


		<h1>Guide AutoAdministrator</h1>		 1.02
Type Document	Guide	Version		
Auteur(s)	CGN – Cédric Guizelin	Date Création	28/06/2016	
Titre	Guide AutoAdministrator	Page	1 / 14	

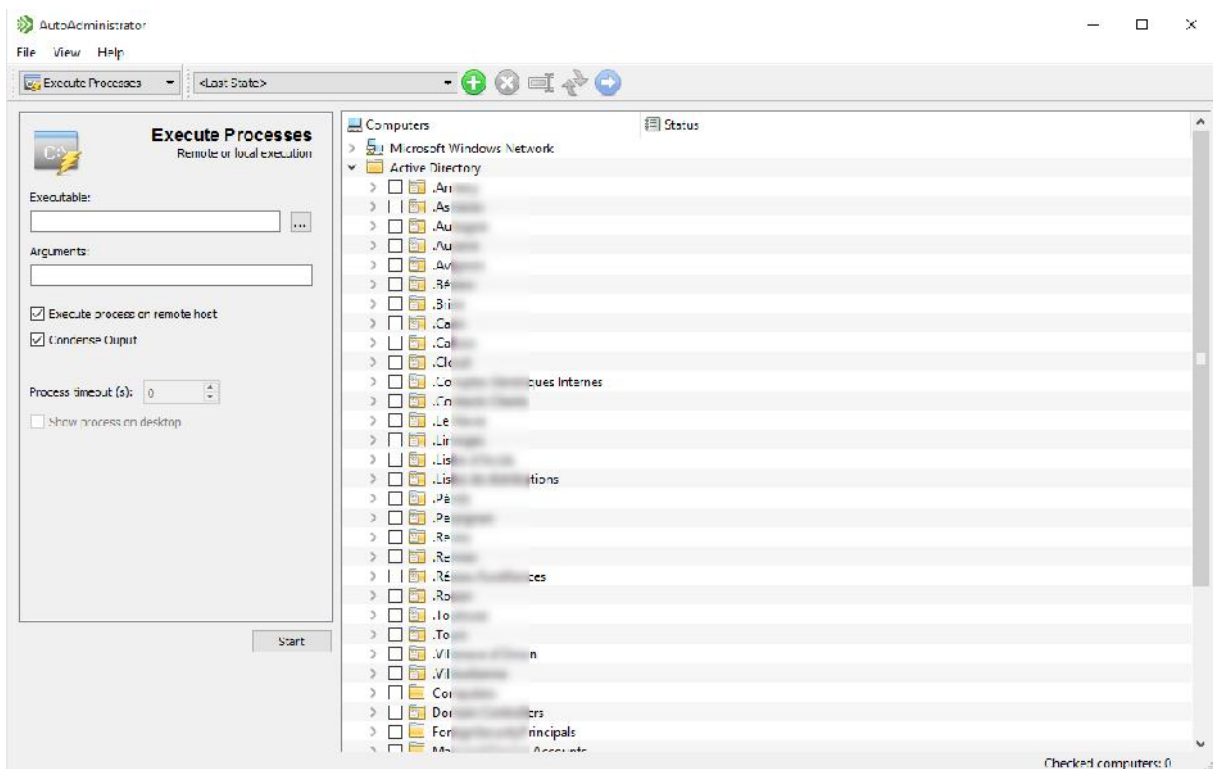
Ce document est un guide pour l'utilisation du logiciel AutoAdministrator (V 2.4.0.4) de NETIKUS.NET


<http://www.autoadministrator.com/>

Logiciel Freeware, permettant d'agir sur de nombreux points d'un domaine.

Il permet de :

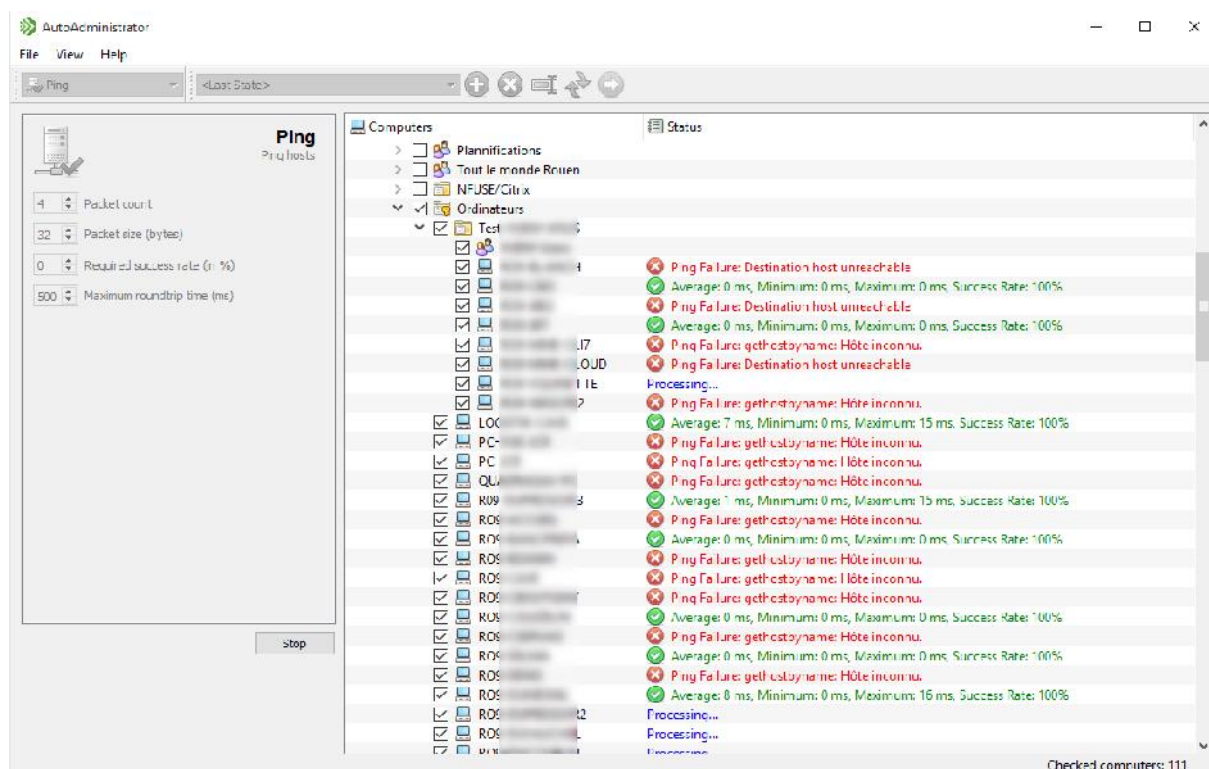
- Faire un test de ping sur les postes
- Gérer un ODBC avec Query/Copy/Delete DSN
- Vérifier/Supprimer/Changer/Reset des mots de passe
- Eteindre/Redémarrer des postes à distance
- Vérifier/Configurer/Stopper/Démarrer... les services
- Vérifier/Ajouter/Supprimer/Modifier... la base de registre
- Copier/Effacer/Synchroniser des fichiers sur des postes
- Vérifier des fichiers sur des postes
- Voir Qui/Combien d'utilisateurs sont connectés et sur quoi
- Exécuter des processus à distance sur des postes (comme psexec)
- Agir sur le WMI



		<h1>Guide AutoAdministrator</h1>		 1.02
Type Document	Guide	Version		
Auteur(s)	CGN – Cédric Guizelin	Date Création	28/06/2016	
Titre	Guide AutoAdministrator	Page	2 / 14	

Surveiller l'état en ligne

Avant d'effectuer une action particulière, il est conseillé de vérifier si les ordinateurs concernés sont disponibles. Avec AutoAdministrator, vous pouvez faire un ping sur plusieurs ordinateurs avec seulement deux clics de souris. Vous pouvez configurer le nombre de paquets, la taille du paquet, le taux de réussite requis et le temps aller-retour maximal. Les deux dernières options déterminent si une machine est marquée comme disponible ou si vous recevez un message d'erreur. Notez que toutes les fonctionnalités de AutoAdministrator peuvent faire un ping avant qu'il ne procède effectivement à l'action, pour vous assurer qu'il n'y a pas les délais d'attente inutiles.




Requête WMI à distance

La fonction WMI est une nouvelle fonctionnalité de AutoAdministrator 2.3. Comme vous le savez sans doute, Windows Management Instrumentation (WMI) est une fonctionnalité très puissante qui vous permet d'accéder à distance littéralement, à chaque élément d'information disponible pour une machine Windows. Vous pouvez récupérer des informations communes telles que les cartes réseau installées ou service packs, mais aussi des données très spécifiques telles que la version du BIOS ou de la taille du volume de données.

Avec AutoAdministrator, vous pouvez maintenant exécuter facilement des requêtes WMI sur plusieurs machines. Comme vous pouvez le voir dans la capture d'écran, vous devez d'abord sélectionner l'espace de noms WMI, puis sélectionnez une classe WMI. Ensuite, vous pouvez choisir plusieurs objets WMI.

Dans mon exemple, j'ai choisi Win32_BootConfiguration classe WMI, qui vous permet de récupérer des informations de WMI objets tels que BootDirectory, LastDrive ou TempDirectory.

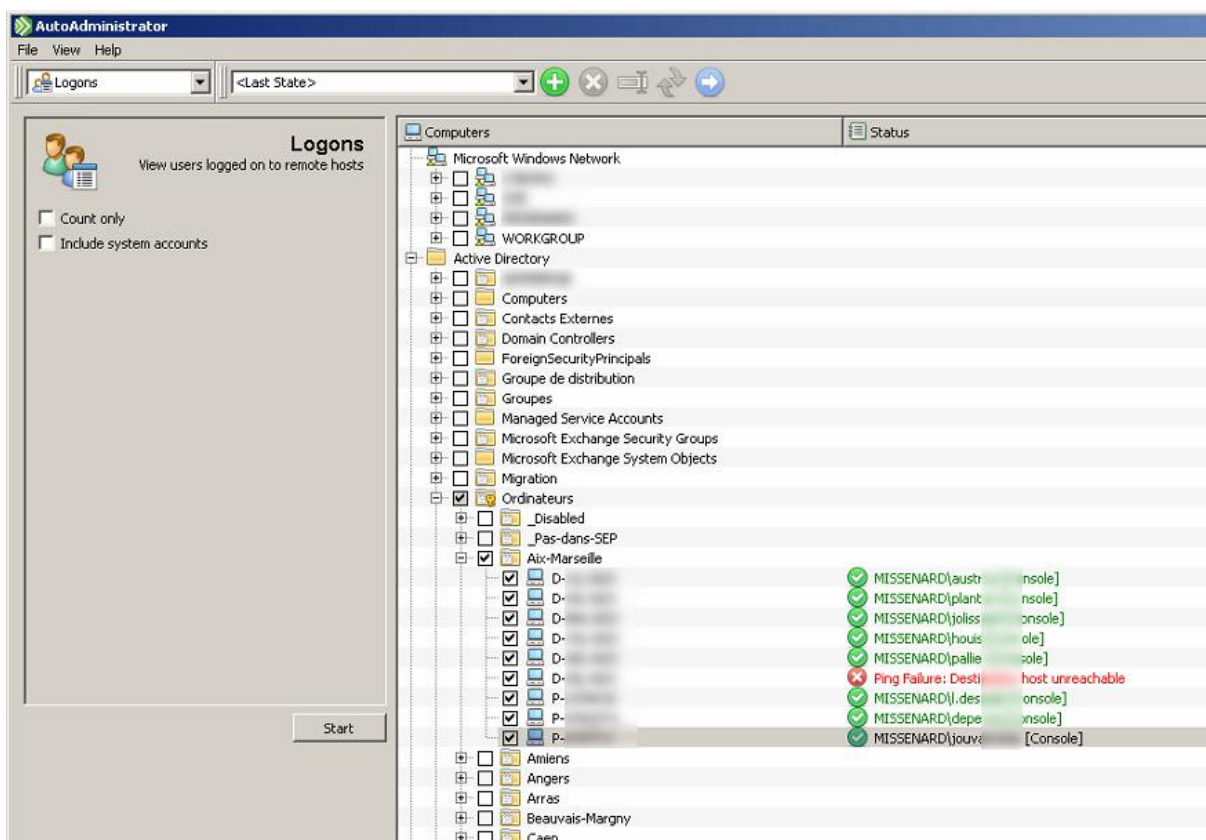
		<h1>Guide AutoAdministrator</h1>		 1.02
Type Document	Guide	Version		
Auteur(s)	CGN – Cédric Guizelin	Date Création	28/06/2016	
Titre	Guide AutoAdministrator	Page	3 / 14	


Interrogation à distance des fichiers de métadonnées

La fonction de l'information de fichier vous permet d'interroger les métadonnées des fichiers sur plusieurs machines distantes. Vous pouvez récupérer la taille du fichier, attributs, date de modification, la version, la société, et la description d'un fichier spécifique. AutoAdministrator vous permet également de calculer plusieurs checksums (CRC-32, MD5, SHA-1, SHA-256). Cette fonction pourrait se révéler très utile dans un certain nombre de situations. Par exemple, s'il y a une épidémie de virus pour lequel votre logiciel anti-virus n'a pas encore les signatures appropriées, vous pouvez identifier les machines infectées en utilisant AutoAdministrator puis utilisez la fonction de gestion de fichiers pour remplacer les fichiers infectés.

Qui est connecté

Avec cette fonctionnalité, vous pouvez récupérer des informations sur les utilisateurs qui sont connectés à des hôtes distants. Comme d'habitude, AutoAdministrator affiche les informations récupérées à côté de chaque nom de l'ordinateur. Il est également possible de simplement compter les utilisateurs qui sont connectés, ce qui pourrait être utile pour les serveurs Terminal Server.



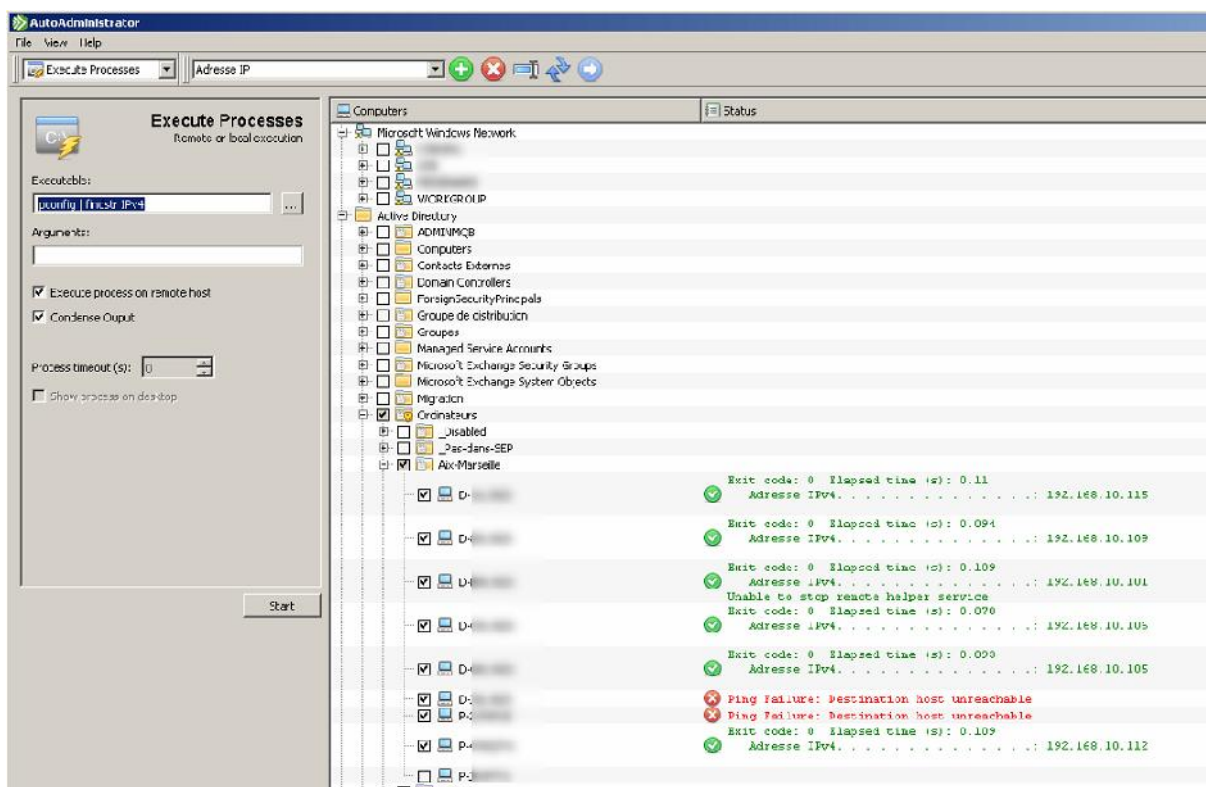
		<h1>Guide AutoAdministrator</h1>		 1.02
Type Document	Guide	Version		
Auteur(s)	CGN – Cédric Guizelin	Date Création	28/06/2016	
Titre	Guide AutoAdministrator	Page	4 / 14	

Exécuter à distance des programmes

L'exécution des processus à distance vous permet d'exécuter toutes sortes de programmes sur des ordinateurs distants, ce qui est assez puissant, car il vous permet de vous passer d'outils tels que psexec et plink.

Le premier, comme vous le savez probablement, vous permet d'exécuter des processus à distance, alors que plink vous permet d'exécuter des commandes UNIX via SSH. Donc, avec cette fonction, vous pouvez émettre des commandes SSH sur un certain nombre de machines UNIX et voir la sortie dans AutoAdministrator.

Obtenir l'adresse IP des postes
 ipconfig | findstr IPv4



Dans la capture d'écran, vous voyez comment j'ai exécuté la commande qui renvoie le résultat des machines distantes qui sont affichées dans le volet des résultats.


Execute process on remote host

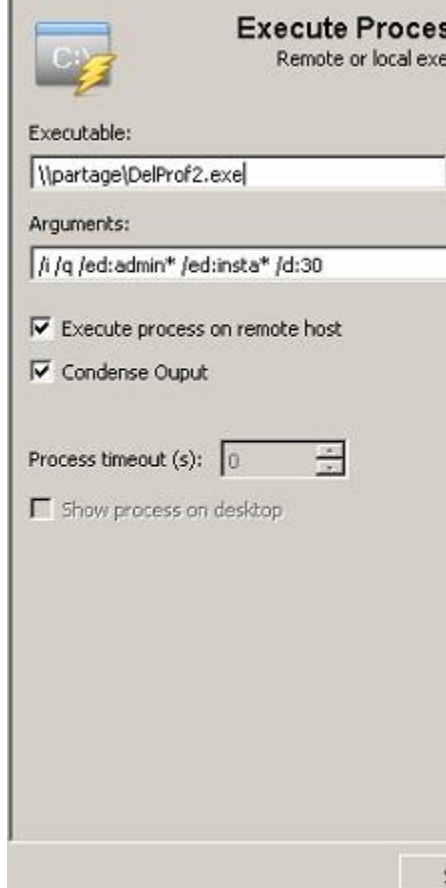
Equivalent à un psexec, pour exécuter sur le poste distant avec vos droits, ou ceux assignés au groupe ou PC.

Si vous choisissez de ne pas l'activer, la variable locale \$hostname sera celle du poste cible

Exemple : ping \$hostname

Le TimeOut & Show process on desktop ne sont disponible que si le script est exécuté en local.

		<h1>Guide AutoAdministrator</h1>			
Type Document	Guide	Version	1.02		
Auteur(s)	CGN – Cédric Guizelin	Date Création	28/06/2016		
Titre	Guide AutoAdministrator	Page	5 / 14		



Supprimer des sessions inactives de plus de 90 jours sans confirmation sauf admin* et insta*
`\\partage\DelProf2.exe /i /q /ed:admin* /ed:insta* /d:90`

Nécessite un partage et l'utilitaire Delprof2
<https://helgeklein.com/free-tools/delprof2-user-profile-deletion-tool/>

Autre utilisation possible :


Désactiver le GWX pour éviter le passage à Windows 10 des postes en Windows 7

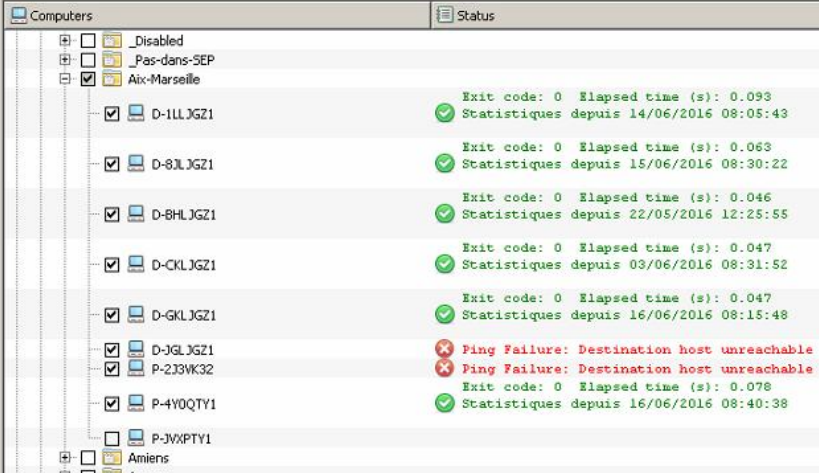
```
REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\GWX /v DisableGWX /t REG_DWORD /d 1 /f
```

Puis désactiver l'upgrade d'OS


```
REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate /v DisableOSUpgrade /t REG_DWORD /d 1 /f
```

Uptime des postes
net statistics server | find "depuis"



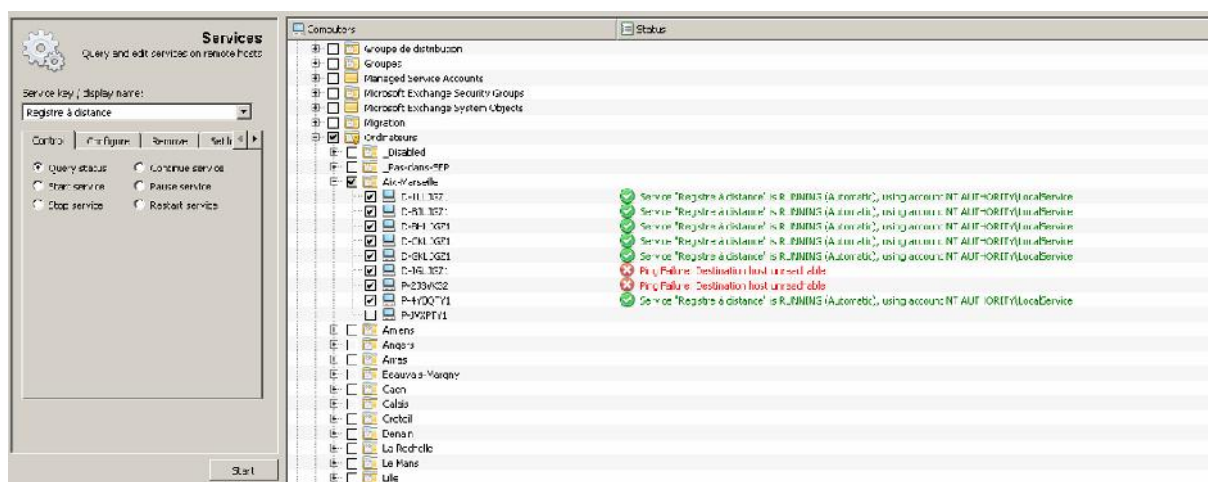


Computer	Exit code	Elapsed time (s)	Statistiques depuis
D-1LLJGZ1	0	0.093	14/06/2016 08:05:43
D-8JLJGZ1	0	0.063	15/06/2016 08:30:22
D-BHLJGZ1	0	0.046	22/05/2016 12:25:55
D-CKLJGZ1	0	0.047	03/06/2016 08:31:52
D-GKLJGZ1	0	0.047	16/06/2016 08:15:48
D-JGLJGZ1	0	0.078	16/06/2016 08:40:38
P-2J3WK32	0	0.078	16/06/2016 08:40:38
P-4V0QTY1	0	0.078	16/06/2016 08:40:38
P-JWXPTY1	0	0.078	16/06/2016 08:40:38


		<h1>Guide AutoAdministrator</h1>		 1.02
Type Document	Guide	Version		
Auteur(s)	CGN – Cédric Guizelin	Date Création	28/06/2016	
Titre	Guide AutoAdministrator	Page	6 / 14	

Exécuter à distance les services Windows

Cette fonction est certainement un autre point fort de AutoAdministrator. La gestion des services système sur plusieurs machines est une caractéristique qui manque à beaucoup de solutions de gestion des systèmes coûteux. AutoAdministrator vous permet des requêtes à distance, démarrer, arrêter, poursuivre, arrêter et redémarrer les services. De plus, vous pouvez configurer le type de démarrage à distance. Vous pouvez utiliser cette fonction, par exemple, pour définir le type de service « Registre à distance » en démarrage sur toutes vos machines en "automatique" pour vous assurer que vous pouvez utiliser toutes les fonctionnalités de AutoAdministrator. Il est également possible de supprimer des services ou à configurer leur compte d'ouverture de session.

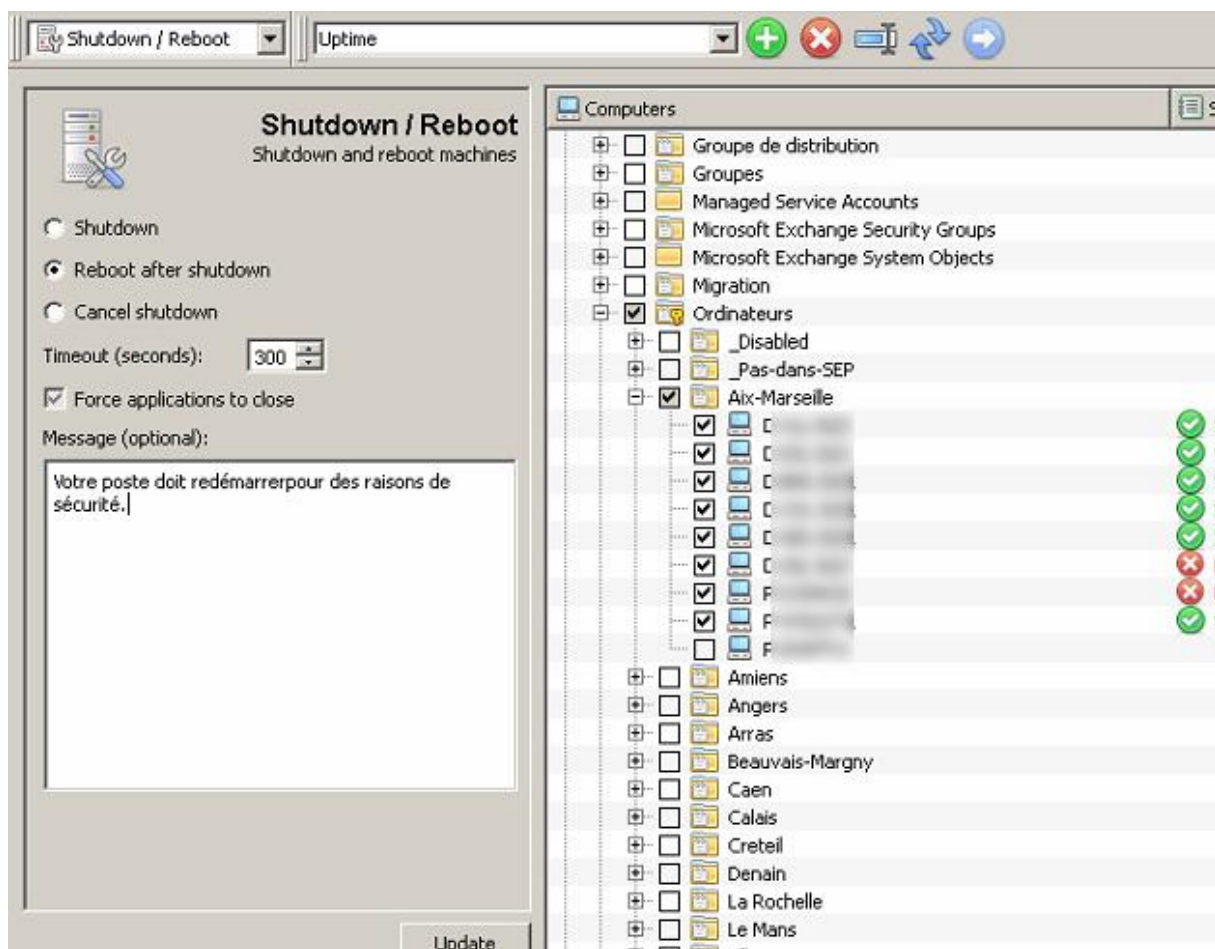



AutoAdministrator affiche uniquement les services qui sont disponibles sur l'ordinateur sur lequel AutoAdministrator a été installé. Toutefois, si vous souhaitez configurer à distance les services d'applications tierces qui ne sont pas installés sur votre PC, il vous suffit de saisir le nom du service. Vous pouvez trouver le nom du service dans l'outil Windows Service en accédant aux propriétés du service. Ne pas confondre le nom du service avec le nom d'affichage de service.

		Guide AutoAdministrator		 1.02
Type Document	Guide	Version		
Auteur(s)	CGN – Cédric Guizelin	Date Création	28/06/2016	
Titre	Guide AutoAdministrator	Page	7 / 14	

Arrêt à distance / redémarrage

Cette fonction vous permet d'arrêter ou de redémarrer plusieurs ordinateurs de votre réseau. Vous pouvez configurer un délai d'attente, après quoi les ordinateurs s'arrêteront. AutoAdministrator avisera les utilisateurs avec un message que vous pouvez personnaliser. Il est possible de forcer les applications ouvertes à se fermer, et vous pouvez également annuler les arrêts à distance.

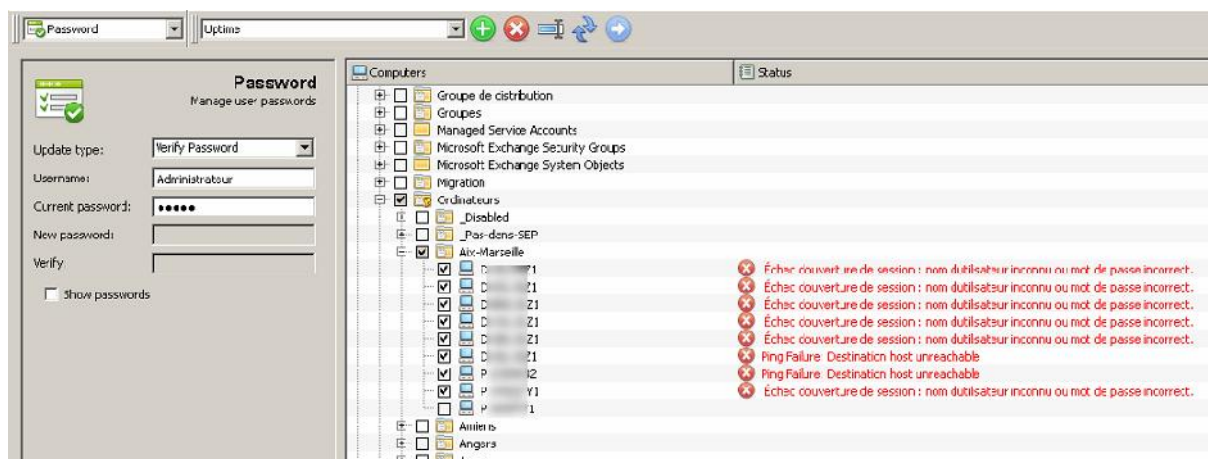


		<h1>Guide AutoAdministrator</h1>		 1.02
Type Document	Guide	Version		
Auteur(s)	CGN – Cédric Guizelin	Date Création	28/06/2016	
Titre	Guide AutoAdministrator	Page	8 / 14	


Gérer les mots de passe à distance

Il vous permet de vérifier, de modifier et de réinitialiser les mots de passe à distance sur plusieurs machines. Cette fonction est particulièrement utile si vous souhaitez modifier le mot de passe administrateur local sur toutes vos machines. La gestion des mots de passe locaux sur plusieurs machines est un peu lourde, la plupart des administrateurs ne changent pas les mots de passe administrateur local assez souvent.

Avec AutoAdministrator, vous pouvez effectuer cette tâche importante de sécurité avec quelques clics de souris. La fonction de vérifier vous permet de vérifier si tous les ordinateurs ont reçu le nouveau mot de passe.

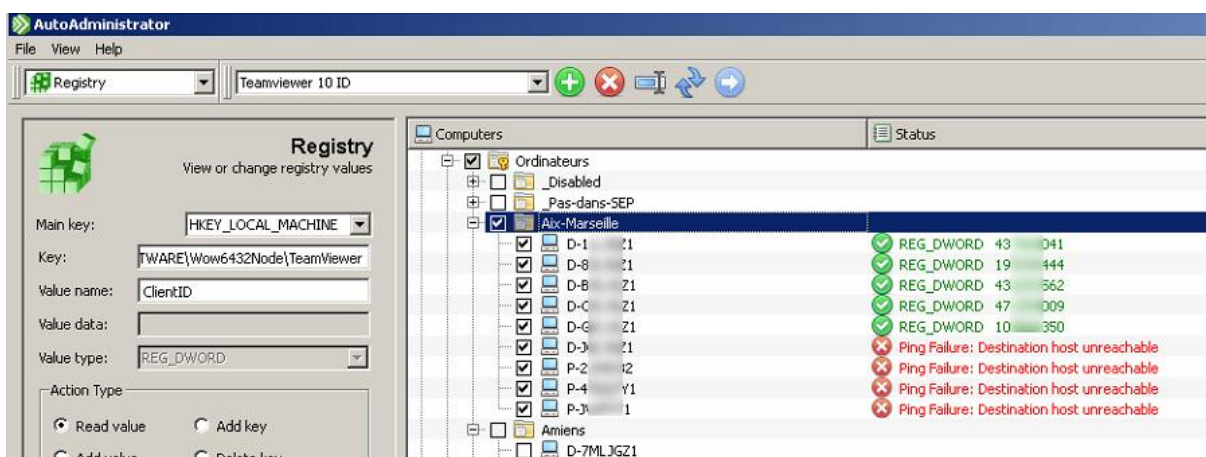


La différence entre le changement et la réinitialisation du mot de passe est que, avec la première option, vous devez spécifier le mot de passe actuel du compte correspondant, alors que la réinitialisation de mot de passe, vous ne devez pas connaître le mot de passe actuel. Je recommande l'utilisation de la fonction de changement parce que, après une réinitialisation de mot de passe, l'utilisateur ne sera plus en mesure d'accéder aux données liées à la sécurité telles EFS fichiers cryptés ou des informations d'identification d'Internet Explorer.

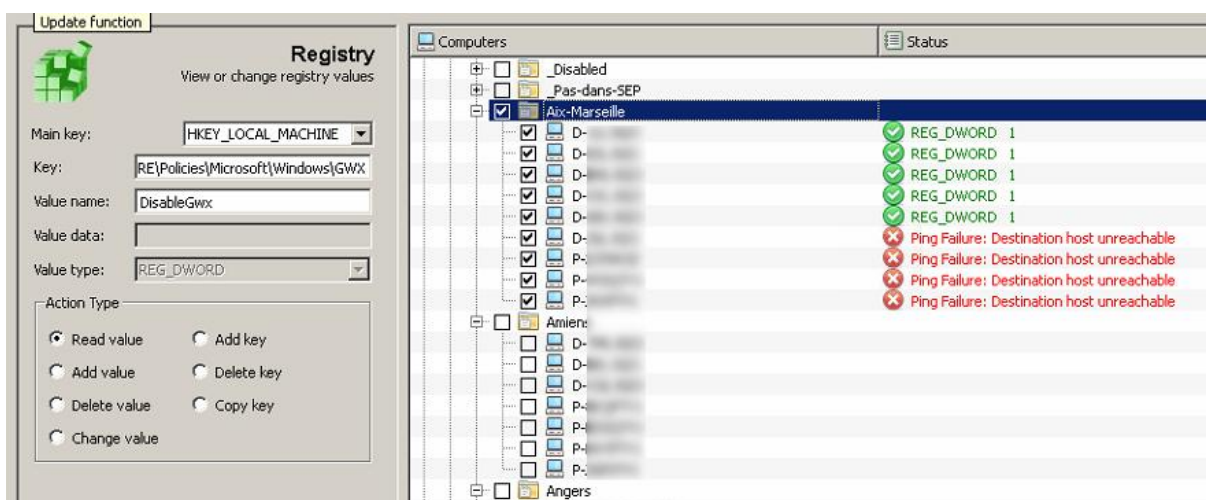
<h1>Guide AutoAdministrator</h1>			
Type Document	Guide	Version	1.02
Auteur(s)	CGN – Cédric Guizelin	Date Création	28/06/2016
Titre	Guide AutoAdministrator	Page	9 / 14

Édition de registre à distance

Une autre caractéristique utile de AutoAdministrator est sa fonction d'édition de registre à distance. Vous pouvez ajouter ou modifier la valeur de la clé de Registre REG_DWORD types, REG_SZ et REG_EXPAND_SZ sur plusieurs machines, quelle que soit la version de Windows qu'ils emploient. Vous pouvez également lire, supprimer ou copier des clés ou des valeurs REG_DWORD. AutoAdministrator ne permet cependant pas de parcourir le Registre. Autrement dit, vous devez connaître le nom de la clé exacte que vous souhaitez modifier. Je recommande d'utiliser la fonction de copie du nom de clé de l'éditeur de registre de Windows. De cette façon, il vous suffit de copier et coller ces longs chemins principaux. Assurez-vous que vous supprimez la clé principale dans le chemin de clé copié (par exemple, HKEY_LOCAL_MACHINE), qui est fournit dans AutoAdministrator.




Interrogation de la clef HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TeamViewer\ClientID pour connaître le code ID Teamviewer d'une machine



Savoir si l'upgrade vers Windows 10 est désactivé

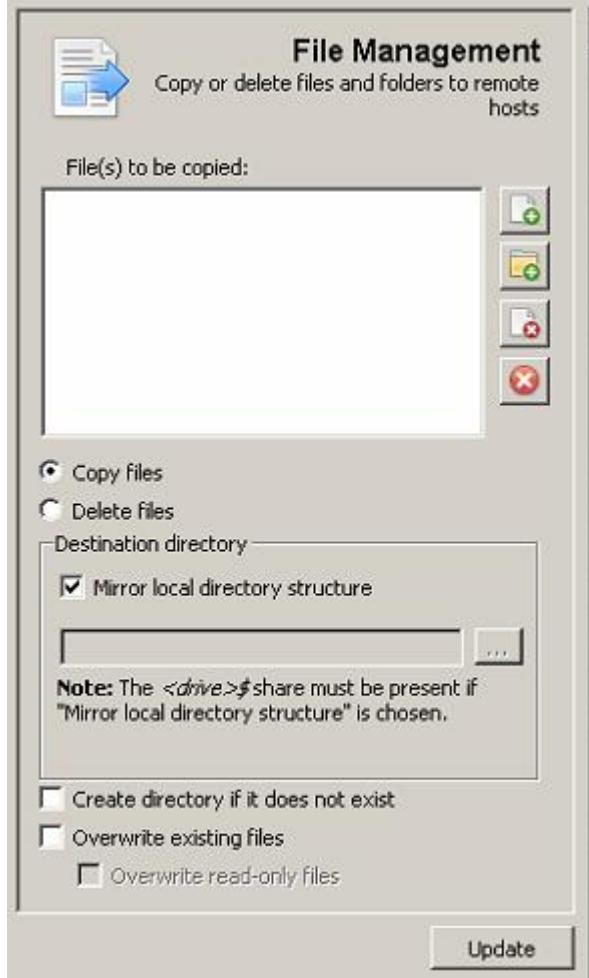
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\GWX\DisableGwx


Avec ADD ou CHANGE, il est possible aussi de l'activer (en mettant 0) ou de le désactiver (1) à distance.

		Guide AutoAdministrator		 1.02
Type Document	Guide	Version		
Auteur(s)	CGN – Cédric Guizelin	Date Création	28/06/2016	
Titre	Guide AutoAdministrator	Page	10 / 14	

Copie de fichiers à distance

La fonction de gestion des fichiers de AutoAdministrator ne permet pas vraiment de modifier à distance les fichiers ; cependant, vous pouvez copier des fichiers et des dossiers sur plusieurs ordinateurs distants. Ces tâches sont généralement réalisées en utilisant des scripts. L'avantage d'utiliser AutoAdministrator est que vous pouvez copier des fichiers avec des droits d'administrateur à un endroit sans trop de tracas. De plus, vous pouvez être sûr que les fichiers atteignent leur destination sans délai. AutoAdministrator peut créer une structure de répertoire automatiquement si elle n'est pas encore disponible sur les machines distantes. Vous pouvez également configurer l'outil pour écraser les fichiers existants ou supprimer des fichiers sur plusieurs machines.

	<p>Exemple :</p> <p>Dupliquer sur plusieurs serveurs une structure identique d'un répertoire modèle avec les applicatifs à déployer sur plusieurs agences.</p>
---	--

		Guide AutoAdministrator		 1.02
Type Document	Guide	Version		
Auteur(s)	CGN – Cédric Guizelin	Date Création	28/06/2016	
Titre	Guide AutoAdministrator	Page	11 / 14	

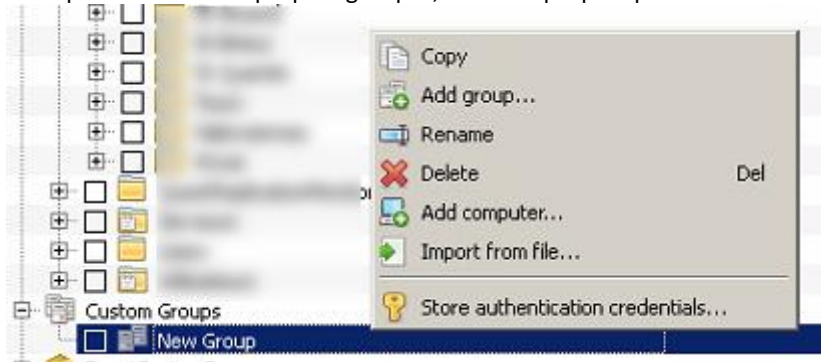
Configuration ODBC d'édition à distance


Open Database Connectivity (ODBC) est une norme pour déplacer des données d'un type de base de données à un autre. Vous pouvez utiliser AutoAdministrator pour interroger, copier et supprimer un DSN système (Data Source Name). Le DSN système, que vous souhaitez gérer, doit être installé sur le PC sur lequel vous exécutez AutoAdministrator. Il est également possible de copier les pilotes correspondants à des ordinateurs distants, remplacer les paramètres existants, et remplacer les fichiers verrouillés lors du prochain redémarrage. Soyez prudent avec cette fonctionnalité, car AutoAdministrator n'a pas de fonction "undo".

Les fonctions de AutoAdministrator sont assez variées et vont vous aider à résoudre de nombreux problèmes d'administration Windows.

Vos propres groupes

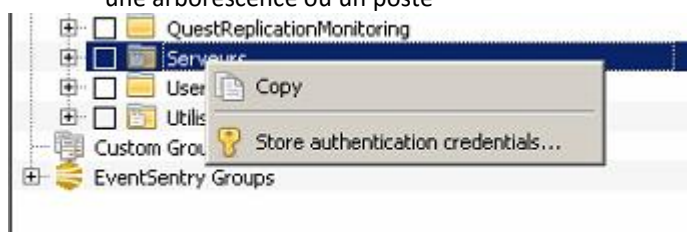
Vous pouvez créer vos propres groupes, avec vos propres postes



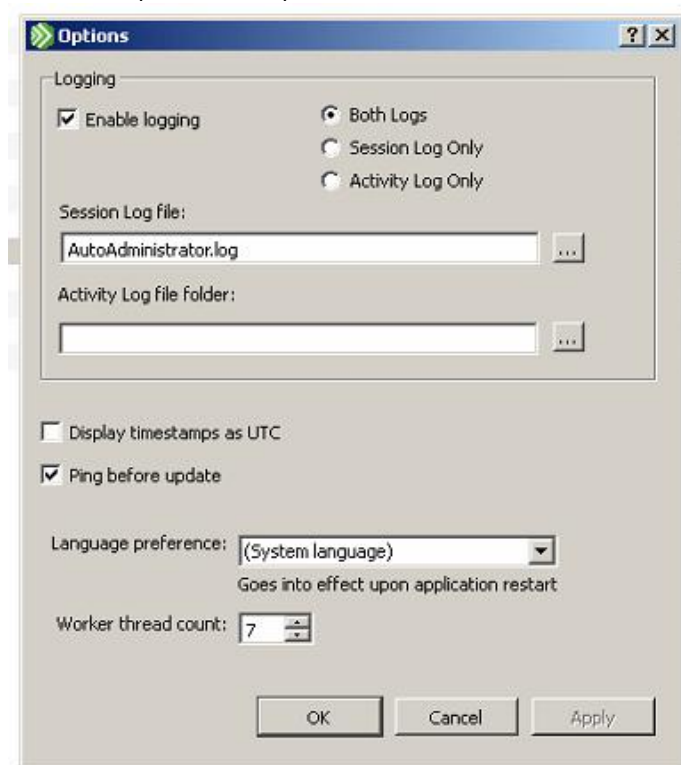
		Guide AutoAdministrator		 1.02
Type Document	Guide	Version		
Auteur(s)	CGN – Cédric Guizelin	Date Création	28/06/2016	
Titre	Guide AutoAdministrator	Page	12 / 14	


A savoir :

- Une fois installé, le logiciel peut être recopié sur une clef USB et utilisé de n'importe quel poste sans nécessiter une installation.
- Les postes distants doivent évidemment avoir les services REGISTRE A DISTANCE d'activés. AutoAdministrator fonctionne avec un UAC élevé généralement
- Si vous ne disposez pas des droits nécessaires sur votre session, il est possible de mettre des droits sur une arborescence ou un poste

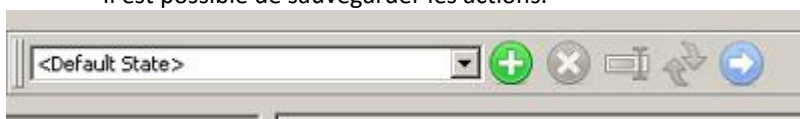


- Dans View -> Options , il est possible d'activer des Logs pour suivre ce qui a été fait, ainsi que le nombre de postes sur lequel les envois sont fait en simultanés. (Par défaut 5)



		Guide AutoAdministrator		 1.02
Type Document	Guide	Version		
Auteur(s)	CGN – Cédric Guizelin	Date Création	28/06/2016	
Titre	Guide AutoAdministrator	Page	13 / 14	

- Il est possible de sauvegarder les actions.



(+) Pour enregistrer l'action définit

(x) Supprimer l'action sélectionner

(_|) Renommer l'action

La double flèche pour Modifier l'action sélectionné par les modifications actuelles

(=>) Appliquer le preset sélectionné

- Pour un Batch, il peut être nécessaire d'ajouter ces lignes en début de script pour avoir l'élévation nécessaire à l'UAC

```
Exit code: 0 Elapsed time (s): 0.437
Requesting administrative privileges...
```

Avec ces lignes, le message apparaîtra, mais le script passera outre.

```
:: BatchGotAdmin
```

```
:-----
```

```
REM --> Check for permissions
```

```
>nul 2>&1 "%SYSTEMROOT%\system32\cacls.exe" "%SYSTEMROOT%\system32\config\system"
```

```
REM --> If error flag set, we do not have admin.
```

```
if '%errorlevel%' NEQ '0' (
```

```
    echo Requesting administrative privileges...
```

```
    goto UACPrompt
```

```
) else ( goto gotAdmin )
```

```
:UACPrompt
```

```
echo Set UAC = CreateObject^("Shell.Application") > "%temp%\getadmin.vbs"
```

```
echo UAC.ShellExecute "%~s0", "", "", "runas", 1 >> "%temp%\getadmin.vbs"
```

```
"%temp%\getadmin.vbs"
```

```
exit /B
```

```
:gotAdmin
```

```
if exist "%temp%\getadmin.vbs" ( del "%temp%\getadmin.vbs" )
```

```
pushd "%CD%"
```

```
CD /D "%~dp0"
```

```
:-----
```

- Attention aux messages d'erreur :

```
✘ Ping Failure: Destination host unreachable
```


Poste non en ligne

```
✘ Ping Failure: gethostbyname: Hôte inconnu.
```

Poste dont les accès sont certainement bloqués (Firewall, Services, GPO, Antivirus, à réinscrire dans le domaine...)

```
✘ Exit code: 259 Elapsed time (s): 0.312
```

Théoriquement, cela voudrait dire que le script a échoué, mais vérifiez sur un poste via le partage administratif ou autre, le code erreur peut être dû au temps d'exécution du script qui lui continue normalement.

		Guide AutoAdministrator		
Type Document	Guide	Version	1.02	
Auteur(s)	CGN – Cédric Guizelin	Date Création	28/06/2016	
Titre	Guide AutoAdministrator	Page	14 / 14	

- Pour exécuter un Powershell en ligne de commande
PowerShell -NoProfile -ExecutionPolicy Bypass C:\folder\file.ps1
-