L’Obstacle : Quand l’Automatisation se heurte à la Sécurité

```
$ sudo glpi-agent --server https://glpi.c1-04.lan/front/inventory.php --debug
[error] SSL certificate verify failed
[error] unable to verify the first certificate
```

Le compte de service fonctionne ?

Le service systemd glpi-agent est actif ?

Le client Linux fait confiance au certificat du serveur GLPI ?

Le problème n’est pas l’agent, mais la cryptographie. Le client Linux est incapable de reconstruire une chaîne de confiance vers l’Autorité de Certification (ADCS).

Démystifier la PKI : L'Analogie de la Mairie

L'ADN (La Clé Privée)

glpi.key
(Générée localement, ne quitte jamais le serveur).

Le Formulaire Cerfa (La CSR)

glpi.csr
(Contient l'identité demandée, signée avec l'ADN).

La Mairie (Le Serveur ADCS)

Microsoft ADCS
(L'autorité qui vérifie la demande et appose son sceau).

La Carte d'Identité (Le Certificat)

glpi.crt
(Le document public prouvant l'identité, validé par la Mairie).

Matrice des Composants Cryptographiques

Fichier	Rôle Technique	Où réside-t-il ?	Règle de Sécurité Absolue
glpi.key	Clé Privée RSA (2048 bits)	Serveur GLPI uniquement	Ne doit jamais être transmise ou copiée.
glpi.csr / .cnf	Demande de signature (Certificate Signing Request)	Serveur GLPI (transitoire)	Peut être supprimée après validation par l'ADCS.
glpi.crt	Certificat Serveur (Clé Publique + Identité)	Serveur GLPI (Apache)	Présenté publiquement à chaque client lors du handshake TLS.
CA.certif.crt	Certificat de l'Autorité Racine (ADCS)	Tous les clients Linux	Doit être injecté dans le magasin de confiance de chaque client.

L'Ingénierie du Certificat : L'Importance du SAN

L'Erreur d'Incohérence

Target FQDN:	glpi-agent.c1-04.lan
Cert CN:	glpi.c1-04.lan

⚠ Résultat : subjectAltName mismatch (Connexion rejetée).

La Solution SAN - Fichier de Configuration

glpi-san.cnf

```
[alt_names]
DNS.1 = glpi.c1-04.lan
DNS.2 = glpi-agent.c1-04.lan
```

Les clients TLS modernes exigent une correspondance stricte dans les Subject Alternative Names (SAN), pas seulement dans le Common Name (CN).

Configuration Serveur : Le VirtualHost Apache

Apache

```
SSLEngine on
SSLCertificateFile    /etc/ssl/glpi/glpi.crt
SSLCertificateKeyFile /etc/ssl/glpi/glpi.key
```

(Carte d'Identité)

(ADN / Clé Privée)

L'Écueil de la Chaîne de Certificats

Dans une PKI ADCS simple, Apache ne doit présenter que le certificat serveur.

Il ne faut pas dupliquer le certificat serveur ni inclure la CA racine dans la directive `SSLCertificateChainFile`. C'est au client de posséder la CA, pas au serveur de l'imposer.

Résolution Client : Établir la Confiance sous Linux

```
$ cp CA.certif.crt /usr/local/share/ca-certificates/
```


```
$ update-ca-certificates --fresh
```

```
$ curl -v https://glpi-agent.c1-04.lan

SSL certificate verify ok.
HTTP/1.1 200 OK
```

CONTEXTE

Les serveurs Linux ne connaissent pas l'ADCS Microsoft par défaut.

L'injection manuelle (ou via Ansible) est obligatoire pour valider la signature cryptographique du serveur Apache.