Devolutions

[TUTORIEL] Comment renforcer la sécurité de votre serveur IIS avec des certificats clients

LES CERTIFICATS SONT FACILES À DÉPLOYER DANS UNE INFRASTRUCTURE ACTIVE DIRECTORY

Les certificats sont faciles à déployer dans une infrastructure **Active Directory (AD)**, mais les utiliser pour gérer les accès, surtout pour les sites Web hébergés sur un serveur IIS (de l'anglais *Internet Information Services*), peut s'avérer ardu en raison de l'absence de documentation pertinente sur Internet. Alors, j'ai décidé de créer ce tutoriel afin de vous aider à configurer cette fonctionnalité sur un serveur IIS. Ce tutoriel peut également servir d'aide-mémoire dans le futur.

Pourquoi devrais-je activer cette fonctionnalité?

Cette fonctionnalité ajoute un niveau d'authentification pour assurer la légitimité d'un client avant que ce client ait accès à un site Web très sensible. Il peut être configuré devant vos sites Web ou en tant que sous-ensemble de vos sites Web. Seuls les utilisateurs ayant le bon certificat verront leur accès accordé.

Est-ce vraiment sécuritaire?

Cette forme d'algorithme d'authentification est renforcée mathématiquement avec de la cryptographie asymétrique. L'authentification du client **TLS** (anciennement SSL) fait partie du protocole Transport Layer Protocol depuis longtemps, et c'est un standard approuvé par l'industrie pour sécuriser les communications.

Cette fonctionnalité sert aussi aux grandes organisations feature qui doivent s'assurer que seuls les utilisateurs autorisés ont accès aux sites Web internes.

Puisque cette fonctionnalité fait partie du standard **TLS**, la plupart des serveurs, tels qu'IIS, Apache et Nginx, la prennent en charge de façon native. Elle est également prise en charge nativement par les navigateurs les plus populaires (p.ex., Internet Explorer, Chrome, Firefox, etc.).

Éléments requis

Voici ce dont vous avez besoin pour ce tutoriel :

- Certificat provenant d'une autorité de certificat reconnue
- Certificat de serveur
- Certificat(s) client(s) (pour les utilisateurs)

Avant de commencer

Si vous devez générer des certificats, veuillez suivre mon article de blogue. Lorsque vous avez terminé, suivez les étapes suivantes :

1. Installer le fichier **ca.crt** (*clé publique*) dans le magasin de certificats du serveur IIS suivant :
Local Computer -> Trusted Root Certification Authorities

2. Fusionner les fichiers **server.crt** (*clé publique*) et **server.key** (*clé privée*) en un seul fichier nommé **server.pfx** à l'aide de la commande suivante :

```
openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
```

Vous serez invité à saisir un mot de passe : choisissez-en un robuste.

Installer le fichier server.pfx dans le magasin de certificats du serveur IIS suivant :

Local Computer -> Personal

3. Chaque client qui aura accès au serveur requiert un certificat. Tout comme le certificat de serveur ci-haut, la **clé publique** (.crt) et la **clé privée** (.key) doivent être fusionnées dans un seul fichier nommé <client name>.pfx. Le fichier résultant, `<client name>.pfx`, doit être installé sur l'ordinateur de l'utilisateur dans le magasin suivant :

Current User -> Personal

J'ai simplifié ce tutoriel en proposant des étapes faciles à suivre. J'explique comment le faire manuellement, puis quelles commandes PowerShell utiliser. Cependant, il est possible d'avoir à modifier certains scripts pour qu'ils correspondent à votre environnement.

Comment configurer IIS

Étape 1 : Activer les fonctionnalités requises

Dans la fenêtre des fonctionnalités de Windows, activez **IIS Client Certificate Mapping Authentication**, fonction qui se retrouve dans la section **Internet Information Services → World Wide Web Services → Security** (voir l'image 1).

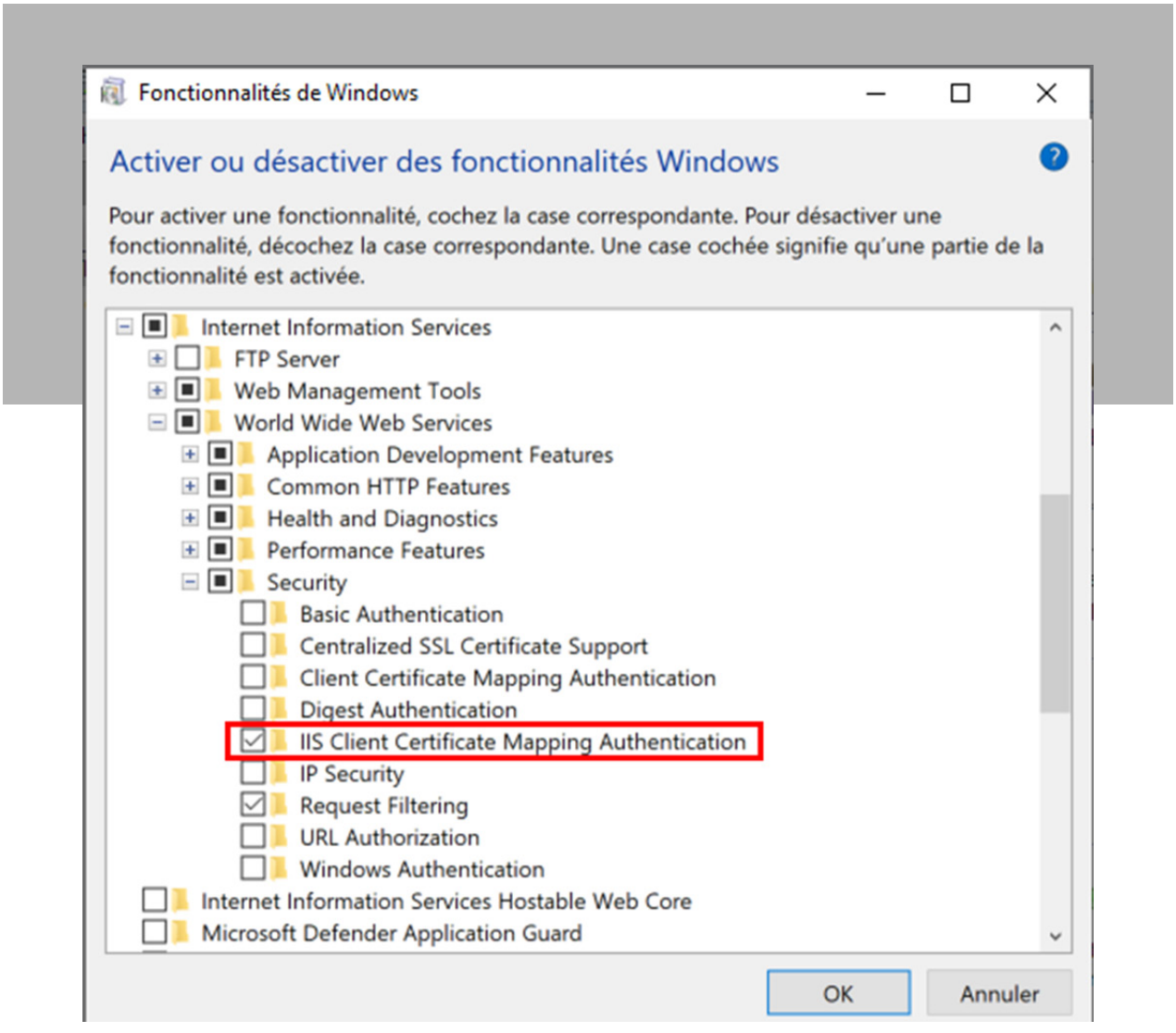
La fenêtre de dialogue Fonctionnalités de Windows peut s'afficher à l'aide du raccourci clavier suivant :

```
WIN + R -> optionalfeatures
```

Sur **Windows Server**, vous pouvez activer cette fonctionnalité dans le gestionnaire de configuration du serveur. Elle peut également être activée en exécutant la commande PowerShell suivante :

```
Enable-WindowsOptionalFeature -Online -FeatureName IIS-IISCertificateMappingAuthenticationEnable-WindowsOptionalFeature -Online -FeatureName IIS-IISCertificateMappingAuthentication
```

Image 1 – Activer la fonctionnalité IIS Client Certificate Mapping



Étape 2 : Configurer une liaison HTTPS

Configurez votre certificat SSL dans la fenêtre **Liaisons** du Gestionnaire des services Internet (IIS). Pour ouvrir la

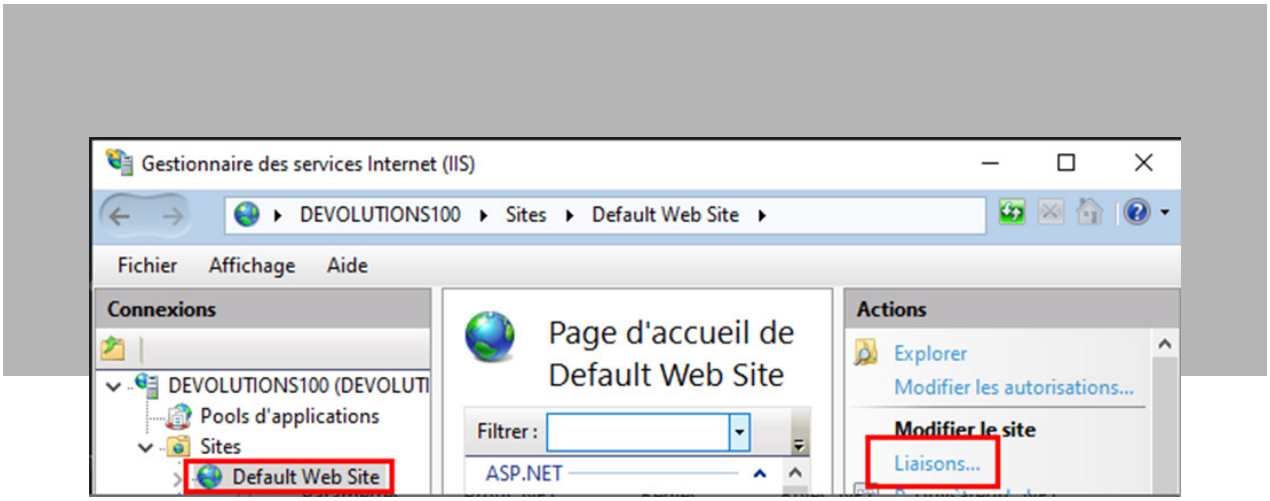
fenêtre des liaisons, **sélectionnez le site Web désiré**, puis cliquez sur **Liaisons**. Puis, ajouter une liaison HTTPS et sélectionnez votre certificat de serveur. Un exemple est illustré ci-bas (images 2 et 3):

Default Web Site → Liaisons... → Ajouter...

Vous pouvez également effectuer cette opération avec quelques commandes simples de PowerShell :

```
# Lister les certificats dans le magasin personnel de l'ordinateur local.
Get-ChildItem -Path CERT:LocalMachine/My

Thumbprint Subject
---------- -------
838E34D06C2FB5C80E99E6B6938C4127134B32A5 CN=localhost
6A11EAFFBB6A7E1F3CE11DAE82956D4F2973320E CN=mathmo.org, O="MathMoOrganisation,
Inc.", S=CA, C=US

# Créer une liaison HTTPS si elle n'exite pas
New-WebBinding -name "Default Web Site" -Protocol https -Port 443

# Obtenir les liaisons
$bindings = Get-WebBinding -Name "Default Web Site"

# Configurer le certificat mathmo.org pour les liaisons
$bindings.AddSslCertificate("6A11EAFFBB6A7E1F3CE11DAE82956D4F2973320E",'My')
```

Image 2 – Ouvrir la fenêtre de dialogue Liaisons



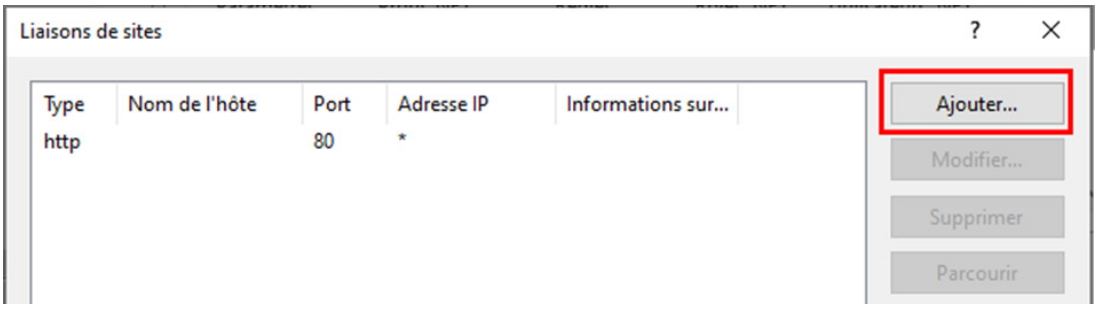
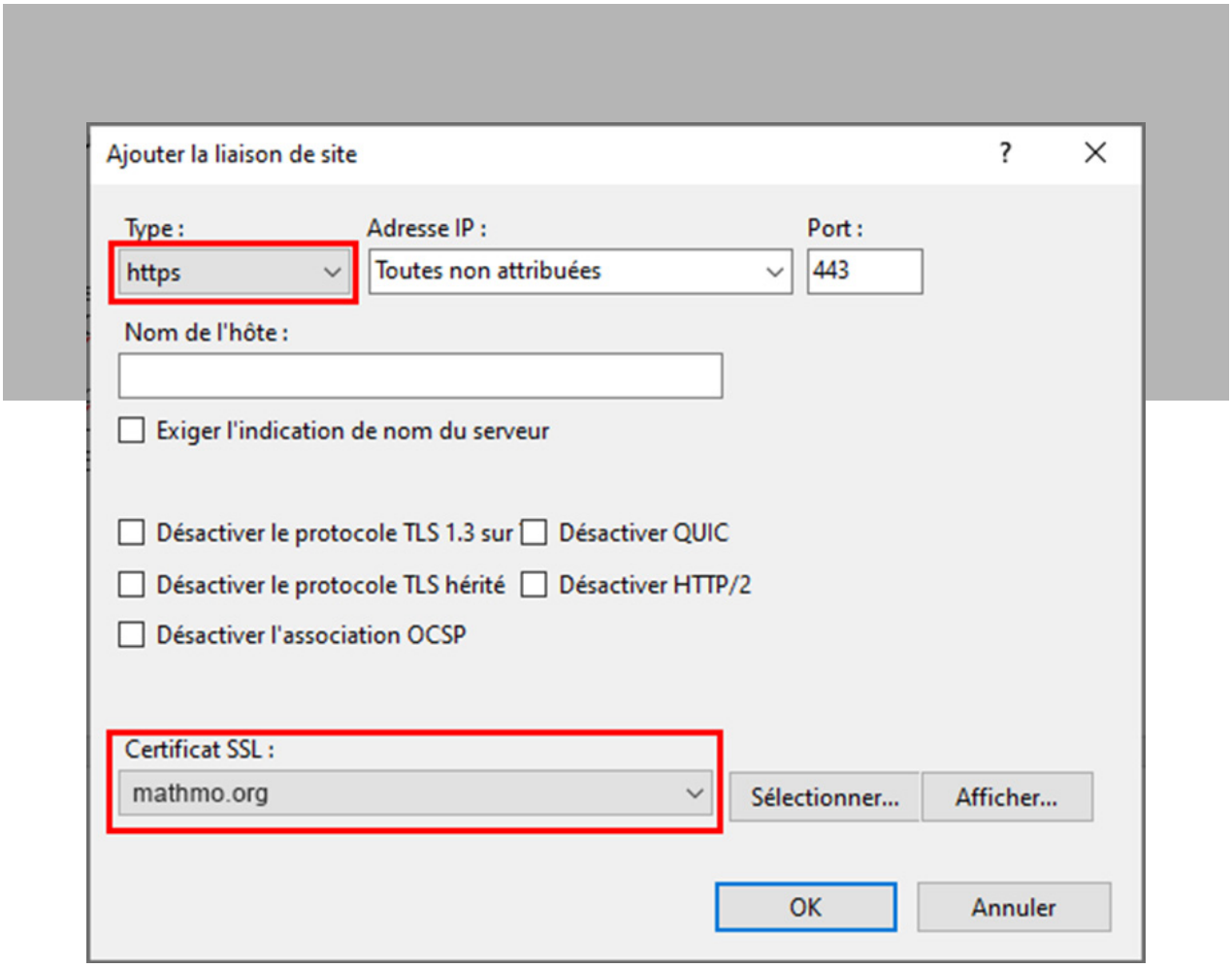


Image 3 – Configurer le certificat de serveur pour la liaison de type HTTPS



Étape 3 - Exiger SSL sur le site Web

Assurez-vous que votre site Web exige SSL ainsi qu'un certificat client. Pour ce faire, sélectionner le site Web désiré, utiliser le filtre pour les paramètres SSL et sélectionner l'option, puis cliquer sur **Ouvrir la fonctionnalité**. Dans l'exemple ci-dessous (voir les images 4 et 5), les étapes sont les suivantes :

Default Web Site → Filtre Paramètres SSL → Sélectionner Paramètres SSL → Ouvrir la fonctionnalité

Cela peut également s'effectuer avec une commande PowerShell :

```
Set-WebConfiguration -Location "Default Web Site" -Filter "system.webserver/security/access" -Value "Ssl,SslNegotiateCert, SslRequireCert"
```

Image 4 – Ouvrir les paramètres de SSL du site Web

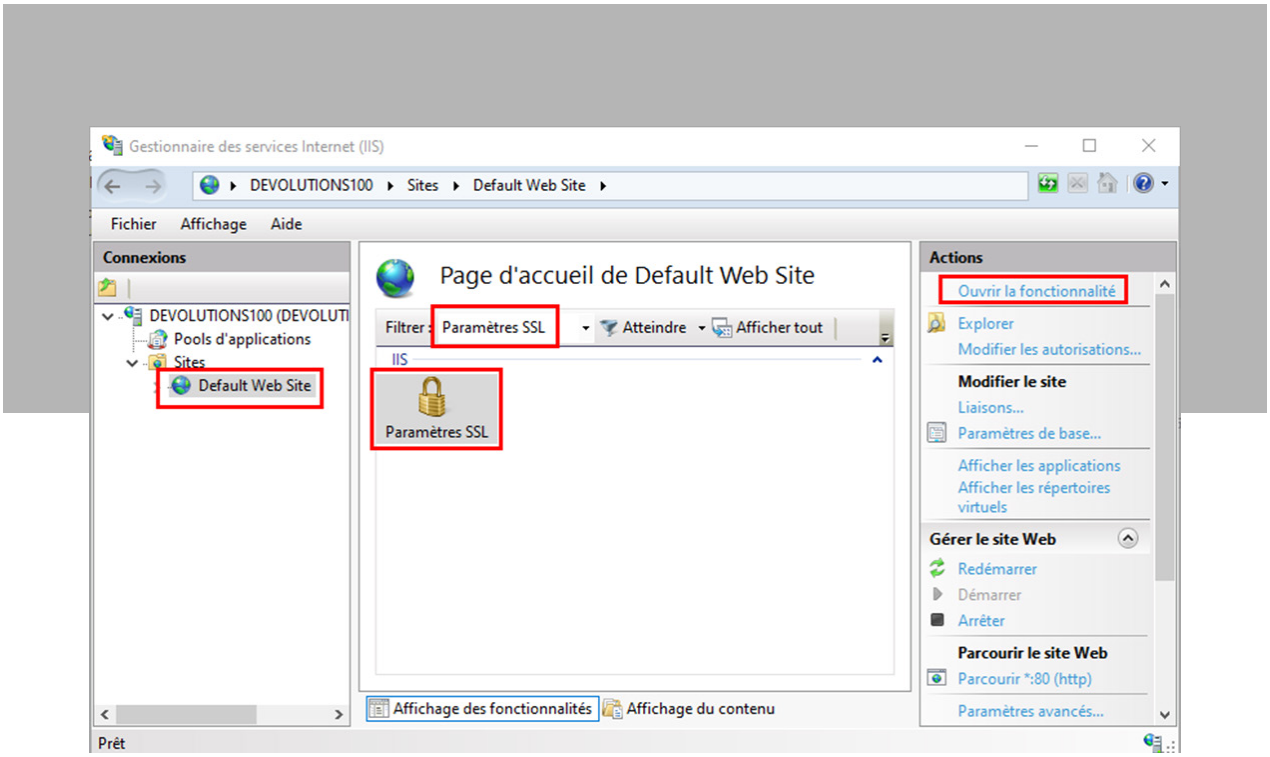
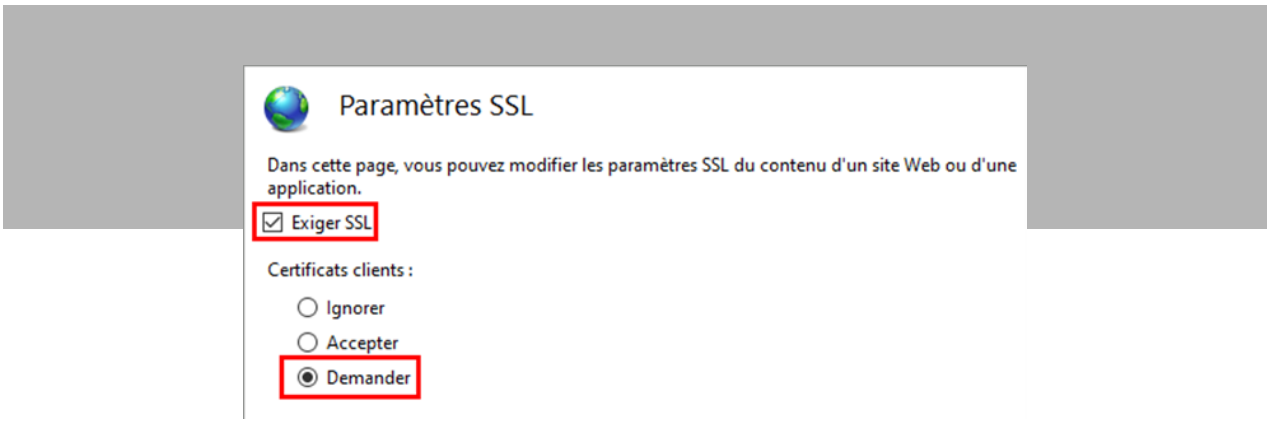


Image 5 – Paramètres SSL



Étape 4 – Désactiver l'authentification anonyme

Assurez-vous de désactiver l'authentification anonyme pour votre site Web en allant dans les paramètres d'authentification (voir les images 6 et 7).

Default Web Site → Authentification → Ouvrir la fonctionnalité

Commande PowerShell :

```
Set-WebConfigurationProperty -filter "/system.WebServer/security/authentication/AnonymousAuthentication" -name enabled -value false -location "Default Web Site"
```

Image 6 – Ouvrir les paramètres d'authentification

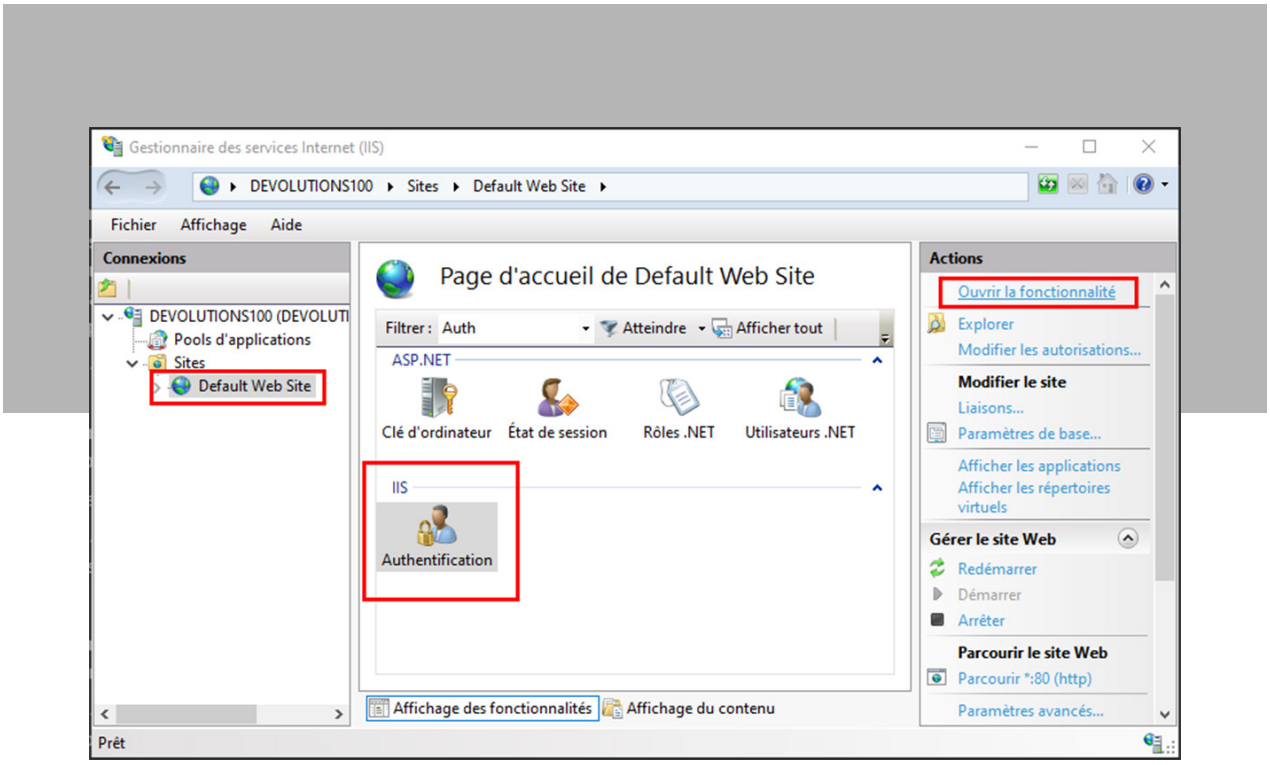
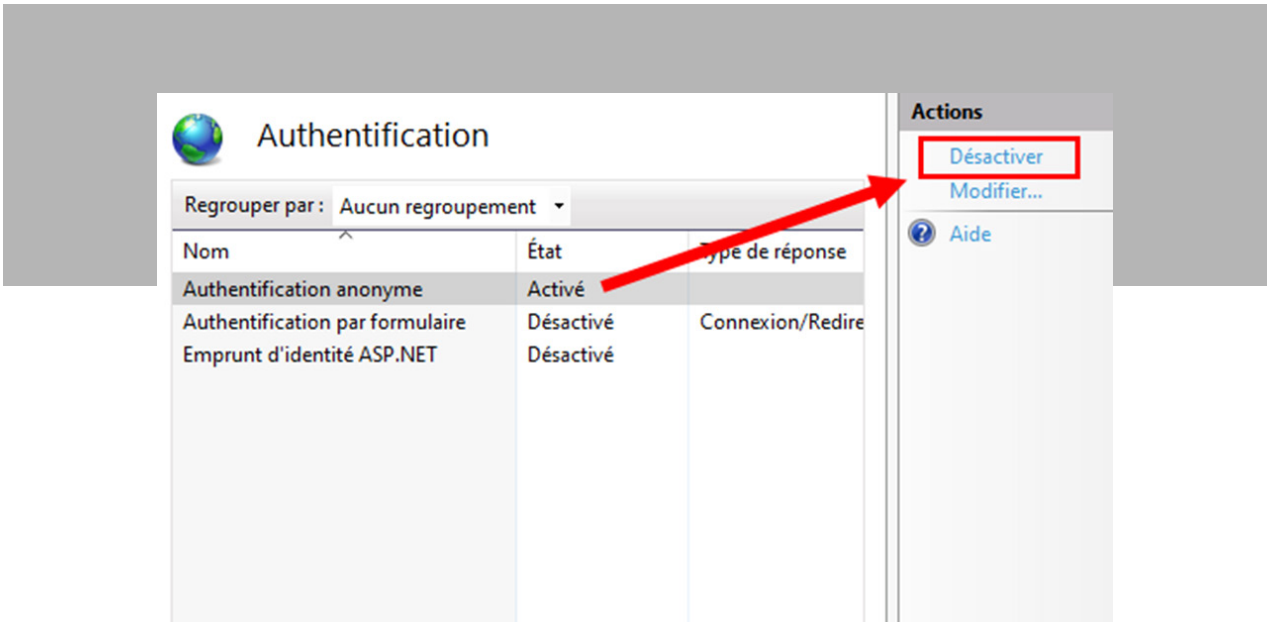


Image 7 – Désactiver l'authentification anonyme

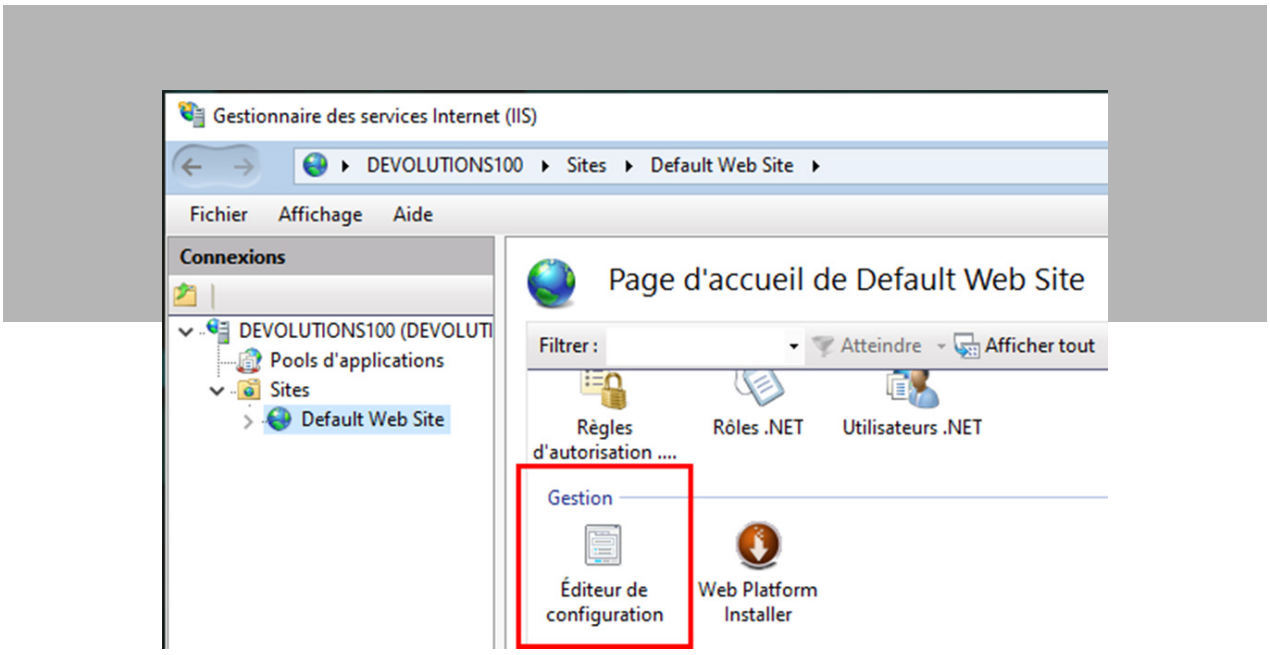


Étape 5 – Activer l'authentification du client sur IIS

Vous êtes maintenant prêt à activer la fonctionnalité sur votre site Web!

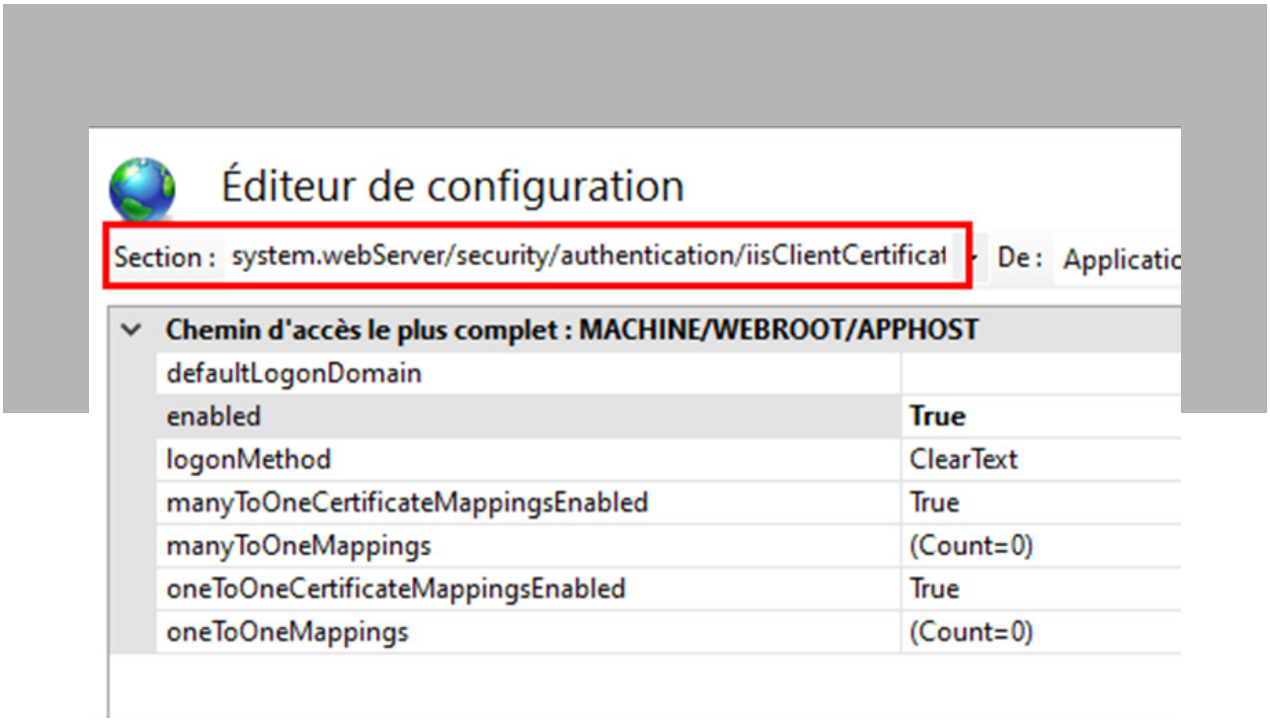
5.1 - Ouvrir l'Éditeur de configuration de votre site Web.

Image 8 – Éditeur de configuration



5.2 - Aller dans la section *system.webServer/security/authentication/iisClientCertificateMappingAuthentication* (voir l'image 9).

Image 9 – Champ Section

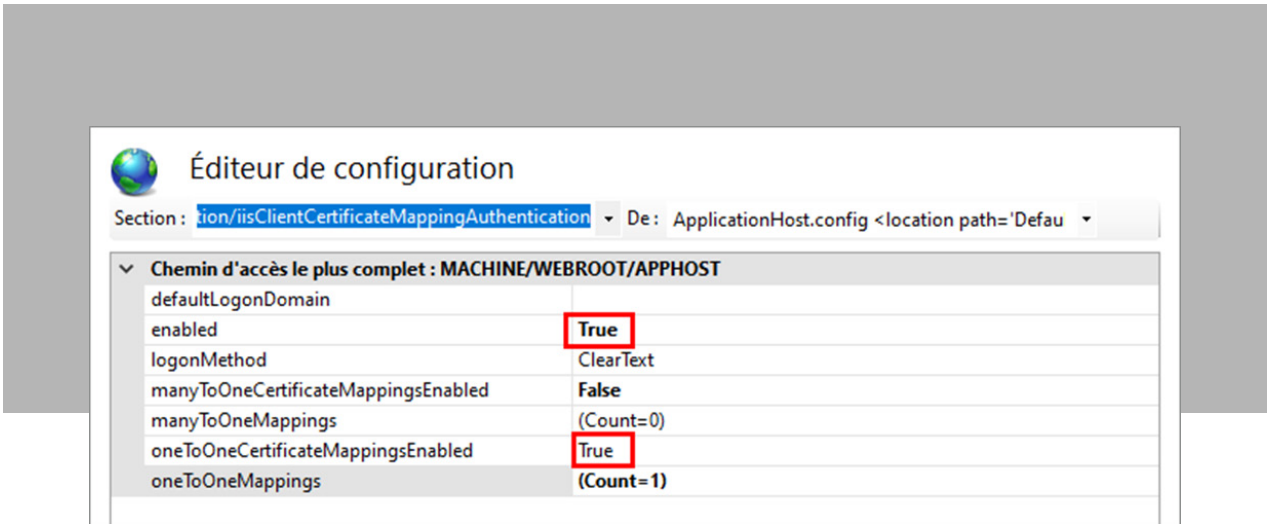


5.3 - Ici, vous pouvez choisir d'activer ***manyToOneCertificateMappingsEnabled*** ou ***oneToOneCertificateMappingsEnabled*** (voir l'image 10).

PowerShell

```
# activer la fonction iiscertificatemappingauthentication pour Default Web Site
Set-WebConfigurationProperty -filter «/system.webServer/security/authentication/
iisClientCertificateMappingAuthentication» -name enabled -Value true -location
«Default Web Site»

# activer oneToOneCertificateMappings pour Default Web Site
Set-WebConfigurationProperty -filter «/system.webServer/security/authentication/
iisClientCertificateMappingAuthentication» -name oneToOneCertificateMappings Enabled
-Value true -location «Default Web Site»
```

Image 10 – Activer la fonctionnalité Authentification et la sous-fonctionnalité oneToOneMappings



Nous recommandons l'option ***oneToOneCertificateMappings***, car chaque utilisateur doit avoir son propre certificat. Toutefois, ***manyToOneMappings*** peut également être utilisée. Cette option réduit le temps de gestion requis, mais peut compromettre la sécurité. En effet, avoir un seul certificat client pour une équipe ou un groupe d'utilisateurs **augmente les risques** de fuite ou de compromission. Normalement, la clé privée d'un certificat client doit rester sur le terminal à partir duquel elle a été générée.

5.4 - Ouvrir la configuration de **oneToOneMappings**

5.5 - Dans la fenêtre, vous pouvez configurer chaque utilisateur avec leur **clé publique** de certificat codée en base64 (*les instructions sur comment l'obtenir sont fournies à la fin de cet article*) et leurs identifiants d'**Active Directory (AD)** (voir les images 11 et 12).

Image 11 – Bouton pour ouvrir la configuration de oneToOneMappings

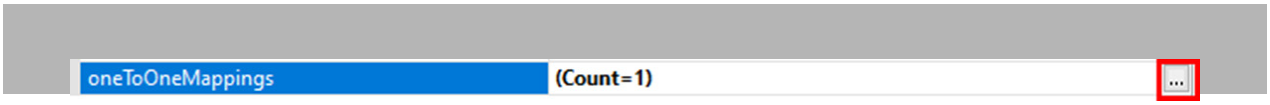
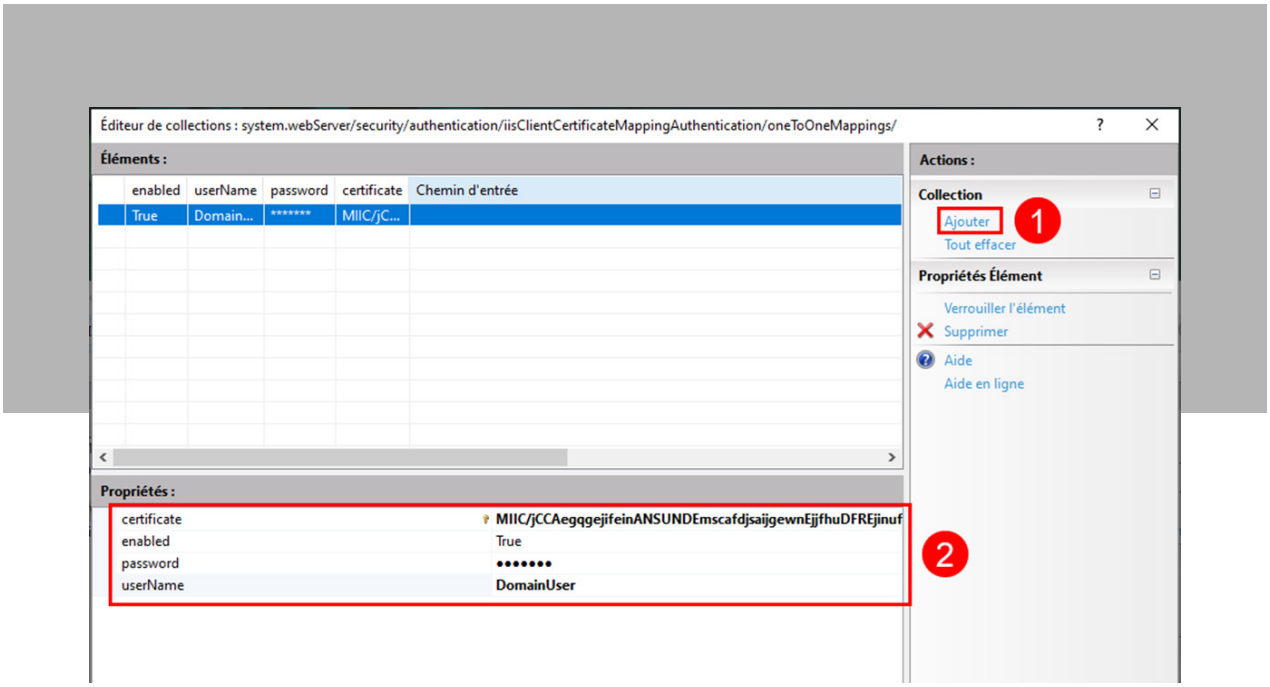


Image 12 – Configurer un utilisateur



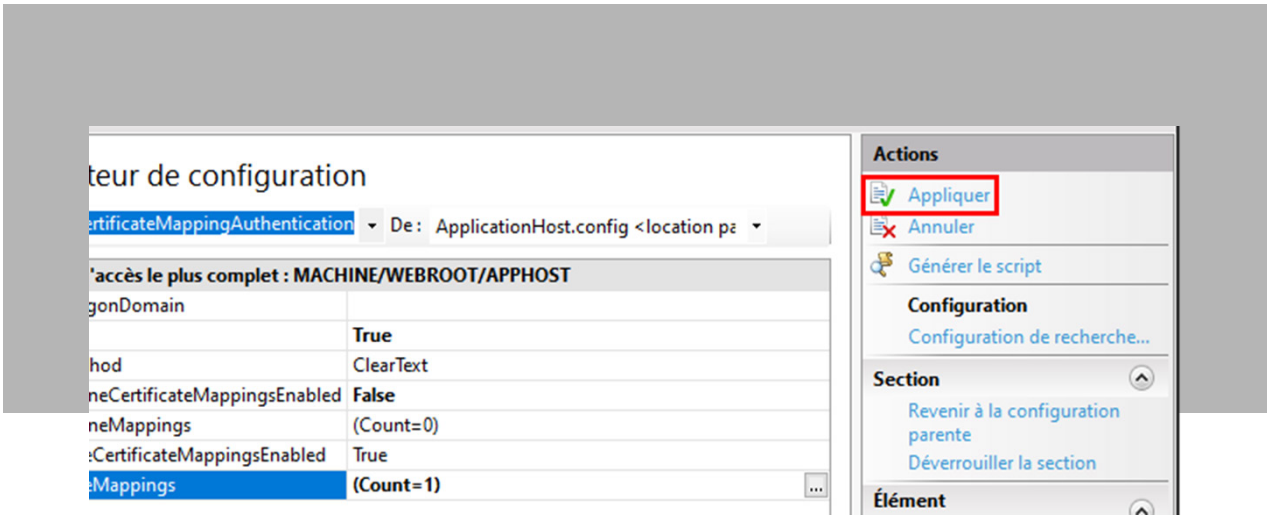
PowerShell

```
# obtenir la collection de oneToOneMappings
$collection = Get-IISConfigSection -SectionPath “system.webServer/security/
authentication/iisClientCertificateMappingAuthentication” -Location “Default Web
Site” | Get-IISConfigCollection -CollectionName “oneToOneMappings”

$username = Read-Host “Username?”
$password = Read-Host “Password?”
$b64CertificatePublicKey = Read-Host “Base64 Certificate Public key?”

# créer le mappage dans oneToOneCertificateMappings
New-IISConfigCollectionElement -ConfigCollection $collection -ConfigAttribute @
{“enabled” = “True”; “userName” = $username; “password” = $password; “certificate”
= $b64CertificatePublicKey}
```

Vérifiez que l’utilisateur ait bien les droits de lecture dans le dossier du site!

5.6 - Fermer l’**Éditeur de collection** et appliquer les nouveaux paramètres de l’Éditeur de configuration (voir l’image 13).

Image 13 – Appliquer les changements

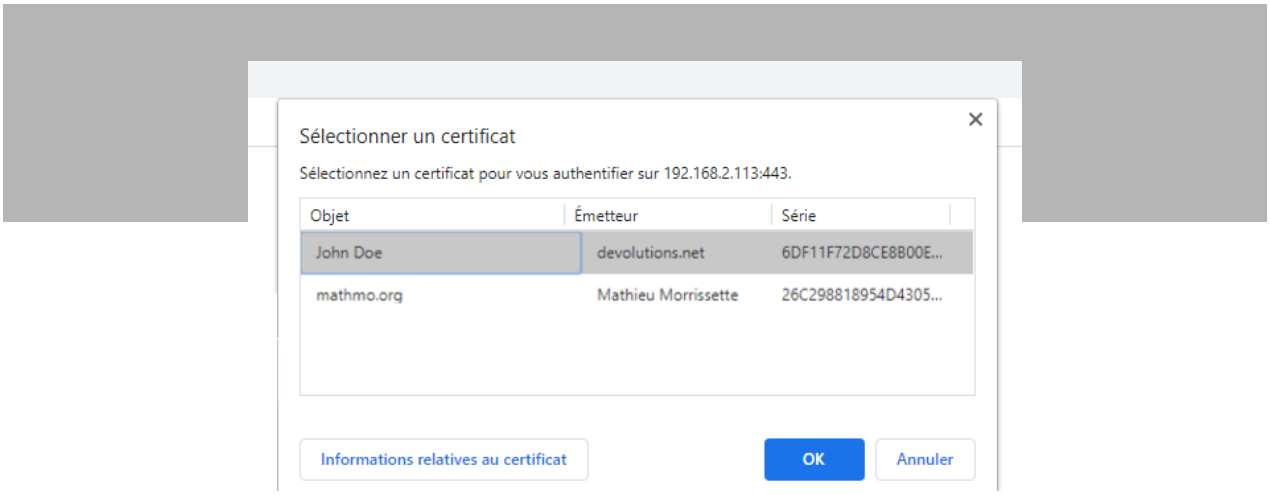


Il est recommandé de redémarrer votre site Web.

Résultat

Si tout fonctionne comme prévu, lorsqu'on ouvre le site Web à partir d'un navigateur, une boîte de dialogue devrait apparaître et forcer l'utilisateur à choisir un certificat pour s'authentifier avant d'accéder au serveur (voir l'image 14).

Image 14 – Fenêtre d'authentification du client TLS dans Google Chrome



Cliquez ici pour des ressources supplémentaires.

Note : Si vous avez suivi cet article de blogue pour générer des certificats auto-signés, la clé publique est alors dans le fichier **client1.crt**. L'en-tête `-----BEGIN CERTIFICATE-----` et le pied de page `-----END CERTIFICATE-----`, ainsi que les sauts de ligne, doivent être supprimés. Voici un exemple :

Fichier: **client1.crt**

```
-----BEGIN CERTIFICATE-----
MIICUjCCAfegAwIBAgIUbfEfctjOiwDqqBR1vupzjdN4qI0wCgYIKoZIzj0EAwIwgZ8xC
zAJBgNVBAYTAkNBMQswCQYDVQQIDAJRQzESMBAGA1UEBwwJTGF2YWx0cmllMRkwFwYDVQQKDB
BEZXZvbHV0aW9ucyBpbmMuMREwDwYDVQQLDAhTZWN1cml0eTEYMBYGA1UEAwwPZGV2b2x1dGl
vbnMubmV0MScwJQYJKoZIhvcNAQkBFhhzZWN1cml0eUBkZXZvbHV0aW9ucy5uZXQwH
hcNMjAwNjI1MTUwMjMyWhcNMjMwMzIyMTUwMjMyWjCBlzELMAkGA1UEBhMCQ0ExC
zAJBgNVBAgMAlFDMRIwEAYDVQQHDAlMYXZhbHRyaWUxGTAXBgNVBAoMEERldm9sdXRpb
25zIGluYy4xETAPBgNVBAsMCFNlY3VyaXR5MREwDwYDVQQDDAhKb2huIERvZTEmMCQGCSqGSIb
3DQEJARYXSm9obkRvZUBkZXZvbHV0aW9ucy5uZXQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwN
CAAT/kLSLRnKIdewU9Ze8KuZbuz7y1PfhTMEfV7ZQ3gRfSxGdRBxftaNFPtxjkmO9hVowyp
tUR8UvGc9Ia8rRX6NwoxcwFTATBgNVHSUEDDAKBggrBgEFBQcDAjAKBggqhkjOPQQDAgNJADB
GAiEAwvtbZNwzaf1RMvanSGorJwxYSSBiPIUg0YmyfIpG6pwCIQCoE9+V3/2ULCj9NtzEYsW2u
PojMQ3ddr1CpE2m07yIdQ==
-----END CERTIFICATE-----
```

Devrait être changé pour :

```
MIICUjCCAfegAwIBAgIUbfEfctjOiwDqqBR1vupzjdN4qI0wCgYIKoZIzj0EAwIwgZ8xC
zAJBgNVBAYTAkNBMQswCQYDVQQIDAJRQzESMBAGA1UEBwwJTGF2YWx0cmllMRkwFwYDVQQKDB
BEZXZvbHV0aW9ucyBpbmMuMREwDwYDVQQLDAhTZWN1cml0eTEYMBYGA1UEAwwPZGV2b2x1dGl
vbnMubmV0MScwJQYJKoZIhvcNAQkBFhhzZWN1cml0eUBkZXZvbHV0aW9ucy5uZXQwH
hcNMjAwNjI1MTUwMjMyWhcNMjMwMzIyMTUwMjMyWjCBlzELMAkGA1UEBhMCQ0ExC
zAJBgNVBAgMAlFDMRIwEAYDVQQHDAlMYXZhbHRyaWUxGTAXBgNVBAoMEERldm9sdXRpb
25zIGluYy4xETAPBgNVBAsMCFNlY3VyaXR5MREwDwYDVQQDDAhKb2huIERvZTEmMCQGCSqGSIb
3DQEJARYXSm9obkRvZUBkZXZvbHV0aW9ucy5uZXQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwN
CAAT/kLSLRnKIdewU9Ze8KuZbuz7y1PfhTMEfV7ZQ3gRfSxGdRBxftaNFPtxjkmO9hVowyp
tUR8UvGc9Ia8rRX6NwoxcwFTATBgNVHSUEDDAKBggrBgEFBQcDAjAKBggqhkjOPQQDAgNJADB
GAiEAwvtbZNwzaf1RMvanSGorJwxYSSBiPIUg0YmyfIpG6pwCIQCoE9+V3/2ULCj9NtzEYsW2u
PojMQ3ddr1CpE2m07yIdQ==
```

J'espère que ce tutoriel vous sera utile. Faites-moi savoir si vous souhaitez que je crée un tutoriel pour activer cette fonctionnalité sur Apache, Nginx ou d'autres serveurs!