SECURISATION DES SERVEURS REMOTE DESKTOP SERVERS (WINDOWS 2008 R2) :

1 OBJECTIFS :

- Sécuriser les serveurs Remote Desktop Service sous Windows 2008 R2.
- Empêcher les utilisateurs de copier des fichiers, d’éxécuter des commandes systèmes.
- Ne pas perturber le fonctionnement du système.
- Permettre aux administrateurs d’administrer le système sans restrictions.
- Permettre aux utilisateurs d’exécuter les programmes de la suite Office 2007.

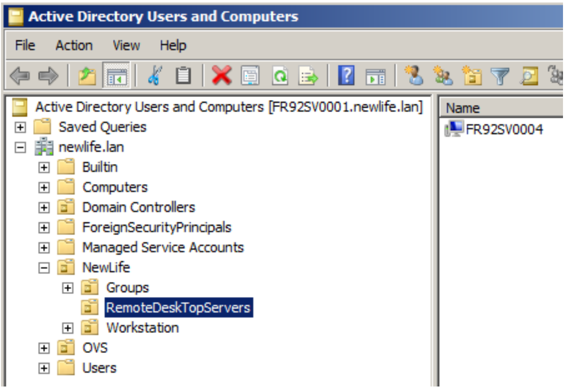
2 SECURISATION DU SERVEUR REMOTE DESKTOP SERVICE (WINDOWS 2008 R2) :

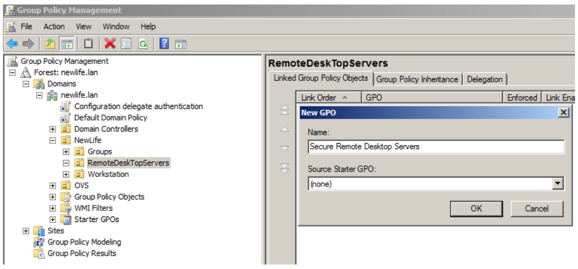
Pour cela, on va :

- Désactiver de nombreuses fonctionnalités de l'interface graphique via les stratégies de groupe.
- Bloquer l'exécution de toutes les applications sauf celles qui sont autorisées via Applocker.

2.1 DEPLACER LE SERVEUR REMOTE DESKTOP HOST SERVICE DANS L'OU REMOTEDESKTOPSERVER :

La première étape consiste à créer une unité d'organisation et de déplacer les comptes ordinateurs des serveurs *Remote DeskTop Services* dans cette unité d'organisation.





Name: Secure Remote Desktop Servers

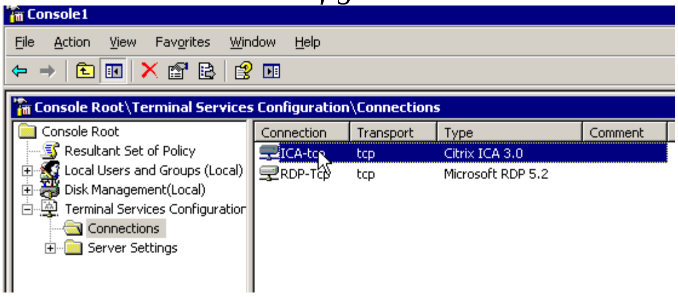
Source Starter GPO: (none)

Créer et lier un objet de stratégie de groupe au niveau de l'unité d'organisation « *RemoteDeskTopServers* » appelé « *Secure Remote Desktop Servers* » :

2.2 CONFIGURATION DES GPO POUR RESTREINDRE LES FONCTIONNALITES DE L’INTERFACE GRAPHIQUE :

Pour sécuriser le serveur *Remote DeskTop Service*, il faut :

- Désactiver le presse papier et le mappage de lecteur réseau au niveau de la console MMC « *Terminal Services Configuration* ».


Console1
File Action View Favorites Window Help
Console Root\Terminal Services Configuration\Connections
Console Root
Resultant Set of Policy
Local Users and Groups (Local)
Disk Management(Local)
Terminal Services Configuratior
Connections
Server Settings

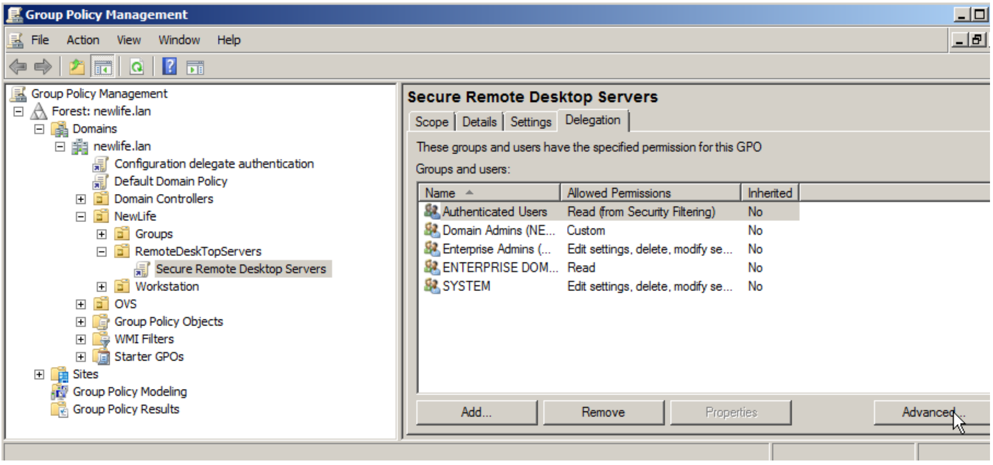
Connection	Transport	Type	Comment
ICA-tcp	tcp	Citrix ICA 3.0	
RDP-Tcp	tcp	Microsoft RDP 5.2	

- Bloquer l’accès à CMD par GPO :
- Bloquer l’accès à certains programmes depuis l’aide : « *Configuration ordinateur | Modèles d’administration | Systèmes | Restreindre l’exécution de ces programmes depuis l’aide en ligne*».
- Bloquer l’accès à l’invite de commande : Configuration Utilisateurs | Modèles d’administration | Système | Désactiver l’accès à l’invite de commande.
- Définir la liste des applications autorisées : Configuration Utilisateurs | Modèles d’administration | Système | Exécuter seulement les applications Windows autorisées.
- Activer l’interface de l’utilisateur personnalisée : Configuration Utilisateurs | Modèles d’administration | Système | Interface Utilisateur personnalisée.
- Empêcher l’accès aux outils de modification du registre : Configuration Utilisateurs | Modèles d’administration | Système | Empêche l’accès aux outils de modification du registre.
- Configurer la GPO pour que les GPO de type « Configuration Utilisateur » s’applique à un compte ordinateur.
- Restreindre l’accès à certaines fonctionnalités / menu dans les programmes Office via GPO (utilisation ADM Office).
- Activer le pare feu de Windows 2008 R2 pour bloquer tous les accès sauf aux contrôleurs de domaine.
- Appliquer les préconisations des articles suivants :
  http://support.microsoft.com/kb/278295/en-us
  http://www.microsoft.com/downloads/en/details.aspx?FamilyID=7f272fff-9a6e-40c7-b64e-7920e6ae6a0d&DisplayLang=en

Il n’y a plus de visionneuse des fichiers d’aide par défaut sous Windows 2008 R2 : http://support.microsoft.com/kb/917607/en-us

2.3 BLOQUER L’APPLICATION DES GPO AUX ADMINISTRATEURS DU SERVEUR :

Afin que les administrateurs puissent gérer le serveur, interdire l’application de la GPO aux groupes correspondant aux administrateurs du serveur (administrateurs du domaine dans l’exemple ci-dessous) :



Group Policy Management

- Group Policy Management
  - Forest: newlife.lan
    - Domains
      - newlife.lan
        - Configuration delegate authentication
        - Default Domain Policy
        - Domain Controllers
        - NewLife
          - Groups
          - RemoteDeskTopServers
            - Secure Remote Desktop Servers
          - Workstation
        - OVS
        - Group Policy Objects
        - WMI Filters
        - Starter GPOs
    - Sites
    - Group Policy Modeling
    - Group Policy Results

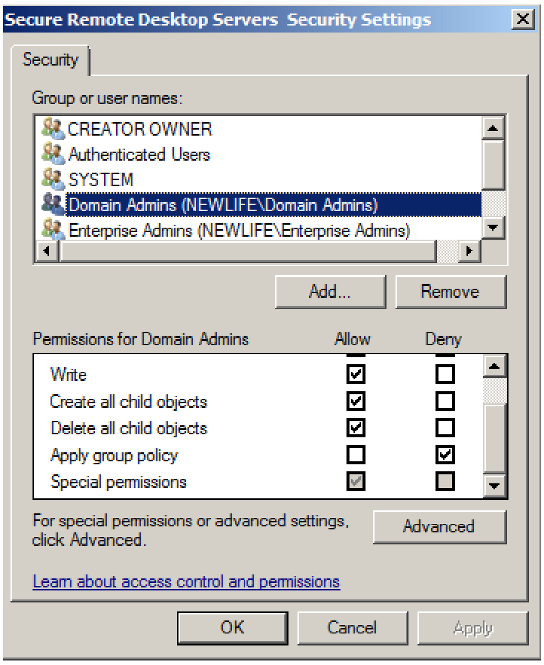
Secure Remote Desktop Servers

Scope | Details | Settings | Delegation

These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (NE...	Custom	No
Enterprise Admins (...	Edit settings, delete, modify se...	No
ENTERPRISE DOM...	Read	No
SYSTEM	Edit settings, delete, modify se...	No



Secure Remote Desktop Servers Security Settings

Security

Group or user names:

- CREATOR OWNER
- Authenticated Users
- SYSTEM
- Domain Admins (NEWLIFE\Domain Admins)
- Enterprise Admins (NEWLIFE\Enterprise Admins)

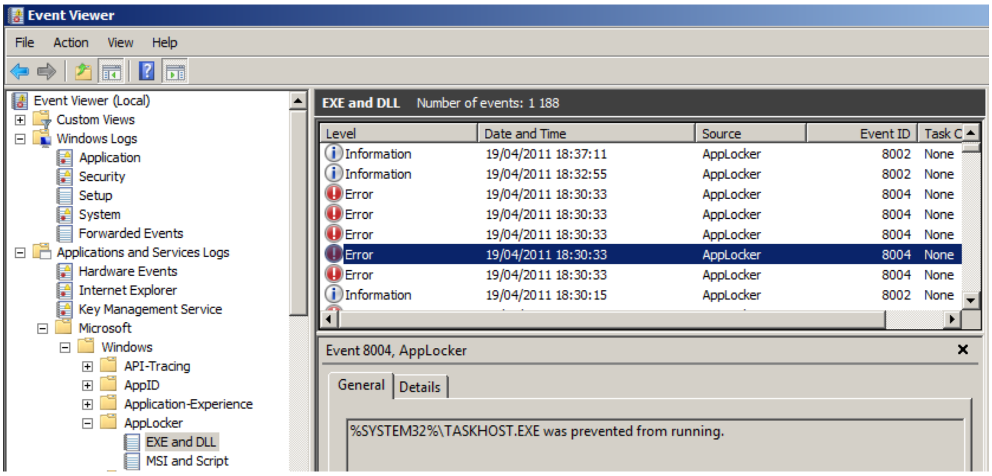
Permissions for Domain Admins	Allow	Deny
Write	☑	□
Create all child objects	☑	□
Delete all child objects	☑	□
Apply group policy	□	☑
Special permissions	☑	□

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

2.4 A SAVOIR SUR APPLOCKER :

- Le mode de fonctionnement d'AppLocker est « *Tout interdire sauf* ». Lorsque l'on crée la première règle AppLocker, on crée indirectement la règle par défaut (non configurable), tout interdire.
- AppLocker ne gère pas les application posix ou le sous système 16 bits. Il faut donc bloquer ces deux sous systèmes. Voir stratégie *Computerconfiguration/Administrative Templates/Windows-Components/Applicationcompatibility* et activer le paramètre « *Deny access to 16bit applications* ».
- Il y a un journal de sécurité dédié pour Applocker dans Windows 2008 R2. Cela peut être pratique pour déterminer les exécutables qui sont nécessaires aux bons fonctionnement de vos applications.



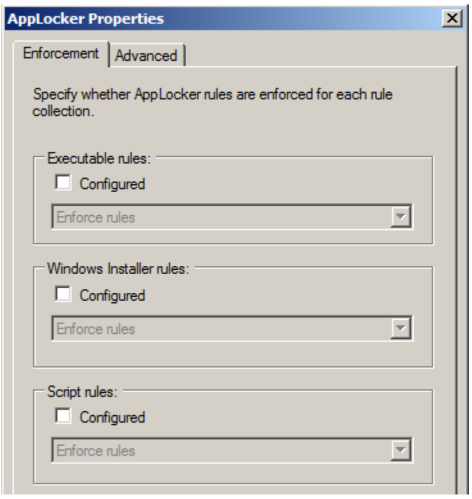
EXE and DLL Number of events: 1 188

Level	Date and Time	Source	Event ID	Task C
Information	19/04/2011 18:37:11	AppLocker	8002	None
Information	19/04/2011 18:32:55	AppLocker	8002	None
Error	19/04/2011 18:30:33	AppLocker	8004	None
Error	19/04/2011 18:30:33	AppLocker	8004	None
Error	19/04/2011 18:30:33	AppLocker	8004	None
Error	19/04/2011 18:30:33	AppLocker	8004	None
Error	19/04/2011 18:30:33	AppLocker	8004	None
Information	19/04/2011 18:30:15	AppLocker	8002	None

Event 8004, AppLocker

%SYSTEM32%\TASKHOST.EXE was prevented from running.

- Il est possible de configurer Applocker en mode Audit uniquement. Attention la configuration par défaut est en mode appliqué.



Specify whether AppLocker rules are enforced for each rule collection.

Executable rules:
☐ Configured
Enforce rules

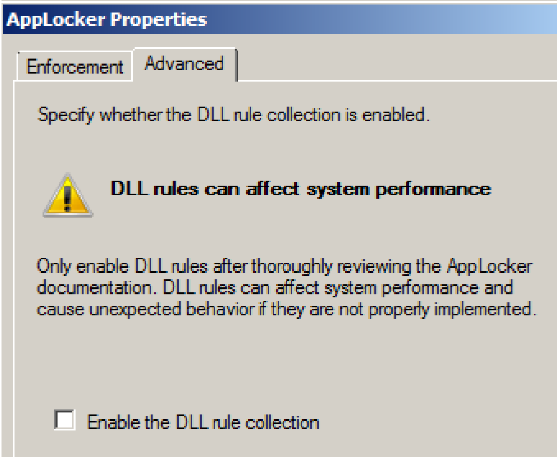
Windows Installer rules:
☐ Configured
Enforce rules

Script rules:
☐ Configured
Enforce rules

- Surveiller la présence des erreurs *Microsoft-Windows-AppLocker* 8004. Elles permettent de savoir quels sont les applications qui sont interdites. Il faut ensuite identifier si c'est normal que cette soit interdite ou non.

```
Log Name:     Microsoft-Windows-AppLocker/EXE and DLL
Source:       Microsoft-Windows-AppLocker
Date:         19/04/2011 19:21:15
Event ID:     8004
Task Category: None
Level:        Error
Keywords:
User:         SYSTEM
Computer:     fr92sv0004.newlife.lan
Description:
%SYSTEM32%\TASKHOST.EXE was prevented from running.
```

- AppLocker gère les formats de fichiers suivants : Les formats pris en charge :
  - Exe : via règles « *Executables Rules* »
  - Com : via règles « *Executables Rules* »
  - Msi : via règles « *Windows Installer* »
  - Msp : via règles « *Windows Installer* »
  - ps1 : via règles « *Script Rules* »
  - bat : via règles « *Script Rules* »
  - cmd : via règles « *Script Rules* »
  - vbs : via règles « *Script Rules* »
  - js: via règles « *Script Rules* »
  - dll : si la case « Enable the dll rule collection » est coché. Attention au performance. Il sera aussi nécessaire de savoir quels sont les DLL utilisés par les applications (très dangereux).


AppLocker Properties

Specify whether the DLL rule collection is enabled.

DLL rules can affect system performance

Only enable DLL rules after thoroughly reviewing the AppLocker documentation. DLL rules can affect system performance and cause unexpected behavior if they are not properly implemented.

☐ Enable the DLL rule collection

- Si un Applocker ne peut pas vérifier le certificat d'une application autorisée à l'aide d'une règle « Publisher », l'application est interdite.

"*If the application's certificate expires while the rule is enforced, the binary file will be blocked from running. A binary file is considered signed as long as the timestamp happened* *during the validity period of both the signing of the certificate and the time stamping of the certificates in the certificate chain.”*

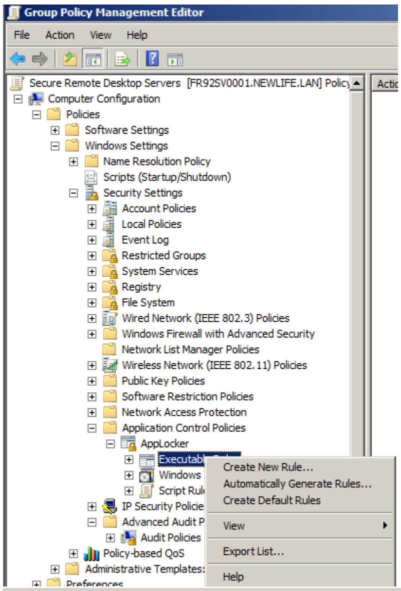
Pour plus d’informations sur Applocker :

- http://windowsteamblog.com/windows/b/springboard/archive/2009/08/18/understanding-windows-7-applocker.aspx
- http://technet.microsoft.com/en-us/library/dd723678(WS.10).aspx
- http://technet.microsoft.com/en-us/library/ee844118(WS.10).aspx
- http://technet.microsoft.com/en-us/library/ee619725(WS.10).aspx
- http://technet.microsoft.com/fr-fr/library/dd723686(WS.10).aspx
- http://www.windowsnetworking.com/articles_tutorials/Introduction-AppLocker-Part1.html
- http://www.windowsnetworking.com/articles_tutorials/Introduction-AppLocker-Part2.html
- http://www.windowsnetworking.com/articles_tutorials/Introduction-AppLocker-Part3.html
- http://www.windowsnetworking.com/articles_tutorials/Introduction-AppLocker-Part4.html
- http://technet.microsoft.com/en-us/windows/dd320283.aspx
- http://microsoftplatform.blogspot.com/2011_01_01_archive.html
- http://technet.microsoft.com/en-us/library/ee460956(WS.10).aspx
- http://technet.microsoft.com/en-us/library/ee460957(WS.10).aspx
- http://technet.microsoft.com/en-us/library/dd723678(WS.10).aspx
- http://microsoftplatform.blogspot.com/2011_01_01_archive.html
- http://64.4.11.252/en-us/library/ee619725(WS.10).aspx#BKMK_CertRevocation

2.5 MISE EN ŒUVRE D'APPLOCKER :

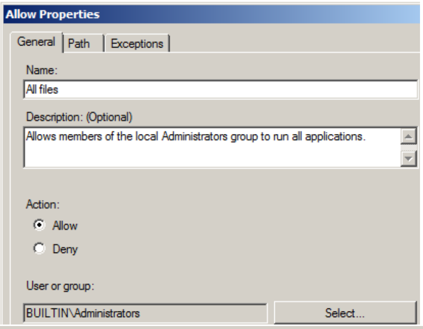
2.5.1 Etape 1 : créer et personnaliser les règles par défaut Applocker :

Editer l'objet de stratégie de groupe.
Créer les règles par défaut. Ce sont ces règles qui vont nous permettre aux systèmes de continuer à fonctionner correctement. Pour cela, cliquer sur « *Create Default rules* » dans les sections « *Executables Rules* », « *Windows Installer* » et « *Script Rules* ». On obtient à chaque fois trois règles autoriser.
Laisser uniquement la règle avec le groupe BUILTIN\Administrateurs (comprendre les comptes membres du groupe Administrators de la base SAM locale). En effet les règles pour les utilisateurs non administrateur sont trop permissives.



Group Policy Management Editor

Secure Remote Desktop Servers [FR92SV0001.NEWLIFE.LAN] Policy
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
        - Local Policies
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Policies
        - Windows Firewall with Advanced Security
        - Network List Manager Policies
        - Wireless Network (IEEE 802.11) Policies
        - Public Key Policies
        - Software Restriction Policies
        - Network Access Protection
        - Application Control Policies
          - AppLocker
            - Executabl
            - Windows
            - Script Rul
        - IP Security Policie
        - Advanced Audit P
          - Audit Policies
      - Policy-based QoS
    - Administrative Templates:
  - Preferences



Allow Properties

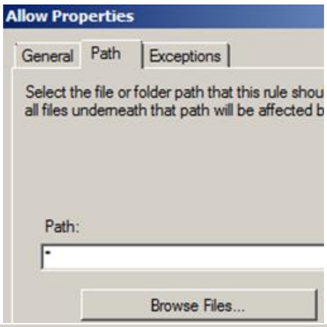
General | Path | Exceptions

Name: All files

Description: (Optional) Allows members of the local Administrators group to run all applications.

Action:
● Allow
○ Deny

User or group: BUILTIN\Administrators

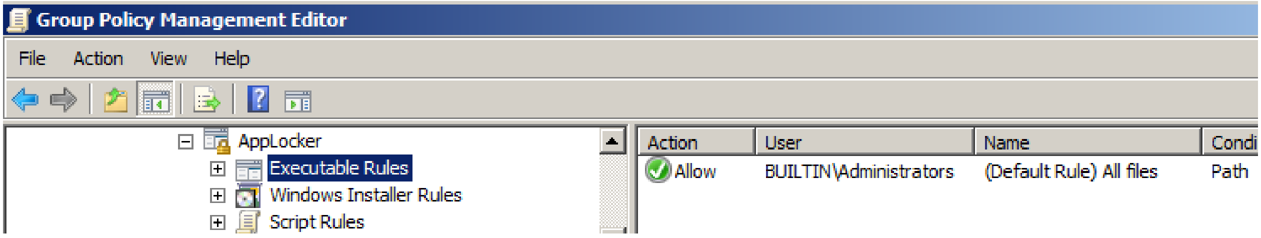


Allow Properties

General | Path | Exceptions

Select the file or folder path that this rule shou
all files underneath that path will be affected b

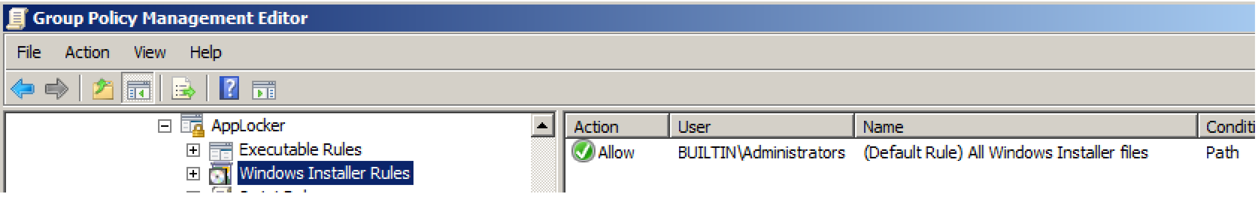
Path: *



Group Policy Management Editor

- AppLocker
  - Executable Rules
  - Windows Installer Rules
  - Script Rules

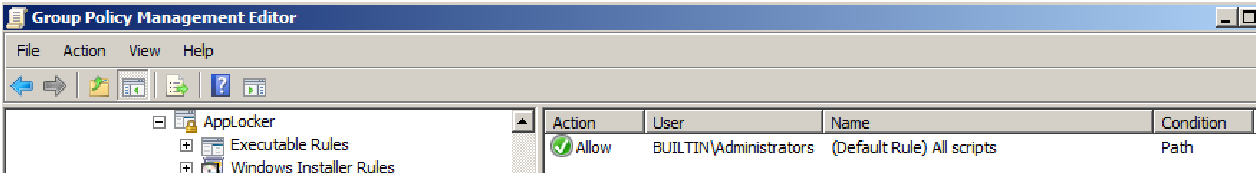
Action	User	Name	Condi
Allow	BUILTIN\Administrators	(Default Rule) All files	Path



Group Policy Management Editor

- AppLocker
  - Executable Rules
  - Windows Installer Rules

Action	User	Name	Condi
Allow	BUILTIN\Administrators	(Default Rule) All Windows Installer files	Path



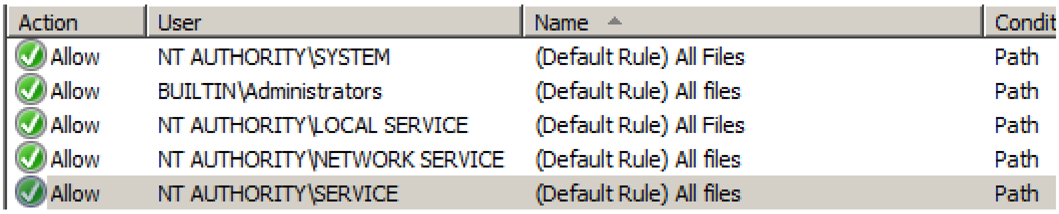
Group Policy Management Editor

- AppLocker
  - Executable Rules
  - Windows Installer Rules

Action	User	Name	Condition
Allow	BUILTIN\Administrators	(Default Rule) All scripts	Path

Créer une règle Autoriser tous les fichiers pour les comptes suivants (même règle que pour le groupe BUILTIN\Administrateurs) :

- NT AUTHORITY\SYSTEM
- NT AUTHORITY\LOCAL SERVICE
- NT AUTHORITY\NETWORK SERVICE
- NT AUTHORITY\NETWORK SERVICE
- NT AUTHORITY\SERVICE.



Action	User	Name	Condit
Allow	NT AUTHORITY\SYSTEM	(Default Rule) All Files	Path
Allow	BUILTIN\Administrators	(Default Rule) All files	Path
Allow	NT AUTHORITY\LOCAL SERVICE	(Default Rule) All Files	Path
Allow	NT AUTHORITY\NETWORK SERVICE	(Default Rule) All files	Path
Allow	NT AUTHORITY\SERVICE	(Default Rule) All files	Path

Remarque :

- Il peut être nécessaire d’autoriser d’autre entité de sécurité prédéfini comme IUSR

Le log ci-dessous semble indiquer que par défaut le compte SYSTEM n’a plus accès à tout.

```
Log Name:      Microsoft-Windows-AppLocker/EXE and DLL
Source:        Microsoft-Windows-AppLocker
Date:          20/04/2011 16:06:47
Event ID:      8004
Task Category: None
Level:         Error
Keywords:
User:          SYSTEM
Computer:      fr92sv0004.newlife.lan
Description:
%SYSTEM32%\CONHOST.EXE was prevented from running.
```

2.5.2 Etape 2 : Les exécutables systèmes à autoriser :

A cette étape, seuls les membres du groupe administrateurs et les comptes SYSTEM peuvent ouvrir une session sur le serveur. Si un utilisateur essaie d'ouvrir une session, cela échoue. La session se ferme car le processus userinit.exe ne peut pas s'exécuter correctement.
Le tableau ci-dessous liste les exécutables à autoriser pour le groupe « *Authenticated users* » :

Processus à autoriser pour « *Authenticated Users* »	**Rôle de ce processus**
%SYSTEM32%\DLLHOST.EXE	Permet de gérer les librairies virtuelles DLL : *http://www.commentcamarche.net/contents/processus/dllhost-exe.php3*
%WINDIR%\explorer.exe	Explorateur Windows
%SYSTEM32%\Userinit.exe	Processus qui initie la session de l'utilisateur. Charge l'explorateur Windows.
%SYSTEM32%\Dwm.exe	http://msdn.microsoft.com/en-us/library/aa969540(v=vs.85).aspx
%SYSTEM32%\gpupdate.exe	Permet d'actualiser les stratégies de groupe.
%SYSTEM32%\CONHOST.EXE :	Ce processus est obligatoire si l'on veut que l'utilisateur puisse exécuter un utilitaire en invite de commande comme GPUPDATE.
%SYSTEM32%\rdpclip.exe	Permet copier / coller entre le client RDS et le serveur RDS : http://support.microsoft.com/kb/309825/en-us
%SYSTEM32%\Rdpinit.exe	Dans le cadre d'une session RemoteApp, lance le processus RDPSHELL.EXE (une version mineur d'explorer.exe) : http://social.technet.microsoft.com/Forums/en/winserverTS/thread/845ac56d-a8c2-4188-96b2-6ae310b84011
%SYSTEM32%\Rdpshell.exe.	S'exécute à la place d'explorer.exe dans le cadre d'une session RemoteApp. http://support.microsoft.com/kb/2384602/en-us et http://blogs.technet.com/b/askperf/archive/2008/02/22/ws2008-terminal-services-remoteapps.aspx
%SYSTEM32%\RUNDLL32.EXE	Permet de charger des DLL comme un programme classique WIN32 : http://www.commentcamarche.net/contents/processus/rundll32-exe.php3
%SYSTEM32%\RUNONCE.EXE	Permet d'exécuter les programmes au démarrage de la session.
%SYSTEM32%\SETHC.EXE	Permet les fonctionnalités d'accessibilité (touches rémanentes…). http://support.microsoft.com/kb/2516889/en-us
%SYSTEM32%\SLUI.EXE	Activation Windows
%WINDIR%\SPLWOW64 :	Si Windows 2008 R2 64 bits, permet l'exécution des programmes 32bit avec la couche driver 64 bit : http://social.technet.microsoft.com/Forums/fr-

	FR/win7fr/thread/c62fb71c-f588-4ce6-875b-9c2bf452acc2/
%SYSTEM32%\TSTHEME.EXE	?
%SYSTEM32%\TASKHOST.EXE	Permet de lancer des DLL en tant que processus. http://answers.microsoft.com/en-us/windows/forum/windows_7-performance/taskhostexe/0882ab46-43ee-4d90-8404-6802f8f4f2cf
%SYSTEM32%\WERMGR.EXE	Windows Erreur Manager.
C:\WINDOWS\system32\ctfmon.exe	Ctfmon.exe active le TIP (Text Input Processor) des modes d'entrée complémentaires ainsi que la barre de langue Microsoft Office. http://support.microsoft.com/kb/282599/fr
C:\windows\system32\usrlogon.cmd	Script de login par défaut.
C:\WINDOWS\Application Compatibility Scripts	Script de login par défaut.
C:\WINDOWS\System32\logon.scr	Penser à autoriser les écrans de veille.
\\nom_dns_domaine\netlogon	Permet d’exécuter les scripts de login.
\\nom_dns_domaine\sysvol	Permet d’exécuter les scripts de login.
\\nom_netbios_domaine\netlogon	Permet d’exécuter les scripts de login.
\\nom_netbios_domaine\sysvol	Permet d’exécuter les scripts de login.
%logonserver%\netlogon	Permet d’exécuter les scripts de login.
%logonserver%\sysvol	Permet d’exécuter les scripts de login.
C:\Program Files\Citrix	Nécessaire si Citrix XenApp est installé sur le serveur Terminal Server
C:\Temp\*\getpaths.cmd	Applications Citrix

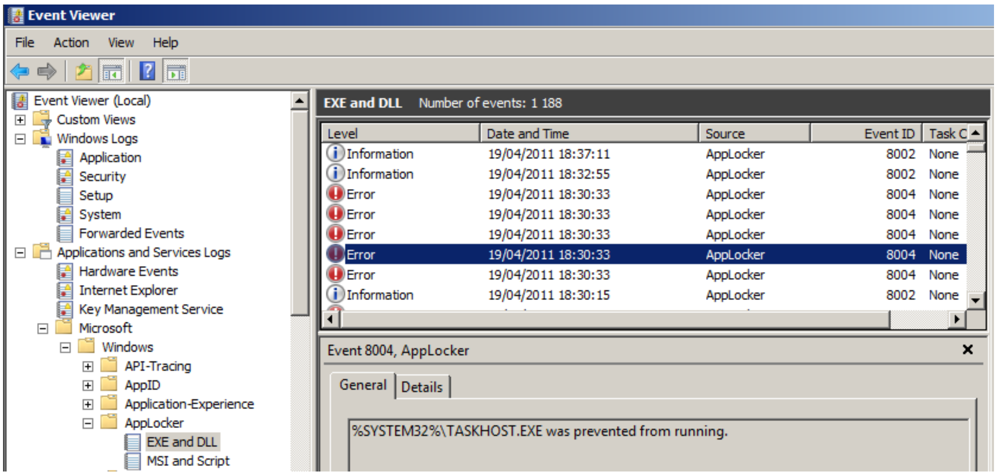
Remarques :

- Winlogon.exe (http://msdn.microsoft.com/en-us/library/Aa379434) s’exécute dans le contexte du compte SYSTEM. Ce n’est donc pas nécessaire de l’autoriser.
- Si l’on utilise une RemoteApp (publication d’une application via le serveur Remote DeskTop Service), il faut autoriser aussi les exécutables suivants Rdpinit.exe, Rdpshell.exe et rdpclip.exe.
- %SYSTEM32%\CONHOST.EXE : processus mère des consoles sous Windows 2008 R2. Voir : http://blogs.technet.com/b/askperf/archive/2009/10/05/windows-7-windows-server-2008-r2-console-host.aspx).
- Les Vmware Tools s’exécutent au démarrage d’une session utilisateur dans le contexte du compte utilisateur. A autoriser éventuellement (%PROGRAMFILES%\VMWARE\VMWARE TOOLS) s’il s’agit d’une machine virtuelle.

Pour plus d’informations, voir articles Microsoft :

- http://microsoftplatform.blogspot.com/2011/01/remote-control-rds-session-in-mixed_26.html
- http://blogs.technet.com/b/askperf/archive/2008/02/22/ws2008-terminal-services-remoteapps.aspx

Applocker dispose d’un journal de sécurité qui permet de savoir quels exécutables ont été autorisés ou bloqués. Le plus simple est d’exécuter les applications avec Applocker d’activer pour déterminer les applications à autoriser.



EXE and DLL Number of events: 1 188

Level	Date and Time	Source	Event ID	Task C
Information	19/04/2011 18:37:11	AppLocker	8002	None
Information	19/04/2011 18:32:55	AppLocker	8002	None
Error	19/04/2011 18:30:33	AppLocker	8004	None
Error	19/04/2011 18:30:33	AppLocker	8004	None
Error	19/04/2011 18:30:33	AppLocker	8004	None
Error	19/04/2011 18:30:33	AppLocker	8004	None
Error	19/04/2011 18:30:33	AppLocker	8004	None
Information	19/04/2011 18:30:15	AppLocker	8002	None

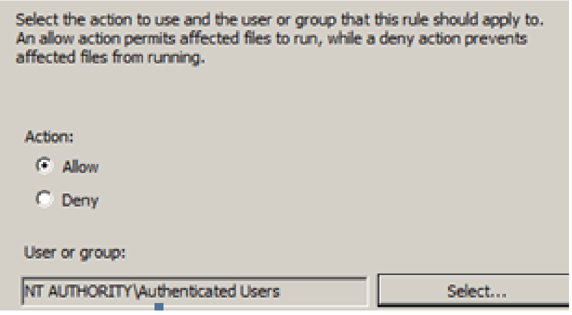
Event 8004, AppLocker

%SYSTEM32%\TASKHOST.EXE was prevented from running.

2.5.3 Etape 3 : Création des règles Applocker pour les « Authenticated users » :

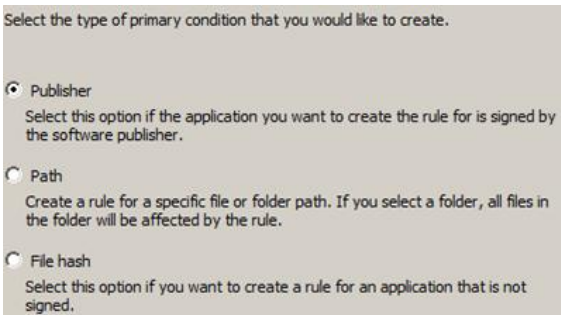
Avec AppLocker, on peut maintenant :

- Créer une règle qui s'applique à un utilisateurs ou à un groupe d'utilisateur.
- Créer des règles qui se basent sur les signatures numériques des programmes. La majorité des programmes sont maintenant signés par les éditeurs (à l'aide de certificat) afin de valider que le programme n'a pas été modifiés par un tiers et prouvé l'identité de l'éditeur (programme provenant d'un éditeur de confiance). Dans l'exemple ci-dessous j'autorise toutes les versions d'Explorer.exe qui sont supérieur à la version 6.0.
- Générer automatiquement des règles à l'aide de la fonctionnalité « *Generate Rules* » en scannant un répertoire.


Select the action to use and the user or group that this rule should apply to. An allow action permits affected files to run, while a deny action prevents affected files from running.

Action:
● Allow
○ Deny

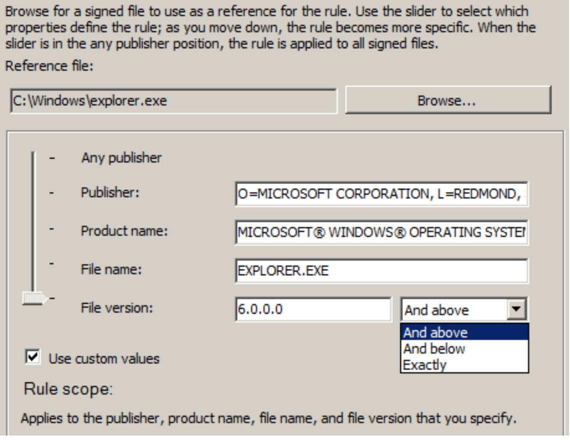
User or group:
NT AUTHORITY\Authenticated Users


Select the type of primary condition that you would like to create.

● Publisher
Select this option if the application you want to create the rule for is signed by the software publisher.

○ Path
Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule.

○ File hash
Select this option if you want to create a rule for an application that is not signed.

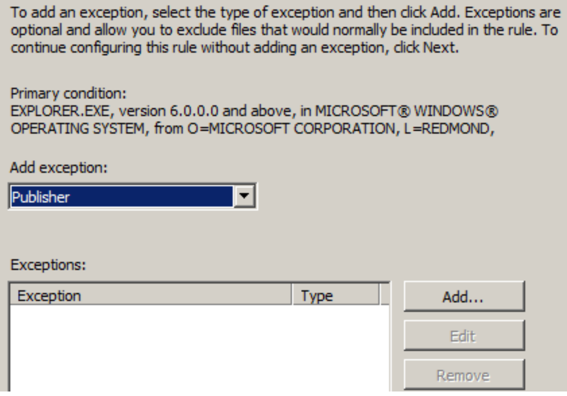

Browse for a signed file to use as a reference for the rule. Use the slider to select which properties define the rule; as you move down, the rule becomes more specific. When the slider is in the any publisher position, the rule is applied to all signed files.

Reference file:
C:\Windows\explorer.exe

Any publisher
Publisher: O=MICROSOFT CORPORATION, L=REDMOND,
Product name: MICROSOFT® WINDOWS® OPERATING SYSTEI
File name: EXPLORER.EXE
File version: 6.0.0.0 And above

☑ Use custom values

Rule scope:
Applies to the publisher, product name, file name, and file version that you specify.


To add an exception, select the type of exception and then click Add. Exceptions are optional and allow you to exclude files that would normally be included in the rule. To continue configuring this rule without adding an exception, click Next.

Primary condition:
EXPLORER.EXE, version 6.0.0.0 and above, in MICROSOFT® WINDOWS® OPERATING SYSTEM, from O=MICROSOFT CORPORATION, L=REDMOND,

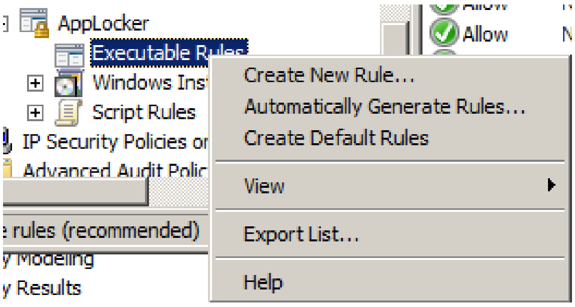
Add exception:
Publisher

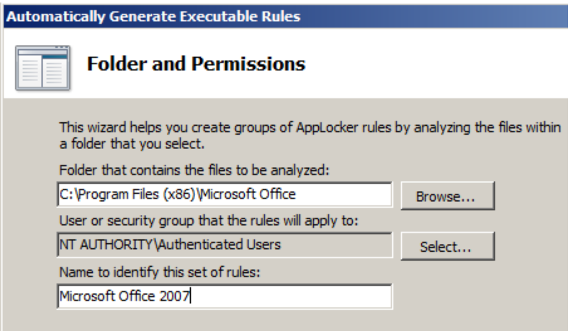
Exceptions:

Exception	Type

On va maintenant créer les règles pour permettre aux utilisateurs non administrateurs d’utiliser les programmes de la suite Office 2007.

Pour cela, on va utiliser la nouvelle fonction de création automatique des règles en cliquant sur « *Automatically Generate Rules* ».
On va demander à cet assistant de créer automatiquement des règles « *Publisher* » et de générer des règles de chemin d’accès pour les exécutables non signées.




Automatically Generate Executable Rules

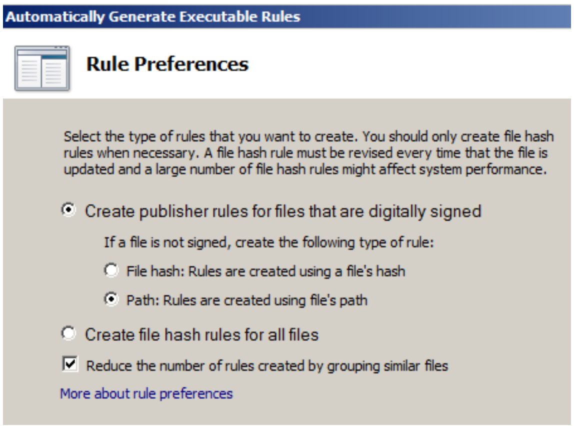
Folder and Permissions

This wizard helps you create groups of AppLocker rules by analyzing the files within a folder that you select.

Folder that contains the files to be analyzed: C:\Program Files (x86)\Microsoft Office [Browse…]

User or security group that the rules will apply to: NT AUTHORITY\Authenticated Users [Select…]

Name to identify this set of rules: Microsoft Office 2007


Automatically Generate Executable Rules

Rule Preferences

Select the type of rules that you want to create. You should only create file hash rules when necessary. A file hash rule must be revised every time that the file is updated and a large number of file hash rules might affect system performance.

● Create publisher rules for files that are digitally signed

If a file is not signed, create the following type of rule:

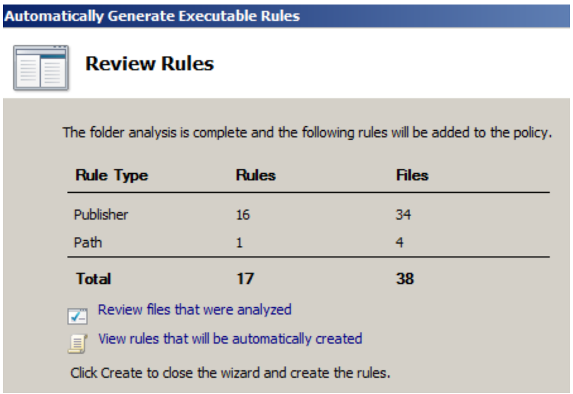
○ File hash: Rules are created using a file's hash

● Path: Rules are created using file's path

○ Create file hash rules for all files

☑ Reduce the number of rules created by grouping similar files

More about rule preferences


Automatically Generate Executable Rules

Review Rules

The folder analysis is complete and the following rules will be added to the policy.

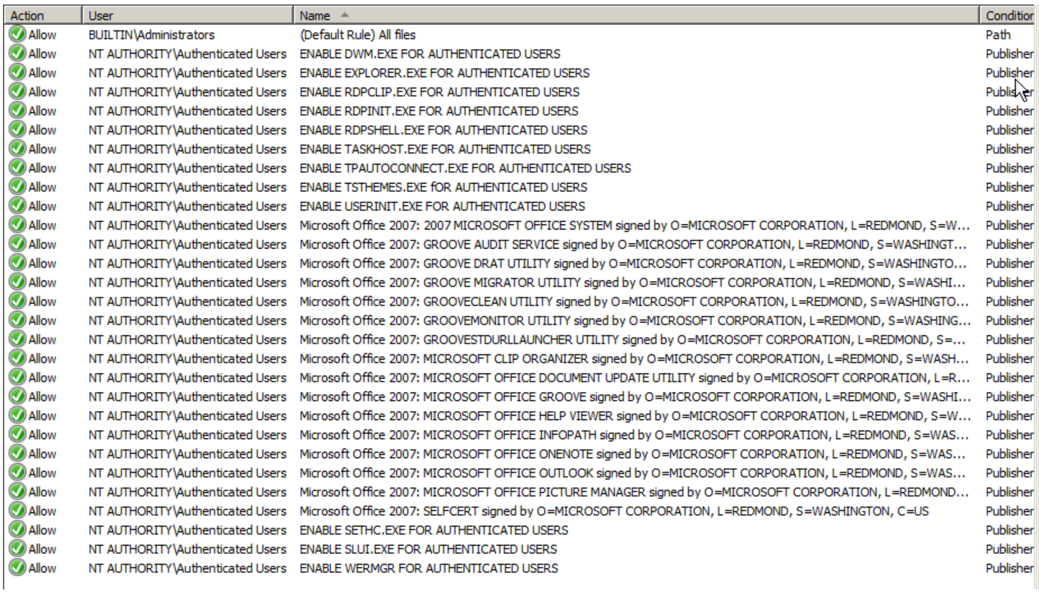
Rule Type	Rules	Files
Publisher	16	34
Path	1	4
Total	**17**	**38**

Review files that were analyzed

View rules that will be automatically created

Click Create to close the wizard and create the rules.

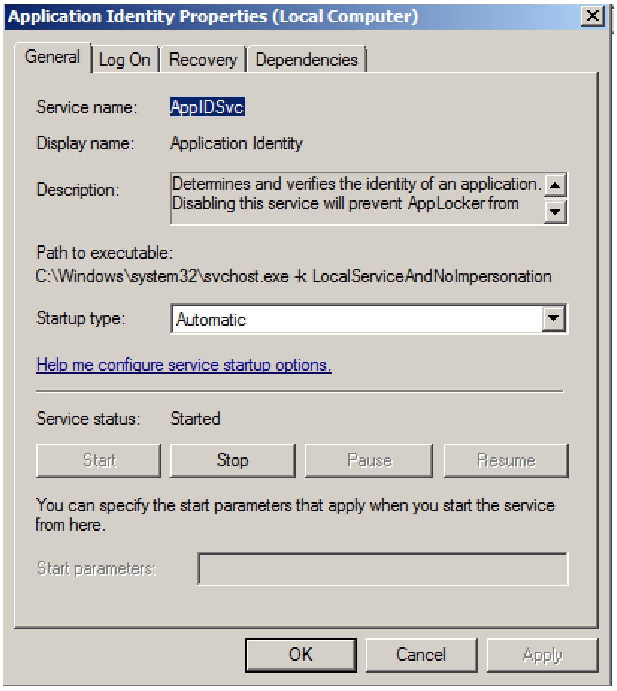
On va éventuellement supprimer tous les exécutables Office que l’on ne souhaite pas autoriser.
On obtient dans notre cas les règles suivantes.



Action	User	Name	Conditior
Allow	BUILTIN\Administrators	(Default Rule) All files	Path
Allow	NT AUTHORITY\Authenticated Users	ENABLE DWM.EXE FOR AUTHENTICATED USERS	Publisher
Allow	NT AUTHORITY\Authenticated Users	ENABLE EXPLORER.EXE FOR AUTHENTICATED USERS	Publisher
Allow	NT AUTHORITY\Authenticated Users	ENABLE RDPCLIP.EXE FOR AUTHENTICATED USERS	Publisher
Allow	NT AUTHORITY\Authenticated Users	ENABLE RDPINIT.EXE FOR AUTHENTICATED USERS	Publisher
Allow	NT AUTHORITY\Authenticated Users	ENABLE RDPSHELL.EXE FOR AUTHENTICATED USERS	Publisher
Allow	NT AUTHORITY\Authenticated Users	ENABLE TASKHOST.EXE FOR AUTHENTICATED USERS	Publisher
Allow	NT AUTHORITY\Authenticated Users	ENABLE TPAUTOCONNECT.EXE FOR AUTHENTICATED USERS	Publisher
Allow	NT AUTHORITY\Authenticated Users	ENABLE TSTHEMES.EXE fOR AUTHENTICATED USERS	Publisher
Allow	NT AUTHORITY\Authenticated Users	ENABLE USERINIT.EXE FOR AUTHENTICATED USERS	Publisher
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: 2007 MICROSOFT OFFICE SYSTEM signed by O=MICROSOFT CORPORATION, L=REDMOND, S=W…	Publisher
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: GROOVE AUDIT SERVICE signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGT…	Publisher
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: GROOVE DRAT UTILITY signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTO…	Publisher
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: GROOVE MIGRATOR UTILITY signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHI…	Publisher
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: GROOVECLEAN UTILITY signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTO…	Publisher
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: GROOVEMONITOR UTILITY signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHING…	Publisher
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: GROOVESTDURLLAUNCHER UTILITY signed by O=MICROSOFT CORPORATION, L=REDMOND, S=…	Publisher
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: MICROSOFT CLIP ORGANIZER signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASH…	Publisher
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: MICROSOFT OFFICE DOCUMENT UPDATE UTILITY signed by O=MICROSOFT CORPORATION, L=R…	Publisher
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: MICROSOFT OFFICE GROOVE signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHI…	Publisher
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: MICROSOFT OFFICE HELP VIEWER signed by O=MICROSOFT CORPORATION, L=REDMOND, S=W…	Publisher
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: MICROSOFT OFFICE INFOPATH signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WAS…	Publisher
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: MICROSOFT OFFICE ONENOTE signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WAS…	Publisher
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: MICROSOFT OFFICE OUTLOOK signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WAS…	Publisher
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: MICROSOFT OFFICE PICTURE MANAGER signed by O=MICROSOFT CORPORATION, L=REDMOND…	Publisher
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: SELFCERT signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher
Allow	NT AUTHORITY\Authenticated Users	ENABLE SETHC.EXE FOR AUTHENTICATED USERS	Publisher
Allow	NT AUTHORITY\Authenticated Users	ENABLE SLUI.EXE FOR AUTHENTICATED USERS	Publisher
Allow	NT AUTHORITY\Authenticated Users	ENABLE WERMGR FOR AUTHENTICATED USERS	Publisher

2.5.4 Etape 4 : Configurer le service « *Application Identity* » :

Il faut maintenant configurer le service « *Application Identity* » pour démarrer automatiquement. Sans ce service AppLocker ne fonctionne pas.
On peut faire cela manuellement ou mieux par GPO (interface grisée dans la console services.msc).


Application Identity Properties (Local Computer)
General
Log On
Recovery
Dependencies

Service name: AppIDSvc

Display name: Application Identity

Description: Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from

Path to executable:
C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation

Startup type: Automatic

Help me configure service startup options.

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

3 DETAILS DE L'OBJET STRATEGIE DE GROUPE :

Secure Remote Desktop Servers

Data collected on: 02/05/2011
10:27:21

hide all

Generalhide

Detailshide

Domain	newlife.lan
Owner	NEWLIFE\Domain Admins
Created	19/04/2011 16:14:06
Modified	02/05/2011 10:27:02
User Revisions	85 (AD), 85 (sysvol)
Computer Revisions	80 (AD), 80 (sysvol)
Unique ID	{50CC4421-34C1-4A73-AAFA-ECA6298D5C11}
GPO Status	Enabled

Linkshide

Location	Enforced	Link Status	Path
RemoteDeskTopServers	No	Enabled	newlife.lan/NewLife/RemoteDeskTopServers

This list only includes links in the domain of the GPO.

Security Filteringhide

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

Delegationhide

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
NEWLIFE\Domain Admins	Custom	No
NEWLIFE\Enterprise Admins	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled)hide

Policieshide

Windows Settingshide

Security Settingshide

Local Policies/Security Optionshide

Deviceshide

Policy	Setting
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled
Devices: Restrict floppy access to locally logged-on user only	Enabled

Interactive Logonhide

Policy	Setting
Interactive logon: Do not display last user name	Enabled

System Serviceshide

Application Identity (Startup Mode: Automatic)hide

Permissions

No permissions specified

Auditing

No auditing specified

Application Control Policieshide

Dll Ruleshide

No rules of type 'Dll Rules' are defined.

Executable Ruleshide

Action	User	Name	Rule Type	Exceptions
Allow	NT AUTHORITY\Authenticated Users	ENABLE USERINIT.EXE FOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	ENABLE WERMGR FOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: GROOVESTDURLLAUNCHER UTILITY signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	ENABLE DLLHOST.EXE FOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: MICROSOFT OFFICE ONENOTE signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: GROOVE DRAT UTILITY signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: GROOVEMONITOR UTILITY signed by O=MICROSOFT CORPORATION, L=REDMOND,	Publisher	No

		S=WASHINGTON, C=US		
Allow	NT AUTHORITY\Authenticated Users	ENABLE RDPINIT.EXE FOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: MICROSOFT OFFICE PICTURE MANAGER signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	ENABLE RDPSHELL.EXE FOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: 2007 MICROSOFT OFFICE SYSTEM signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	ENABLE TPAUTOCONNECT.EXE FOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: MICROSOFT OFFICE GROOVE signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	ENABLE RUNDLL32.EXE FOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: GROOVE MIGRATOR UTILITY signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	ENABLE EXPLORER.EXE FOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	ENABLE TASKHOST.EXE FOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\Authenticated	ENABLE DWM.EXE FOR	Publisher	No

	Users	AUTHENTICATED USERS		
Allow	NT AUTHORITY\Authenticated Users	ENABLE RDPCLIP.EXE FOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: GROOVE AUDIT SERVICE signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	ENABLE SLUI.EXE FOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: MICROSOFT OFFICE DOCUMENT UPDATE UTILITY signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	ENABLE RUNONCE.EXE FOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: MICROSOFT OFFICE HELP VIEWER signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	ENABLE SPLWOW64.EXE FOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: MICROSOFT CLIP ORGANIZER signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	ENABLE TSTHEMES.EXE fOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: MICROSOFT OFFICE	Publisher	No

		OUTLOOK signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US		
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: SELFCERT signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	ENABLE VMWARE TOOLS FOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	ENABLE GPUPDATE FOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: MICROSOFT OFFICE INFOPATH signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	Microsoft Office 2007: GROOVECLEAN UTILITY signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Publisher	No
Allow	NT AUTHORITY\Authenticated Users	ENABLE SETHC.EXE FOR AUTHENTICATED USERS	Publisher	No
Allow	NT AUTHORITY\SERVICE	(Default Rule) All files	Path	No
Allow	NT AUTHORITY\SYSTEM	(Default Rule) All Files	Path	No
Allow	NT AUTHORITY\LOCAL SERVICE	(Default Rule) All Files	Path	No
Allow	NT AUTHORITY\NETWORK SERVICE	(Default Rule) All files	Path	No
Allow	BUILTIN\Administrators	(Default Rule) All files	Path	No

Windows Installer Ruleshide

Action	User	Name	Rule Type	Exceptions

Allow	BUILTIN\Administrators	(Default Rule) All Windows Installer files	Path	No

Script Ruleshide

Action	User	Name	Rule Type	Exceptions
Allow	BUILTIN\Administrators	(Default Rule) All scripts	Path	No

Administrative Templateshide

Policy definitions (ADMX files) retrieved from the local machine.

System/Device Installationhide

Policy	Setting	Comment
Do not send a Windows error report when a generic driver is installed on a device	Enabled	
Prevent Windows from sending an error report when a device driver requests additional software during installation	Enabled	

System/Group Policyhide

Policy	Setting	Comment
User Group Policy loopback processing mode	Enabled	

Mode:	Replace

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Device and Resource Redirectionhide

Policy	Setting	Comment
Do not allow clipboard redirection	Enabled	
Do not allow COM port redirection	Enabled	
Do not allow drive redirection	Enabled	
Do not allow LPT port redirection	Enabled	
Do not allow smart card device redirection	Enabled	
Do not allow supported Plug and Play device redirection	Enabled	

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Printer Redirectionhide

Policy	Setting	Comment
Redirect only the default client printer	Enabled	
Use Remote Desktop Easy Print printer driver first	Enabled	

Windows Components/Windows Installerhide

Policy	Setting	Comment
Disable Windows Installer	Enabled	

Disable Windows Installer	Always

User Configuration (Enabled)hide

Policieshide

Administrative Templateshide

Policy definitions (ADMX files) retrieved from the local machine.

Control Panelhide

Policy	Setting	Comment
Prohibit access to the Control Panel	Enabled	

Desktophide

Policy	Setting	Comment
Hide Internet Explorer icon on desktop	Enabled	
Hide Network Locations icon on desktop	Enabled	
Prevent adding, dragging, dropping and closing the Taskbar's toolbars	Enabled	
Remove Computer icon on the desktop	Enabled	
Remove My Documents icon on the desktop	Enabled	
Remove Properties from the Computer icon context menu	Enabled	
Remove Properties from the Documents icon context menu	Enabled	
Remove Recycle Bin icon from desktop	Enabled	
Remove the Desktop Cleanup Wizard	Enabled	

Start Menu and Taskbarhide

Policy	Setting	Comment
Add Logoff to the Start Menu	Enabled	
Lock all taskbar settings	Enabled	
Lock the Taskbar	Enabled	
Remove access to the context menus for the taskbar	Enabled	
Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands	Enabled	
Remove Balloon Tips on Start Menu items	Enabled	
Remove Help menu from Start Menu	Enabled	
Remove Homegroup link from Start Menu	Enabled	
Remove links and access to Windows	Enabled	

Update		
Remove Music icon from Start Menu	Enabled	
Remove Network Connections from Start Menu	Enabled	
Remove Network icon from Start Menu	Enabled	
Remove Pictures icon from Start Menu	Enabled	
Remove pinned programs list from the Start Menu	Enabled	
Remove Recorded TV link from Start Menu	Enabled	
Remove Run menu from Start Menu	Enabled	
Remove Search Computer link	Enabled	
Remove Search link from Start Menu	Enabled	
Remove the Action Center icon	Enabled	
Remove Videos link from Start Menu	Enabled	
Turn off personalized menus	Enabled	

Systemhide

Policy	Setting	Comment
Don't display the Getting Started welcome screen at logon	Enabled	
Prevent access to registry editing tools	Enabled	

Disable regedit from running silently?	Yes

Policy	Setting	Comment
Prevent access to the command prompt	Enabled	

Disable the command prompt script processing also?	Yes

Policy	Setting	Comment
Restrict these programs from being launched from Help	Enabled	

Enter executables separated by commas:	*
Example: calc.exe,paint.exe	

System/Ctrl+Alt+Del Optionshide

Policy	Setting	Comment
Remove Task Manager	Enabled	

System/Scriptshide

Policy	Setting	Comment
Run legacy logon scripts hidden	Enabled	

Windows Components/Application Compatibilityhide

Policy	Setting	Comment
Prevent access to 16-bit applications	Enabled	
Turn off Program Compatibility Assistant	Enabled	

Windows Components/Internet Explorerhide

Policy	Setting	Comment
Prevent Internet Explorer Search box from displaying	Enabled	
Search: Disable Find Files via F3 within the browser	Enabled	
Turn on menu bar by default	Enabled	

Windows Components/Internet Explorer/Browser menushide

Policy	Setting	Comment
Disable Context menu	Enabled	
Disable Open in New Window menu option	Enabled	
Disable Save this program to disk option	Enabled	
File menu: Disable New menu option	Enabled	
File menu: Disable Open menu option	Enabled	
File menu: Disable Save As Web Page Complete	Enabled	
File menu: Disable Save As... menu option	Enabled	
Help menu: Remove 'For Netscape Users' menu option	Enabled	
Help menu: Remove 'Send Feedback' menu option	Enabled	
Help menu: Remove 'Tip of the Day' menu option	Enabled	
Help menu: Remove 'Tour' menu option	Enabled	
Tools menu: Disable Internet Options... menu option	Enabled	

Windows Components/Task Schedulerhide

Policy	Setting	Comment
Hide Advanced Properties Checkbox in Add Scheduled Task Wizard	Enabled	
Hide Property Pages	Enabled	
Prevent Task Run or End	Enabled	

Prohibit Browse	Enabled
Prohibit Drag-and-Drop	Enabled
Prohibit New Task Creation	Enabled
Prohibit Task Deletion	Enabled

Windows Components/Windows Explorerhide

Policy	Setting	Comment
Display the menu bar in Windows Explorer	Enabled	
Do not display the Welcome Center at user logon	Enabled	
Hide these specified drives in My Computer	Enabled	

Pick one of the following combinations	Restrict all drives

Policy	Setting	Comment
Hides the Manage item on the Windows Explorer context menu	Enabled	
No Computers Near Me in Network Locations	Enabled	
No Entire Network in Network Locations	Enabled	
Prevent access to drives from My Computer	Enabled	

Pick one of the following combinations	Restrict all drives

Policy	Setting	Comment
Prevent users from adding files to the root of their Users Files folder.	Enabled	
Remove "Map Network Drive" and "Disconnect Network Drive"	Enabled	
Remove File menu from Windows Explorer	Enabled	
Remove Hardware tab	Enabled	
Remove Search button from Windows Explorer	Enabled	
Remove Security tab	Enabled	
Remove Windows Explorer's default context menu	Enabled	

Removes the Folder Options menu item from the Tools menu	Enabled	
Request credentials for network installations	Enabled	
Turn off common control and window animations	Enabled	
Turn off Windows+X hotkeys	Enabled	

Windows Components/Windows Messengerhide

Policy	Setting	Comment
Do not allow Windows Messenger to be run	Enabled	
Do not automatically start Windows Messenger initially	Enabled	