

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/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 le CSR sur Proxmox

La clé privée existante sera utilisée.

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
```

Crée 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
```

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.cerAfficher 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.pemAfficher plus de lignes Si tu as une chaîne complète (intermédiaire + root), concatène : Shellcat pve.cer intermediate.cer root.cer > /etc/pve/local/pve-ssl.pemAfficher plus de lignes Et place la racine seule dans : Shellcp root.cer /etc/pve/local/pve-root-ca.pemAfficher plus de lignes Proxmox demande bien un fichier séparé pour la root.

□ Étape 4 — Redémarrer les services Proxmox Shellsystemctl restart pveproxysystemctl restart pvedaemonAfficher 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=1770025328>

Last update: 2026/02/02 10:42

