1. Installer un certificat signé par une CA Microsoft dans Proxmox

1.1. Principe

Proxmox utilise :

- **/etc/pve/local/pve-ssl.key** ⇒ clé privée
- **/etc/pve/local/pve-ssl.pem** ⇒ certificat serveur
- **/etc/pve/pve-root-ca.pem** ⇒ certificat de la CA (ou chaîne complète) s'il existe un certificat signé, sinon ce fichier n'existe pas

L'objectif est donc de :

- Générer une CSR depuis Proxmox
- Faire signer la CSR par la CA Microsoft (via la console web ou certreq)
- Importer le certificat + la chaîne dans les fichiers attendus par Proxmox
- Redémarrer les services

1.2. Générer le CSR sur Proxmox

La clé privée existante sera utilisée.

Dans le nœud Proxmox (SSH) :

- Créer un fichier san.cnf pour ajouter un SAN (recommandé) avec ce contenu :

```
[ req ]
default_bits = 2048
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn

[ dn ]
CN = proxmox.lab.local

[ req_ext ]
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = proxmox.lab.local
```

- générer le CSR

```
openssl req -new -key pve-ssl.key \
  -out proxmox.lab.local.csr \
  -config san.cnf
```

- vérification de l'empreinte de ta CSR (optionnel) :

```
# openssl req -in proxmox.lab.local.csr -noout -text
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN=proxmox.lab.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:cc:98:da:a3:41:21:8f:97:56:72:b2:39:fe:20:
                    ...
                    c1:96:9b:c8:7a:a5:8f:dc:c7:df:0f:52:19:5e:40:
                    63:79
                Exponent: 65537 (0x10001)
```

```
        Attributes:
            Requested Extensions:
                X509v3 Subject Alternative Name:
                    DNS:proxmox.lab.local
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        61:dc:b9:44:2c:77:82:26:f5:ff:47:1b:69:d8:88:af:4c:4a:
        ...
        c0:f0:57:8e:b2:60:d0:62:2e:06:c2:54:96:25:03:f0:04:c8:
        f1:51:9c:3f
```

1.3. Faire signer la CSR par la Microsoft CA

- accéder au site http://ADCS_SERVER/certsrv
- Cliquez sur **Demander un certificat**
- Cliquez sur **demande de certificat avancée**
- copier-coller le contenu du fichier .csr encodé au format Base 64 et choisissez le modèle de certificat
- Téléchargez ensuite :
    - le certificat au format Base64 (certnew.cer)
    - la chaîne CA certificate (Root CA + éventuellement la subCA) (certnew.p7b)

1.4. Installer le certificat sur Proxmox

Placer les fichiers :

- copier le certificat

```
cp certnew.cer /etc/pve/local/pve-ssl.pem
```

- placer le certificat de la CA dans /etc/pve/local/pve-root-ca.pem:

```
cp certnew.pb7 /etc/pve/local/pve-root-ca.pem
```

1.5. Redémarrer les services Proxmox

```
systemctl restart pveproxy
systemctl restart pvedaemon
```

- vérification :

```
openssl x509 -in /etc/pve/local/pve-ssl.pem -noout -text
```

- depuis le navigateur, le certificat doit maintenant être valide, signé par la CA Microsoft.

 Bonus : automatisation renouvellement (ADCS modèle avec auto-enroll) Si ton modèle de certificat est compatible, je peux aussi t'aider à automatiser la génération/renouvellement via un script shell ou API ADCS.

From:
https://siocours.lycees.nouvelle-aquitaine.pro/ - **Les cours du BTS SIO**

Permanent link:
https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/reseau/cloud/proxmox/installcertificat?rev=1770027283

Last update: **2026/02/02 10:14**