

Travaux Pratiques - Gestion des stratégies d'exécution et déblocage de scripts PowerShell

Objectifs :

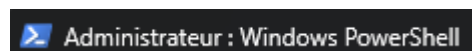
- Comprendre et manipuler les stratégies d'exécution PowerShell.
- Apprendre à débloquer un script téléchargé pour pouvoir l'exécuter.
- Savoir exécuter un script PowerShell en respectant les politiques de sécurité.

Consignes :

Vous allez réaliser plusieurs étapes pour explorer et manipuler les stratégies d'exécution de PowerShell, puis tester l'exécution d'un script téléchargé.

Etape 1 : Visualiser les stratégies d'exécution

1. Ouvrez PowerShell en mode administrateur.



2. Tapez la commande suivante pour afficher les stratégies d'exécution appliquées aux différents scopes : `Get-ExecutionPolicy -List`
3. Notez les stratégies affichées pour chaque niveau (MachinePolicy, UserPolicy, Process, CurrentUser, LocalMachine).

```
PS C:\WINDOWS\system32> Get-ExecutionPolicy

Scope ExecutionPolicy
-----
MachinePolicy Undefined
UserPolicy Undefined
Process Undefined
CurrentUser Undefined
LocalMachine RemoteSigned
```

Etape 2 : Modifier la stratégie d'exécution utilisateur

1. Changez la stratégie d'exécution pour l'utilisateur courant afin d'autoriser l'exécution des scripts locaux signés ou non : `Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser`
2. Validez la modification en tapant T (Oui) lorsqu'on vous le demande.

3. Vérifiez que la modification est bien prise en compte avec : Get-ExecutionPolicy -List

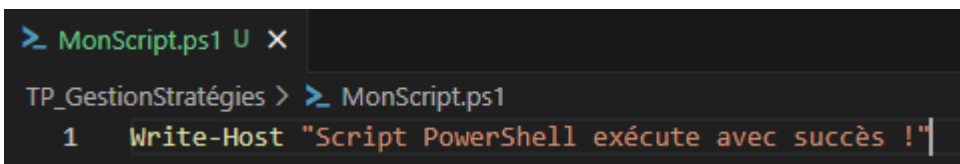
```
PS C:\WINDOWS\system32> Set-ExecutionPolicy RemoteSigned -Scope CurrentUser

Modification de la stratégie d'exécution
La stratégie d'exécution permet de vous prémunir contre les scripts que vous jugez non fiables. En modifiant la
stratégie d'exécution, vous vous exposez aux risques de sécurité décrits dans la rubrique d'aide
about_Execution_Policies à l'adresse https://go.microsoft.com/fwlink/?LinkID=135170. Voulez-vous modifier la stratégie
d'exécution ?
[0] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide (la valeur par défaut est « N ») : o
PS C:\WINDOWS\system32> Get-ExecutionPolicy -List

Scope ExecutionPolicy
-----
MachinePolicy Undefined
UserPolicy Undefined
Process Undefined
CurrentUser RemoteSigned
LocalMachine RemoteSigned
```

Etape 3 : Téléchargement et déblocage d'un script

1. Créez un fichier PowerShell appelé MonScript.ps1 contenant la ligne suivante :
Write-Host "Script PowerShell exécute avec succès !"



```
> MonScript.ps1 U X
TP_GestionStratégies > > MonScript.ps1
1 Write-Host "Script PowerShell exécute avec succès !"
```

2. Simulez un téléchargement Internet en ajoutant la marque de blocage :

- Sur ce fichier, faites un clic droit > Propriétés > cochez la case Débloquer > puis cliquez sur Appliquer.

3. Alternative : débloquez le fichier avec la commande PowerShell suivante :
Unblock-File -Path "C:\\Chemin\\Vers\\MonScript.ps1"

Etape 4 : Exécuter le script

1. Lancez l'exécution de votre script dans PowerShell avec : .\\MonScript.ps1

2. Observez le résultat et vérifiez qu'il s'exécute sans message d'erreur.

```
PS C:\Users\Valentin Foure\Desktop\Dossier\Windows PowerShell\Projet\PowerShell\TP_GestionStratégies> .\\MonScript.ps1
Script PowerShell exécute avec succès !
```

Etape 5 (facultative) : Contourner la stratégie d'exécution

1. Ouvrez une nouvelle session PowerShell avec la stratégie d'exécution contournée :
powershell.exe -ExecutionPolicy Bypass

2. Depuis cette session, tentez d'exécuter votre script sans le débloquer.

Questions à rendre avec votre TP

1. Quelle est la politique d'exécution par défaut sur votre machine ?
2. Pourquoi est-il nécessaire de débloquent un script téléchargé avant exécution ?
3. Quels sont les risques liés à l'utilisation d'une politique Bypass ?
4. Quelle politique d'exécution recommanderiez-vous en entreprise ? Pourquoi ?