PortailSIO

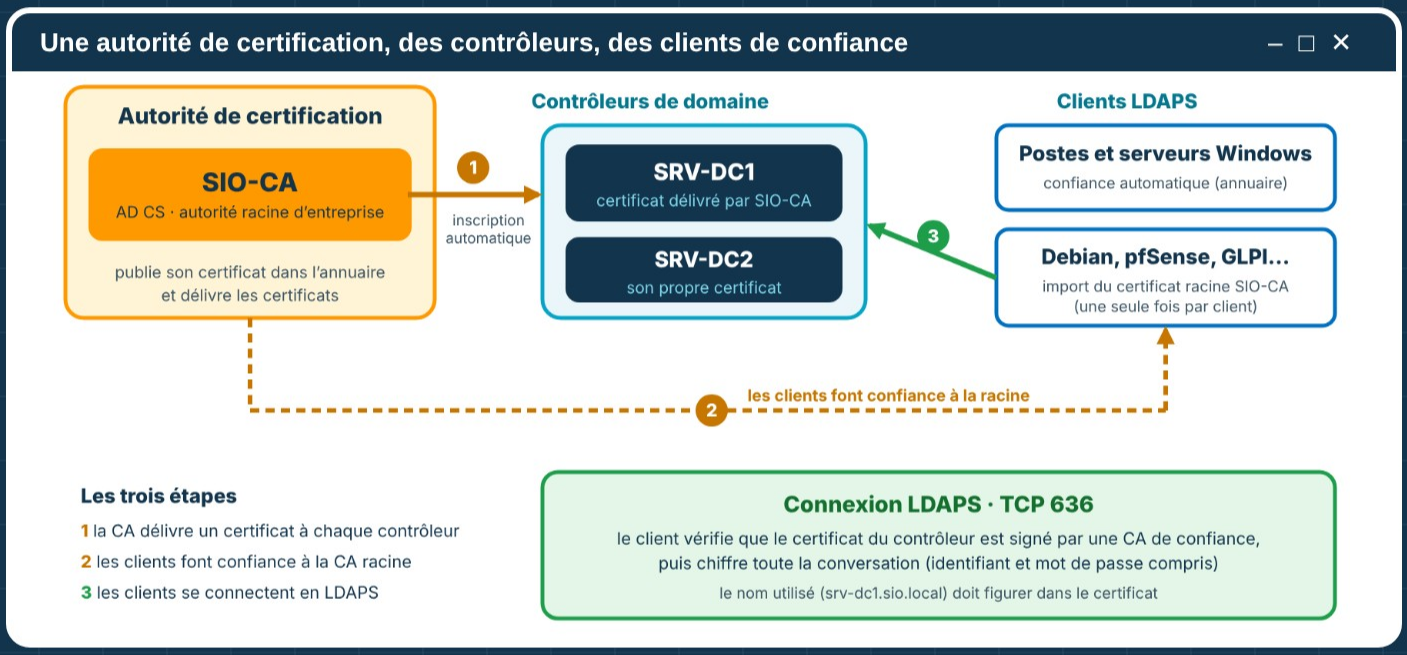
NOUVELLE FORMULE

TUTORIEL

WINDOWS SERVER 2025 · AD CS

Activer et tester LDAPS





1 Comprendre LDAP, LDAPS et la signature LDAP

2 Installer l'autorité de certification AD CS

3 Délivrer un certificat aux contrôleurs de domaine

4 Tester LDAPS depuis Windows

5 Faire confiance à la CA sur les clients Linux

6 Auditer et renforcer la signature LDAP

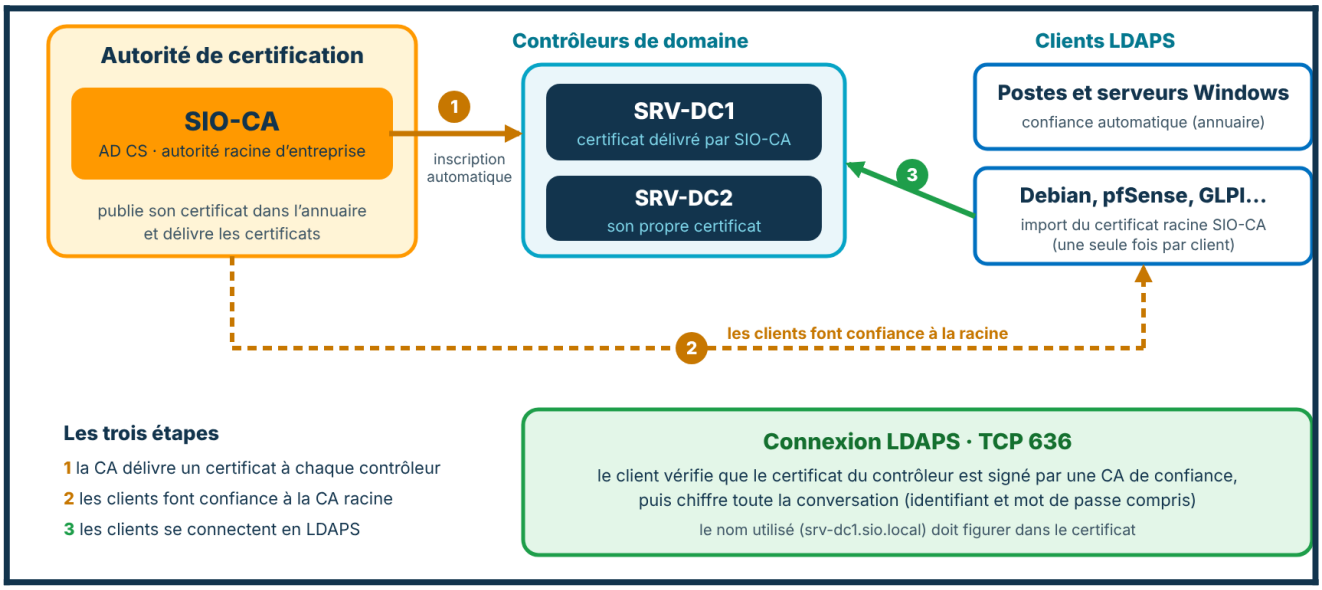
CC BY-NC
Utilisation commerciale interdite
© PortailSIO – 11/2026

Ce tutoriel en ligne
Scannez le QR code. Tous les tutoriels :
portail.sio-ndlp.fr/tutoriels.php

Ce tutoriel a été réalisé avec l'hyperviseur © Proxmox VE. Il peut être réalisé dans un environnement de virtualisation personnel à l'aide des logiciels © VirtualBox ou © VMware Player. Il **suppose que vous disposez du domaine sio.local** construit dans les tutoriels précédents (contrôleurs **SRV-DC1** et **SRV-DC2** sous Windows Server 2025) et d'une machine **Debian 13** pour tester.

LDAP est le protocole que les applications utilisent pour interroger l'annuaire Active Directory : GLPI, Nextcloud, pfSense, Zabbix, un VPN, une messagerie… Par défaut, il circule **en clair** : l'identifiant et le mot de passe de l'utilisateur peuvent être lus par quiconque écoute le réseau. **LDAPS** (LDAP over SSL/TLS) chiffre toute la conversation, à condition que le contrôleur de domaine présente un **certificat** en lequel le client a confiance.

C'est aussi devenu **obligatoire en pratique** : sur un domaine neuf, **Windows Server 2025 refuse par défaut les connexions LDAP en clair** avec identifiant et mot de passe. Dans ce tutoriel, nous installons une **autorité de certification** (AD CS), nous délivrons un certificat aux deux contrôleurs, nous testons LDAPS depuis Windows et depuis Debian, puis nous contrôlons qu'aucun client n'utilise encore une connexion non protégée.



Dans le cadre de ce tutoriel, nous utilisons les machines suivantes (VLAN SERVEURS, réseau 192.168.20.0 /24) :

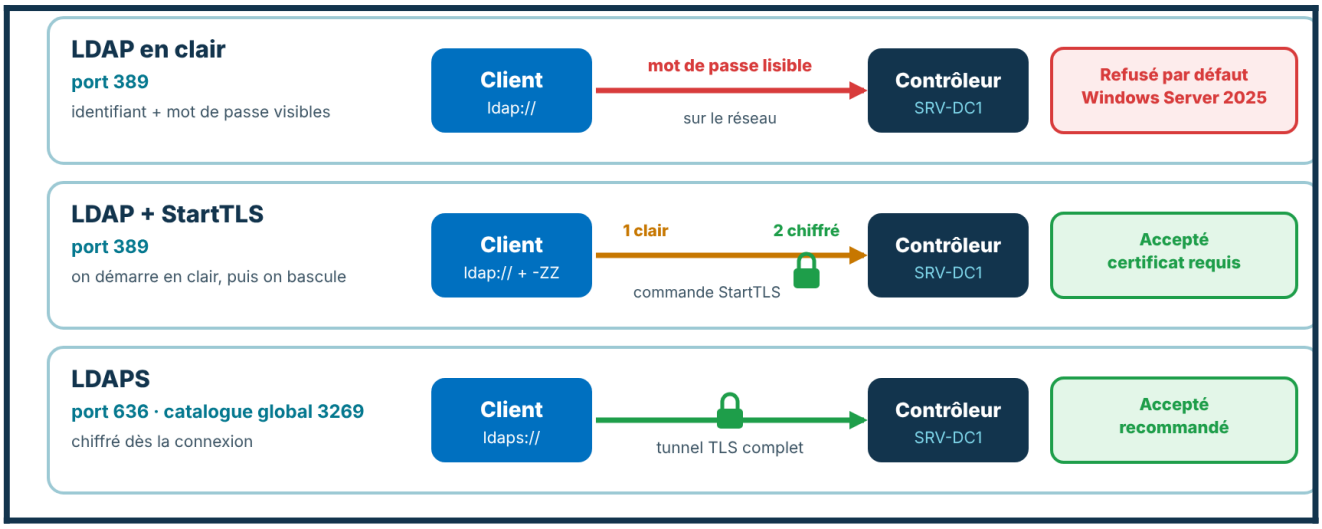
Machine	Rôle	Système	Adresse IP
SRV-DC1	Contrôleur de domaine, DNS, annuaire principal, **autorité de certification SIO-CA**	Windows Server 2025	192.168.20.250
SRV-DC2	Contrôleur de domaine, DNS, annuaire de secours	Windows Server 2025	192.168.20.251
SRV-LINUX	Client de test LDAPS (DNS = les deux contrôleurs)	Debian 13	192.168.20.64

Les adresses, les noms et les mots de passe d'exemple sont à adapter à votre environnement. Les commandes Windows sont exécutées dans **PowerShell** ouvert **en tant qu'administrateur** sur **SRV-DC1** (sauf indication contraire) ; les commandes Debian, avec un compte autorisé à utiliser `sudo` (ou directement en `root`, sans le préfixe `sudo`).

01 ÉTAPE 1 SUR 6 Comprendre LDAP, LDAPS et la signature LDAP

A – Les trois façons de joindre l'annuaire

Un client peut joindre un contrôleur de domaine de trois manières. Seules les deux dernières protègent le mot de passe d'un utilisateur :



Mode	Port	Protection	Avec Windows Server 2025
LDAP en clair (`ldap://`)	389	Aucune : mot de passe lisible sur le réseau	**Refusé** pour l'identifiant et le mot de passe (« simple bind »)
LDAP + StartTLS	389	Chiffré après une commande de bascule	Accepté, certificat requis
LDAPS (**`ldaps://`**)	636	Chiffré dès la connexion (TLS)	Accepté, certificat requis : **recommandé**
LDAPS sur le catalogue global	3269	Idem, pour les recherches dans toute la forêt	Accepté, certificat requis

Windows Server 2025 impose par défaut deux protections, sur les domaines neufs : la **signature LDAP** (les connexions LDAP non chiffrées doivent signer leurs messages ; les connexions en clair avec mot de passe sont rejetées) et la **liaison de canal** (*channel binding*, « Si pris en charge » par défaut), qui relie l'authentification au tunnel TLS. LDAPS satisfait la première sans effort : le chiffrement TLS garantit lui-même l'intégrité des messages.

B – Préparer un compte de test en lecture seule

Pour constater le problème, puis tester LDAPS, il faut un compte ordinaire du domaine et un utilisateur à rechercher. Sur **SRV-DC1**, créez les unités d'organisation, le compte **svc-ldap** et l'utilisateur **amartin** (si ces objets existent déjà, ignorez les messages « existe déjà ») :

POWERSHELL

```
$base = "DC=sio,DC=local"
New-ADOrganizationalUnit -Name "Comptes de service" -Path $base
New-ADOrganizationalUnit -Name "Utilisateurs" -Path $base
$mdp = Read-Host -AsSecureString "Mot de passe de svc-ldap"
New-ADUser -Name "svc-ldap" -SamAccountName "svc-ldap" `
    -UserPrincipalName "svc-ldap@sio.local" `
    -Path "OU=Comptes de service,$base" -AccountPassword $mdp `
    -Enabled $true -PasswordNeverExpires $true -CannotChangePassword $true
```

POWERSHELL

```
$mdp = Read-Host -AsSecureString "Mot de passe de amartin"
New-ADUser -Name "Alice Martin" -GivenName Alice -Surname Martin `
    -SamAccountName amartin -UserPrincipalName amartin@sio.local `
    -EmailAddress amartin@sio.local -Path "OU=Utilisateurs,$base" `
    -AccountPassword $mdp -Enabled $true
```

C – Constater le refus du LDAP en clair

Sur **SRV-LINUX**, le serveur doit utiliser les contrôleurs comme DNS (`sudo nano /etc/resolv.conf`) :

/etc/resolv.conf

```
search sio.local
nameserver 192.168.20.250
nameserver 192.168.20.251
```

1. Installez l'outil de test LDAP, puis tentez une recherche en **LDAP en clair** (port 389) avec le compte de service ; saisissez son mot de passe quand il est demandé :

TERMINAL

```
sudo apt install -y ldap-utils
ldapsearch -H ldap://srv-dc1.sio.local -x -D "svc-ldap@sio.local" -W \
    -b "DC=sio,DC=local" "(sAMAccountName=amartin)" dn
```

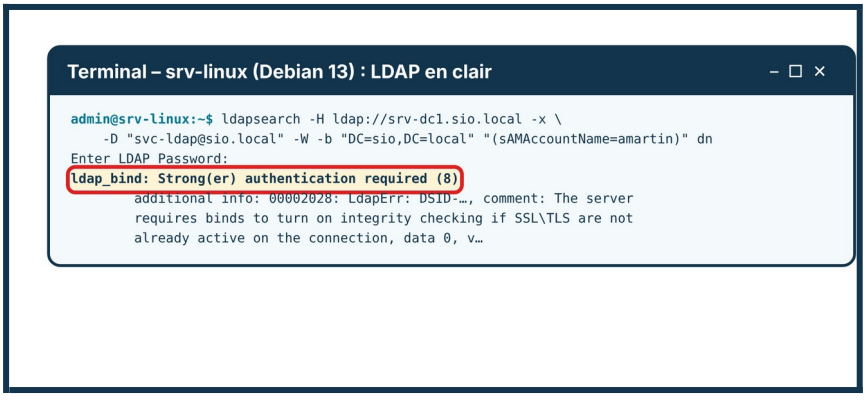


Figure 1 – Debian : le LDAP en clair est refusé

À SAVOIR

Le message ci-dessus est le symptôme classique : « Strong(er) authentication required (8) », avec le commentaire « The server requires binds to turn on integrity checking if SSL\TLS are not already active ». Il apparaît dans GLPI, Nextcloud, pfSense, Zabbix… dès qu'ils sont configurés en `ldap://` sur un domaine Windows Server 2025.

✔ POINT DE CONTRÔLE

- Vous savez distinguer **LDAP** (389), **StartTLS** (389 chiffré) et **LDAPS** (636)
- Le compte **svc-ldap** et l'utilisateur **amartin** existent
- `ldapsearch` en `ldap://` renvoie « **Strong(er) authentication required** » : le problème est reproduit

02 ÉTAPE 2 SUR 6 Installer l'autorité de certification AD CS

Pour que les clients fassent confiance à un contrôleur, son certificat doit être signé par une **autorité de certification** (AC, ou CA en anglais) qu'ils connaissent. Dans un domaine Windows, la solution naturelle est **AD CS** (Active Directory Certificate Services) en **autorité d'entreprise** : elle publie son certificat dans l'annuaire (les postes du domaine lui font alors confiance automatiquement) et délivre d'elle-même les certificats aux contrôleurs de domaine.

REMARQUE IMPORTANTE

Pour ce laboratoire, la CA est installée **sur SRV-DC1** : c'est simple, mais **déconseillé en production**. En production, on utilise un **serveur dédié** (idéalement une racine hors ligne et une AC émettrice). Le nom de la CA ne pourra plus être changé : choisissez-le avec soin (ici **SIO-CA**).

A – Installer le rôle

Sur **SRV-DC1**, installez le rôle **Services de certificats Active Directory** (autorité de certification) avec ses outils de gestion :

POWERSHELL

```
Install-WindowsFeature ADCS-Cert-Authority -IncludeManagementTools
```

B – Configurer l'autorité d'entreprise

La configuration se fait en une commande. Le compte utilisé doit être membre du groupe **Administrateurs de l'entreprise** (c'est le cas du compte **Administrateur** du domaine racine). On crée une **autorité racine d'entreprise** nommée **SIO-CA**, avec une clé RSA de 4096 bits valable 10 ans :

POWERSHELL

```
$params = @{
    CAType              = "EnterpriseRootCa"
    CACommonName        = "SIO-CA"
    CryptoProviderName  = "RSA#Microsoft Software Key Storage Provider"
    KeyLength           = 4096
    HashAlgorithmName   = "SHA256"
    ValidityPeriod      = "Years"
    ValidityPeriodUnits = 10
}
Install-AdcsCertificationAuthority @params -Force
```

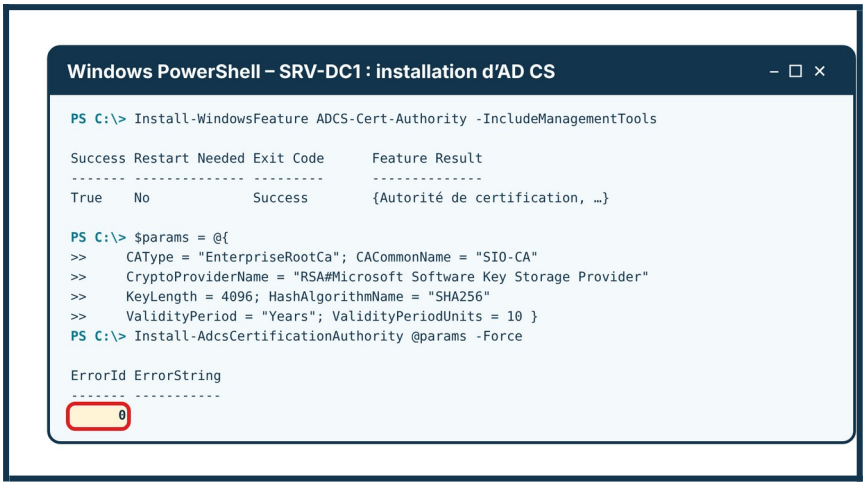


Figure 2 – Installation du rôle et configuration de la CA

À SAVOIR

Le tableau « ErrorId 0 » signifie que la configuration s'est terminée sans erreur. En cas de problème, relancez la commande avec `-Verbose` et consultez le fichier `%windir%\cerocm.log`.

Paramètre	Valeur	Rôle
CAType	`EnterpriseRootCa`	Autorité d'entreprise intégrée à AD DS, sans autorité supérieure
CACommonName	`SIO-CA`	Nom de l'autorité, visible dans tous les certificats qu'elle signe
CryptoProviderName	`RSA#Microsoft Software Key Storage Provider`	Stockage de la clé privée de la CA par Windows (CNG)
KeyLength, HashAlgorithmName	`4096`, `SHA256`	Taille de la clé de la CA et algorithme de signature
ValidityPeriod, Units	`Years`, `10`	Durée de vie du certificat de la CA (les certificats délivrés vivent moins longtemps)

C – Vérifier que l'autorité fonctionne

1. Contrôlez que le service est démarré et que l'autorité répond (la commande `certutil -ping` doit indiquer que l'interface de la CA est active) :

```powershell
Get-Service certsvc
certutil -ping
```

2 Ouvrez la console **Autorité de certification** (`certsrv.msc`) : **SIO-CA** porte une coche verte, et le dossier « **Modèles de certificats** » contient le modèle **Authentification Kerberos**, que les contrôleurs de domaine utiliseront à l'étape suivante :

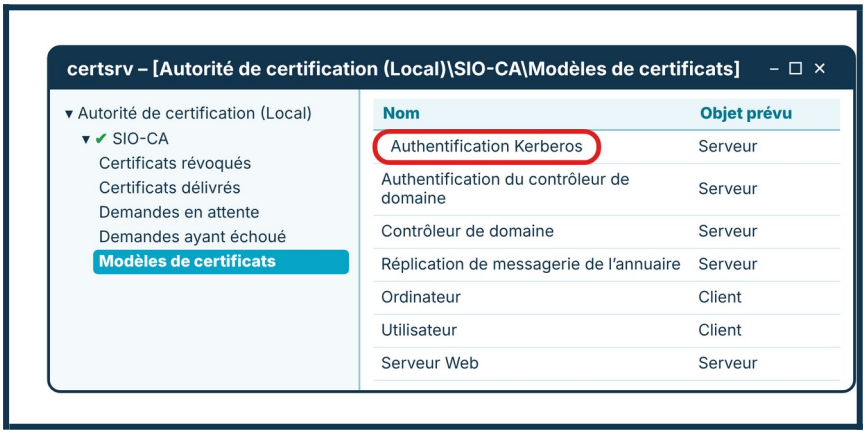


Figure 3 – Console Autorité de certification : modèles de certificats

À SAVOIR

Ces modèles sont les « formulaires » à partir desquels l'autorité délivre ses certificats. Le modèle **Authentification Kerberos** est celui que Microsoft recommande pour les contrôleurs de domaine : il contient le nom du contrôleur et l'usage « Authentification du serveur ».

✔ POINT DE CONTRÔLE

- `Get-Service certsvc` indique **Running**
- La console `certsrv.msc` affiche **SIO-CA** avec une coche verte
- Le modèle **Authentification Kerberos** figure dans les modèles de certificats

ÉTAPE 3 SUR 6

03 Délivrer un certificat aux contrôleurs de domaine

Un contrôleur de domaine active LDAPS **tout seul** dès qu'il trouve un certificat valable dans son magasin : il n'y a rien à configurer dans AD DS. Le certificat doit respecter ces exigences :

Exigence	Pourquoi
Dans le magasin Ordinateur local > Personnel **du contrôleur**	C'est là que le contrôleur le cherche
Une clé privée **associée, sans protection forte de la clé**	Le contrôleur doit pouvoir s'en servir sans intervention
Usage Authentification du serveur **(OID** `1.3.6.1.5.5.7.3.1`**)**	Sans cet usage, le certificat est ignoré pour LDAPS
Le nom complet **du contrôleur (**`srv-dc1.sio.local`**) dans le CN ou le nom alternatif (SAN)**	Le client compare ce nom à celui qu'il a contacté
Délivré par une AC de confiance **pour le contrôleur et les clients**	Sinon le client refuse la connexion

A – Activer l'inscription automatique des contrôleurs

Le modèle **Authentification Kerberos** est publié par défaut et accessible aux contrôleurs de domaine. Il suffit qu'ils **demandent eux-mêmes** leur certificat : c'est l'« inscription automatique », activée par une stratégie de groupe. Sur **SRV-DC1** :

1 Ouvrez la **Gestion des stratégies de groupe** (`gpmc.msc`), développez le domaine puis l'unité d'organisation **Domain Controllers**, faites un clic droit sur **Default Domain Controllers Policy** et choisissez « **Modifier** »

2. Allez dans « Configuration ordinateur » > « Stratégies » > « Paramètres Windows » > « Paramètres de sécurité » > « **Stratégies de clé publique** », puis double-cliquez sur « **Client des services de certificats – Inscription automatique** »
3. Choisissez « **Activé** » et cochez **les deux cases** proposées, puis cliquez « **OK** » :



Figure 4 – Stratégie : inscription automatique des certificats

À SAVOIR

La première case renouvelle automatiquement les certificats avant leur expiration, la seconde les remplace quand le modèle change. Dans un domaine de production, créez plutôt une stratégie dédiée (par exemple « Inscription automatique des contrôleurs ») liée à l'unité d'organisation **Domain Controllers**.

B – Obtenir le certificat sur chaque contrôleur

Sur **SRV-DC1**, puis sur **SRV-DC2**, forcez l'application de la stratégie et la demande de certificat, puis listez les certificats utilisables pour l'authentification de serveur (on y reconnaît l'usage par son OID, valable quelle que soit la langue de Windows) :

POWERSHELL (SRV-DC1 ET SRV-DC2)

```
gpupdate /force
certreq -autoenroll -q
$srv = "1.3.6.1.5.5.7.3.1"
Get-ChildItem Cert:\LocalMachine\My |
    Where-Object { $_.EnhancedKeyUsageList.ObjectId -contains $srv } |
    Select-Object @{n="DNS";e={$_.DnsNameList -join ", "}}, Issuer, NotAfter
```

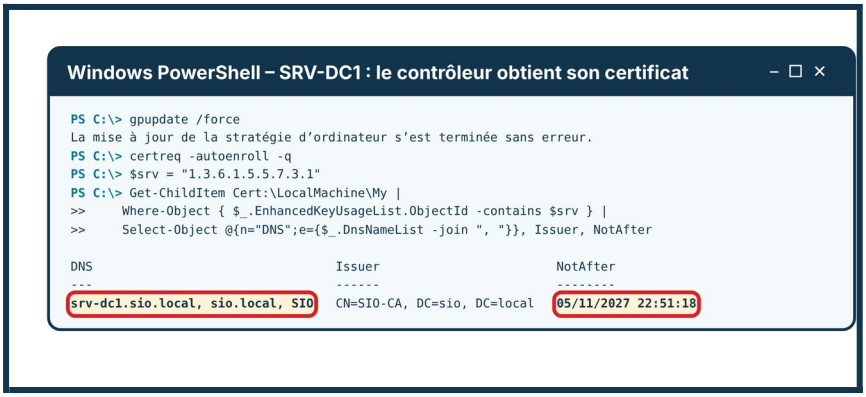


Figure 5 – Le contrôleur a obtenu son certificat

À SAVOIR

La colonne « DNS » doit contenir le nom complet du contrôleur et « Issuer » le nom de la CA (SIO-CA). Si la liste est vide, attendez une minute et recommencez ; sinon, faites la demande à la main : `certlm.msc` > Personnel > Certificats > clic droit > Toutes les tâches > Demander un nouveau certificat > modèle « Authentification Kerberos ».

C – Contrôler le certificat

Dans `certlm.msc` (certificats de l'ordinateur), « Personnel » > « Certificats », double-cliquez le certificat du contrôleur : onglet « **Détails** », contrôlez l'**usage avancé de la clé** et l'**autre nom de l'objet** :

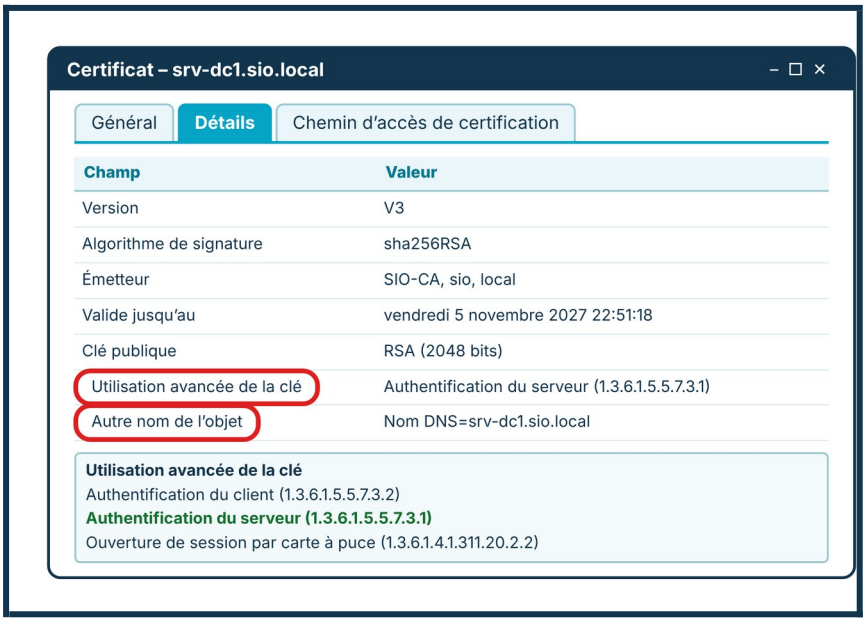


Figure 6 – Détail du certificat du contrôleur

À SAVOIR

Ces deux champs sont ceux qui comptent pour LDAPS. Le certificat délivré par le modèle Authentification Kerberos contient aussi d'autres usages (authentification du client, carte à puce) : c'est normal.

À SAVOIR

Le contrôleur **détecte seul** un nouveau certificat : aucun service à redémarrer. Si plusieurs certificats valables sont présents (un ancien auto-signé, par exemple), il peut en choisir un au hasard : supprimez les inutiles.

D – Variante laboratoire : un certificat auto-signé

Sans autorité de certification, un certificat **auto-signé** par contrôleur suffit pour un essai (c'est la méthode des tutoriels GLPI et Nextcloud). Sur **SRV-DC1**, puis sur **SRV-DC2** (en changeant le nom) ; **ne combinez pas cette méthode avec AD CS** sur le même contrôleur :

POWERSHELL

```
# SRV-DC2 : remplacer par srv-dc2.sio.local
$fqdn = "srv-dc1.sio.local"
$cert = New-SelfSignedCertificate -Subject "CN=$fqdn" -DnsName $fqdn `
    -CertStoreLocation Cert:\LocalMachine\My -KeyAlgorithm RSA `
    -KeyLength 2048 -HashAlgorithm SHA256 -NotAfter (Get-Date).AddYears(2)
New-Item -ItemType Directory -Path C:\Temp -Force | Out-Null
# SRV-DC2 : srv-dc2.cer
Export-Certificate -Cert $cert -FilePath C:\Temp\srv-dc1.cer
```

Chaque client devra faire confiance à **chaque** certificat de contrôleur (un `.cer` par contrôleur, à renouveler tous les deux ans) au lieu d'**une seule** autorité : AD CS est la bonne solution dès que l'on dépasse le laboratoire.

✔ **POINT DE CONTRÔLE**

- `gpupdate /force` et `certreq -autoenroll -q` s'exécutent sur **chaque** contrôleur sans erreur
- Chaque contrôleur possède un certificat « Authentification du serveur » à son **nom complet**, délivré par **SIO-CA**
- Le magasin « Personnel » ne contient pas d'autre certificat de serveur (ancien, auto-signé)

04 ÉTAPE 4 SUR 6 Tester LDAPS depuis Windows

A – Se connecter avec l'outil ldp

ldp.exe est l'outil graphique de Microsoft pour interroger un annuaire LDAP ; il est installé sur chaque contrôleur de domaine. Testez d'abord la connexion chiffrée sur **SRV-DC1** :

1. Lancez `ldp` (touches **Windows + R**) puis, dans le menu « **Connexion** », cliquez « **Se connecter…** »
2. Saisissez le **nom complet** `srv-dc1.sio.local`, le port **636**, cochez « **SSL** » et cliquez « **OK** » :

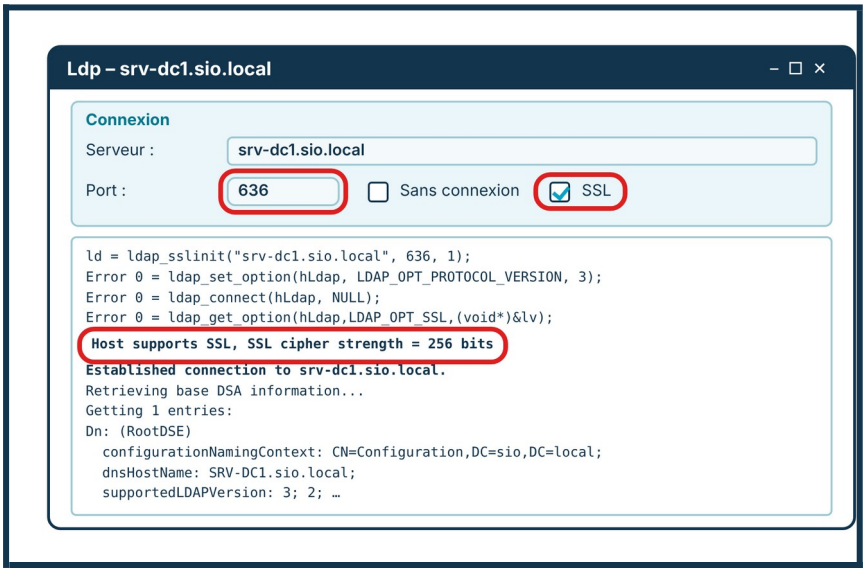


Figure 7 – Ldp : connexion SSL sur le port 636

À SAVOIR

La connexion réussit quand le volet de droite affiche « Host supports SSL » puis « Established connection » et le contenu de la racine de l'annuaire (RootDSE). Un échec s'accompagne du code 81 (« serveur injoignable ») : voir le tableau de dépannage.

3. Recommencez avec `srv-dc2.sio.local`. Utilisez toujours le **nom** du contrôleur, jamais son adresse IP : le nom doit correspondre à celui qui figure dans le certificat

B – Vérifier le port 636 des deux contrôleurs d'un seul coup

Depuis n'importe quel serveur Windows du domaine, ce petit script teste le port **636** des deux contrôleurs (le résultat doit être **True** deux fois) :

POWERSHELL

```
"srv-dc1.sio.local","srv-dc2.sio.local" | ForEach-Object {
    Test-NetConnection $_ -Port 636 -WarningAction SilentlyContinue |
    Select-Object ComputerName, RemotePort, TcpTestSucceeded }
```

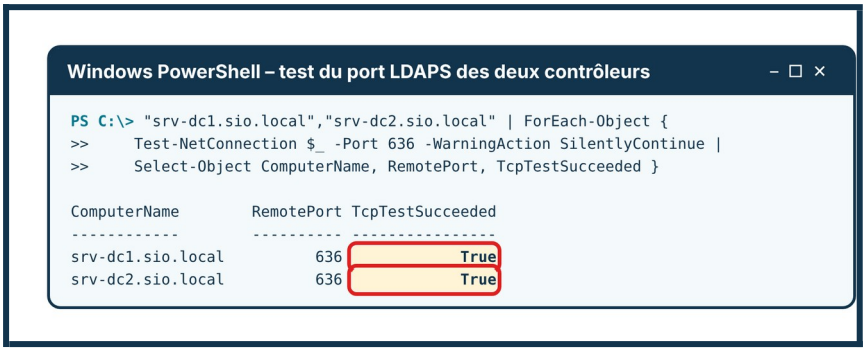


Figure 8 – Test du port LDAPS des deux contrôleurs

À SAVOIR

Ce test prouve seulement que le port est ouvert. Seul un client qui **valide le certificat** (ldp, ou ldapsearch à l'étape suivante) prouve que le certificat est correct. Le port **3269** (catalogue global en SSL) s'active en même temps avec le même certificat.

À SAVOIR

Les postes et serveurs **Windows du domaine** font confiance à SIO-CA sans rien faire : l'autorité d'entreprise publie son certificat dans l'annuaire, et chaque machine le récupère à sa prochaine actualisation de stratégie (`gpupdate`). Il reste à traiter les clients **qui ne sont pas Windows** : c'est l'étape suivante.

✔ **POINT DE CONTRÔLE**

- `ldp` se connecte à **srv-dc1.sio.local** puis à **srv-dc2.sio.local** en SSL sur le port **636**
- `Test-NetConnection` renvoie **True** sur le port 636 des deux contrôleurs

05 ÉTAPE 5 SUR 6 Faire confiance à la CA sur les clients Linux

Un client **Debian** ne connaît pas SIO-CA : il refuserait le certificat des contrôleurs. Il suffit de lui faire importer **une seule fois** le certificat de la CA : tous les certificats qu'elle signera ensuite (contrôleurs actuels et futurs, renouvellements compris) seront acceptés.

A – Constater l'absence de confiance

Sur **SRV-LINUX**, regardez comment Debian juge le certificat présenté par le contrôleur :

TERMINAL

```
openssl s_client -connect srv-dc1.sio.local:636 </dev/null 2>&1 \
    | grep -E 'Verification|Verify return code'
```



Figure 9 – Debian : la CA n'est pas encore connue

À SAVOIR

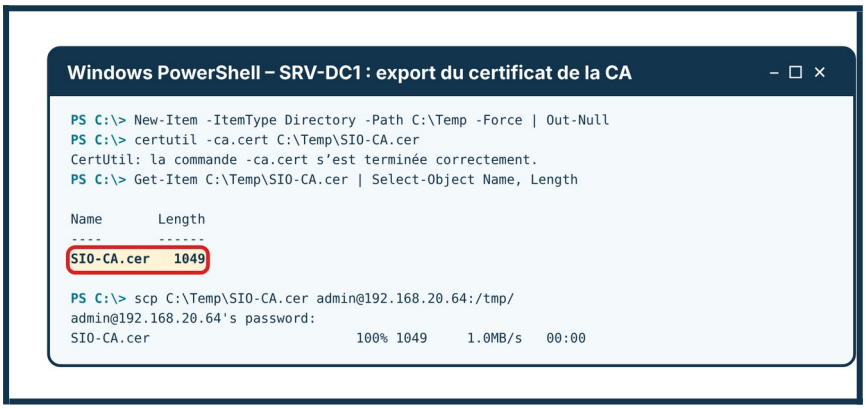
« unable to get local issuer certificate » (code 20) veut dire : le client n'a pas trouvé, dans ses autorités de confiance, la CA qui a signé le certificat. Le certificat n'est pas en cause, c'est la confiance qui manque.

B – Exporter le certificat de la CA

Sur **SRV-DC1**, exportez le certificat de SIO-CA dans un fichier, puis copiez-le vers **SRV-LINUX** (ou utilisez WinSCP, ou un partage) :

POWERSHELL

```
New-Item -ItemType Directory -Path C:\Temp -Force | Out-Null
certutil -ca.cert C:\Temp\SIO-CA.cer
scp C:\Temp\SIO-CA.cer admin@192.168.20.64:/tmp/
```



À SAVOIR

Ce fichier ne contient que la partie **publique** de la CA : il peut circuler librement. N'exportez jamais la clé privée de la CA. Le fichier est au format DER, que `openssl` convertit à l'étape suivante.

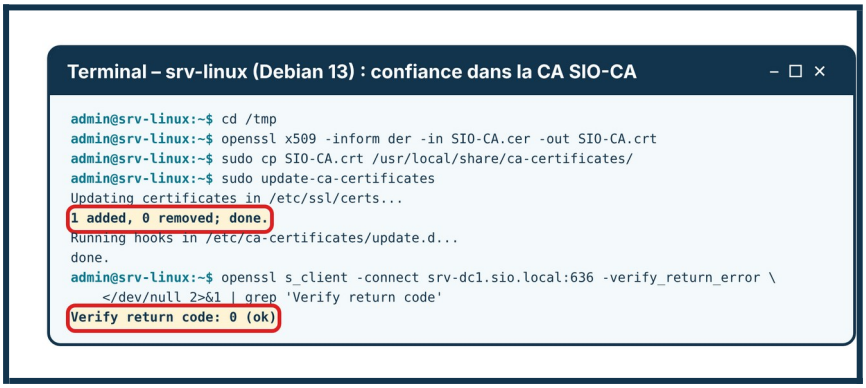
Figure 10 – Export du certificat de la CA et copie vers Debian

C – Installer le certificat dans Debian

Sur **SRV-LINUX**, convertissez le certificat au format attendu (PEM), ajoutez-le aux autorités de confiance du système, puis refaites le contrôle de l'étape A : cette fois, le code doit être **0** :

TERMINAL

```
cd /tmp
openssl x509 -inform der -in SIO-CA.cer -out SIO-CA.crt
sudo cp SIO-CA.crt /usr/local/share/ca-certificates/
sudo update-ca-certificates
openssl s_client -connect srv-dc1.sio.local:636 -verify_return_error \
    </dev/null 2>&1 | grep 'Verify return code'
```



À SAVOIR

« 1 added » prouve que la CA est maintenant dans les autorités de confiance de Debian. Si vous aviez utilisé la variante auto-signée, il faudrait importer le fichier de **chaque** contrôleur de la même façon. Répétez le contrôle avec `srv-dc2.sio.local`.

Figure 11 – Debian : confiance dans la CA SIO-CA

D – Interroger l'annuaire en LDAPS

Dernière vérification : la même recherche qu'à l'étape 1, mais cette fois en **LDAPS**. Elle doit réussir et renvoyer l'utilisateur **amartin** :

TERMINAL

```
ldapsearch -H ldaps://srv-dc1.sio.local -x -D "svc-ldap@sio.local" -W \
    -b "DC=sio,DC=local" "(sAMAccountName=amartin)" dn mail
```



Figure 12 – Debian : recherche réussie en LDAPS

À SAVOIR

« result: 0 Success » et la ligne `dn:` prouvent que le certificat, le nom, le compte de service et le port 636 fonctionnent ensemble. L'option `-x` utilise une connexion simple (identifiant et mot de passe) : sans le chiffrement de LDAPS, Windows Server 2025 l'aurait refusée.

E – Les autres clients

Chaque application qui interroge l'annuaire a son propre magasin d'autorités de confiance. Le principe est toujours le même : lui donner le certificat de **SIO-CA**, puis utiliser `ldaps://` et le port **636** avec le **nom complet** du contrôleur :

Client	Où importer le certificat de la CA
Debian (GLPI, Nextcloud, ldapsearch, PHP…)	`/usr/local/share/ca-certificates` puis `sudo update-ca-certificates` ; redémarrer `php8.4-fpm` pour les applications PHP
Application Java	`keytool -importcert -cacerts -alias SIO-CA -file SIO-CA.crt` (magasin `cacerts` de Java)
pfSense	« Système > Gestionnaire de certificats > Autorités » : ajouter SIO-CA, puis la choisir dans le serveur d'authentification LDAP
Windows hors domaine	Double-clic sur le `.cer` > Installer le certificat > « Autorités de certification racines de confiance »

✔ POINT DE CONTRÔLE

- Avant l'import, `openssl s_client` répond **code 20** ; après l'import, **Verify return code: 0 (ok)** pour `srv-dc1` et `srv-dc2`
- `ldapsearch -H ldaps://…` renvoie l'entrée de **Alice Martin** (« result: 0 Success »)

06 ÉTAPE 6 SUR 6
Auditer et renforcer la signature LDAP

LDAPS fonctionne. Reste à s'assurer que **plus aucun client** n'utilise de connexion LDAP non protégée, puis à **interdire** ces connexions. Sur un domaine neuf en Windows Server 2025, c'est déjà le comportement par défaut ; sur un domaine plus ancien ou mis à niveau, les connexions non protégées sont encore acceptées tant qu'on ne les bloque pas.

A – Les trois paramètres de sécurité des contrôleurs

Ils se trouvent dans la stratégie des contrôleurs de domaine : « Configuration ordinateur » > « Stratégies » > « Paramètres Windows » > « Paramètres de sécurité » > « Stratégies locales » > « **Options de sécurité** » :

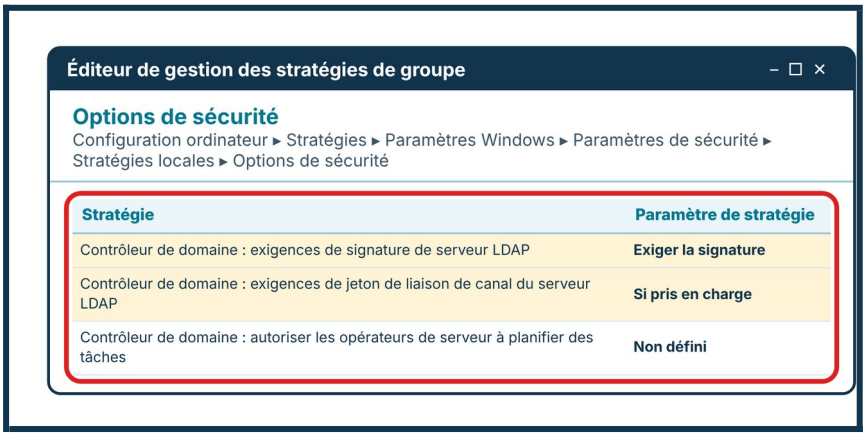


Figure 13 – Options de sécurité : exigences LDAP des contrôleurs

À SAVOIR

Les intitulés en français peuvent différer légèrement selon la version de Windows ; on les retrouve en cherchant « LDAP » dans la liste.

Paramètre (nom Microsoft)	Valeurs	Valeur recommandée
Domain controller: LDAP server signing requirements	Aucune / **Exiger la signature**	**Exiger la signature** (comportement par défaut en Windows Server 2025 sur un domaine neuf)
Domain controller: LDAP server signing requirements enforcement	Activé / Désactivé (Windows Server 2025)	**Activé** : il prend le pas sur le paramètre précédent
Domain controller: LDAP server channel binding token requirements	Jamais / **Si pris en charge** / Toujours	**Si pris en charge** ; **Toujours** une fois l'audit terminé sans alerte

La signature concerne les connexions **non chiffrées** (LDAP sur le port 389). La liaison de canal concerne les connexions **chiffrées** qui s'authentifient par SASL : un simple identifiant et mot de passe sur LDAPS, comme dans GLPI ou Nextcloud, n'est pas concerné.

B – Repérer les clients qui se connectent sans protection

Les contrôleurs consignent ces connexions dans le journal « **Directory Service** ». Quatre événements sont utiles :

Événement	Signification
2886	Au démarrage : le contrôleur avertit qu'il n'interdit pas les connexions non protégées
2887	Résumé quotidien : connexions non protégées **acceptées** (compteurs, sans détail)
2888	Résumé quotidien : connexions non protégées **refusées** parce que la signature est exigée
2889	Détail par client : **adresse IP**, **compte** utilisé et **type** de connexion (1 = identifiant et mot de passe en clair)

1. Pour obtenir le détail (événement 2889), activez la journalisation « **16 LDAP Interface Events** » au niveau 2 sur chaque contrôleur, laissez travailler les applications quelques jours, puis listez les clients concernés :

POWERSHELL

```
reg add HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics `
    /v "16 LDAP Interface Events" /t REG_DWORD /d 2 /f
Get-WinEvent -FilterHashtable @{LogName="Directory Service"; Id=2889} |
    Select-Object TimeCreated, @{n="Client";e={$_.Properties[0].Value}},
      @{n="Compte";e={$_.Properties[1].Value}},
      @{n="Type";e={$_.Properties[2].Value}}
```

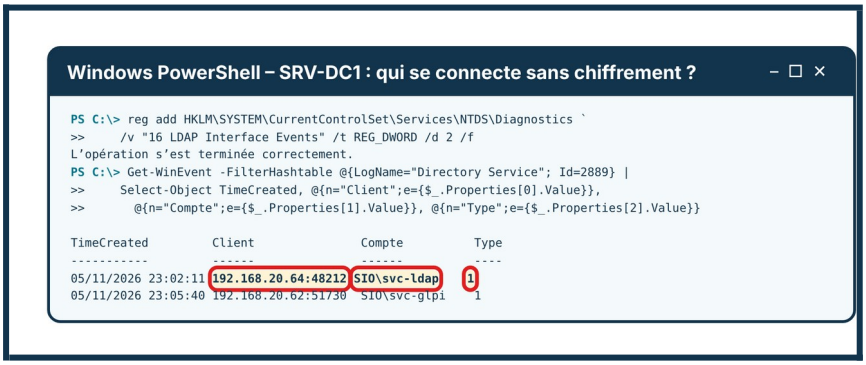


Figure 14 – Qui se connecte encore sans chiffrement ?

À SAVOIR

Chaque ligne désigne une application à corriger : l'adresse IP dit **quel serveur**, le compte dit **quelle configuration** (ici un test avec `svc-ldap` et l'ancien GLPI configuré en `ldap://`). Une liste vide signifie qu'aucun client ne se connecte sans protection.

REMARQUE IMPORTANTE

La journalisation détaillée ralentit un peu les contrôleurs : **remettez-la à 0 après l'audit** (même commande avec `/d 0`).

C – Corriger les clients, puis renforcer

1. Pour **chaque** client listé, passez-le en **LDAPS** : serveur `ldaps://srv-dc1.sio.local`, port **636**, certificat de SIO-CA importé (étape 5), puis testez-le. C'est ce que font les tutoriels GLPI et Nextcloud
2. Relevez de nouveau l'événement **2889** quelques jours : il ne doit plus lister de client (sauf un test volontaire)
3. Dans la stratégie des contrôleurs, placez la signature LDAP sur « **Exiger la signature** » et, une fois les événements de liaison de canal (**3039**) éteints, la liaison de canal sur « **Toujours** ». Appliquez avec `gpupdate /force` sur les contrôleurs
4. Refaites le test de l'étape 1-C : le LDAP en clair doit être **refusé**, le LDAPS (étape 5-D) doit **réussir**

À SAVOIR

Procédez **contrôleur par contrôleur** et gardez un moyen de revenir en arrière : repasser le paramètre sur « Aucune » / « Jamais » rétablit l'ancien comportement le temps de corriger un client oublié. Les certificats de la CA et des contrôleurs ont une durée de vie : les certificats Kerberos se renouvellent tout seuls grâce à l'inscription automatique, vérifiez-le une fois par an dans le gestionnaire de certificats.

✔ **POINT DE CONTRÔLE**

- Le journal **Directory Service** ne contient plus d'événement **2889** (hors test volontaire)
- La signature LDAP est sur « **Exiger la signature** » sur les deux contrôleurs
- Le LDAP en clair est **refusé** et le LDAPS **fonctionne** depuis Debian
- La journalisation « 16 LDAP Interface Events » est **revenue à 0**

Notre domaine **sio.local** est maintenant protégé : une autorité de certification d'entreprise délivre leur certificat aux contrôleurs, les clients Linux lui font confiance, et plus aucun mot de passe LDAP ne circule en clair. Les applications (GLPI, Nextcloud, pfSense, Zabbix…) peuvent s'appuyer sur `ldaps://` en toute sécurité.

Dépannage : les symptômes les plus fréquents

Symptôme	Cause probable	Solution
`ldapsearch` : « **Strong(er) authentication required (8)** »	Connexion LDAP en clair refusée par Windows Server 2025	Utiliser `ldaps://` et le port **636** (ou StartTLS avec l'option `-ZZ`), jamais `ldap://` avec mot de passe
« Can't contact LDAP server (-1) »	Port 636 fermé, pas de certificat sur le contrôleur, CA non reconnue ou nom incorrect	`Test-NetConnection` sur le port 636 ; `ldp` sur le contrôleur ; `openssl s_client` depuis le client
`openssl` : « **unable to get local issuer certificate** » **(code 20)**	Le certificat de SIO-CA n'est pas importé sur le client	Refaire l'étape 5 (export, `update-ca-certificates`)
« certificate is not yet valid » ou « has expired »	Horloge du client ou du serveur décalée, ou certificat expiré	Synchroniser l'heure (`chrony`) ; contrôler `NotAfter` dans `certlm.msc`
« Hostname mismatch » ou refus alors que le certificat est reconnu	Connexion par adresse IP ou par un alias absent du certificat	Utiliser le **nom complet** du contrôleur (`srv-dc1.sio.local`), présent dans le certificat
`ldp` **: erreur 81, rien sur le port 636**	Pas de certificat « Authentification du serveur » valable sur le contrôleur	`gpupdate /force` puis `certreq -autoenroll -q` ; demande manuelle dans `certlm.msc` ; vérifier le modèle publié sur la CA
L'inscription automatique ne délivre rien	Stratégie non appliquée au contrôleur, ou droit « Inscrire » absent sur le modèle	Vérifier la stratégie (étape 3-A) et les droits du modèle ; journal « CertificateServices-Lifecycles-System »
Le contrôleur présente un autre certificat que prévu	Plusieurs certificats valables dans le magasin « Personnel »	Supprimer les certificats inutiles (ancien, auto-signé)
Une application cesse de se connecter après le renforcement	Elle utilisait `ldap://` avec mot de passe	Identifier le client (événements 2888 et 2889), le passer en `ldaps://`, ou revenir temporairement en arrière

Pense-bête : où regarder

Où / commande	Utilité
`certsrv.msc`	Console de l'autorité de certification : modèles, certificats délivrés, demandes
`certlm.msc`	Certificats de l'ordinateur : magasin « Personnel » d'un contrôleur, dates d'expiration
`gpmc.msc`	Stratégies de groupe : inscription automatique, options de sécurité LDAP
`ldp`	Test graphique d'une connexion LDAPS (port 636) et exploration de l'annuaire
`certreq -autoenroll -q`	Forcer la demande des certificats d'un contrôleur
`certutil -ca.cert <fichier>`	Exporter le certificat public de la CA pour les clients non Windows
`openssl s_client -connect <contrôleur>:636`	Voir le certificat présenté et la validation depuis un client Linux
`ldapsearch -H ldaps://… -x -D … -W`	Tester l'annuaire sans passer par une application
Journal « Directory Service » (2886 à 2889)	Repérer les clients qui se connectent sans protection