Mise en place du TLS/SSL pour WSUS

Présentation

Par défaut, WSUS ne chiffre pas les données. De nombreuses failles ont été découvertes, et pour les corriger, il faut activer le SSL. Pour cela, on aura besoin de modifier la GPO de l'emplacement du WSUS (remplacer http:// par https://) et d'ajouter un certificat.
Un exemple de l'importance du SSL:

Vidéo YouTube faite par 2 intervenants au Black Hat

La mise en place du SSL demandera plus de performance sur le serveur, dû au chiffrement.

Pour la suite, il est nécessaire d'avoir de nombreux modules, comme "Scripts et outils de gestion IIS", GroupPolicy.

Sélectionner des rôles de serveurs

Rôles

Avant de commencer Type d'installation Sélection du serveur

Rôles de serveurs

Fonctionnalités Confirmation

Résultat

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Attestation d'intégrité de l'appareil
☐ Hyper-V
Serveur de télécopie
Serveur DHCP
Serveur DNS
■ Serveur Web (IIS) (11 sur 43 installé(s))
■ Outils de gestion (2 sur 7 installé(s))
✓ Console de gestion IIS (Installé)
✓ Scripts et outils de gestion IIS
Service de gestion
Serveur FTP Serve
Service Guardian hôte
Services AD DS
Services AD LDS (Active Directory Lightweight Dire
Services AD RMS (Active Directory Rights Manager
Services Bureau à distance
Services d'activation en volume

Description

Le composant Scripts et outils de gestion d'IIS fournit une infrastructure pour gérer par programmation un serveur web IIS 10 à l'aide de commandes dans une fenêtre de commande ou en exécutant des scripts. Vous pouvez utiliser ces outils quand vous voulez automatiser des commandes dans des fichiers de commandes ou quand vous voulez éviter la surcharge liée à la gestion d'IIS à l'aide de l'interface utilisateur.

Activation du SSL sur WSUS

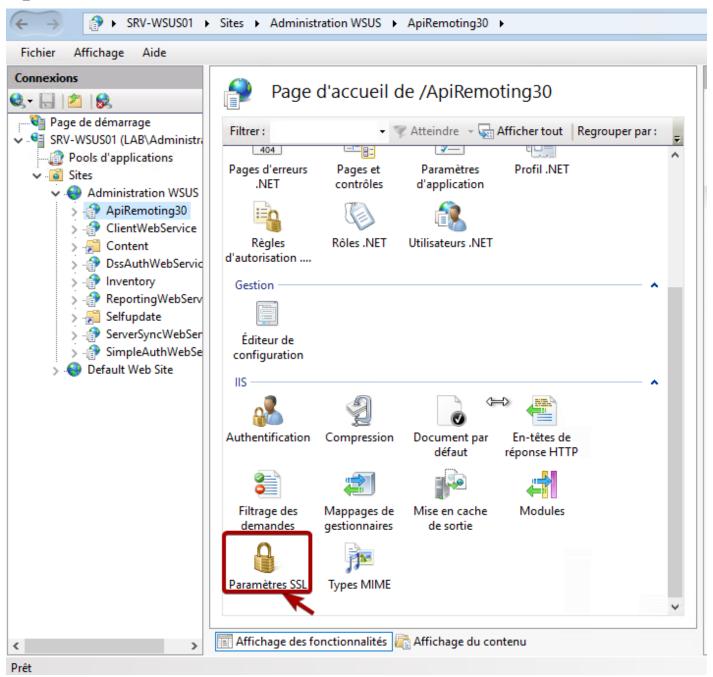
Dans mon cas, j'ai récupéré le certificat et la clé privée depuis mon serveur web (fullchain.pem et privkey.pem). J'ai converti en .pfx. Une page est disponible pour cela. De plus j'ai défini un mot de passe.

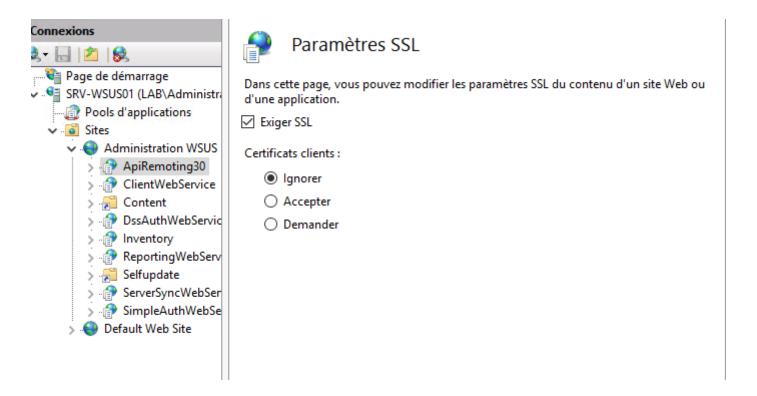
```
Import-Module ServerManager
Add-WindowsFeature Web-Scripting-Tools
Install-WindowsFeature GPMC
Install-Module -Name PowerShellGet -Force
Install-Module —Name IISAdministration
Import-Module WebAdministration
Import-Module IISAdministration
Import-Module GroupPolicy

$myFQDN=(Get-WmiObject win32_computersystem).DNSHostName+"."+(Get-WmiObject win32_computersystem).Domain; Write-Host $myFQDN
# 1. Create a self-signed certificate
```

```
$SelfSignedHT = @{
DnsName = "$($env: COMPUTERNAME).$($env: USERDNSDOMAIN)". ToLower()
CertStoreLocation = "Cert: \LocalMachine\My"
}
New-SelfSignedCertificate @SelfSignedHT
$cert = Get-ChildItem -Path Cert: \LocalMachine\My -SSLServerAuthentication
# 2. Export its public key
Export-Certificate - Cert $cert - Type CERT - FilePath ~/documents/cert.cer
# 3. Import the public key in the Trusted Root Certificate Authorities store
Import-Certificate -FilePath ~/documents/cert.cer -CertStoreLocation Cert: \LocalMachine\Root
# 4. Select this certificate in the SSL bindings
$cert | New-Item IIS: \SslBindings\0. 0. 0. 0! 8531
# MANUALLY require SSL IIS - voir plus bas
# 6. Switch WSUS to SSL
& 'C: \Program Files\Update Services\Tools\WsusUtil.exe' configuressl $("$myFQDN".ToLower())
# 7. Change your GPO to point to the new URL
$key = 'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate'
suri = 'https: //{0}: 8531' - f s("smyFQDN". ToLower())
Get-GPO -All | Foreach-Object {
if ($_ | Get-GPRegistryValue -Key $key -ValueName WUServer -EA 0) {
 $ | Set-GPRegistryValue - Key $key - ValueName WUServer - Value $uri - Type String
 $ | Set-GPRegistryValue - Key $key - ValueName WUStatusServer - Value $uri - Type String
}
}
```

Sur IIS, pour chaque page, on change les paramètres SSL.

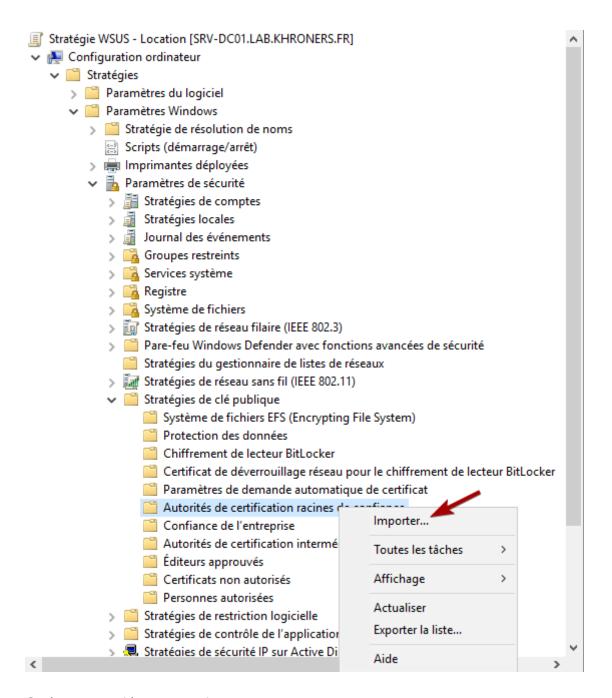




On fait cela pour SimpleAuthWebService, DSSAuthWebService, ServerSyncWebService, APIRemoting30 et ClientWebService.

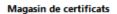
Publication du certificat

Dans la GPO "WSUS - Location", on importe le certificat.



On importe ~/documents/cert.cer.





Les magasins de certificats sont des zones système où les certificats sont conservés.

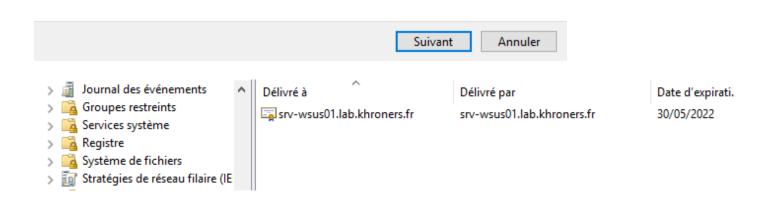
Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier un emplacement pour le certificat.

- Sélectionner automatiquement le magasin de certificats en fonction du type de certificat
- Placer tous les certificats dans le magasin suivant

Magasin de certificats :

Autorités de certification racines de confiance

Parcourir...



Conclusion

Dans la console WSUS, on est bien en SSL.

État des mises à jour

Mises à jour avec des erreurs :

Mises à jour requises par des ordinateurs : 9
 Mises à jour installées/non applicables : 718

Statistiques du serveur

Mises à jour non approuvées : 730 Mises à jour approuvées : 23 Mises à jour refusées : 768 Ordinateurs : 5 Groupes d'ordinateurs : 2 État de téléchargement

Mises à jour nécessitant des fichiers: 0

Connexion

0

Type: Local/SSL Port: 8531

Rôle de l'utilisateur : Administrateur Version du serveur : 10.0.17763.678

Ressources

On peut vérifier les logs de Windows Update d'un client via l'invité Powershell :

Get-Windowsupdatelog

Revision #10

Created 29 May 2021 23:11:19 by Khroners

Updated 30 December 2021 23:45:14 by Khroners