

Fiche 11 : Sécurité d'exécution des scripts

1. Lancement d'un script

Il est impossible d'exécuter un script d'extension .ps1 en double-cliquant dessus.

Afin d'éviter le détournement de commande, Windows PowerShell a besoin du chemin exact du script, soit **c:\chemin\script.ps1** ou **.\script.ps1** si le script est dans le répertoire courant.

Pour appeler un script PowerShell dans l'invite de commandes : `powershell c:\chemin\script.ps1`

2. Stratégie pour l'exécution de scripts

Dans PowerShell, il existe quatre paramètres de stratégie d'exécution des scripts qui sont :

Restricted : paramètre par défaut, n'autorise pas l'exécution des scripts,
AllSigned : n'exécute que les scripts de confiance, donc signés,
RemoteSigned : exécute les scripts locaux sans obligation de confiance et les scripts de confiance issus d'Internet,
Unrestricted : autorise l'exécution de tous les scripts.

Pour être un script de confiance, il faut :

- que le script soit signé par un certificat de signature de code, certificat numérique de classe III (voir §4),
- que l'autorité de certification ayant délivré ce certificat soit approuvée sur le poste (via son certificat),
- que le script ne soit pas modifié après la signature.

Commande pour connaître la stratégie en cours de PowerShell :

```
PS C:\> Get-ExecutionPolicy
Restricted
```

Commande pour définir la stratégie sur AllSigned :

```
PS C:\> Set-ExecutionPolicy AllSigned
```

Commande pour afficher la liste des certificats de l'utilisateur (tout certificat installé est accessible via le lecteur cert:) :

```
PS C:\> Get-ChildItem cert:\CurrentUser\my
    Directory: Microsoft.PowerShell.Security\Certificate::CurrentUser\my
Thumbprint                               Subject
-----
CE2E8F6F26626D12A542A213E78397A3853B4306 CN=administrateur, C=FR
```

Commandes pour récupérer le premier certificat et signer un script avec :

```
PS C:\> $cert=Get-ChildItem cert:\CurrentUser\My -codesigning
PS C:\> Set-AuthenticodeSignature c:\script\testsignature.ps1 $cert
```

Si il y a plusieurs certificats, Il est possible de spécifier le numéro du certificat avec la commande suivante :

```
PS C:\> $cert=@(Get-ChildItem cert:\CurrentUser\My -codesigning)[0]
```

La copie chiffrée apparaît sous forme de commentaires cryptés en bas du script :

```
1 Write-Output "script test signature"
2
3 # SIG # Begin signature block
4 # MIIESQYJKoZIhvcNAQcCoIIEOjCCBDYCAQEExCzAJBgUrDgMCGGUAMGkGCisGAQQB
5 # gjcCAQSGWzBZMDQGCisGAQQBggjcCAR4wJgIDAQAABAfzDtgWUsITrckOsYpfvNR
```

Il est possible de signer tous les scripts d'un dossier avec le code suivant :

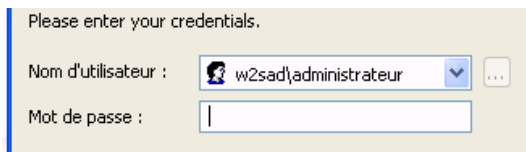
```
PS C:\> Get-ChildItem c:\script\*.ps1 | ForEach-Object {Set-AuthenticodeSignature $_.fullname $cert}
```

3. Identification différente lors de l'exécution d'un script

Par exemple, pour les connexions WMI, il est possible de spécifier des informations d'identification différentes à l'aide du paramètre *-Credential*. La commande *Get-Credential* permet même de stocker ces informations dans une variable.

Exemple de script qui utilise des informations d'identification particulières pour une connexion WMI :

```
1 $login=Get-Credential -Credential w2sad\administrateur
2 Get-WmiObject Win32_NetworkAdapterConfiguration -ComputerName w2sad -Credential $login
```



Get-Credential ouvre une boîte de dialogue pour la saisie du mot de passe et conserve ces informations dans une variable pour un usage multiple dans le script. Le mot de passe n'est plus en dur dans le script.

4. Mise en place de certificats pour une stratégie AllSigned

Ici, cette mise en place est réalisée avec une autorité de certification gérée sous Windows 2000 server.

1) Installer l'autorité de certification sur le serveur :



Vérifier que le serveur Web par défaut est fonctionnel.

2) Sur le poste avec PowerShell, demander un certificat pour une signature de code avec l'URL suivante :

<http://IPServer/certsrv/>

Sur la page d'accueil :

- Sélectionner Demander un certificat et bouton Suivant,
- Sélectionner Demande avancée et bouton Suivant,
- Sélectionner Soumettre une demande ... en utilisant un formulaire et bouton Suivant,
- Remplir éventuellement les informations d'identification
- Sélectionner le type d'utilisation prévu : Certificat de signature de code

Type d'utilisation prévu :

Certificat de signature de code

- Cocher : Marquer les clés comme étant exportable (Pour copier/extraire le certificat avec la clé) :
 - ☒ Marquer les clés comme étant exportables
 - ☐ Exporter les clés vers un fichier

- Bouton Soumettre, on obtient le message : votre demande de certificat a été reçue.

3) Délivrer le certificat à partir de l'autorité de certification sur le serveur

- Programmes/Outils d'administration/Autorité de certification,
- Dans le dossier Demandes en attente, clique droit sur la demande, Menu Toutes les tâches/Délivrer.



4) Sur le poste avec PowerShell, récupérer le certificat toujours avec l'URL : <http://IPServer/certsrv/>

Sur la page d'accueil :

- Sélectionner Vérifier un certificat en attente et bouton Suivant,
- Dans la liste : la requête de certificat à vérifier, sélectionner le certificat et bouton Suivant,
- A l'aide de cette page, installer le certificat demandé :

Certificat émis

Le certificat que vous avez demandé a été émis.

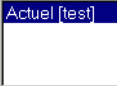
 [Installer ce certificat](#)

5) Sur le poste avec PowerShell, récupérer le certificat de l'autorité de certification toujours avec la même URL

Sur la page d'accueil :

- Sélectionner Récupérer le certificat de l'autorité de certification et bouton Suivant,
- Télécharger le certificat de l'Autorité de certification à l'aide du lien :

Choisissez le fichier à télécharger :

Certificat d'Autorité de certification : 

☒ Codé DER ou ☐ Crypté en Base64

[Télécharger le certificat de l'Autorité de certification](#)

[Télécharger le chemin du certificat de l'Autorité de certification](#)

[Télécharger la dernière liste de révocation de certificats](#)

- Spécifier le chemin où le certificat sera stocké,
- Installer le certificat en double-cliquant sur le fichier téléchargé.

6) Vérifier la présence des certificats avec Internet Explorer

- Menu Outils/Options Internet.../Onglet Contenu/Bouton Certificat...
- Onglet Personnel pour Afficher/Exporter/Supprimer le certificat de signature de code,
- Onglet Autorités ... ou Onglet Éditeurs approuvés pour Afficher/Exporter/Supprimer le certificat de

l'AC.