Atelier : Signature de code PowerShell

1. Objectif

La société Corp souhaite sécuriser les exécutions de script PowerShell dans l'entreprise. Seuls les scripts PowerShell signés par un éditeur d'entreprise validé seront autorisés.

Dans cet atelier pratique, nous allons personnaliser le modèle de signature de code, obtenir un certificat basé sur ce modèle et l'utiliser pour signer nos scripts PowerShell. Nous déploierons automatiquement le certificat éditeur sur tous les ordinateurs du domaine à l'aide d'une stratégie du groupe. Nous testerons également l'impact d'une modification du script et de la révocation du certificat de signature de code.

Les ordinateurs virtuels utilisés dans cet atelier sont les suivants :

- S1 : contrôleur de domaine
- S2 : autorité de certification racine entreprise (CorpRootCa)
- W10 : client Active Directory

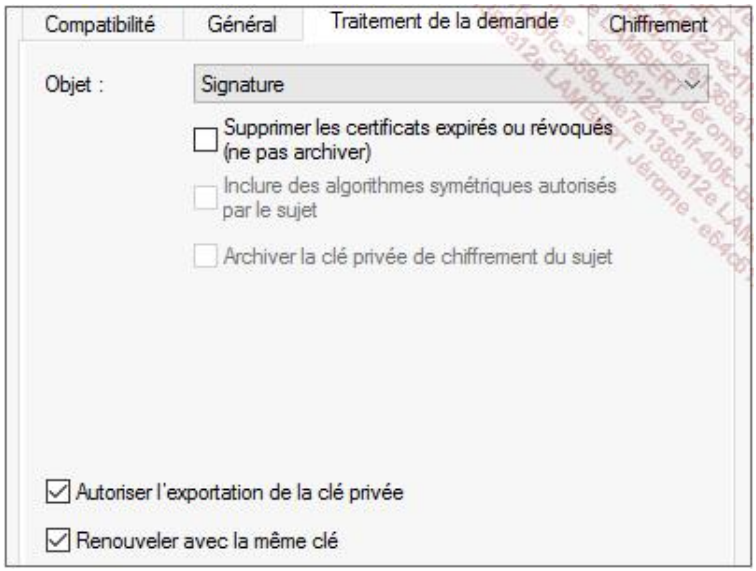
2. Obtenir un certificat de signature de code

Créer un nouveau modèle de certificats Signature de code

- Connectez-vous sur le serveur s2 en tant que Corp\Admin.
- Ouvrez la console de gestion **Autorité de certification**.
- Développez CorpRootEntCA.
- Faites un clic droit sur **Modèles de certificats** et sélectionnez le menu **Gérer**.

La console de gestion Modèles de certificats s'affiche.

- Faites un clic droit sur le modèle **Signature de code** et sélectionnez le menu **Dupliquer le modèle**.
- Sélectionnez l'onglet **Compatibilité**, développez la liste déroulante **Autorité de certification**, sélectionnez **Windows Server 2016** et cliquez sur le bouton **OK** pour accepter les modifications résultantes.
- Développez la liste déroulante **Destinataire du certificat**, sélectionnez **Windows 10 / Windows Server 2016** et cliquez le bouton **OK** pour accepter les modifications résultantes.
- Sélectionnez l'onglet **Général**, saisissez **Corp Signature du code** dans la zone **Nom complet**.
- Sélectionnez l'onglet **Sécurité**, ajoutez le compte Corp\Admin puis cochez les autorisations **Lecture** et **Inscrire** pour cet utilisateur.
- Sélectionnez l'onglet **Traitement de la demande** et cochez les cases **Autoriser l'exportation de la clé privée**.
- Cochez **Renouveler avec la même clé**.



Le renouvellement avec les mêmes clés permet le support des anciens scripts signés.

- Fermez la fenêtre de gestion Modèles de certificats.

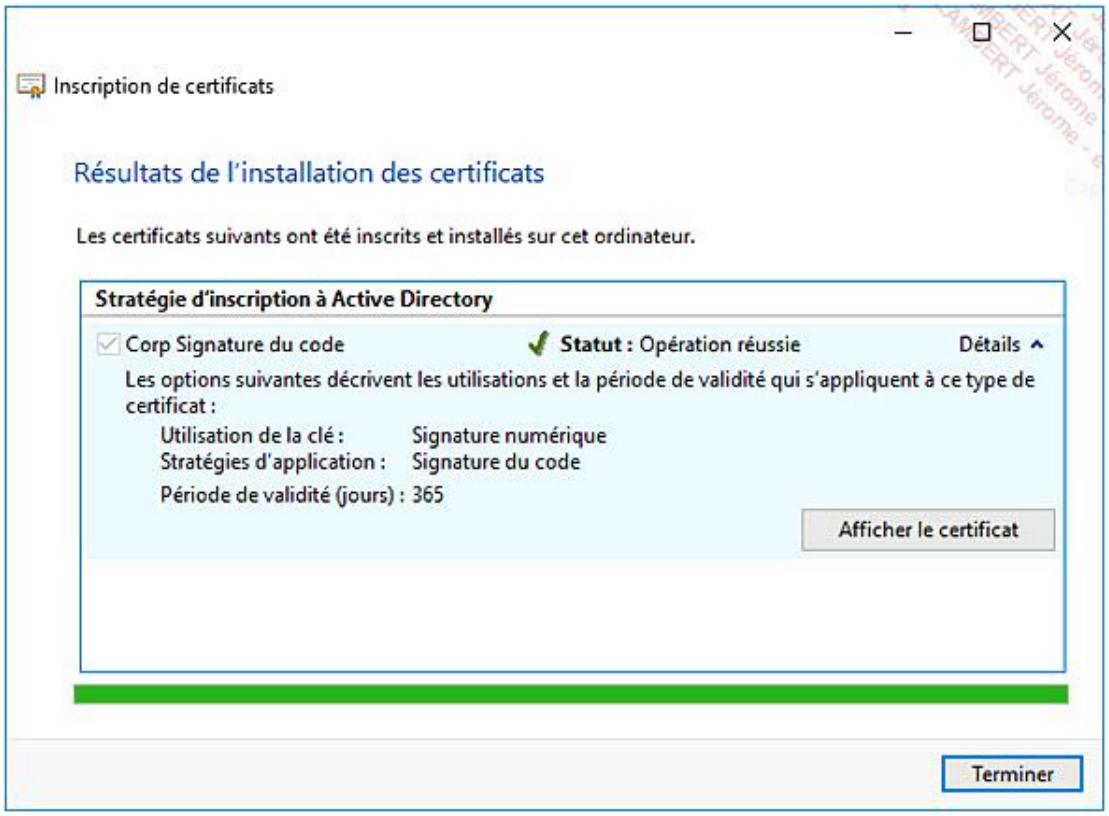
Publier le nouveau modèle de certificat

- Dans la fenêtre Autorité de certification, faites un clic droit sur **Modèles de certificats** et sélectionnez les menus **Nouveau\Modèle de certificat à délivrer**.
- Dans la fenêtre Activer les modèles de certificats, sélectionnez le modèle de certificat **Corp Signature du code** et cliquez sur le bouton **OK**.

Le nouveau modèle de certificat peut maintenant être distribué par l'autorité de certification.

Inscrire un certificat d'agent de récupération de clé

- Connectez-vous en tant que Corp\Admin sur l'ordinateur client w10.
- Ouvrez une invite de commande PowerShell et exécutez la commande **`certmgr.msc`**.
- Dans la console Certificats - Utilisateur Actuel, faites un clic droit sur le dossier Personnel et sélectionnez les menus **Toutes les tâches et Demander un nouveau certificat**.
- Dans l'assistant Inscription de certificats, dans la fenêtre Avant de commencer, lisez les recommandations puis cliquez sur le bouton **Suivant**.
- Dans la fenêtre Sélectionner la stratégie d'inscription de certificat, validez que la sélection par défaut est bien **Stratégie d'inscription à Active Directory** puis cliquez sur le bouton **Suivant**.
- Dans la fenêtre Demander des certificats, cochez le modèle **Corp Signature du code**.
- Développez le menu **Détails** du modèle Utilisateur (cliquez sur l'icône flèche vers le bas à droite du menu **Détails**), cliquez sur le bouton **Propriétés** et, dans la zone **Nom convivial** de l'onglet **Général**, saisissez **Certificat Corp Signature du code Admin**.
- Cliquez sur les boutons **OK** et **Inscription**.



Un certificat de signature de code a bien été délivré pour une durée de vie par défaut d'une année.

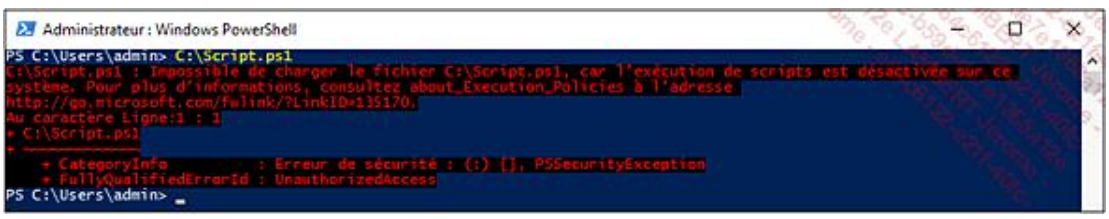
3. Modifier le niveau d'exécution PowerShell

Créer un script PowerShell

- Sur l'ordinateur client w10, créez un nouveau fichier texte nommé c:\script.txt.
- Modifiez le fichier pour ajouter la commande **`Get-Service`** et enregistrez le fichier.
- Dans l'explorateur Windows, sélectionnez le menu **Affichage** et cochez **Extensions de noms de fichiers**.
- Modifiez l'extension du fichier en .ps1.

L'icône du fichier se modifie en une icône de fichier PowerShell.

- Ouvrez une invite de commande PowerShell et exécutez la commande `C:\Script.ps1`.



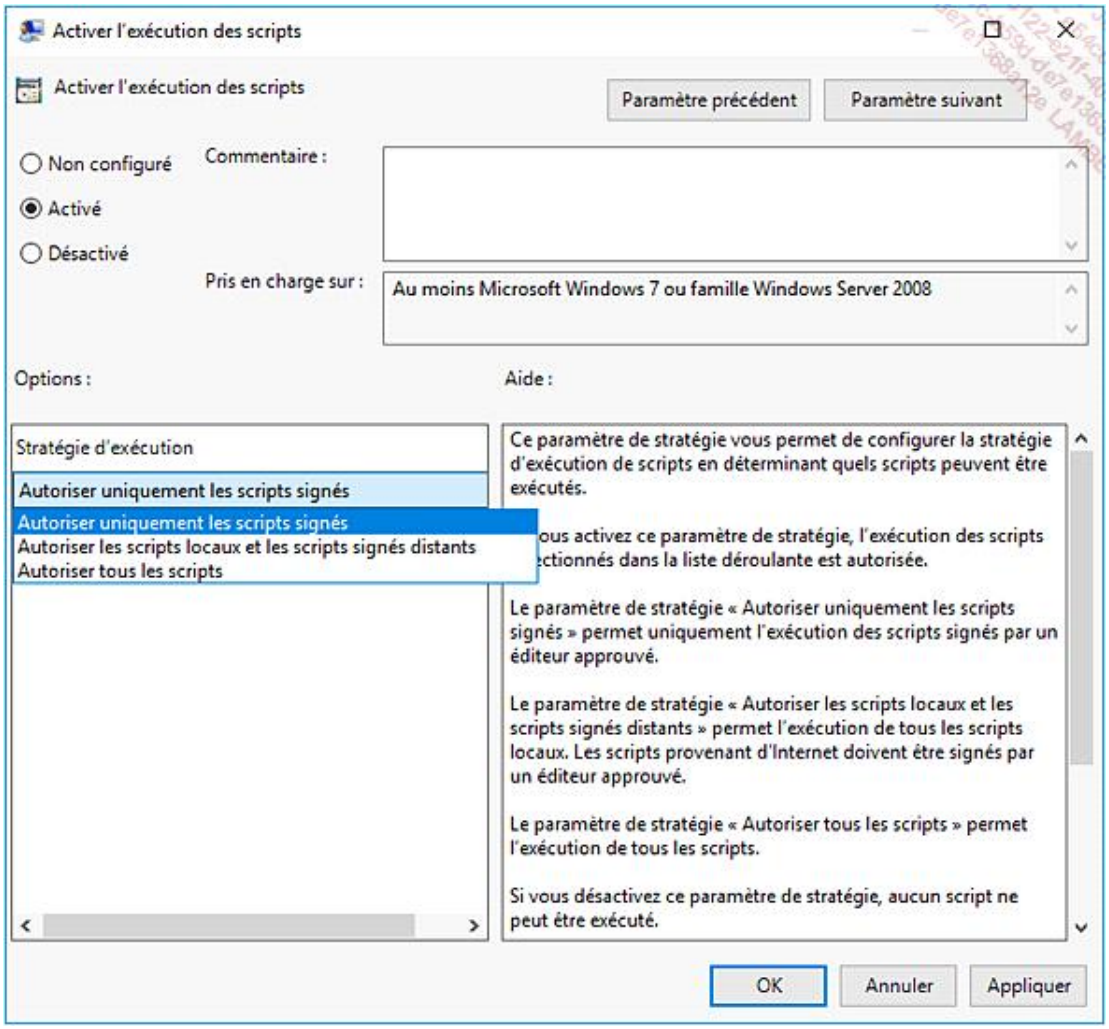
Un message d'erreur PowerShell indique que l'exécution de script est désactivée sur l'ordinateur client.

- Exécutez la commande `Get-ExecutionPolicy`.

La valeur est à Restricted. L'exécution de script n'est pas autorisée.

Autoriser l'exécution de scripts signés par stratégie de groupe

- Connectez-vous sur le contrôleur de domaine s1 en tant que Corp\admin.
- Ouvrez la console de gestion Gestion des stratégies de groupe et développez **Gestion de stratégie de groupe\Forêt:corp.lan\Domaines\corp.lan\Objets de stratégie de groupe**.
- Faites un clic droit sur **Default Domain Policy** et sélectionnez le menu **Modifier**.
- Dans la console Editeur des stratégies de groupe, développez **Configuration ordinateur\Stratégies\Modèles d'administration\Composants Windows\Windows PowerShell**.
- Faites un clic droit sur **Activer l'exécution des scripts** et sélectionnez le menu **Propriétés**.
- Cochez **Activer**.
- Développez la liste déroulante **Stratégie d'exécution** et sélectionnez **Autoriser uniquement les scripts signés**.
- Cliquez sur le bouton **OK**.



Seuls les scripts signés seront autorisés pour exécution !

- Fermez les consoles de gestion Editeur de stratégies de groupe et Gestion des stratégies de groupe.
- Redémarrez le client w10 afin d'appliquer la stratégie de groupe.

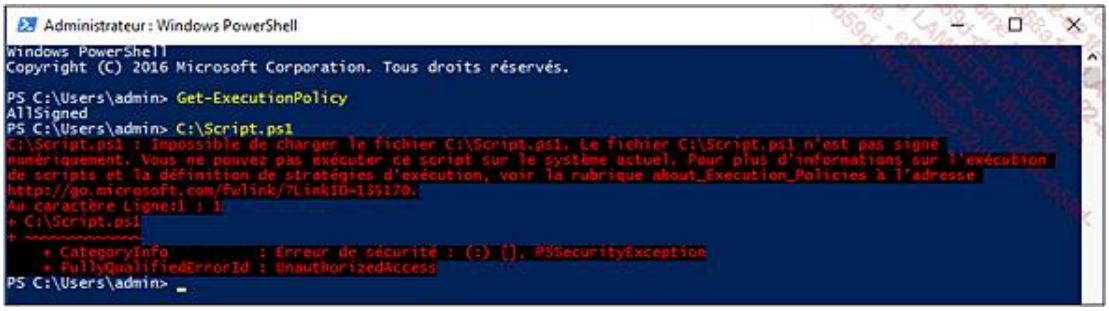
- Connectez-vous en tant que Corp\Admin sur l'ordinateur client w10.
- Ouvrez une invite de commande PowerShell et exécutez la commande :

```
Get-ExecutionPolicy
```

La valeur est à AllSigned. L'exécution de scripts signés est maintenant autorisée.

- Exécutez la commande `C:\Script.ps1`.

L'exécution du script échoue.



Un message d'erreur PowerShell indique que notre script n'est pas signé numériquement et qu'il ne peut donc pas être exécuté.

4. Signature du script

- Connectez-vous en tant que Corp\Admin sur l'ordinateur client w10.
- Exécutez les commandes suivantes pour signer le script PowerShell :

```
> Cd cert:
> Dir
... Explore le magasin de certificats

> Cd CurrentUser\my
> Dir
... Sélectionne le magasin de certificat de l'utilisateur local et
liste son contenu. Le certificat de l'utilisateur apparaît, identifié
par son empreinte numérique

> Dir -CodeSigningCert
... Cette commande renvoie la liste des certificats qui peuvent être
utilisés pour la signature de code PowerShell

> $cert = dir -CodeSigningCert
... Stocke le certificat de signature de code de l'utilisateur
dans une variable ($cert) afin de simplifier la syntaxe
de la commande suivante

> Set-AuthenticodeSignature C:\Script.ps1 -Certificate $cert
... Signe le script PowerShell Script.ps1 avec le certificat
```

de signature de code de l'utilisateur

```
PS Cert:\CurrentUser\my> Dir -CodeSigningCert


   PSParentPath : Microsoft.PowerShell.Security\Certificate::CurrentUser\my

Thumbprint                                Subject
----------                                -------
998DB9C5982BBE1746D844B9B43A548ADE33F075  CN=Admin, CN=Users, DC=corp, DC=lan


PS Cert:\CurrentUser\my> $cert = dir -CodeSigningCert
PS Cert:\CurrentUser\my> $cert


   PSParentPath : Microsoft.PowerShell.Security\Certificate::CurrentUser\my

Thumbprint                                Subject
----------                                -------
998DB9C5982BBE1746D844B9B43A548ADE33F075  CN=Admin, CN=Users, DC=corp, DC=lan


PS Cert:\CurrentUser\my> Set-AuthenticodeSignature C:\Script.ps1 -Certificate $cert


    Répertoire : C:\

SignerCertificate                         Status                                 Path
-----------------                         ------                                 ----
998DB9C5982BBE1746D844B9B43A548ADE33F075  Valid                                  Script.ps1
```

La signature du script s'effectue rapidement avec quelques commandes PowerShell.

- Exécutez la commande `C:\Script.ps1`.
- Saisissez **O** pour n'exécuter le script qu'une seule fois.

```
Administrateur : Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Tous droits réservés.

PS C:\Users\admin> C:\Script.ps1

Voulez-vous exécuter le logiciel de cet éditeur non approuvé ?
Le fichier C:\Script.ps1 est publié par CN=Admin, CN=Users, DC=corp, DC=lan et n'est pas approuvé sur votre système.
N'exécutez que des scripts provenant d'éditeurs approuvés.
[N] Ne jamais exécuter  [N] Ne pas exécuter  [O] Exécuter une fois  [T] Toujours exécuter  [?] Aide
(la valeur par défaut est « N ») :o

Status   Name               DisplayName
------   ----               -----------
Stopped  AJRouter           Service de routeur AllJoyn
Stopped  ALG                Service de la passerelle de la couc...
Stopped  AppIDSvc           Identité de l'application
Running  Appinfo            Informations d'application
Stopped  AppMgmt            Gestion d'applications
Stopped  AppReadiness       Préparation des applications
```

Le script signé peut maintenant être exécuté !

- Ouvrez le fichier de script PowerShell avec l'application Bloc-notes.

Le fichier inclut une signature de code.

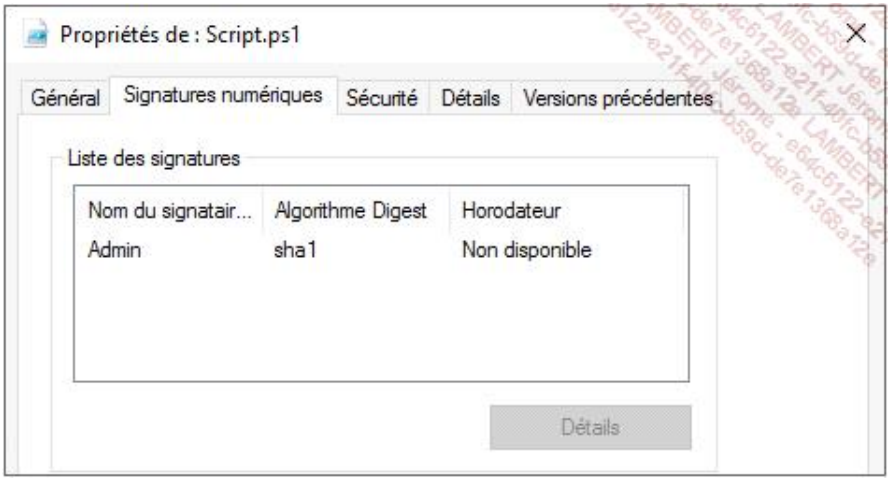
Le fichier de script inclut le bloc de signature à la fin du fichier !

5. Éditeur authentifié

L'éditeur du script (celui qui a signé le script) peut-être visible dans les propriétés du script.

a. Visualiser le certificat de l'éditeur approuvé

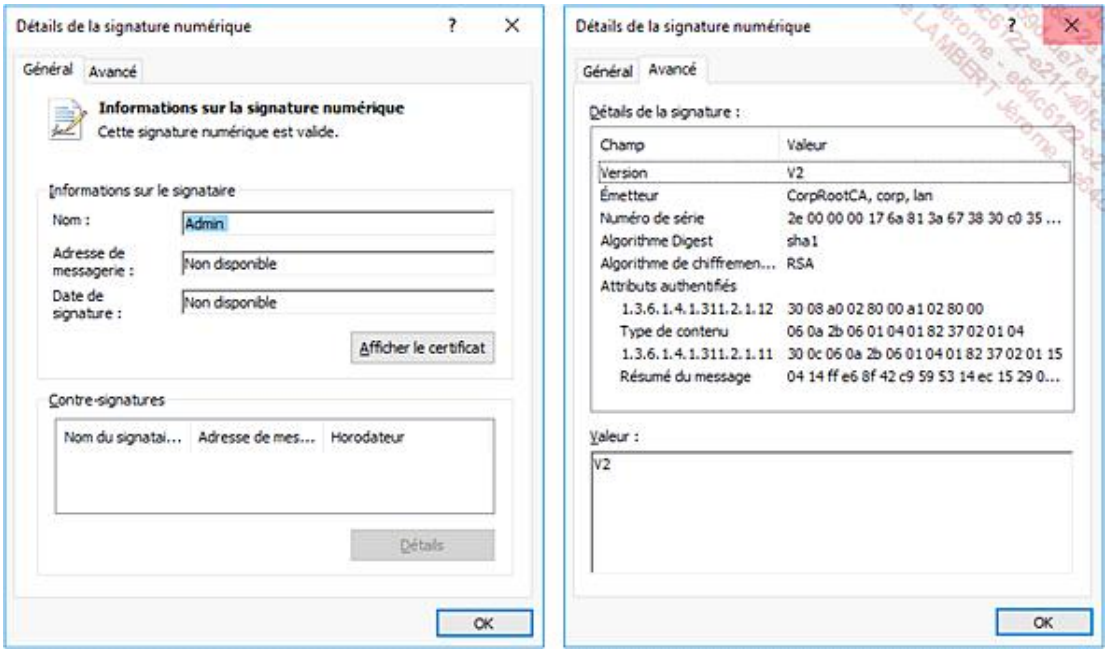
- Affichez les propriétés du fichier de script PowerShell, sélectionnez l'onglet **Signatures numériques** et validez le nom du signataire.



L'éditeur ou signataire du fichier est visible dans les propriétés du script signé.

- Sélectionnez le signataire (admin), cliquez sur le bouton **Détails** puis cliquez sur **Afficher le certificat** pour vérifier le certificat utilisé pour la signature du script.

Notez ici que le certificat affiché ne contient pas la clé privée du signataire mais uniquement sa clé publique utilisée pour valider la signature du script !



*Les onglets **Général** et **Avancé** présentent le certificat utilisé pour valider la signature et d'autres informations comme les algorithmes de chiffrement et de signature (ici Sha1).*

- Exécutez la commande `C:\Script.ps1`.

Une confirmation est à nouveau demandée.

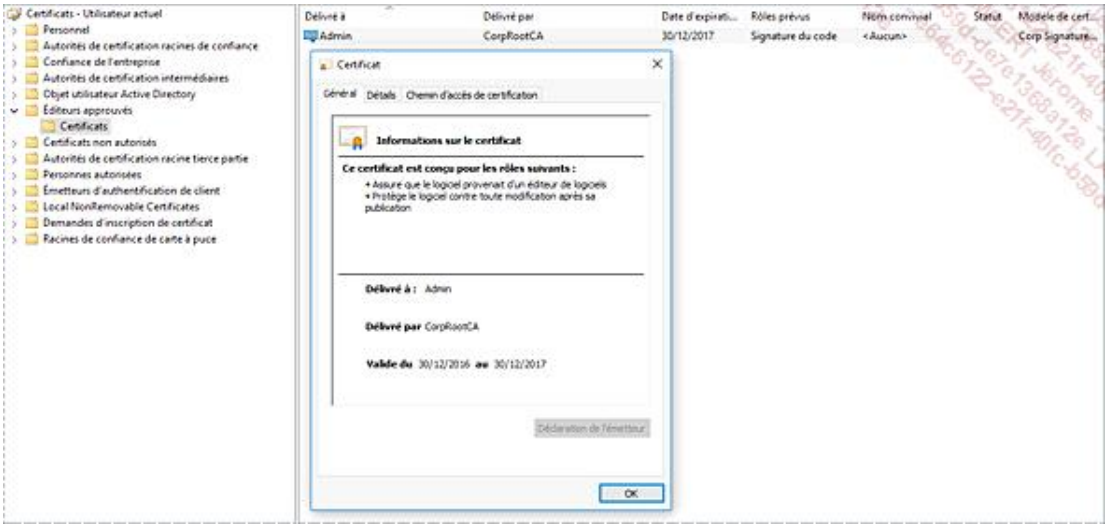
- Saisissez **o** pour n'exécuter le script qu'une seule fois.
- Exécutez la commande `C:\Script.ps1`.

Une confirmation est à nouveau demandée

- Saisissez **t** pour n'exécuter le script qu'une seule fois.
- Exécutez la commande `C:\Script.ps1`.

Aucune demande de confirmation n'est demandée. Le script s'exécute automatiquement.

- Exécutez la commande **`Certmgr.msc`** pour ouvrir la console de gestion de certificat de l'utilisateur local.
- Développez **Certificats - Utilisateur actuel\Editeurs approuvés\Certificats**.



Le conteneur Éditeurs approuvés\Certificats contient le certificat de l'éditeur, signataire du script PowerShell !

- Sélectionnez le certificat de l'éditeur et supprimez-le.
- Exécutez la commande `C:\Script.ps1`.

  Une confirmation est à nouveau demandée.
- Saisissez **t** pour n'exécuter le script qu'une seule fois.
- Exécutez la commande :

```
C:\Script.ps1
```

Aucune demande de confirmation n'est demandée. Le script s'exécute automatiquement.

- Dans la console de gestion de certificat de l'utilisateur local, validez que le certificat de l'éditeur apparaît à nouveau dans le conteneur Certificats - Utilisateur actuel\Editeurs approuvés\Certificats.

Disposer d'un certificat d'éditeur\Signataire du code PowerShell sur l'ordinateur local permet donc une exécution transparente du script (pas de demande de confirmation).

b. Déployer les certificats d'éditeur par stratégies de groupe

- Dans le gestionnaire de certificat de l'utilisateur local, développez **Editeurs approuvés\Certificats**, sélectionnez à nouveau le certificat de l'éditeur et supprimez-le

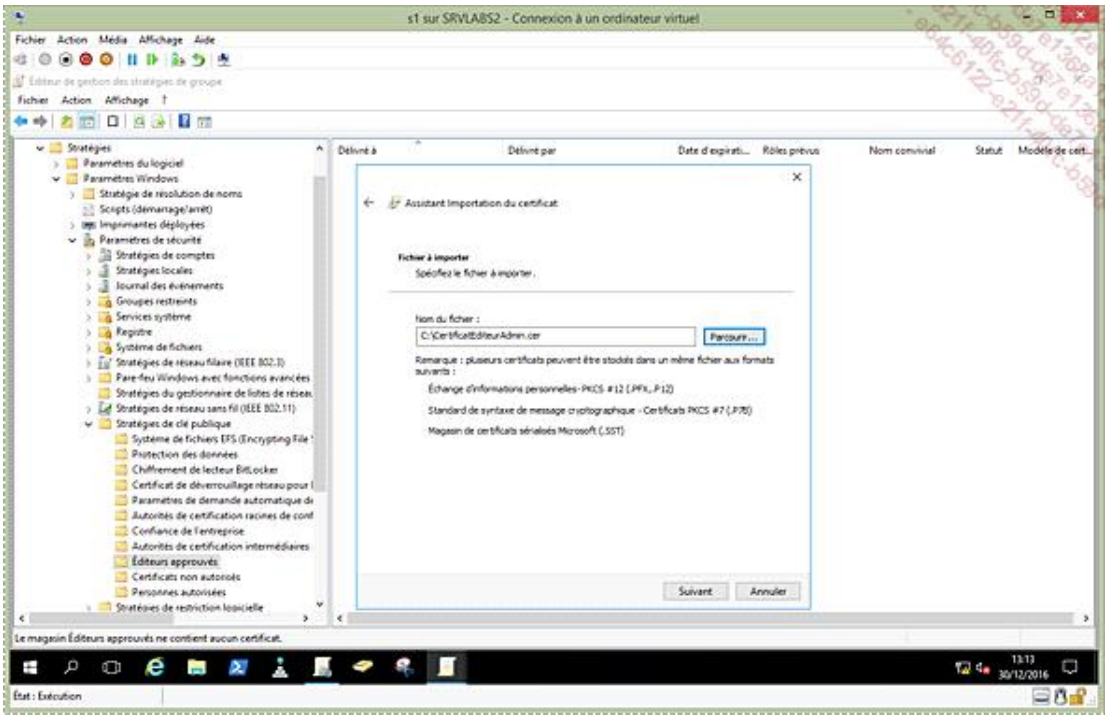
Exporter le certificat de l'éditeur

- Dans le gestionnaire de certificat de l'utilisateur local, développez **Certificats - Utilisateur actuel\Personnel\Certificats**.
- Faites un clic droit sur le certificat, sélectionnez le menu **Toutes les tâches** puis le menu **Exporter**.
- La boîte de dialogue Assistant exportation du certificat s'affiche, cliquez sur le bouton **Suivant**.
- Sélectionnez **Non, ne pas exporter la clé privée** puis cliquez sur le bouton **Suivant**.
- Acceptez le format de fichier par défaut (.cer) et cliquez sur le bouton **Suivant**.

- Dans la zone **Nom de fichier** saisissez **C:\CertificatEditeurAdmin**, cliquez sur le bouton **Enregistrer** puis sur le bouton **Suivant** et sur le bouton **Terminer**.
- Cliquez sur **OK** sur le message indiquant que l'exportation a réussi.
- Transférez le fichier C:\CertificatEditeurAdmin.cer sur le contrôleur de domaine s1 (en utilisant le partage caché administratif \\s1\c$ par exemple…).

Déploiement de l'éditeur par stratégie de groupe

- Connectez-vous sur le contrôleur de domaine s1 en tant que Corp\admin.
- Ouvrez la console de gestion Gestion des stratégies de groupe et développez **Gestion de stratégie de groupe\Forêt:corp.lan\Domaines\corp.lan\Objets de stratégie de groupe**.
- Faites un clic droit sur **Default Domain Policy** et sélectionnez le menu **Modifier**.
- Dans la console Editeur des stratégies de groupe, développez **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies de clé publique**.
- Faites un clic droit sur **Editeurs approuvés** et sélectionnez le menu **Importer**.
- Dans la fenêtre Assistant Importation du certificat, cliquez sur le bouton **Suivant**.
- Dans la fenêtre Fichier à importer, cliquez sur le bouton **Parcourir** et sélectionnez le fichier C:\CertificatEditeurAdmin.cer et cliquez sur le bouton **Suivant**.



- Dans la fenêtre Magasin de certificat, validez que le magasin de certificat sélectionné pour l'importation est bien **Editeurs approuvés**.
- Cliquez sur les boutons **Suivant** et **Terminer**.
- Cliquez sur **OK** sur la fenêtre indiquant que l'importation a réussi.

Le certificat apparaît maintenant dans la fenêtre de stratégie.

- Sur l'ordinateur client w10, exécutez la commande **`Gpupdate`** pour actualiser les stratégies de groupe.

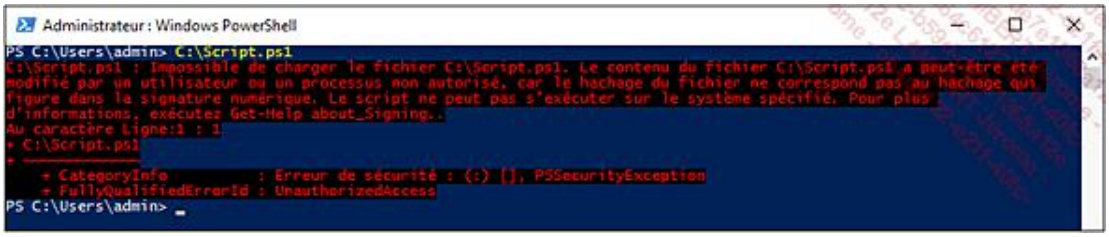
- Dans la console de gestion de certificat de l'utilisateur local, validez que le certificat de l'éditeur apparaît à nouveau dans le conteneur Certificats - Utilisateur actuel\Editeurs approuvés\Certificats.
- Exécutez la commande `C:\Script.ps1`.

Aucune demande de confirmation n'est demandée. Le script s'exécute automatiquement.

6. Intégrité du script

- Modifiez le contenu du script et essayer d'exécuter à nouveau le script.

Le script ne peut plus être exécuté.



Le message d'erreur de PowerShell indique que le hachage du fichier ne correspond pas au hachage qui figure la signature numérique.

- Signez à nouveau le script PowerShell en exécutant les commandes :

```
> $cert = dir cert:\CurrentUser\my -CodeSigningCert
> Set-AuthenticodeSignature c:\script.ps1 -Certificate $cert
```

- Exécutez le script PowerShell.

Le script s'exécute à nouveau correctement.

7. Horodatage du script

Nous allons maintenant appliquer un horodatage numérique au script PowerShell afin qu'il reste exécutable même après l'expiration du certificat de signature.

a. Connexion à Internet

Le serveur de temps utilisé pour l'horodatage (Comodo.com) étant sur Internet, une carte réseau supplémentaire doit être ajoutée à l'ordinateur client w10 afin d'autoriser sa connexion Internet.

Ajouter une carte réseau pour la connexion Internet

- Arrêtez l'ordinateur client w10.
- Ouvrez le menu **Fichier\Paramètres** de l'ordinateur virtuel w10 et sélectionnez **Ajouter un matériel**.
- Dans la zone **Sélectionnez les périphériques à ajouter**, sélectionnez **Carte réseau** puis cliquez sur le bouton **Ajouter**.

- Développez la liste déroulante **Commutateur virtuel**, sélectionnez **PcInternet** et cliquez sur le bouton **OK**.

Le commutateur virtuel PcInternet, autorisant une connexion Internet pour les ordinateurs virtuels, a été créé dans l'atelier pratique du chapitre Plateforme de test.

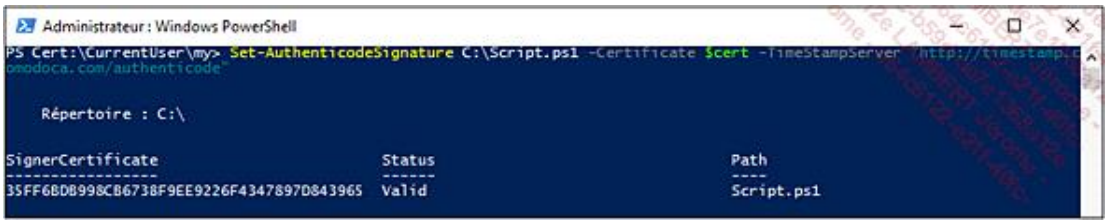
- Redémarrez l'ordinateur client w10.
- Connectez-vous sur l'ordinateur client w10 en tant que Corp\Admin.
- Ouvrez une invite de commande PowerShell et exécutez la commande **`Ping www.google.com`** pour valider la connexion à Internet.

b. Horodatage du script

Signature avec horodatage

- Appliquez un horodatage au script PowerShell en exécutant la commande suivante :

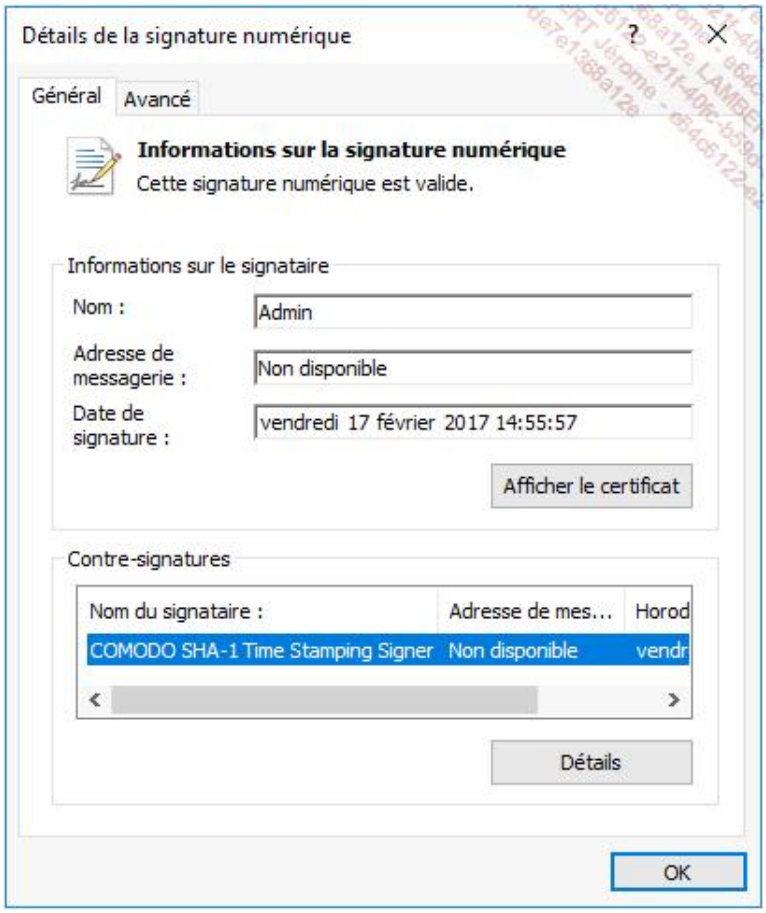
```
> Set-AuthenticodeSignature C:\Script.ps1 -Certificate $cert
-TimeStampServer http://timestamp.comodoca.com/authenticode
... signe et applique en horodatage utilisant le serveur
de temps de Comodo
```



Le script est signé à nouveau mais avec l'ajout d'un horodatage (il restera toujours exécutable sauf en cas de révocation).

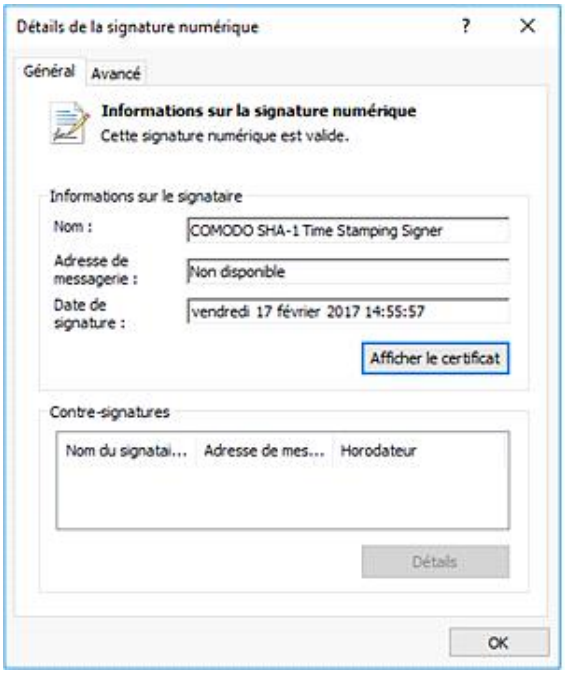
Valider l'horodatage

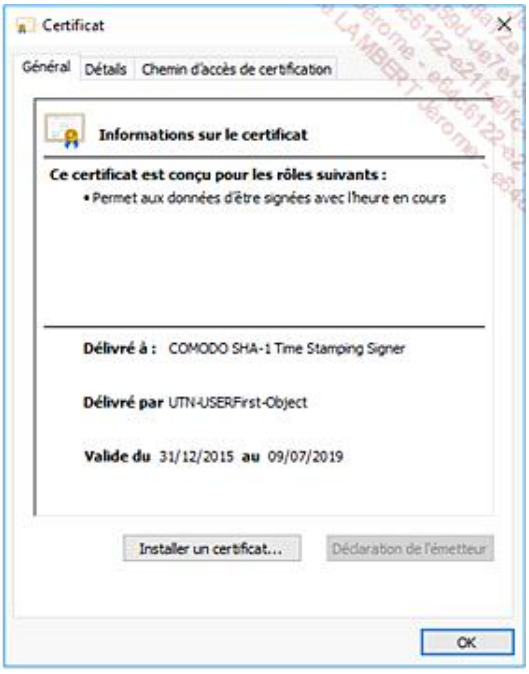
- Faites un clic droit sur le fichier C:\Script.ps1 et sélectionnez le menu **Propriétés**.
- Sélectionnez l'onglet **Signature de code** puis cliquez sur le bouton **Détails**.



*La zone **Contre-signatures** indique l'utilisation d'un serveur de temps (COMODO SHA-1 Time Stamping Signer).*

- Dans la zone **Contre-signatures**, sélectionnez le nom du destinataire **Comodo** puis cliquez sur le bouton **Détails**.
- Validez le nom du signataire et les dates et heures de la signature.
- Cliquez sur le bouton **Afficher le certificat** pour afficher le certificat du serveur de temps Comodo.





Un horodatage a été appliqué par le serveur Comodo (avec un algorithme de Hachage SHA-1) à la date et heure indiquées. Le certificat du serveur de temps peut être affiché.

8. Révocation de certificats de signature de scripts

Pour la réalisation de cet atelier, reportez-vous aux ateliers du chapitre Révocation de certificat dans l'entreprise (section Révocation de certificats de signature de scripts).

Si vous souhaitez reporter cet atelier de vocation, effectuez un point de contrôle (nommé **SignaturePowerShell**) sur tous les ordinateurs virtuels afin de pouvoir restaurer cet environnement lorsque vous réaliserez l'atelier.