I. Généralités

Un certificat auto-signé (self-signed certificate) est un type de certificat numérique qui est signé par la même entité par laquelle il est émis. En d'autres termes, l'émetteur et sujet sont identiques. Contrairement à un certificat signé par une autorité de certification, qui est une entité de confiance tierce, un certificat auto-signé ne dispose pas de cette vérification par un tiers. Un certificat auto signé est souvent utilisé pour les environnements de développement, des tests internes ou des applications privées où la confiance externe n'est pas requise. Comme ils ne sont pas signés par une autorité de certification reconnue, les navigateurs et autres systèmes de validation de certificats ne leur font pas automatiquement confiance.

Dans une architecture client-serveur, les certificats auto-signés ont des usages spécifiques, principalement dans des environnements de développement ou pour des systèmes internes où la sécurité et la confiance peuvent être gérées localement.

Lorsque le serveur et le client sont sur la même machine, la configuration est généralement plus simple car il n'y a pas besoin de gérer la distribution des certificats à plusieurs machines. Le client doit être configuré pour accepter le certificat auto-signé. Notons que les clés privées et les certificats sur la machine pour éviter toute compromission locale.

Lorsque le serveur et le client sont sur des machines différentes, le certificat auto-signé doit être distribué à toutes les machines clientes. Cela implique un processus manuel ou automatisé pour ajouter le certificat au magasin de certificats de confiance de chaque client. Chaque client doit être configuré pour faire confiance au certificat auto-signé à l'aide de processus spécifiques pour importer des certificats dans des magasins de certificats de confiance. Par ailleurs, La sécurité devient plus complexe car les communications passent par des réseaux externes. Il est crucial de protéger les clés privées et de s'assurer que le certificat n'est pas compromis pendant le transfert.

II. Génération d'un certificat auto signé

1. Vérification de l'existence d'un certificat auto-signé

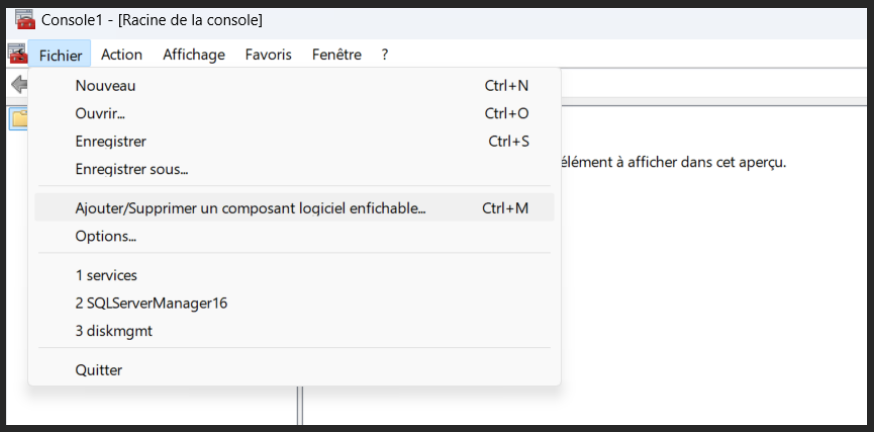
a. Tapez *Win + R* pour ouvrir la boîte de dialogue *Exécuter*

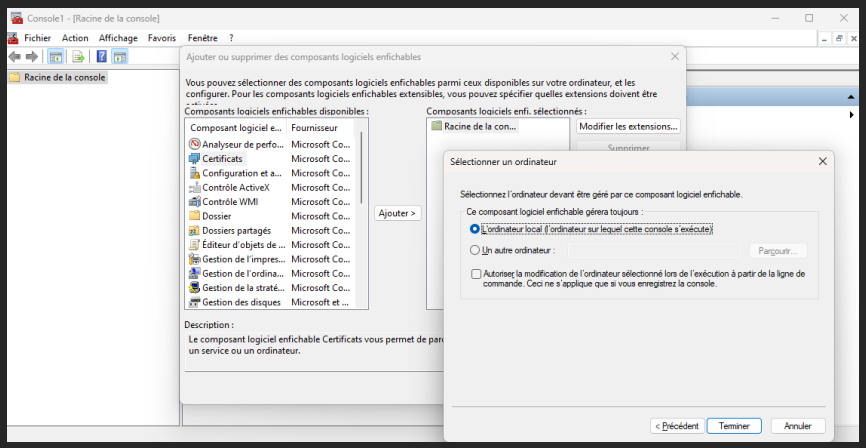
b. Tapez *mmc* et appuyer sur *Entrée*

c. Cliquez sur *Fichier*, puis sur *Ajouter/Supprimer un composant logiciel enfichable*

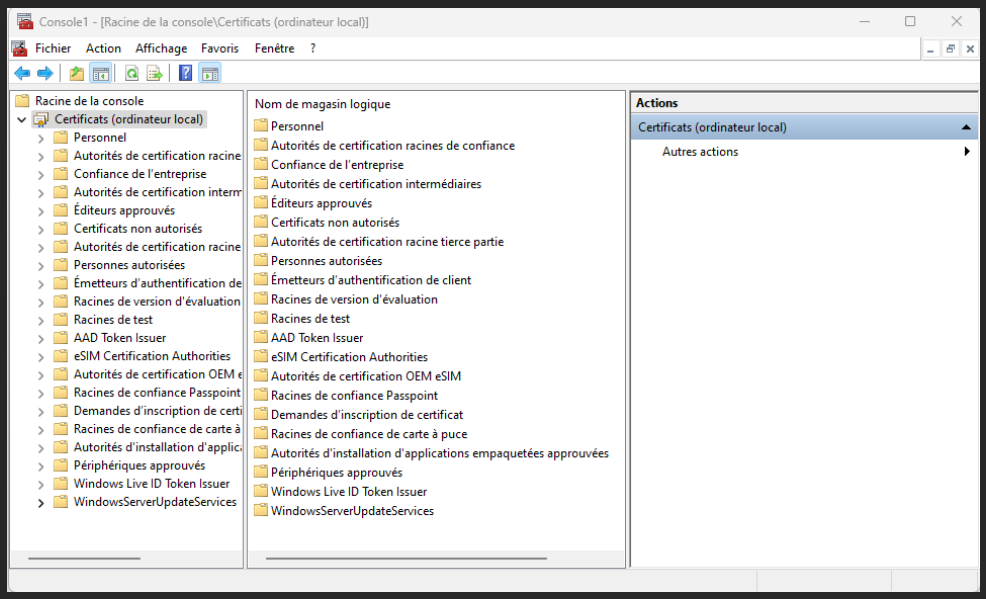
d. Sélectionnez *Certificats*, puis *Ajouter*

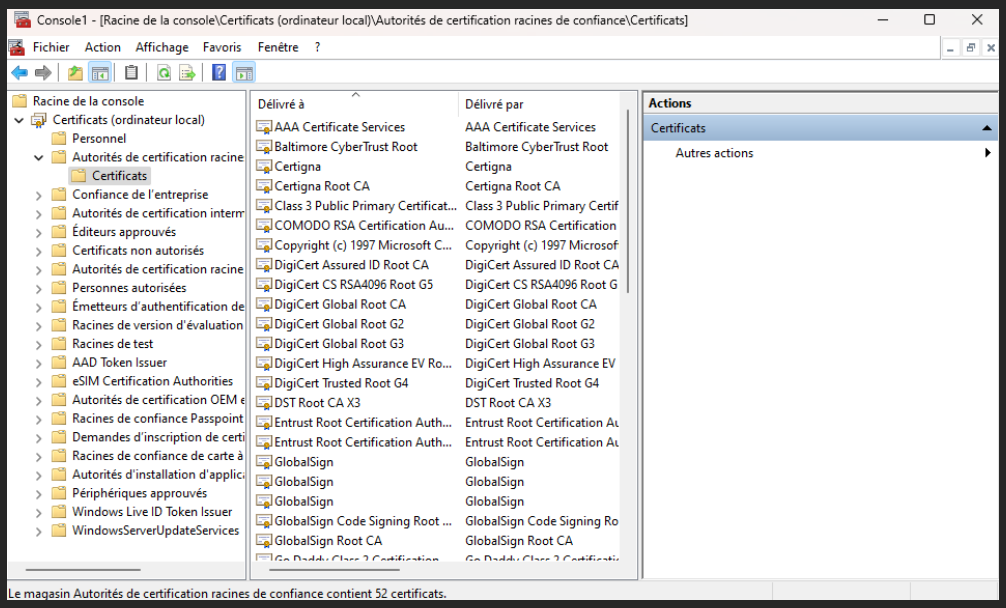
e. Sélectionnez *Compte d'ordinateur*, puis *Ordinateur local*





- La vérification des certificats auto-signés se fait en développant *Certificats (Ordinateur local)*, puis en sélectionnant *Personnel*, puis Certificats.
- Il est aussi possible de vérifier également dans *Autorités de certification racines de confiance*, puis *Certificats*, pour voir si un certificat auto-signé est enregistré là.





2. Génération d'un Certificat auto-signé avec PowerShell

a. Tapez sur *Win + X*, puis sélectionnez *Windows PowerShell (Admin)* ou *Windows Terminal (Admin)*.

b. Générez le Certificat Auto-signé

Ligne de commandes

```
New-SelfSignedCertificate -DnsName "ServerName" -CertStoreLocation "cert:\LocalMachine\My" -KeyLength 2048 -NotAfter (Get-Date).AddYears(1) -FriendlyName "My Self-Signed Certificate"
```

c. Exporter le Certificat et la Clé Privée (optionnel) PFX format :

Ligne de commandes

```
$cert = Get-ChildItem -Path cert:\LocalMachine\My | Where-Object { $_.Subject -like "*ServerName*" }

$password = ConvertTo-SecureString -String "YourPassword" -Force -AsPlainText

Export-PfxCertificate -Cert $cert -FilePath "C:\Path\To\YourCert.pfx" -Password $password
```

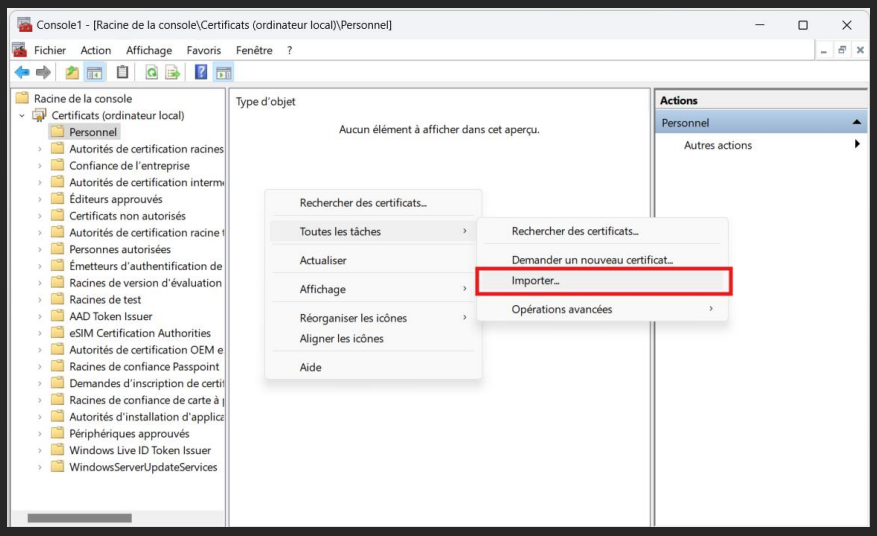
3. Génération d'un Certificat auto-signé avec OpenSSL
4. ISS

III. Example d'utilisation : SQL Server

1. Importer le certificat dans le magasin des certificats Windows

Un magasin de certificat de sécurité (certificate store) est un emplacement sécurisé dans un ordinateur ou un serveur où sont stockés les certificats numériques. Ces certificats sont utilisables pour l'authentification des utilisateurs/appareils (SSL/TLS), le chiffrement des communications et la validation des signatures numériques. Deux types de magasins de certificats existent : (1) magasin de certificats utilisateur (spécifiques à un utilisateur), (2) magasin de certificats machine (utilisés par tous les utilisateurs de l'ordinateur). Sur Windows, le gestionnaire de certificats accessible via la commande : *certmgr.msc*, à partir d'un *terminal*.

a. Section *II.1. (a. → e.)*
b. Clic droit, puis sélectionner *Toutes les tâches*, puis *Importer*
c. Sélectionner le fichier PFX créé



2. Configurer le serveur SQL pour utiliser le certificat

a. Ouvrir *SQL Server Configuration Manager*

b. Sélectionner *SQL Server Network Configuration*, puis *Protocoles pour [Instance]*

c. Clic droit sur *Propriétés* sur *Protocoles pour [Instance]*

d. Sous la zone *Certificats*, sélectionner le *certificat* qui a été importé

e. S'assurer que le certificat a le même nom que le serveur

f. S'assurer que le flag *'Force to Encryption'* est mis à *Oui* si cela est nécessaire

g. Redémarrer le service SQL Server pour que les changements prennent effet

- Dans *SQL Server Configuration Manager*, aller sur *SQL Server Services*
- *Clic droit sur l'instance SQL Server désiré, puis Redémarrer*

3. Configurer le client pour qu'il utiliser le certificat

Example :

- ODBC :

Ligne de commandes
Driver={ODBC Driver 17 for SQL Server};Server=myServerAddress;Database=myDataBase;Uid=myUsername;Pwd=myPassword;Encrypt=yes;TrustServerCertificate=yes;

- Java

Ligne de commandes

```
String connectionUrl =
"jdbc:sqlserver://myServerAddress;databaseName=myDataBase;user=myUsername;password=myPassword;encrypt=true;trustServerCertificate=true;";;
```