

# Installer un certificat signé par une CA Microsoft dans Proxmox

## Principe

Proxmox utilise :

- `/etc/pve/local/pve-ssl.key` ⇒ clé privée
- `/etc/pve/local/pve-ssl.pem` ⇒ certificat serveur
- `/etc/pve/local/pve-root-ca.pem` ??? ⇒ certificat de la CA (ou chaîne complète)

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

## Générer la clé privée + CSR sur Proxmox

La génération de la demande I(CSR) permet de renseigner le Common Name (CN) en indiquant exactement le nom FQDN du nœud Proxmox.

Dans le nœud Proxmox (SSH) :

```
openssl genrsa -out pve-ssl.key 4096
openssl req -new -key pve-ssl.key -out pve.csr
```

Afficher plus de lignes  Important : dans le Common Name (CN), mets exactement le nom FQDN du nœud Proxmox Ex : pve1.mondomaine.local Tu peux vérifier l'empreinte de ta CSR (optionnel) : `ShellopenSSL req -in pve.csr -noout -text`Afficher plus de lignes

□ Étape 2 — Faire signer la CSR par la Microsoft CA Option A : via <https://certsrv>

Menu Request a certificate advanced certificate request Copier/coller le contenu de pve.csr Choisir le modèle Web Server (ou ton modèle personnalisé) Récupérer le certificat au format Base64 (.cer) Récupérer aussi la CA Root et éventuellement la sub-CA

Option B : via PowerShell / certreq (si tu veux automatiser) Créer un fichier pve.inf : `[Version] Signature="$Windows NT$"`

```
[NewRequest] Subject = "CN=pve1.mondomaine.local" Exportable = TRUE KeyLength = 4096 KeySpec = 1 KeyUsage = 0xA0
MachineKeySet = TRUE SMIME = FALSE PrivateKeyArchive = FALSE ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
RequestType = PKCS10
```

```
[Extensions] 2.5.29.17 = "{text}" continue = "DNS=pve1.mondomaine.local"
```

Puis : `PowerShellcertreq -new pve.inf pve.csrcertreq -submit pve.csr pve.cer`Afficher plus de lignes

□ Étape 3 — Installer le certificat sur Proxmox Placer les fichiers : `Shellcp pve-ssl.key /etc/pve/local/pve-ssl.keycp pve.cer /etc/pve/local/pve-ssl.pem`Afficher plus de lignes Si tu as une chaîne complète (intermédiaire + root), concatène : `Shellcat pve.cer intermediate.cer root.cer > /etc/pve/local/pve-ssl.pem`Afficher plus de lignes Et place la racine seule dans : `Shellcp root.cer /etc/pve/local/pve-root-ca.pem`Afficher plus de lignes Proxmox demande bien un fichier séparé pour la root.

□ Étape 4 — Redémarrer les services Proxmox `Shellsystemctl restart pveproxysystemctl restart pvedaemon`Afficher plus de lignes Pour vérifier : `ShellopenSSL x509 -in /etc/pve/local/pve-ssl.pem -noout -text``Afficher plus de lignes Puis ouvre l'interface → le certificat doit maintenant être valide, signé par ta 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:

/ - **Les cours du BTS SIO**

Permanent link:

</doku.php/reseau/cloud/proxmox/installcertificat?rev=1770025045>

Last update: **2026/02/02 10:37**

