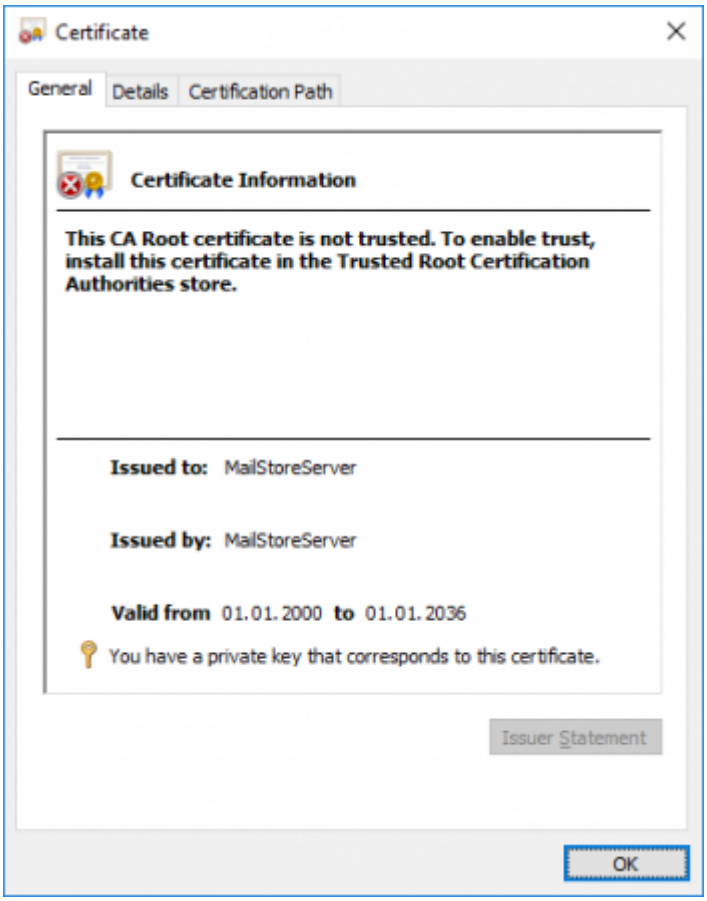
Comment déployer un certificat SSL auto-signé dans Mailstore ?

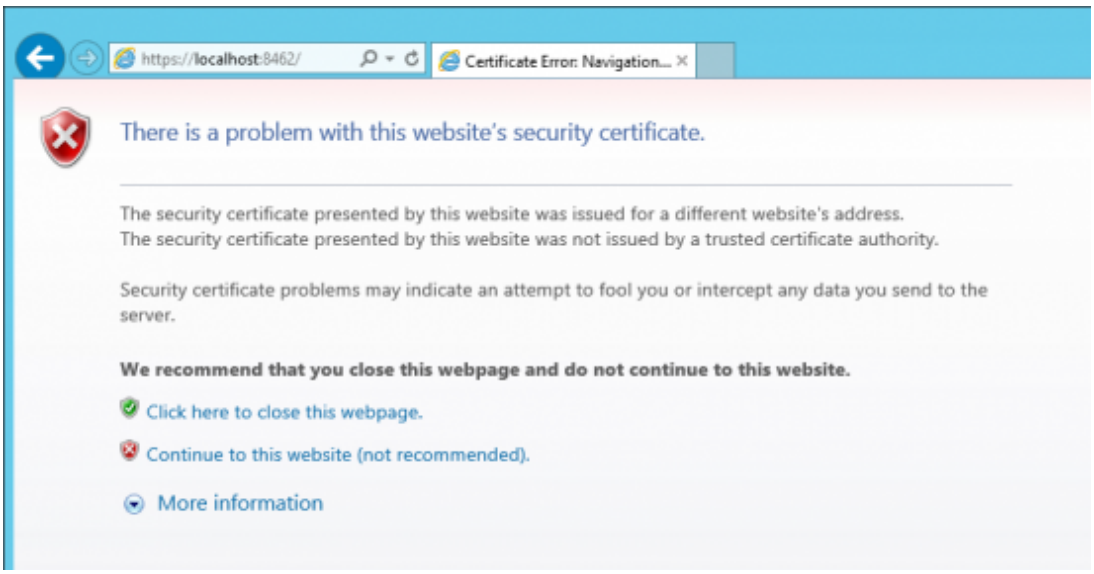
Guillaume - 2020-07-02 - Mailstore

Contexte

Pendant l'installation de MailStore Server, un certificat SSL généré est utilisé par tous les composants MailStore pour les connexions cryptées. Étant donné que le certificat est émis avec un nom de serveur *MailStoreServer* et ne provient pas d'une autorité de certification (CA) approuvée, il n'est pas approuvé par le côté client.



Pour cette raison, le message d'avertissement suivant s'affiche lors de l'appel à MailStore Web Access via HTTPS (SSL) ou lors de l'utilisation du complément Outlook avec le paramètre de *connexion sécurisée* activé:



Lors de l'utilisation d'un certificat auto-signé, les conditions suivantes doivent être remplies pour que le client ne reçoive pas d'avertissement de certificat.

- Le nom d'hôte de l'ordinateur du serveur MailStore doit figurer dans le champ *Objet* ou *Autre nom* d'objet du certificat. Dans le cas de Firefox et Chrome, les champs *Subject Alternative Name* sont obligatoires.
- Le client doit utiliser l'un de ces noms lors de la connexion au serveur MailStore.
- L'émetteur du certificat doit être fiable.
- Le certificat ne doit pas être expirer.

Cet article décrit l'option de déployer des certificats auto-signés à l'aide d'une stratégie de groupe. Une alternative consiste à utiliser des certificats SSL officiellement signés émis par l'autorité de certification de votre entreprise ou une autorité de certification externe de confiance, telle que VeriSign ou eTrust.

Pour configurer MailStore Server et vos clients pour l'utilisation d'un certificat auto-signé, veuillez procéder comme suit:

Préparation d'un certificat auto-signé

Alternative 1: utilisation du certificat généré automatiquement

Le certificat créé lors de l'installation est émis vers *MailStoreServer* .

Par conséquent, un *MailStoreServer* d'enregistrement A ou CNAME doit être présent sur le serveur DNS qui peut être utilisé pour atteindre l'ordinateur du serveur MailStore.

Ce certificat ne peut pas être utilisé si vous avez besoin d'une compatibilité avec Firefox et Chrome.

Alternative 2: créer un certificat à l'aide de la configuration du service du serveur MailStore

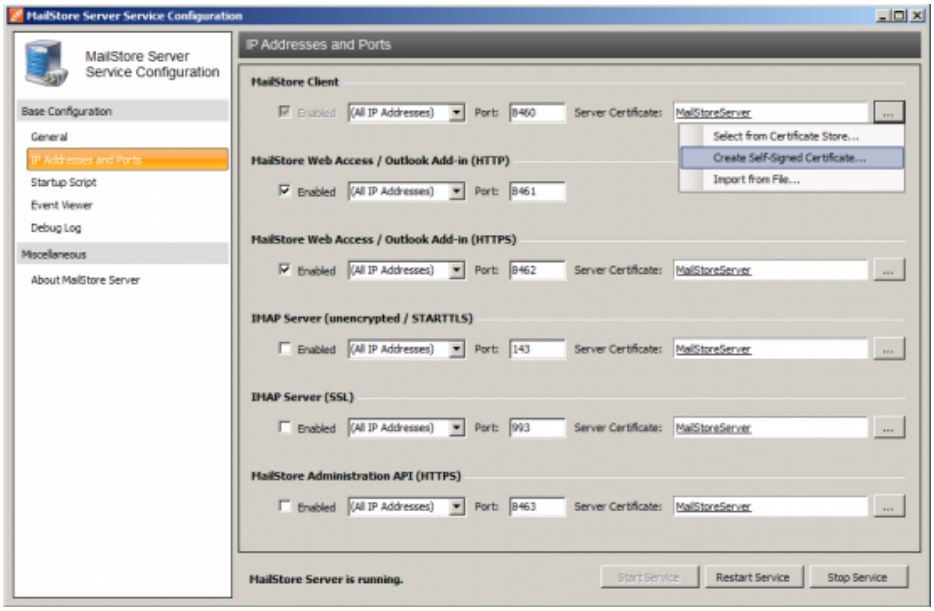
Cette alternative doit être préférée lorsque vous souhaitez utiliser un nouveau certificat avec des paramètres par défaut. Ces paramètres sont essentiellement:

- Le champ *Objet* défini par l'utilisateur. Cela équivaut au nom d'hôte de l'ordinateur du serveur MailStore.
- Le certificat valable 20 ans.
- L'algorithme de signature SHA256.
- *Les* champs *Subject Alternative Name* ne sont pas définis.
- La valeur *FriendlyName* n'est pas définie.

Étant donné que *les* champs *Subject Alternative Name* ne sont pas définis, ce certificat ne peut pas être utilisé avec Firefox et Chrome.

Pour créer le certificat, procédez comme suit:

- Ouvrez la configuration du service du serveur MailStore.
- Cliquez sur *Adresses IP et ports* .
- Cliquez sur le bouton à côté du champ *Certificat de serveur* et sélectionnez *Créer un certificat auto-signé ...*



- Comme nom pour le nouveau certificat, entrez le nom du serveur de la machine MailStore Server, par exemple mailstore.mydomain.local, et cliquez sur *OK* .
- Si nécessaire, remplacez tous les certificats de serveur supplémentaires par le nouveau certificat. Pour ce faire, cliquez sur le bouton à côté du champ *Certificat de serveur* et sélectionnez *Sélectionner dans le magasin de certificats ...*

Alternative 3: créer un certificat à l'aide de Certreq

Cette alternative doit être préférée si le certificat doit être conforme à des exigences qui ne peuvent pas être satisfaites avec les paramètres par défaut. Par exemple, si vous devez utiliser d' *autres noms de sujet* ou si vous souhaitez une période de validité limitée.

- Connectez-vous à l'ordinateur du serveur MailStore.
- Préparez un fichier texte request.inf avec le contenu suivant:

```
;----------------- request.inf -----------------
[Version]
Signature="$Windows NT$"
[NewRequest] ;
replace Subject attributes in the line below with real values
Subject = "CN=mailstoreserver.example.com, OU=Department,
O=Organisation, L=Locality, S=State, C=Country"
HashAlgorithm = sha256
KeySpec = 1
KeyLength = 2048
Exportable = TRUE
FriendlyName = mailstoreserver.example.com
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = Cert
KeyUsage = 0xa0
ValidityPeriodUnits = 20
ValidityPeriod = Years
[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.1 ; this is for Server Authentication
[Extensions]
2.5.29.17 = "{text}"
_continue_ = "DNS=mailstoreserver.example.com&"
_continue_ = "DNS=mailstoreserver&"
_continue_ = "DNS=172.31.1.5&"
_continue_ = "IPADDRESS=172.31.1.5&"
```

- Ajustez *Subject* , *FriendlyName* , *ValidityPeriodUnits* , *ValidityPeriod* selon vos besoins.
- Ajoutez ou supprimez des lignes *_continue_* dans la section *Extensions* et ajustez-les en fonction de vos besoins. Tous les noms d'hôtes valides doivent apparaître dans la section *Extensions* .
- Enregistrez le fichier.
- Ouvrez une invite de commande élevée et accédez au répertoire dans lequel le *fichier request.inf* est stocké.
- Créez le certificat en exécutant la commande suivante:

```
certreq -new request.inf request.csr
```

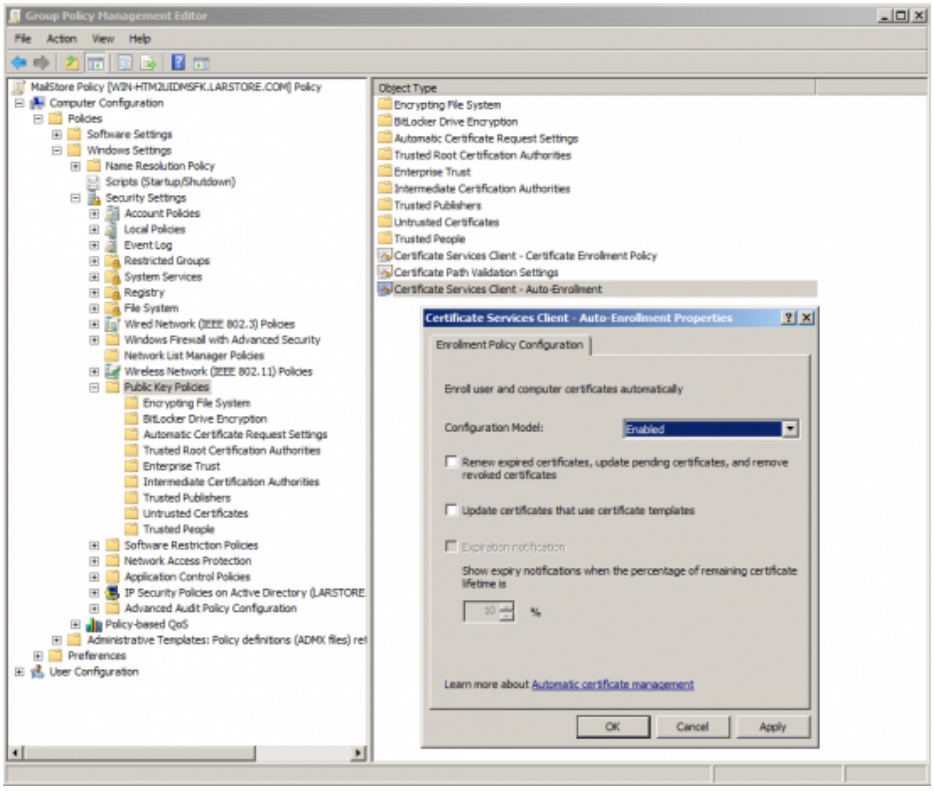
- Ouvrez la configuration du service du serveur MailStore.
- Cliquez sur *Adresses IP et ports* .
- Cliquez sur le bouton à côté du champ *Server Certificate* (...) et sélectionnez *Select from Certificate Store...*
- Sélectionnez le certificat créé précédemment et appuyez sur *OK* .
- Remplacez les autres certificats en cliquant sur le bouton à côté du champ *Server Certificate* (...) et sélectionnez *Select from Certificate Store...*

Déployer un certificat auto-signé
Avant de pouvoir déployer le certificat auto-signé, il doit être exporté à partir du magasin de certificats actuel. Veuillez procéder comme suit:

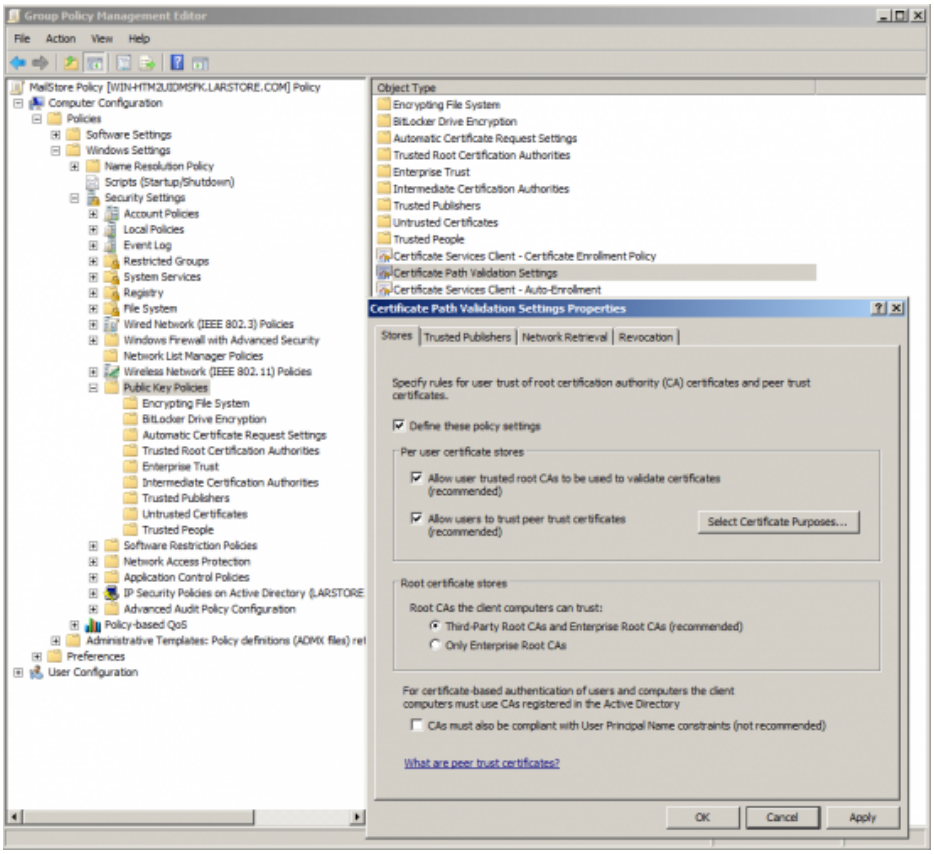
- Ouvrez la configuration du service du serveur MailStore.
- Cliquez sur *IP-Adresses and Ports*.
- Cliquez sur le certificat.
- Ouvrez l' onglet *Détails* .
- Cliquez sur *Copy to File*.
- Suivez les instructions de l'assistant d'exportation de certificat pour exporter le certificat **sans** la clé privée au format encodé DER dans un fichier.

Une fois le certificat exporté dans un fichier, créez une stratégie de groupe, puis pour déployer le certificat, personnalisez l'objet de stratégie de groupe comme suit:

- Ouvrez l'objet de stratégie de groupe à l'aide de l' *éditeur* de *gestion des stratégies de groupe* de votre serveur Windows.
- Développez *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* > *Public Key Policies*.
- Cliquez avec le bouton droit sur *Trusted Root Certification Authorities* and select *Import..*
- Suivez les instructions de l'assistant d'importation de certificat pour importer le certificat à partir du fichier.
- Sous *Public Key Policies ,* ouvrez les propriétés *Certificate Services Client - Auto-Enrollment* .



- Changez *Configuration Model* en *activé* et cliquez sur *OK* .
- Sous *Public Key Policies* , ouvrez les propriétés de *Certificate Path Validation Settings*.



- Cochez la case *Define these policy settings* et cliquez sur *OK* .

La stratégie de groupe sera activée une fois le poste de travail redémarré, l'intervalle d'actualisation de la stratégie de groupe est atteint ou une mise à jour de la stratégie de groupe est déclenchée manuellement.

Ajout de la compatibilité avec Firefox
Firefox possède sa propre gestion de certificats et n'utilise pas le magasin de certificats Windows par défaut. Depuis Firefox 52, vous pouvez dire à Firefox d'utiliser également le magasin de certificats Windows.

- Ouvrez Firefox et entrez *about: config* dans la barre d'adresse.
- Le cas échéant, confirmez l'avertissement de sécurité.
- Recherchez *security.enterprise_roots.enabled* et définissez sa valeur sur *true* . Si le paramètre n'existe pas encore, créez-le en tant que *booléen* .
- Redémarrez Firefox.

Ces étapes doivent être effectuées manuellement sur chaque poste de travail.