

Base de connaissances > Mailstore > Que faire si j'ai le message d'erreur :
«L'authentification a échoué car la partie distante a fermé le flux de transport»

Que faire si j'ai le message d'erreur : «L'authentification a échoué car la partie distante a fermé le flux de transport»

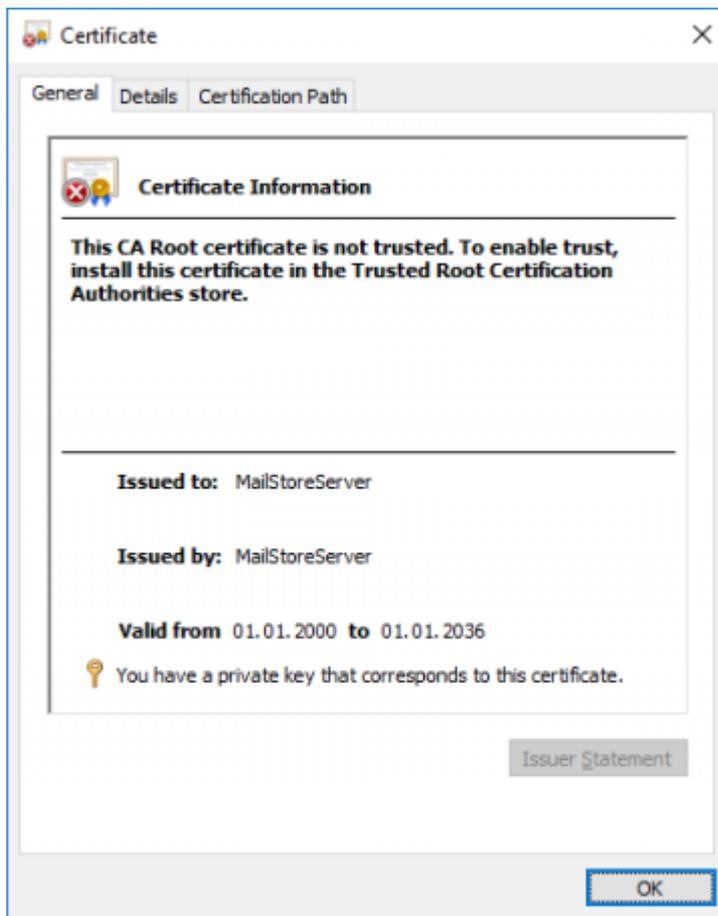
Guillaume - 2020-07-29 - Mailstore

Contexte

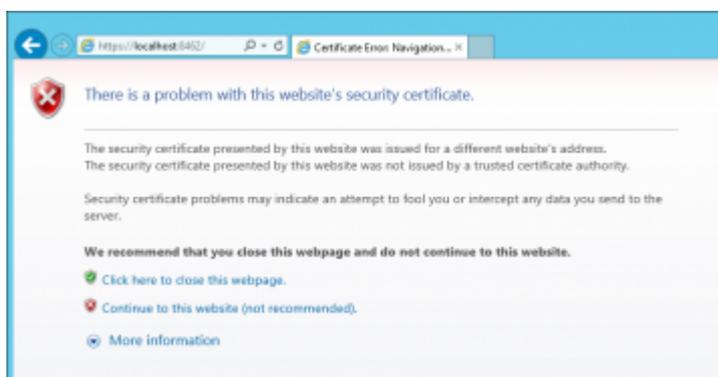
Pour garantir l'authenticité et la sécurité, MailStore Server utilise des certificats TLS dans tous les services qu'il fournit. Lors de l'installation, MailStore Server permet soit

- créer un certificat auto-signé,
- utiliser un certificat existant,
- ou obtenir un certificat de Let's Encrypt.

Le choix par défaut de création de certificats auto-signés est souvent utilisé lors de la première installation de MailStore Server, car il ne possède aucune dépendance externe. Bien que cela convienne parfaitement dans une configuration hors production, cela n'est pas recommandé pour une utilisation en production, car les certificats auto-signés ne sont pas approuvés par un autre ordinateur client, car ils ne sont pas signés par une autorité de certification de confiance, et l'utilisateur peut s'habituer à ignorer les avertissements de certificat.



Pour cette raison, le message d'avertissement suivant ou similaire s'affiche lors de l'ouverture de MailStore Web Access lorsqu'un certificat auto-signé est utilisé.



Pour éliminer les avertissements, augmenter la sécurité et améliorer la convivialité, MailStore doit être reconfiguré pour utiliser un certificat signé par une autorité de certification de confiance.

Ce qui suit décrit comment demander et installer manuellement des certificats à partir d'une autorité de certification approuvée. Une alternative à cela pourrait être d'obtenir des certificats de manière plus automatisée auprès de Let's Encrypt.

Conditions préalables

- Une [autorité de certification \(CA\)](#) de confiance
- outil *certreq* (disponible sur la plupart des installations Windows par défaut)

Créer un nouveau certificat

À moins qu'un certificat pour le nom d'hôte à utiliser pour accéder au serveur MailStore existe déjà, suivez les instructions ci-dessous pour créer un nouveau certificat et l'importer dans le magasin de certificats de Windows.

Création d'une demande de signature de certificat (CSR)

Ce qui suit décrit comment générer une demande de signature de certificat à l'aide de l'outil *certreq*.

- Connectez-vous à l'ordinateur du serveur MailStore.
- Préparez un fichier texte `request.inf` avec le contenu suivant, ajustez les valeurs *Subject* et *FriendlyName* en fonction de vos besoins. Ajustez également les *noms alternatifs de sujet (SAN)* dans la section *[Extensions]*. Veuillez noter que le *nom commun (CN)* dans l'*objet* n'est pas pertinent pour la vérification par les clients et que tous les noms d'hôte doivent être inclus en tant que SAN. Des noms d'hôte supplémentaires peuvent être ajoutés en ajoutant des lignes *_continue_* supplémentaires.

```
;----- 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=CountryCode"
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 = PKCS10
KeyUsage = 0xa0
[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.1 ; this is for Server Authentication
[Extensions]
2.5.29.17 = "{text}"
_continue_ = "DNS=*.example.com&"
_continue_ = "DNS=mailstoreserver.example.com&"
```

- Enregistrez le fichier.
- Ouvrez une invite de commandes avec élévation de privilèges et accédez au répertoire dans lequel le *request.inf* est stocké (avec *cd repertoire*).
- Créez le CSR en exécutant la commande suivante:

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

Validation de la demande de signature de certificat

Pour vérifier que le CSR est correct, exécutez la commande suivante pour l'afficher dans un format lisible par l'homme:

```
certutil -dump request.csr
```

Soumettre la demande de signature de certificat

Soumettez le CSR à votre autorité de certification préférée. En règle générale, vous téléchargez le fichier CSR sur un site Web de l'autorité de certification. L'AC peut demander la plate-forme serveur pendant le processus de soumission. Sélectionner *IIS 7* ou *Aucun des éléments répertoriés* devrait être suffisant. Après l'approbation réussie du CSR, vous obtiendrez le certificat signé en retour.

Remarque: de nos jours, le certificat est principalement signé par des autorités de certification intermédiaires. Il est nécessaire que le certificat de l'autorité de certification intermédiaire soit importé dans le magasin de certificats. Des informations détaillées sur le processus d'installation des certificats CA intermédiaires sont généralement incluses dans la livraison électronique de votre certificat.

Importer le certificat

- Ouvrez une invite de commandes avec élévation de privilèges et accédez au répertoire dans lequel le fichier de certificat est stocké.
- Exécutez la commande suivante pour importer le certificat dans le magasin de certificats personnels de l'ordinateur:

```
certreq -accept certificate.cer
```

Vérification de l'importation

- Connectez-vous à l'ordinateur du serveur MailStore en tant qu'administrateur.
- Ouvrez la *console de gestion Microsoft (MMC)*
- Ajoutez le composant logiciel enfichable de certificat en suivant ces étapes:
 - Cliquez sur *Fichier > Ajouter / Supprimer un composant logiciel enfichable > Certificat > Ajouter>*
 - Sélectionnez *Compte d'ordinateur* et cliquez sur *Suivant>*

- Sélectionnez *Ordinateur local* et cliquez sur *Terminer*
- Fermez toutes les fenêtres de dialogue ouvertes
- Cliquez sur *Certificats (ordinateur local) > Personnel > Certificats*
- Double-cliquez sur le certificat précédemment importé
- Assurez-vous que la clé privée du certificat est disponible:

Valid from 01/ 01/ 2000 **to** 01/ 01/ 2036

 You have a private key that corresponds to this certificate.

Réparation du magasin de certificats

Parfois, la clé privée correspondante est introuvable bien que le certificat ait été importé avec succès dans le magasin de certificats approprié. Essayez de réparer le magasin de certificats comme suit:

- Ouvrez un PowerShell élevé et exécutez la commande suivante:

```
Get-ChildItem Cert:\LocalMachine\My | select Subject, Serialnumber, Thumbprint, HasPrivateKey
```

- Vérifiez les sujets, les numéros de série et les empreintes digitales des certificats installés, pour identifier le certificat à utiliser par MailStore.
- Réparez le magasin de certificats correspondant en exécutant la commande suivante, où *SerialNumber* est le numéro de série du certificat à utiliser.

```
certutil -repairstore my SerialNumber
```

Utilisation du certificat avec MailStore

- Ouvrez la configuration du service du serveur MailStore.
- Sélectionnez *Paramètres réseau* .
- Dans la section pour laquelle vous souhaitez changer de certificat, cliquez sur le bouton à côté du champ *Certificat de serveur* et sélectionnez *Sélectionner dans le magasin de certificats ...*
- Choisissez le nouveau certificat dans le magasin de certificats.
- Confirmez votre sélection et redémarrez le service MailStore Server.

Importer un certificat existant

En règle générale, les certificats sont échangés entre les ordinateurs au moyen de conteneurs d'échange d'informations personnelles (PFX / P12). Ceux-ci peuvent, par exemple, être créés à l'aide des fonctions d'exportation des *certificats* Snap-In MMC .

Facultatif: création d'un conteneur PFX avec OpenSSL / LibreSSL

Lorsque le CSR d'origine n'a pas été créé avec les propres outils de Windows ou même pas créé sur un ordinateur Windows, il est peu probable que la clé privée ou le certificat soit disponible dans le magasin de certificats Windows de l'ordinateur MailStore Server, mais

stocké sur le fichier système à la place.

Dans ce cas, un conteneur d'échange d'informations personnelles (PFX) doit d'abord être créé. Celui-ci doit contenir le certificat, la clé privée et tous les certificats de la chaîne de certificats. Après cela, le conteneur PFX peut être importé dans le magasin de certificats de Windows.

Les étapes suivantes doivent être exécutées pour convertir les fichiers de certificat en un conteneur PFX avec OpenSSL ou LibreSSL:

- Copiez le certificat, la clé privée et les certificats de la chaîne de certificats dans le répertoire OpenSSL ou LibreSSL.
- Ouvrez une invite de commandes avec élévation de privilèges et accédez à ce répertoire.
- Créez le conteneur PFX en exécutant la commande suivante, ajustez les noms de fichiers nécessaires:

```
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -certfile CACert.crt
```

Importer un conteneur PFX

- Ouvrez la configuration du service du serveur MailStore.
- Sélectionnez *Paramètres réseau* .
- Dans la section pour laquelle vous souhaitez changer de certificat, cliquez sur le bouton à côté du champ *Certificat de serveur* et sélectionnez *Importer à partir du fichier ...*
- Choisissez le fichier PFX.
- Si le fichier PFX a été protégé par mot de passe, vous êtes invité à fournir le mot de passe maintenant.
- Confirmez votre sélection et redémarrez le service MailStore Server.