# 05 - Gérer les certificats de confiance

Les certificats jouent un rôle essentiel dans la protection et la validation de l'authentification et d'autres tâches liées à la sécurité. L'un des principes fondamentaux qui activent ces fonctionnalités est un certificat de confiance. Pour qu'un certificat soit effectif, chaque utilisateur, appareil ou application qui l'utilise doit approuver l'autorité de certification qui l'a émis.

## Qu'est-ce qu'un certificat de confiance ?

Lorsque vous utilisez des certificats, il est important de prendre en compte les personnes ou les éléments qui peuvent avoir besoin d'évaluer leur authenticité et leur validité. Il existe trois types de certificats que vous pouvez utiliser :

- Les certificats internes d'une autorité de certification d'organisation comme un serveur hébergeant le rôle AD CS.
- Les certificats externes d'une autorité de certification publique, par exemple une organisation qui fournit des logiciels de cybersécurité commerciaux ou des services d'identité.
- Un certificat auto-signé.

Si vous déployez une autorité de certification racine d'entreprise et que vous l'utilisez pour inscrire des certificats sur les appareils joints à un domaine de vos utilisateurs, ces appareils acceptent les certificats inscrits comme approuvés. Toutefois, un appareil de groupe de travail considère ces mêmes certificats comme non approuvés.
Pour résoudre ce problème, vous pouvez :

- Obtenir des certificats publics auprès d'une autorité de certification externe pour les appareils de groupe de travail. Cela implique le coût supplémentaire des certificats publics.
- Configurer les appareils de groupe de travail pour qu'ils fassent confiance à l'autorité de certification racine d'entreprise. Cela demande une configuration supplémentaire.

# Gérer les certificats et les certificats de confiance dans Windows

Vous pouvez gérer les certificats qui sont stockés dans le système d'exploitation Windows à l'aide d'un ensemble d'outils, notamment Windows Admin Center, le composant logiciel enfichable Certificats de Microsoft Management Console, Windows PowerShell et l'outil de ligne de commande `certutil`. Chacun d'eux vous donne accès aux magasins de certificats de l'utilisateur actuel, de l'ordinateur local et de ses services. Chaque magasin comprend plusieurs dossiers, notamment :

| Boutique | Description |
|---|---|
| Personnel | Contient les certificats émis pour l'utilisateur local, l'ordinateur local ou son service, en fonction du magasin sélectionné |
| Autorités de certification racines de confiance | Contient les certificats d'autorités de certification racines de confiance. |
| Confiance de l'entreprise | Contient les listes de certificats de confiance pour implémenter des approbations de certificats auto-signés d'autres organisations. |
| Autorités de certification intermédiaires | Contient les certificats émis pour des AC secondaires dans la hiérarchie de certification. |

Pour vous assurer que les appareils de groupe de travail approuvent votre autorité de certification racine d'entreprise, exportez son certificat du dossier Autorités de certification racines de confiance vers un ordinateur joint au domaine et importez-le dans le même dossier sur ces appareils.

> **Notes**
>
> Vous pouvez également obtenir le certificat de l'autorité de certification racine d'entreprise à partir du partage CertEnroll sur le serveur qui héberge ce rôle.

# Atelier

## Objectif

- Faire une demande de signature de certificat pour un serveur Apache HTTP server installé sur le système Rocky linux 10

## Pré-requis

- Installer une VM Rocky Linux version 10
  Le compte est désactiver ; l'utilisateur `bob` est sudoer (donc membre du groupe `wheel`)
- Faire la configuration IP :
  - FQDN : srvlinux.staff.local
  - Adresse IP : 10.14.0.12/16
  - Gateway : 10.14.255.254
  - Dns : 10.14.0.10
- Installer Apache HTTP server

```
dnf install httpd -y
systemctl status httpd.service
```

> 🖊 **Le service `httpd` est arrêté et désactivé.**

## Demande de signature de certificat (CSR)

- Dans le dossier personnel de l'utilisateur `bob`, créer un dossier `certs` :

```
mkdir -m 700 certs && cd certs
```

- Créer un fichier `staff.local.cnf` pour déclarer des paramètres du certificat :

```
[ req ]
default_bits = 4096
prompt = no
default_md = sha512
distinguished_name = dn
req_extensions = req_ext

[ dn ]
CN = www.staff.local

[ req_ext ]
subjectAltName = DNS: www.staff.local
```

- Générer une clé privée et une demande de signature de certificat :

```
openssl req -new -nodes -keyout www.staff.local.key -out
www.staff.local.csr -config openssl-san.cnf
```

- Décomposition de la commande :
  - `openssl req` : Lance la sous-commande OpenSSL dédiée à la création et au traitement des demandes de certificats X.509 (CSR) au format PKCS#10.
  - `-new` : Indique que l'on souhaite générer une nouvelle demande de certificat.
  - `-nodes` : Spécifie que la clé privée ne doit pas être chiffrée par une passphrase — utile pour automatiser le démarrage de certains services où l'entrée manuelle du mot de passe n'est pas souhaitée.
  - `-keyout www.staff.local.key` : Définit le fichier de sortie où sera enregistrée la nouvelle clé privée générée.
  - `-out www.staff.local.csr` : Définit le fichier de sortie qui contiendra la demande CSR à transmettre à l'Autorité de Certification (CA).
  - `-config openssl-san.cnf` : Utilise un fichier de configuration OpenSSL particulier (ici `openssl-san.cnf`), généralement pour inclure des extensions comme les SAN, nécessaires pour que le certificat soit valide avec plusieurs noms DNS ou adresses IP.

## Traitement de la demande

- Sur le serveur Windows CA, copier le fichier `www.staff.local.csr` dans le dossier `c:\Certs` avec WinSCP par exemple.
- Nous allons utiliser le modèle de certificat `Production Web Server`
  (Conçu dans le module `03 - Gérer l'inscription de certificats`)
- Dans un terminal (cmd ou powershell), taper :

```
certreq -submit -attrib "CertificateTemplate:ProductionWebServer"
.\www.staff.local.csr www.staff.local.cer
```

Une Boite de dialogue fournit la liste des autorités de certification.
Nous avons qu'une seule autorité qui est proposée.
Faire `Ok`

- Si tout va bien, vous avez ce message qui indique que le certificat a été émis dans le répertoire courant :

```
Stratégie d'inscription à Active Directory
  {4959D5D0-8877-45C6-9902-F8AE1072F5EF}
  ldap:
Identifiant de requête : 5
IDDemande : « 5 »
Certificat récupéré(Délivré) Délivré
```

## Installation du certificat sur le serveur Linux

- Sur le serveur Windows CA, renommer le fichier `c:\Certs\www.staff.local.cer` en `c:\Certs\www.staff.local.pem`
- Copier le fichier `c:\Certs\www.staff.local.pem` dans le dossier `/home/bob/certs`
- Sur le serveur Rocky Linux, élever ses privilèges en super-utilisateur :

```
sudo -i
```

- copier le fichier :

```
cp /home/bob/certs/www.staff.local.pem /etc/pki/tls/certs/
```

- Copier la clé privé :

```
cp /home/bob/certs/www.staff.local.key /etc/pki/tls/private/
```

# Configurer Apache HTTP Server

- Installer le module SSL/TLS d'Apache :

```
dnf install mod_ssl -y
```

- Aller dans le dossier `/etc/httpd/conf.d` et faire une copie du fichier `ssl.conf` :

```
cd /etc/httpd/conf.d
cp ssl.conf ssl.conf.backup
```

- Configurer le site virtuel `www.staff.local` :

```
mv ssl.conf vhost-www.staff.local-HTTPS.conf
```

- Editer vhost-www.staff.local-HTTPS.conf

```
[...]
DocumentRoot   "/var/www/www.staff.local"
ServerName     www.staff.local:443
ServerAlias    staff.local:443

[...]
SSLCertificateFile /etc/pki/tls/certs/www.staff.local.pem

[...]
SSLCertificateKeyFile /etc/pki/tls/private/www.staff.local.key

[...]
```

- Editer vhost-www.staff.local-HTTP.conf

```
<virtualhost *:80>
    servername      www.staff.local
    ServerAlias     staff.local
    DocumentRoot    "/var/www/www.staff.local"
    redirect "/"    "https://www.staff.local"
</virtualhost>
```

- Dans le dossier `/var/www/` créer la page d'accueil du site virtuel :

```
mkdir /var/www/www.staff.local
echo "Hello tout le monde !" > /var/www/www.staff.local/index.html
```

- Démarrer et activer le service puis vérifier :

```
systemctl enable httpd --now
systemctl status httpd
```

- Paramétrer le firewall :

```
firewall-cmd --list-all
firewall-cmd --add-service={http,https} --permanent
firewall-cmd --reload
firewall-cmd --list-services
```

- Tester avec `curl` :

```
curl -k https://www.staff.local
curl http://www.staff.local
```

- Tester avec `lynx` :

```
dnf install lynx

lynx https://www.staff.local
lynx http://www.staff.local
```