http://www.lolokai.com/blog/2012/05/14/restriction-logicielle-avec-applocker/

# **Restriction logicielle avec** AppLocker

taochy.samuel

14 mai 2012

## Introduction

Après la mise en place de DNS, DHCP, WSUS... Je vous propose aujourd'hui de voir ensemble AppLocker ou une solution de restriction logicielle sous Windows.

Une des tâches pour un administrateur dans une entreprise, est de savoir contrôler les logiciels qui s'exécutent sur les machines. Je m'explique, il est indispensable d'un point de vue sécurité que l'administrateur n'autorise pas l'utilisation et l'installation de n'importe quels logiciels. Or l'administrateur ne peut contrôler physiquement l'ajout de logiciel par les utilisateurs car il faudrait être derrière chaque postes. Depuis XP il existe des solutions appelées « Sofware Restriction Policy ». Très peu populaires car elle ne sont pas réellement complètes et simple d'utilisation elles ont été remplacées par AppLocker depuis Windows 7 et Windows Server 2008 R2. AppLocker va simplifier la vie de l'administrateur car grâce au stratégie de groupe il pourra configurer AppLocker pour restreindre l'utilisation et l'installation des logiciels.

Je ne vous en dis pas plus et vous propose de découvrir cette solution avec moi.

### Installation

Pour cet article j'ai utilisé une machine sous Windows Server 2008 R2 contrôleur de domaine et une machine Windows 7 appartenant à ce domaine.

1 sur 7

itz controleur de domaine et une machine windows / appartenant à ce domaine.

Pour commencer on va utiliser une stratégie de groupe déjà créée et y configurer notre AppLocker. Personnellement j'ai créé une stratégie « Restriction logicielle ». Pour configurer clique droit sur la stratégie -> Modifier.



Une fois arrivé sur la fenêtre « Editeur de gestion des stratégies de groupe » il faut trouver AppLocker pour cela Configuration Ordinateur -> Stratégies -> Paramètre Windows -> Paramètre de sécurité -> Stratégie de controle de l'application -> AppLocker.



Maintenant on va s'intéresser aux types de règles. Sous AppLocker il est possible de trouver 3 types de règles:

Règle de l'exécutable: On va créer une règle pour un

fichier exécutable un .exe, .com...

Règles Windows Installer: On va créer une règle pour un fichier .msi.

tichier executable un .exe, .com...

Règles Windows Installer: On va créer une règle pour un fichier .msi.

Règle de Script: On va créer une règle basé sur un script.

Pour commencer nous allons créer des règles d'exécutables par défaut. Pour cela clique droit sur Règle de l'exécutable -> Règles par défaut.

#### /!\ Sachez que par défaut tout ce qui n'est pas autorisé est interdit /!\



Nous avons 3 règles qui ont été créées.

La première règle permet à tous les utilisateurs du domaine d'exécuter les logiciels présents dans le répertoire « Program Files »

La seconde règle permet à tous les utilisateurs du domaine d'exécuter les logiciels présents dans le répertoire « Windows »

La dernière règles permet au groupe Administrateurs d'exécuter toutes les applications.



Maintenant nous avons vu ce qu'est une règle sous AppLocker, je vous propose d'en customiser une. Pour cela, je vous propose de prendre la règle par défaut autorisant les administrateurs à exécuter toutes les applications. On va créer une exception. Imaginons nous sommes en entreprise, celle-ci possède déjà une solution de VoIP et refuse d'utiliser une solution comme Skype. Pour cela nous allons créer une exception dans la règle qui autorise lles Administrateurs d'exécuter toutes les applications.



#### -> Double clique sur la règle -> Onglet Exception.

Il y a 3 moyens de créer des exceptions :

Via l'éditeur: c'est à dire qu'on ajoute une exception en utilisant la signature électronique de l'application. <RECOMMANDÉE>

Via le chemin d'accès: c'est à dire qu'on ajoute une exception en utilisant le chemin d'un répertoire. La règle va s'appliquer dans tout le répertoire.

Via le Hash: c'est à dire onajoute une exception en utilisant le hash de fichier d'installation vu qu'un exécutable a un hash unique on peut créer une exception en stipulant le hash du fichier.

De notre côté nous allons suivre les recommandations Microsoft et créer une exception via l'éditeur. Pour cela procurez-vous l'installation de Skype et sélectionnez Editeur. Puis, faites Ajouter et Sélectionnez l'exécutable de Skype.

05/10/2016 20:03

4 sur 7

EACEPTION VIA LEUTEUL. LOUL CEIA PLOCULEZ-VOUS LITSTANATION DE ORYPE EL sélectionnez Editeur. Puis, faites Ajouter et Sélectionnez l'exécutable de Skype. Une fois arrivé à l'éditeur faites parcourir et choisissez l'installation de Skype.

	And the state of the second se	0.7		* 10 ( 10 min 10 min 10 min 10 min	
•					
	F Section (1997)		ten fastes		-
				<u> </u>	

Une fois fait, il récupère la signature de Skype, l'éditeur donc « Skype » et le nom du fichier et sa version. Nous allons nous arrêter sur la fenêtre de l'éditeur car il nous propose de faire pas mal de choses.



Tout d'abord à gauche, il y a un curseur qui balait soit version, soit nom du fichier, soit nom de l'éditeur ou soit Tout éditeur. Cela nous permet de gérer le niveau d'exception qu'on veut mettre.

Version du fichier: Stipule la version du fichier qui est interdit d'être installée. En sélectionnant la checkbox « Utiliser des valeurs personnalisées » on peut changer la version du fichier ou demander d'interdire les versions plus récentes ou plus anciennes ou juste celle la.

Nom du fichier: À ce niveau qu'importe la version du fichier il interdira

juoto oono ia.

Nom du fichier: À ce niveau qu'importe la version du fichier il interdira l'exécution du fichier nommé comme dans le descriptif (ici « skypesetup.exe »).

Nom de l'éditeur: Là on va bloquer l'installation de tout les logiciels que l'éditeur reconnu par sa signature.

**Tout éditeur:** À ce niveau on ne bloque plus véritablement un logiciel mais tout logiciel qui possède une signature.

Pour notre exemple j'ai bloqué skype par le nom de l'éditeur.

The set of the se	Internet         Internet
Anne menetari alfanezi bela bir unan et ar "Databler" ir alge Marte a bir entiment [1 Tan Annen Barra Angeling an 	a (New York (New York))
Barrier Barrier Transmith St Damini Barrier Barrier Transmith St Damini Barrier Barrier Transmither Barrier Barrier Barrier Transmither	Fire
Table is via searching Design is a sign Particular is a sign Particular is a sign of the searching Design of the searching searching searching Design of the searching	Direction of the second state
e A Selador dana	

Une fois que vous avez fini votre selection cliquez sur Ok et appliquer. Et voila votre AppLocker est activé et configuré. Pour vérifier que cela fonctionne, allez sur une machine Windows 7 de votre réseau, vérifiez que le service « Identité de l'Application » est activé.

and the second second	Q Investor Band	10.1	1		64) V	20 D D D D D D D D D D D D D D D D D D D	
	Modified dis Tampite Johns	BACK COLUMN	Deptation:	DMC.	Title in concernant	Terr on more or not an	
	100 C 100	Parmine Carpon	Read of the second		Princel .	Turbes into	
	State Incompa	Shorease is both.	101010-0		1001,00	Tartere inst	
	Table & Control of the local division of the	Californite diser-	GPA 49.98-		franal	furthers would	
		Linder Linderer	14100100-	2414	bienetter (Hb	Der Lief Horse-	
	The other	Desire (Depthalant	Table Section		field	Sendene hand	
	and the second second second second	Testor An Invit-	Part Bar-		recal.	Derthere issue	
	dening makine a fashorbin	Automatic Physics	100010-0		Minut .	Number of State	
	righting	Automatic to the	La Minana	1004	autorubpe.	Suttere lister	
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Contraction of the	1089-881		Table 1	Submersed	
		Designment of an		Des.	- frend	Coverna.	
		Technology in the second	Pagetti Br	Dec.	A sender	Technic load	
		AND 001812-	Period Inc.		Paral I	200-0102-0028	
		The subsection of the subsecti	Automation.		7004714	Service and	
		a title de factions.	10.000		the second se	Call Line Book	
		<ol> <li>Alle system in 4</li> </ol>	Later state	-	hariuri	Systematical	
		Concerner in Sector.	Distances	Des.	- Nanadi	Design had	
		The second street.	report (m		Party .	Surface could	
		Mathematical Sci.	mant in	Sere.	Activity fields	Terffere face	
		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Acces 64		Page 1	140-000-00-0	
		And and a second second	Management.	1.1.1	Concerne .	Subleme house	
		100-10-10-10-10-10-10-10-10-10-10-10-10-	CP (MILLION	and a	allerere .	for our built	
		2010/01/01/01 01	10.000		The second se	100-102 10-0	
		and the property of the proper	10.000.000	See.	milerolage	Declare your	
		in promotion frigore.	Care main.		THE OF	Service doesn.	
		Repair to sense	to be an in-		-	Service boat	
		Name of the part of the local division of th	Company With	-		Sarvine Server	
		and the second s	Contract inter-	-	and the second s	Contract of the second s	
		Manager 147 Yes	Heyesen		Preserved.	Tandare work	

Faites une « gpupdate /force » dans un terminal pour rafraîchir vos stratégies et lancez l'installation.



Un message d'erreur est normalement apparut vous informant que cette installation a été interdite. 🙂

## **Conclusion:**

Dans ce simple article nous avons vu la solution AppLocker, un outil simple pour faire de la restriction logicielle sur un réseau. Nous avons simplement vu comment le configurer les 3 types de règles puis les exceptions, comment les configurer. En résumé je dirais que AppLocker est un outil simple et très efficace, il surpasse de loin pour moi les Software Restriction Policy. Le seul bémol serai sa non disponibilité pour des machines avec un ancien OS.