.3.2 Le principe :

Lorsque vous vous loguez, vous récupérer un jeton qui contient le GUID de votre compte et des groupes dont vous être membres.

Ce jeton est présenté à chaque fois que vous avez besoin d'accéder à une ressource. Le principe de l'UAC est de disposer maintenant de deux jetons :

• Un jeton limité : par défaut vous présentez ce jeton.

 Un jeton normal : ce jeton est présenté seulement après confirmation de votre part que vous voulez bien effectuer la tâche qui nécessite des droits de type « administrateur ».

Quand on essaie d'exécuter une tâche qui nécessite des droits « *administrateur* » en mode invite de commande, on obtient le message « *L'opération demandée nécessite une élévation* ».

Il faut lancer la console en mode administrateur pour cela, aller dans le menu démarrer et faire clic droit sur invite de commande et exécuter en tant qu'administrateur. http://www.laboratoire-microsoft.org/tips-26488-ipconfig-release-sous-Vista.html



### Il est important de noter que l'UAC est complètement configurable via stratégie de groupe :

Fichier Action Affichage ?								
I Stratégie Configuration des machines [WIN-CH1Y9QPIKWY.	Stratégie 🔺	Paramètres de stratégie						
🖃 👰 Configuration ordinateur	Comptes : statut du compte Administrateur	Non défini						
🖃 🧰 Stratégies	🐻 Comptes : statut du compte Invité	Non défini						
🕀 🚞 Paramètres du logiciel	Console de récupération : autoriser la copie de disquettes et l'accès à tous les lecteurs et dossiers	Non défini						
🖃 🧮 Paramètres Windows	Console de récupération : autoriser l'ouverture de session d'administration automatique	Non défini						
🖹 Scripts (démarrage/arrêt)	💹 Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur int	Non défini						
Paramètres de sécurité	Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation	Non défini						
Stratégies de comptes	Contrôle de compte d'utilisateur : autoriser les applications UIAccess à demander l'élévation sans utilis	Non défini						
🖃 🚰 Strategies locales	Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs en mo	Non défini						
Strategie diaudit	🐻 Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les utilisateurs standard	Refuser automatiquement les c						
Options de sécurité	Contrôle de compte d'utilisateur : détecter les installations d'applications et demander l'élévation	Non défini						
Journal des événements	Contrôle de compte d'utilisateur : élever uniquement les applications UIAccess installées à des emplac	Non défini						
Groupes restreints	Contrôle de compte d'utilisateur : élever uniquement les exécutables signés et validés	Non défini						
Services système	Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'ad	Non défini						
T Registre	💹 Contrôle de compte d'utilisateur : virtualiser les échecs d'écritures de fichiers et de Registre dans des	Non défini						
🕀 📆 Système de fichiers	Contrôleur de domaine : conditions requises pour la signature de serveur LDAP	Non défini						
표 🚺 Stratégies de réseau filaire (IEEE 802.3)	Contrôleur de domaine : permettre aux opérateurs du serveur de planifier des tâches	Non défini						
🕀 🧮 Pare-feu Windows avec fonctions avanc	Contrôleur de domaine : refuser les modifications de mot de passe du compte ordinateur	Non défini						
Stratégies du gestionnaire de listes de re	Cryptographie système : force une protection forte des clés utilisateur enregistrées sur l'ordinateur	Non défini						
🕀 🌆 Stratégies de réseau sans fil (IEEE 802. :	DCOM : Restrictions d'accès à un ordinateur au format du langage SDDL (Security Descriptor Definitio	Non défini						
🕀 🧰 Stratégies de clé publique	DCOM : Restrictions de démarrage d'ordinateur au format du langage SDDL (Security Descriptor Defin	Non défini						
E Stratégies de restriction logicielle	Membre de domaine : ancienneté maximale du mot de passe du compte ordinateur	Non défini						
Network Access Protection	Membre de domaine : chiffrer numériquement les données des canaux sécurisés (lorsque cela est pos	Non défini						
🕀 🌏 Stratégies de sécurité IP sur Active Dire	Membre de domaine : chiffrer ou signer numériquement les données des canaux sécurisés (toujours)	Non défini						
🕀 🏭 QoS basée sur la stratégie	Membre de domaine : désactive les modifications de mot de passe du compte ordinateur	Non défini						
H Modeles d'administration : définitions de stratégi Defférences	Membre de domaine : nécessite une clé de session forte (Windows 2000 ou ultérieur)	Non défini						
Preferences     Payamètres Windows	Membre de domaine : signer numériquement les données des canaux sécurisés (lorsque cela est possi	Non défini						
Parametres windows Paramètres du Pappagu de configuration	Objets système : les différences entre majuscules et minuscules ne doivent pas être prises en compte	Non défini						
Configuration utilizateur	Objets système : renforcer les autorisations par défaut des objets système internes (comme les liens	Non défini						
🖂 🝋 Coningeration delisateur								

#### 4.3.3 Pour plus d'informations sur l'UAC:

http://technet2.microsoft.com/WindowsVista/en/library/0d75f774-8514-4c9e-ac08-4c21f5c6c2d91033.mspx?mfr=true

#### 4.4 EFS : NOUVEAUX ASSISTANTS :

EFS permet de sécuriser l'accès à vos données. Il vient combler les défauts des permissions NTFS

En effet, il est nécessaire de rappeler que par défaut tout administrateur d'une machine peut prendre possession d'un fichier et d'un dossier et donc se donner les droits pour accéder à ce dossier / fichier.

Microsoft apporte un début de réponse avec EFS.

EFS va permettre de chiffrer les données présentes sur un serveur ou en local.

Les données sont chiffrées à l'aide d'une clé secrète, elle-même chiffrée à l'aide d'un certificat utilisateur. Seules les personnes disposant du certificat (clé privé et clé publique) peuvent déchiffrer la clé secrète et donc les données.

Msreport - Guillaume MATHIEU

#### http://msreport.free.fr

La connaissance s'accroît quand on la partage.

Une des nouveautés sympathique d'EFS avec Windows Vista est la possibilité d'exporter ses certificats depuis le composant « Utilisateurs » du panneau de configuration de Windows Vista.

De plus en cas de changement de certificats utilisateur, il est possible de déchiffrer automatiquement tous les fichiers chiffrés avec l'ancien certificat pour les chiffrer avec le nouveau certificat.

	0	Système de fichiers EFS (Encrypting File System)						
se		Sélectionner ou créer un certificat de chiffrement de fichiers						
•		Sélectionnez un certificat de chiffrement de fichiers, ou créez un nouveau certificat. Si vous avez déjà chiffré les fichiers, vous pouvez les mettre à jour pour utiliser ce certificat.						
		Utiliser ce certificat Si vous utilisez une carte à puce, sélectionnez le certificat sur la carte à puce.						
		Détails du certificat :						
ALC: NO PARTY OF ALC: N		Délivré à : Sophie Ribet Délivré par : arkema-WIN-CH1Y9QPIK Expiration : 23/06/2009	Afficher le certificat					
		Créer un certificat						
		Pourquoi ai-je besoin d'un certificat pour chiffrer mes fichiers ?						
			Suivant Annuler					

Pour plus d'informations sur EFS avec Windows Vista, voir les articles ci-dessous : <u>http://blog.windows.free.fr/index.php/tag/efs</u> http://technet.microsoft.com/fr-fr/magazine/cc162489(TechNet.10).aspx

Problème EFS avec Windows Vista : http://support.microsoft.com/kb/939391/fr

#### 4.5 PRISE EN CHARGE DU MUI DANS WINDOWS VISTA :

Les versions Entreprise et Ultimate de Windows Vista sont MUI. Il est possible d'installer des packs de langues et basculer très rapidement d'une langue d'affichage à un autre. Pour plus d'informations : <u>http://technet2.microsoft.com/WindowsVista/en/library/85e289ca-9fd8-4963-b06a-</u> 5ecc457006c71033.mspx?mfr=true

#### 5 SE FORMER RAPIDEMENT AVEC WINDOWS VISTA :

Lire en priorité les STEP BY STEP de Windows Vista. Ils sont très bien faits. Ces derniers sont téléchargeables à l'adresse suivante : <u>http://www.microsoft.com/downloads/details.aspx?familyid=311f4be8-9983-4ab0-9685-f1bfec1e7d62&displaylang=en</u>

Consulter la bibiothèque Windows Vista en français (site technet) à l'adresse suivante : <u>http://technet2.microsoft.com/WindowsVista/fr/library/90a564b9-34af-4a6b-937f-</u> <u>324e1862244b1036.mspx?mfr=true</u>

Consulter aussi le guide de sécurité de Windows Vista à cette adresse: <u>http://www.microsoft.com/downloads/details.aspx?familyid=a3d1bbed-7f35-4e72-bfb5-</u> <u>b84a526c1565&displaylang=fr&Hash=Zt45%2bDwkQ4feoCLxf7cYg3ISoNL%2fT129Wz2MN</u> <u>UFS%2bvyuc3CfRZ71F5O0ojmwvoYpQo79Jdd6xo2w1KLnqj%2fc6Q%3d%3d</u> This document was created with Win2PDF available at <a href="http://www.win2pdf.com">http://www.win2pdf.com</a>. The unregistered version of Win2PDF is for evaluation or non-commercial use only.