

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.

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

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

Rôles

☐ Attestation d'intégrité de l'appareil

☐ Hyper-V

☐ Serveur de télécopie

☐ Serveur DHCP

☐ Serveur DNS

☒ Serveur Web (IIS) (11 sur 43 installé(s))

☒ Serveur Web (9 sur 34 installé(s))

☒ Outils de gestion (2 sur 7 installé(s))

☒ Console de gestion IIS (Installé)

☒ Compatibilité avec la gestion IIS 6 (1 sur 4 i

☒ Scripts et outils de gestion IIS

☐ Service de gestion

☐ Serveur FTP

☐ Service Guardian hôte

☐ Services AD DS

☐ Services AD LDS (Active Directory Lightweight Dire

☐ Services AD RMS (Active Directory Rights Manage

☐ 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'
$uri = 'https://{0}:8531' -f $("myFQDN".ToLower())
Get-GPO -All | ForEach-Object {
    if ($_ | 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.

SRV-WSUS01 > Sites > Administration WSUS > ApiRemoting30

Fichier Affichage Aide

Connexions

- Page de démarrage
- SRV-WSUS01 (LAB\Administrat...
- Pools d'applications
- Sites
 - Administration WSUS
 - ApiRemoting30
 - ClientWebService
 - Content
 - DssAuthWebServic
 - Inventory
 - ReportingWebServ
 - Selfupdate
 - ServerSyncWebSer
 - SimpleAuthWebSe
 - Default Web Site

Page d'accueil de /ApiRemoting30

Filtrer : 404 Atteindre Afficher tout Regrouper par :

Pages d'erreurs .NET

Pages et contrôles

Paramètres d'application

Profil .NET

Règles d'autorisation

Rôles .NET

Utilisateurs .NET

Gestion

Éditeur de configuration

IIS

Authentification

Compression

Document par défaut

En-têtes de réponse HTTP

Filtrage des demandes

Mappages de gestionnaires

Mise en cache de sortie

Modules

Paramètres SSL

Types MIME

Affichage des fonctionnalités Affichage du contenu

Prêt

Connexions

Page de démarrage

SRV-WSUS01 (LAB\Administr

Pools d'applications

Sites

Administration WSUS

ApiRemoting30

ClientWebService

Content

DssAuthWebService

Inventory


ReportingWebServ

Selfupdate

ServerSyncWebSer

SimpleAuthWebSe

Default Web Site

 Paramètres SSL

Dans cette page, vous pouvez modifier les paramètres SSL du contenu d'un site Web ou d'une application.

☒ Exiger SSL

Certificats clients :

☒ Ignorer

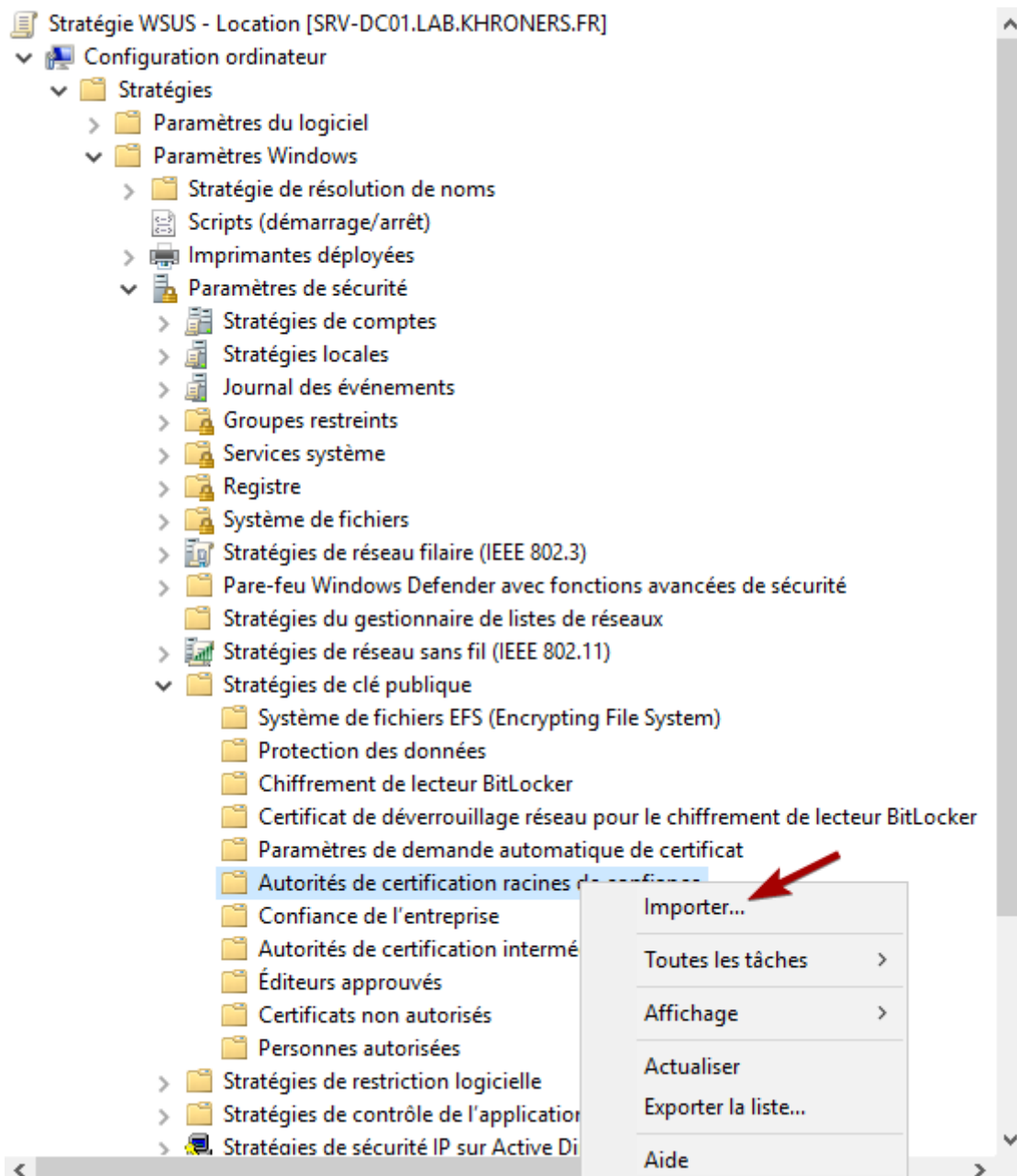
☐ Accepter

☐ Demander

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.

Magasin de certificats

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...

Suivant

Annuler

>  Journal des événements	^	Délivré à	^	Délivré par	Date d'expirati.
>  Groupes restreints		 srv-wsus01.lab.khroners.fr		srv-wsus01.lab.khroners.fr	30/05/2022
>  Services système					
>  Registre					
>  Système de fichiers					
>  Stratégies de réseau filaire (IE)					

Conclusion

Dans la console WSUS, on est bien en SSL.

État des mises à jour



Mises à jour avec des erreurs :	0
Mises à jour requises par des ordinateurs :	9
Mises à jour installées/non applicables :	718

État de téléchargement

Mises à jour nécessitant des fichiers : 0

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

Connexion

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- Windowsupdate log
```

Revision #10

Created 29 May 2021 23:11:19 by Khroners

Updated 30 December 2021 23:45:14 by Khroners