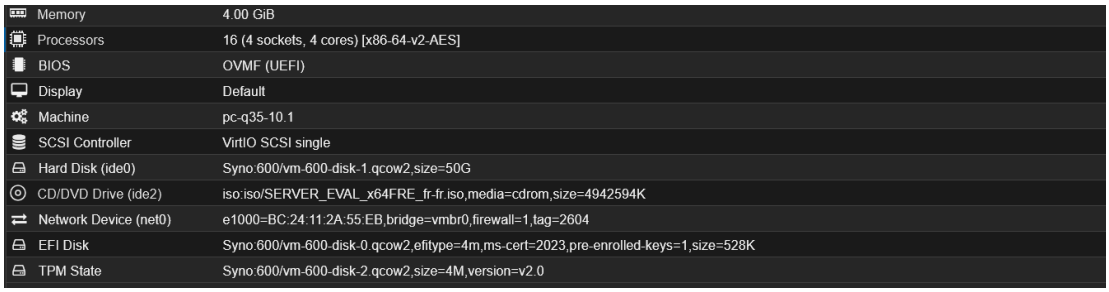
● PROCÉDURE TECHNIQUE · V2.0 · 09/04/2026

Active Directory

Windows Server 2022

Installation · OU · Utilisateurs · Groupes · GPO · Autorité de Certification

Paramètre	Valeur
Domaine AD	qscarpa.lan
Contrôleur	AD-1 — 10.2.0.201
Plage DHCP	10.2.0.200 — 10.2.0.210
Passerelle	10.2.0.254
OS	Windows Server 2022 Evaluation x64
Hyperviseur	Proxmox VE
Auteur	Quentin SCARPA
Date	09/04/2026



Configuration VM Proxmox — VM 600 (Windows Server 2022)

Active Directory Domain Services

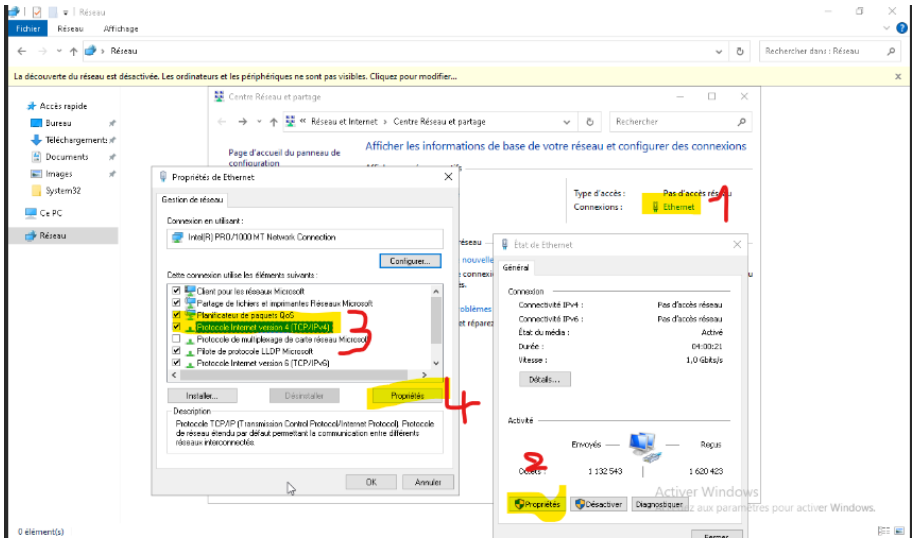
Installation du rôle AD DS et promotion du serveur en contrôleur de domaine

01 Configuration réseau préalable

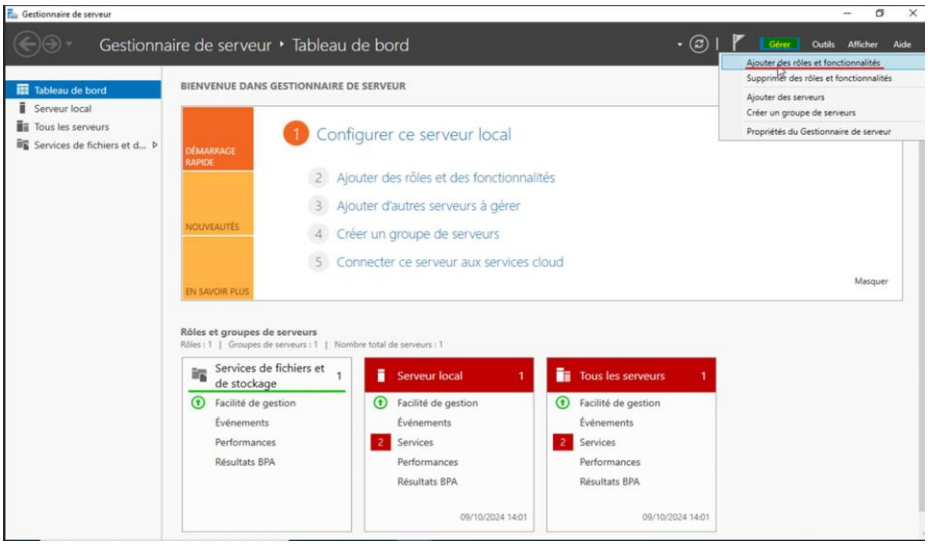
Avant toute installation, l'adresse IP du serveur doit être statique. Le serveur se désignera lui-même comme DNS primaire afin de résoudre le domaine Active Directory.

> ⚠ Sans DNS correctement configuré pointant vers le serveur lui-même, l'Active Directory ne peut pas fonctionner. Cette étape est critique.

ÉTAPE 1 Configurer l'adresse IP statique du serveur



Panneau de configuration → Réseau → Propriétés Ethernet



Propriétés TCP/IPv4 — IP statique 10.2.0.201, DNS = 10.2.0.201

Propriété	Valeur
Adresse IP	10.2.0.201
Masque de sous-réseau	255.255.255.0
Passerelle par défaut	10.2.0.254
DNS préféré	10.2.0.201 (lui-même)
DNS auxiliaire	10.2.0.254

ℹ L'adresse IP du serveur doit être configurée en DNS préféré car l'AD utilise DNS pour localiser le contrôleur de domaine. C'est pourquoi on saisit sa propre IP.

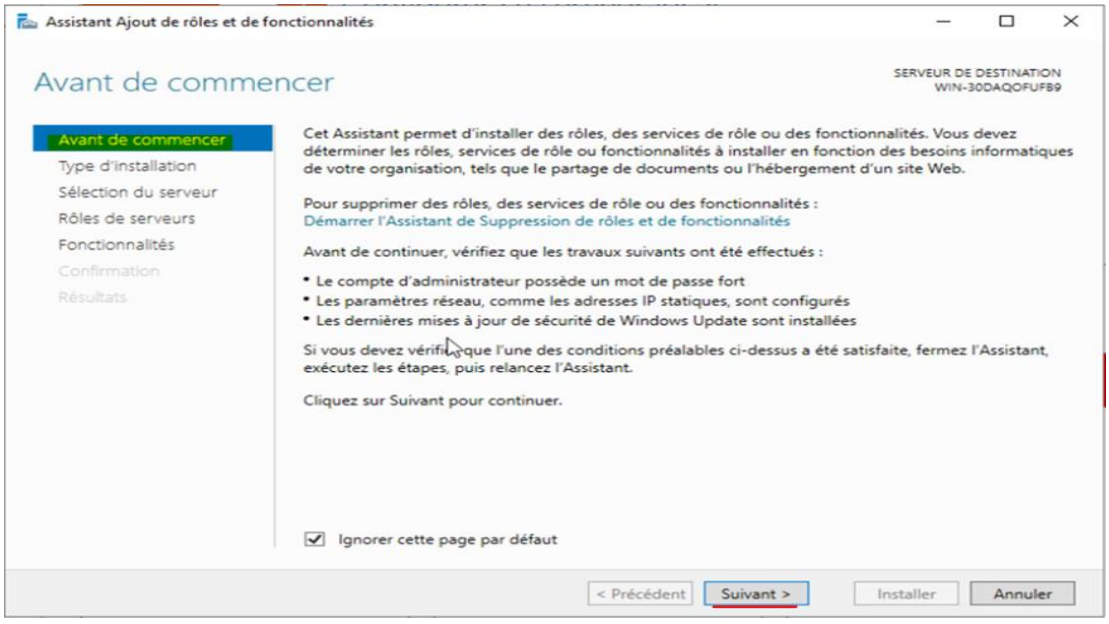
ÉTAPE 2 **Renommer le serveur**

⚙ POWERSHELL
```
# Renommer le serveur et redémarrer
Rename-Computer -NewName 'AD-1' -Restart

# Après redémarrage, vérifier :
hostname    # doit retourner : AD-1
```

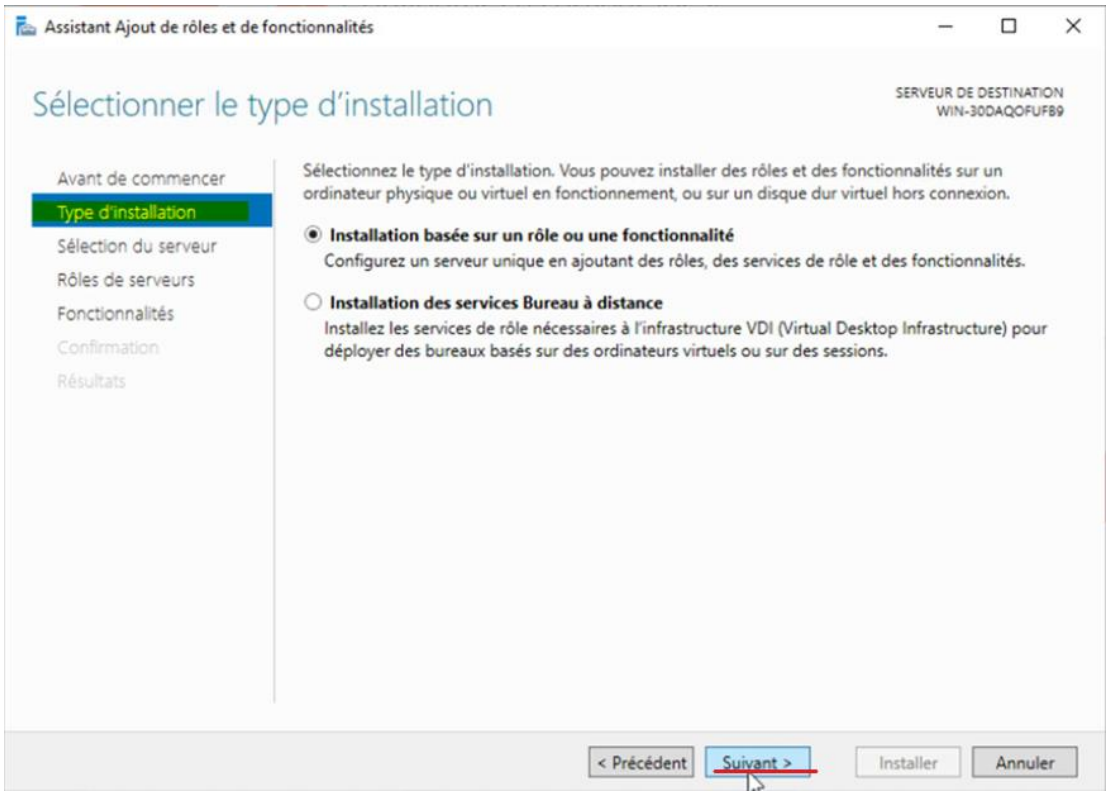
02 Installation du rôle AD DS

L'installation se fait via le Gestionnaire de serveur ou PowerShell. Les deux méthodes sont présentées.

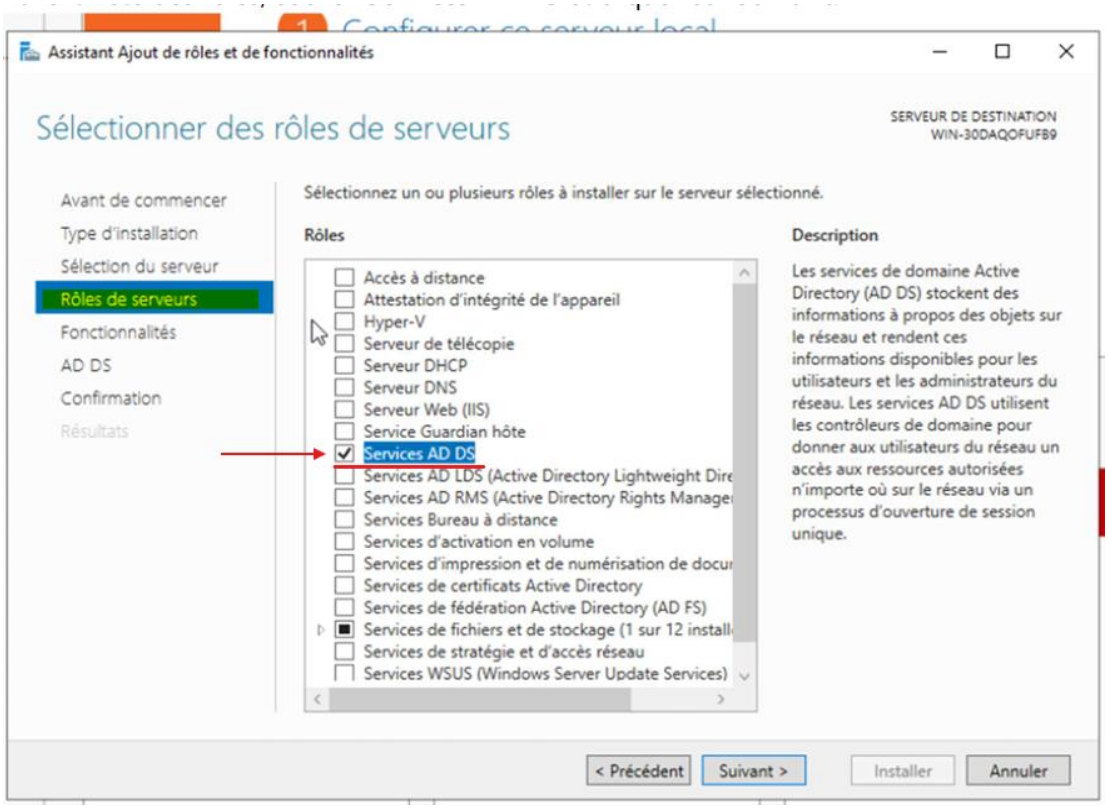
ÉTAPE 3 **Ouvrir le Gestionnaire de serveur et ajouter des rôles**



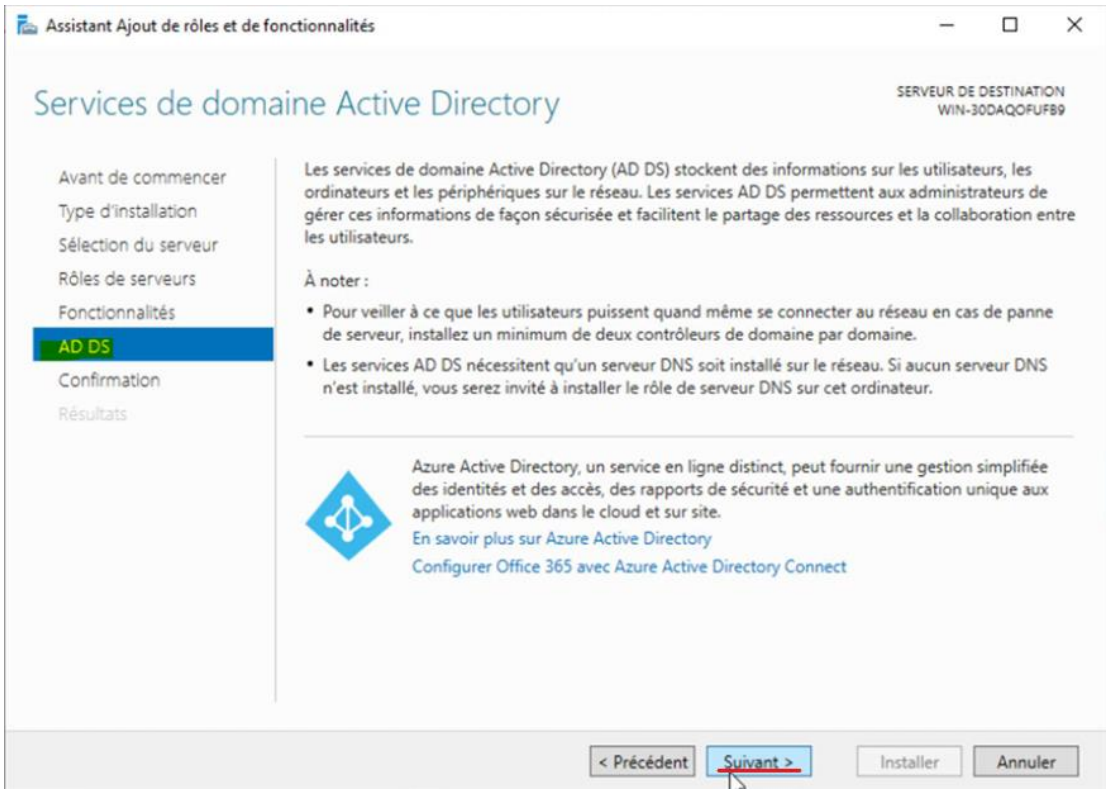
Gestionnaire de serveur → Tableau de bord → Gérer → Ajouter des rôles et fonctionnalités



Assistant Ajout de rôles : Type d'installation → Installation basée sur un rôle ou une fonctionnalité



Sélection des rôles → cocher 'Services AD DS'



Confirmation — Cliquer Installer et attendre la fin

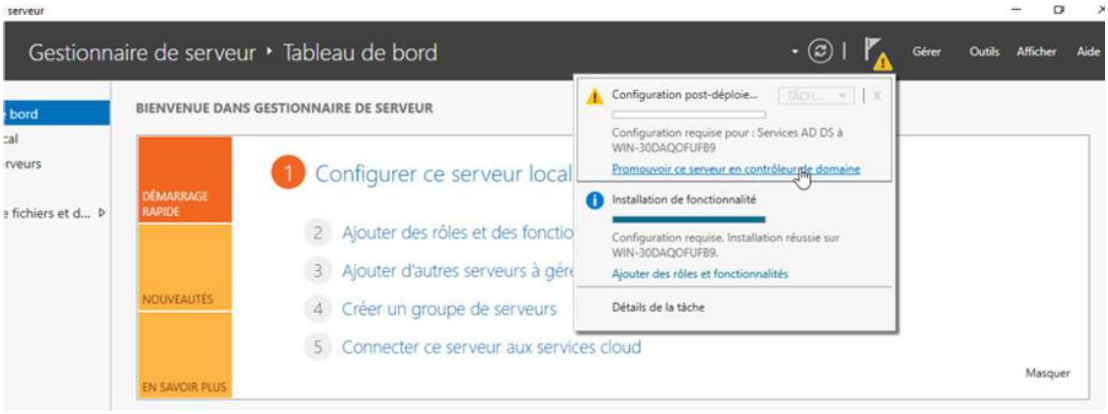
ℹ L'installation prend 2 à 5 minutes. Ne pas redémarrer — la promotion en contrôleur de domaine vient juste après.

⚙ POWERSHELL
```
# Alternative PowerShell (résultat identique)
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
```

03 Promotion en contrôleur de domaine

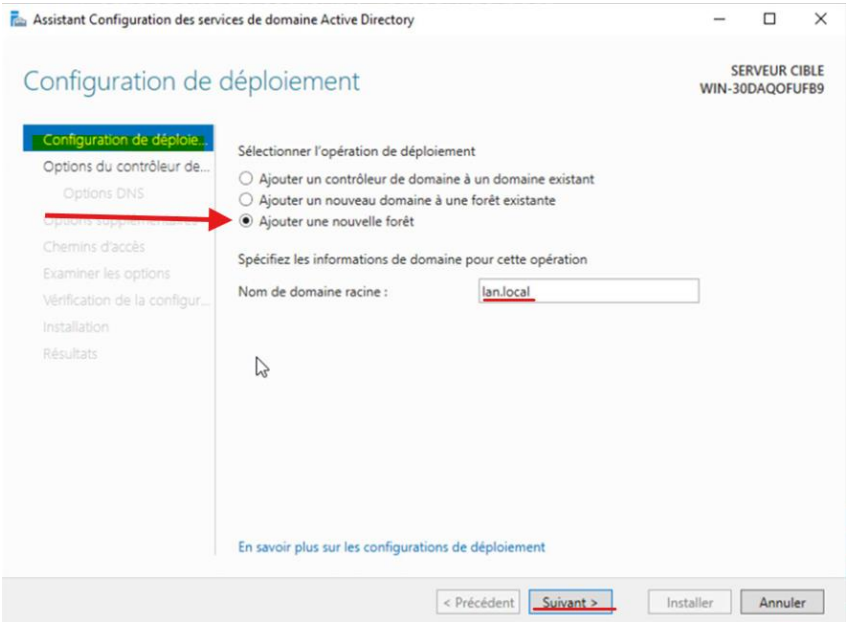
ÉTAPE 4 **Lancer l'assistant de promotion DCPROMO**

Cliquer sur le drapeau d'avertissement → Promouvoir ce serveur en contrôleur de domaine



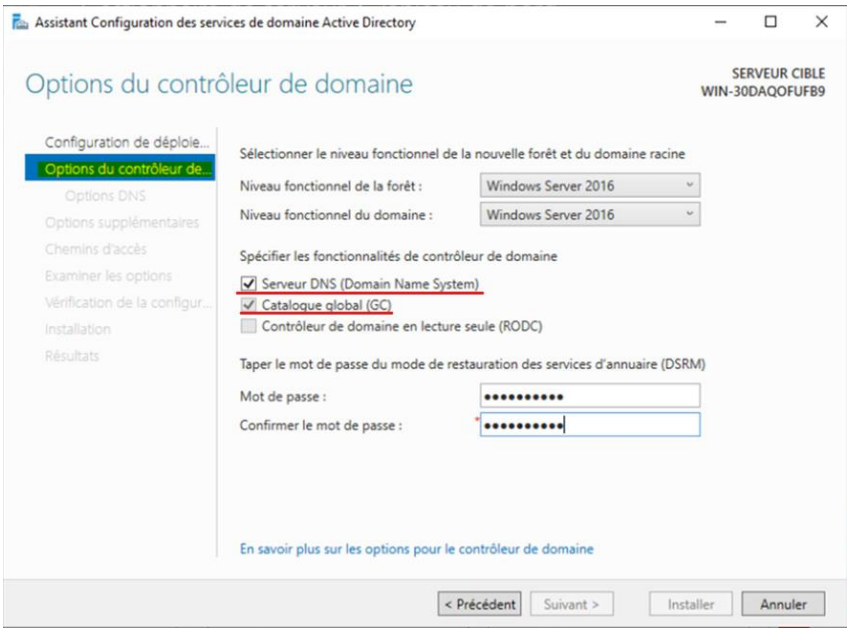
La notification apparaît après l'installation du rôle AD DS

ÉTAPE 5 — Configurer le déploiement — Nouvelle forêt



Configuration de déploiement : Ajouter une nouvelle forêt → qscarpa.lan

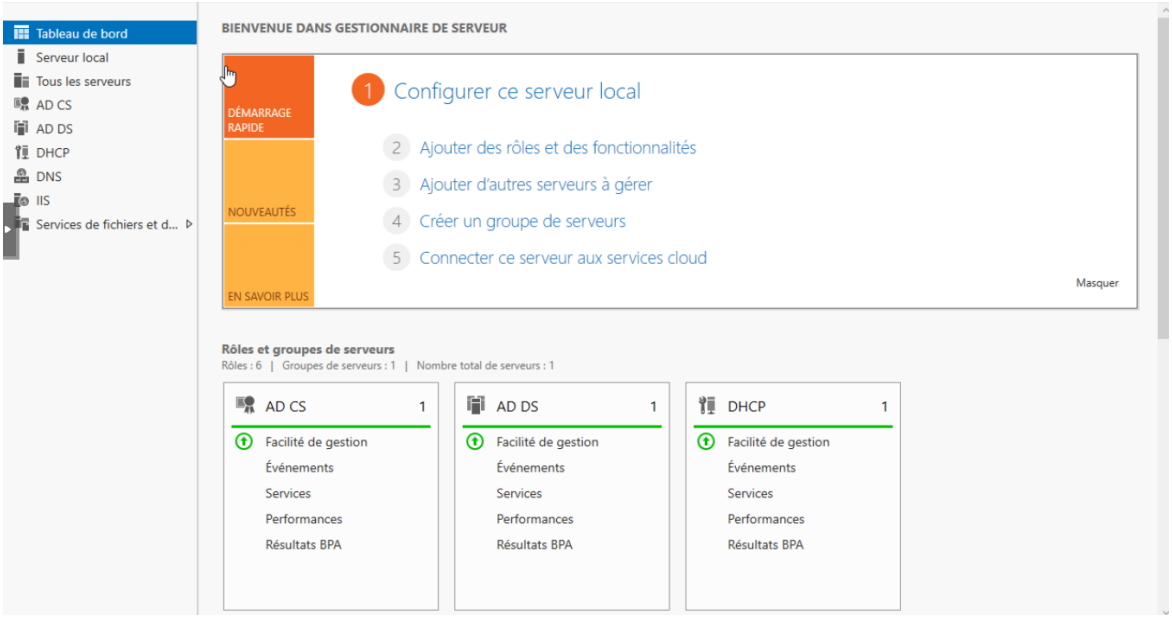
Paramètre DCPROMO	Valeur à saisir
Opération de déploiement	Ajouter une nouvelle forêt
Nom de domaine racine	qscarpa.lan
Niveau fonctionnel forêt	Windows Server 2016
Niveau fonctionnel domaine	Windows Server 2016
Serveur DNS	✓ Coché (installé automatiquement)
Catalogue global (GC)	✓ Coché
Mot de passe DSRM	Mot de passe fort (à conserver)
Nom NetBIOS	QSCARPA (auto-détecté)
Chemins NTDS/SYSVOL	Laisser par défaut



Options du contrôleur de domaine — Niveau fonctionnel + mot de passe DSRM

✓ Cliquer Suivant jusqu'à Installer. Le serveur redémarre automatiquement. Après redémarrage, se connecter avec QSCARPA\Administrateur.

ÉTAPE 6 Vérifier l'installation de l'AD



Gestionnaire de serveur — AD CS, AD DS, DHCP, DNS présents = installation réussie

```powershell
# Vérification complète de l'AD
dcdiag /v

# Vérifier le contrôleur de domaine
Get-ADDomainController -Filter *
```

```
# Vérifier le domaine
Get-ADDomain
```

Debugging — Installation AD DS

Problème	Cause probable	Solution
'Le domaine existe déjà'	Conflit réseau ou AD existant	Vérifier qu'aucun autre serveur AD n'existe sur le réseau avec nslookup
Erreur dcdiag après promotion	DNS mal configuré	Exécuter dcdiag /test:dns et corriger les erreurs
Connexion refusée après redémarrage	Mauvais format de login	Utiliser QSCARPA\Administrateur et non Administrateur seul
Le niveau fonctionnel est grisé	Version OS trop ancienne	Windows Server 2022 supporte jusqu'à WS 2016 en niveau fonctionnel minimum recommandé
Promotion échoue avec erreur DNS	DNS préféré mal configuré	Vérifier que l'IP du serveur est bien en DNS préféré (étape 1)

Structure OU & Utilisateurs

Création de l'arborescence, des groupes et des comptes utilisateurs

04 Créer la structure d'Unités d'Organisation (OU)

L'arborescence OU organise les objets du domaine (utilisateurs, ordinateurs, groupes) de façon logique, généralement par direction ou localisation. Voici la structure utilisée dans ce projet :

```
baptiste.lan
├─ Entreprise_1
│  ├─ Direction-Commerciale
│  │  ├─ Imprimantes
│  │  ├─ Ordinateurs
│  │  └─ Utilisateurs → gr-direction-commerciale
│  ├─ Direction-Financiere
│  │  ├─ Ordinateurs
│  │  └─ Utilisateurs → gr-direction-financiere
│  └─ Direction-Informatique
│  ├─ Ordinateurs
│  └─ Utilisateurs → gr-direction-informatique
```

Structure OU par direction avec groupes de sécurité associés

ℹ Ouvrir la console ADUC : Gestionnaire de serveur → Outils → Utilisateurs et ordinateurs Active Directory

ÉTAPE 7

Créer l'arborescence OU via PowerShell

POWERSHELL

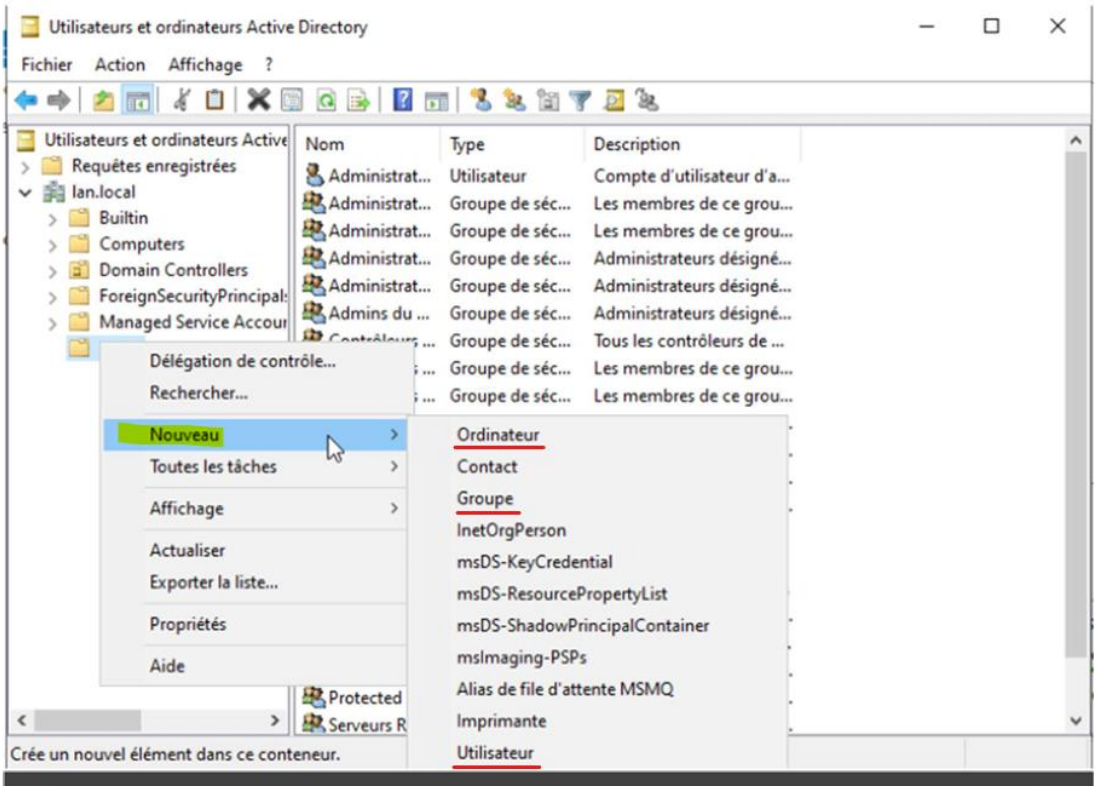
```
# OU racine SOCIETE
New-ADOrganizationalUnit -Name 'SOCIETE' -Path 'DC=qscarpa,DC=lan'

# Sous-OUs de SOCIETE
New-ADOrganizationalUnit -Name 'DSI' -Path 'OU=SOCIETE,DC=qscarpa,DC=lan'
New-ADOrganizationalUnit -Name 'DJ'  -Path 'OU=SOCIETE,DC=qscarpa,DC=lan'
New-ADOrganizationalUnit -Name 'DT'  -Path 'OU=SOCIETE,DC=qscarpa,DC=lan'

# Sous-OUs de DSI
New-ADOrganizationalUnit -Name 'Utilisateurs' -Path 'OU=DSI,OU=SOCIETE,DC=qscarpa,DC=lan'
New-ADOrganizationalUnit -Name 'Ordinateurs'  -Path 'OU=DSI,OU=SOCIETE,DC=qscarpa,DC=lan'
```

05 Créer les groupes de sécurité

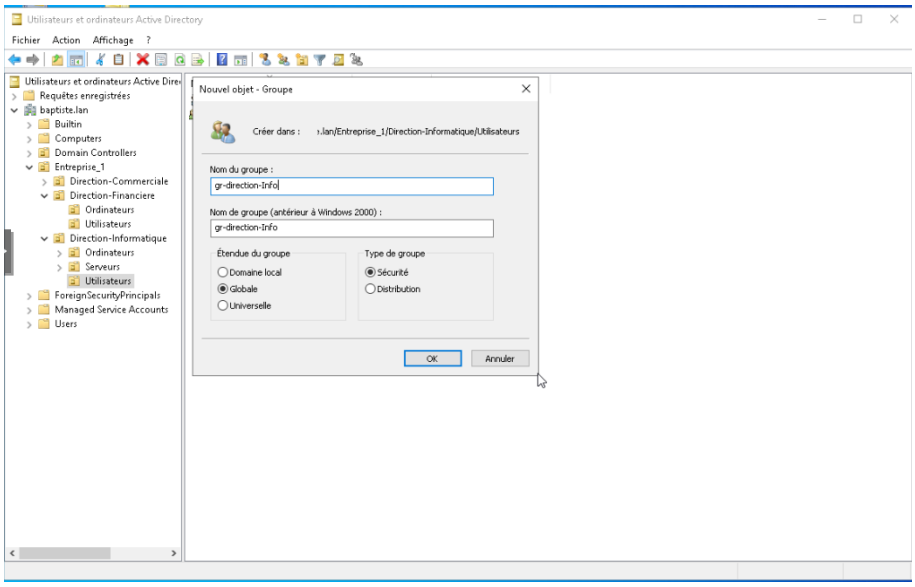
Un groupe de sécurité regroupe des utilisateurs et permet d'appliquer des permissions et des GPO en bloc plutôt qu'individuellement.

ÉTAPE 8

Créer le groupe gr-DSI via la console ADUC



ADUC → clic droit dans l'OU → Nouveau → Groupe

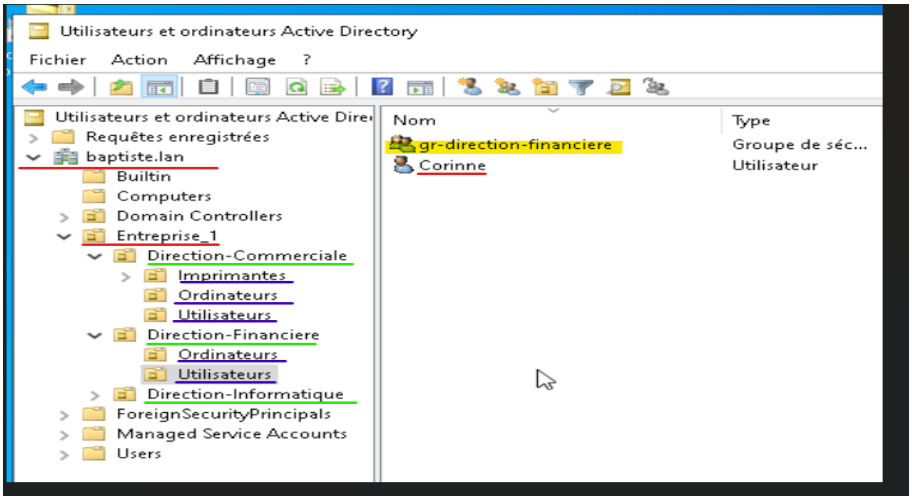


Formulaire de création du groupe : nom, étendue Globale, type Sécurité

```powershell
# Créer le groupe gr-DSI
New-ADGroup -Name 'gr-DSI' \
  -GroupScope Global \
  -GroupCategory Security \
  -Path 'OU=Utilisateurs,OU=DSI,OU=SOCIETE,DC=qscarpa,DC=lan' \
  -Description 'Groupe de sécurité — Direction des Systèmes d Information'

# Vérifier
Get-ADGroup -Identity 'gr-DSI'
```

06 Créer les utilisateurs

ÉTAPE 9 **Créer l'utilisateur via ADUC**

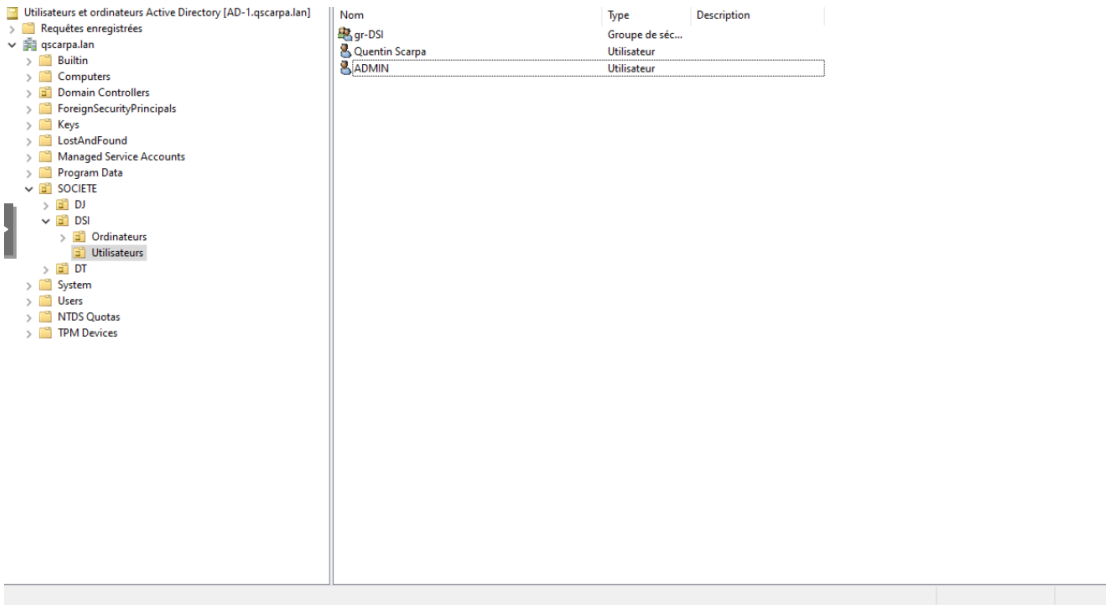


ADUC → Nouveau → Utilisateur : prénom, nom, identifiant de session

ÉTAPE 10 Créer les utilisateurs via PowerShell

⚙ POWERSHELL

```
# Utilisateur Quentin Scarpa
New-ADUser -Name 'Quentin Scarpa' \
  -GivenName 'Quentin' -Surname 'Scarpa' \
  -SamAccountName 'qscarpa' \
  -UserPrincipalName 'qscarpa@qscarpa.lan' \
  -Path 'OU=Utilisateurs,OU=DSI,OU=SOCIETE,DC=qscarpa,DC=lan' \
  -AccountPassword (ConvertTo-SecureString 'P@ssw0rd123!' -AsPlainText -Force) \
  -ChangePasswordAtLogon $true \
  -Enabled $true

# Utilisateur ADMIN
New-ADUser -Name 'ADMIN' \
  -SamAccountName 'ADMIN' \
  -UserPrincipalName 'ADMIN@qscarpa.lan' \
  -Path 'OU=Utilisateurs,OU=DSI,OU=SOCIETE,DC=qscarpa,DC=lan' \
  -AccountPassword (ConvertTo-SecureString 'P@ssw0rd123!' -AsPlainText -Force) \
  -Enabled $true

# Ajouter les deux utilisateurs au groupe gr-DSI
Add-ADGroupMember -Identity 'gr-DSI' -Members 'qscarpa','ADMIN'

# Ajouter ADMIN aux Admins du domaine
Add-ADGroupMember -Identity 'Domain Admins' -Members 'ADMIN'
```

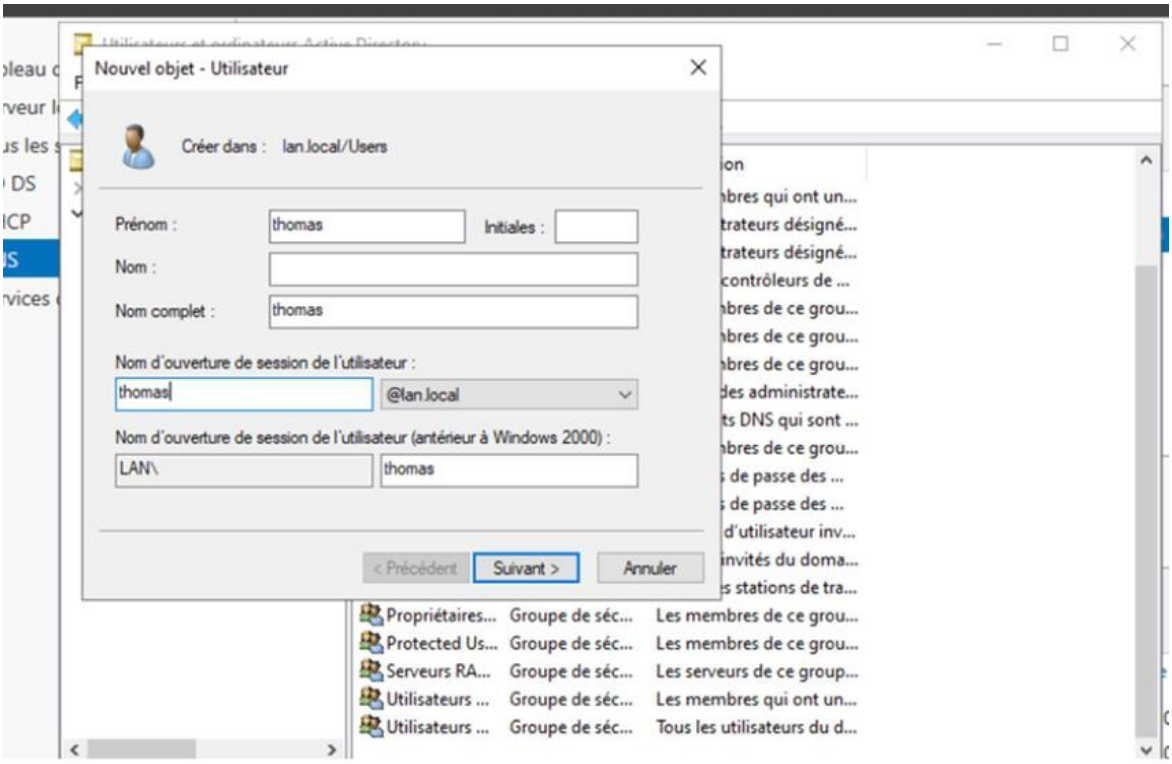


ADUC — Arborescence finale : gr-DSI, Quentin Scarpa, ADMIN dans OU=DSI

ÉTAPE 11 Vérifier les utilisateurs et groupes

⚙ POWERSHELL

```
# Lister tous les utilisateurs du domaine
Get-ADUser -Filter * | Select Name, SamAccountName, Enabled

# Vérifier les membres de gr-DSI
Get-ADGroupMember -Identity 'gr-DSI'

# Vérifier un utilisateur spécifique
Get-ADUser -Identity 'qscarpa' -Properties *
```



Console ADUC — Structure complète du domaine avec groupes et utilisateurs

Debugging — Utilisateurs & Groupes

Problème	Cause probable	Solution
Erreur de complexité mot de passe	Politique de complexité activée	Utiliser min. 8 car., 1 maj., 1 chiffre, 1 symbole ou désactiver temporairement la politique
L'utilisateur ne peut pas se connecter	Compte désactivé ou UPN incorrect	Get-ADUser qscarpa | Select Enabled — activer avec Enable-ADAccount -Identity qscarpa
OU introuvable lors de la création	Chemin DN incorrect	Vérifier : Get-ADOrganizationalUnit -Filter * | Select DistinguishedName
L'objet n'apparaît pas dans ADUC	Filtre de vue actif	Affichage → Fonctionnalités avancées dans ADUC
Erreur 'Accès refusé' à la création	Droits insuffisants	Se connecter en tant que QSCARPA\Administrateur ou Domain Admin

GPO — Stratégies de groupe

Barre des tâches · Autorité de certification · Signature SMB

07 GPO — Masquer la barre des tâches

ℹ Ouvrir la console GPMC : Gestionnaire de serveur → Outils → Gestion des stratégies de groupe

ÉTAPE 12 Créer une nouvelle GPO sur l'OU DSI

Dans la console GPMC : clic droit sur OU=DSI → Créer un objet GPO dans ce domaine, et le lier ici.
Nommer la GPO : GPO-MasquerBarreDesTaches

ÉTAPE 13 Configurer la GPO via l'éditeur

Clic droit sur la GPO → Modifier. Naviguer vers :

- Configuration utilisateur → Modèles d'administration → Menu Démarrer et Barre des tâches

Paramètre	Chemin	Valeur
Masquer la barre des tâches	Menu Démarrer et Barre des tâches	Activé
Verrouiller la barre des tâches	Menu Démarrer et Barre des tâches	Activé
Masquer le secteur de notification	Menu Démarrer et Barre des tâches	Activé

ÉTAPE 14 Méthode alternative — Registre (plus fiable sous Windows 11)

Configuration utilisateur → Préférences → Paramètres Windows → Registre → Nouveau :

⚙ REGISTRE GPO

```
Ruche    : HKEY_CURRENT_USER
Chemin   : SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced
Valeur   : TaskbarAl
Type     : REG_DWORD
Données  : 0   (barre à gauche / masquée)
```

ÉTAPE 15 Appliquer et vérifier la GPO

⚙ POWERSHELL

```
# Sur le client — forcer l'application
gpupdate /force


# Vérifier les GPO appliquées
```

```
gpresult /r

# Rapport HTML détaillé
gpresult /h C:\gpo_rapport.html

# Si la barre ne disparaît pas, relancer l'Explorateur
taskkill /f /im explorer.exe && start explorer.exe
```

08 GPO — Autorité de Certification (AD CS)

L'Autorité de Certification (AC) permet d'émettre des certificats numériques pour les utilisateurs et ordinateurs du domaine, activant LDAPS, l'auto-enrôlement et l'authentification par certificat.

ÉTAPE 16 Installer le rôle AD CS

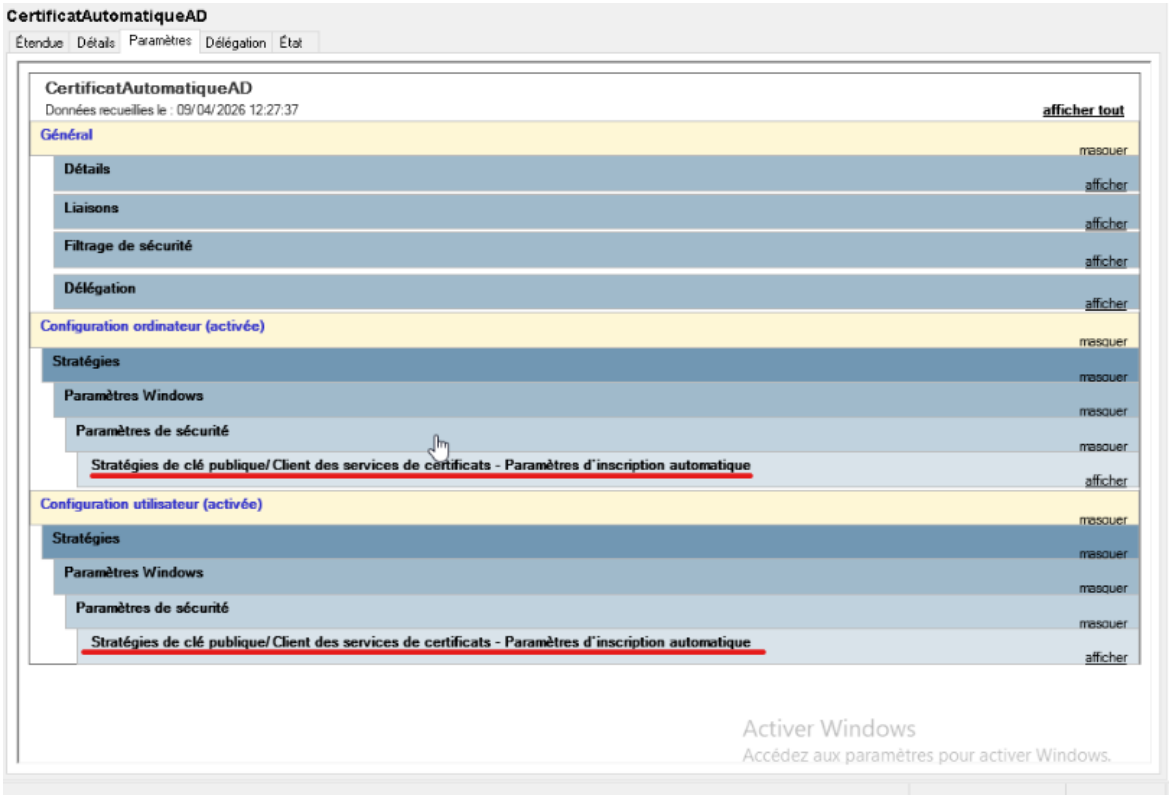
⚙ POWERSHELL

```
# Installer l'Autorité de Certification
Install-WindowsFeature -Name AD-Certificate -IncludeManagementTools

# Configurer l'AC racine d'entreprise
Install-AdcsCertificationAuthority \
  -CAType EnterpriseRootCa \
  -CACommonName 'QSCARPA-CA' \
  -Force
```

ÉTAPE 17 Créer la GPO d'auto-enrôlement des certificats

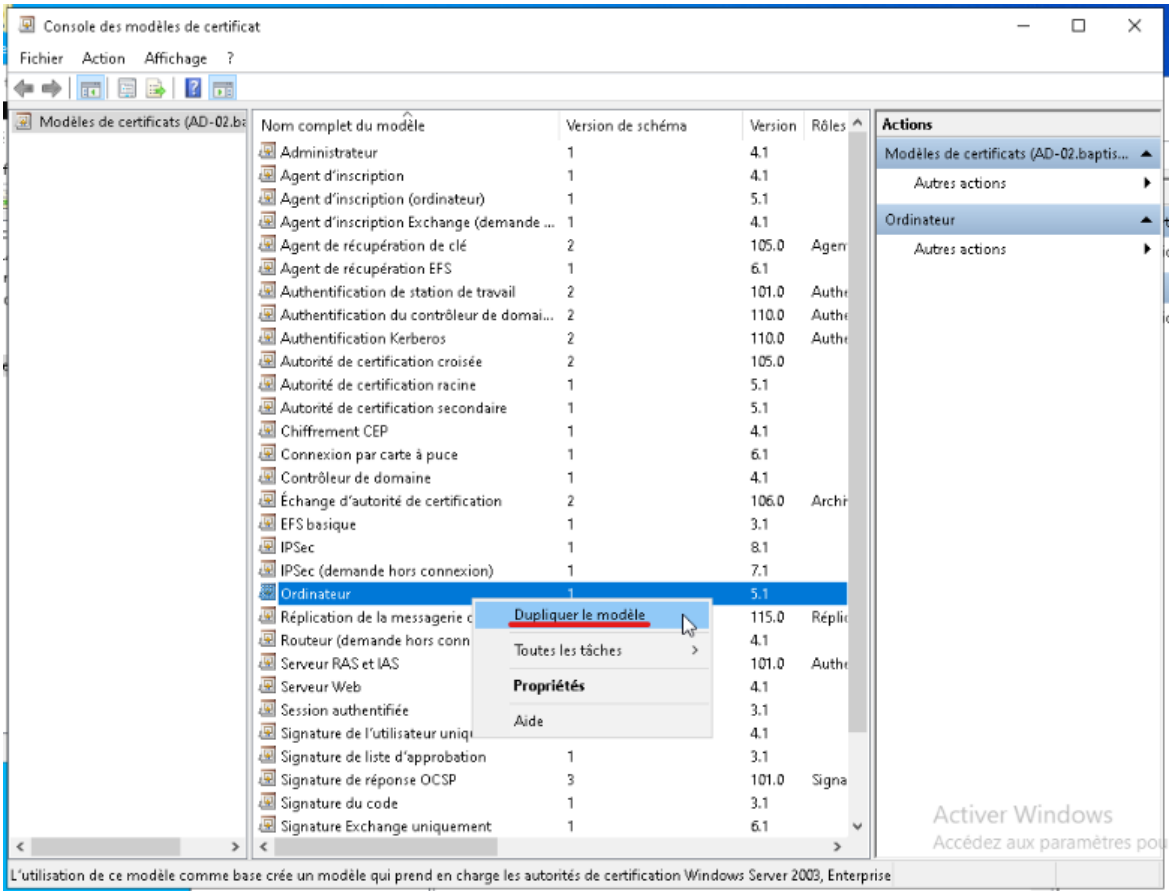
Dans l'éditeur GPO, naviguer vers :

- Configuration ordinateur → Stratégies → Paramètres Windows → Paramètres de sécurité → Stratégies de clé publique
- Client d'inscription de certificat — inscription automatique → Activé
- Cocher : Renouveler les certificats arrivés à expiration

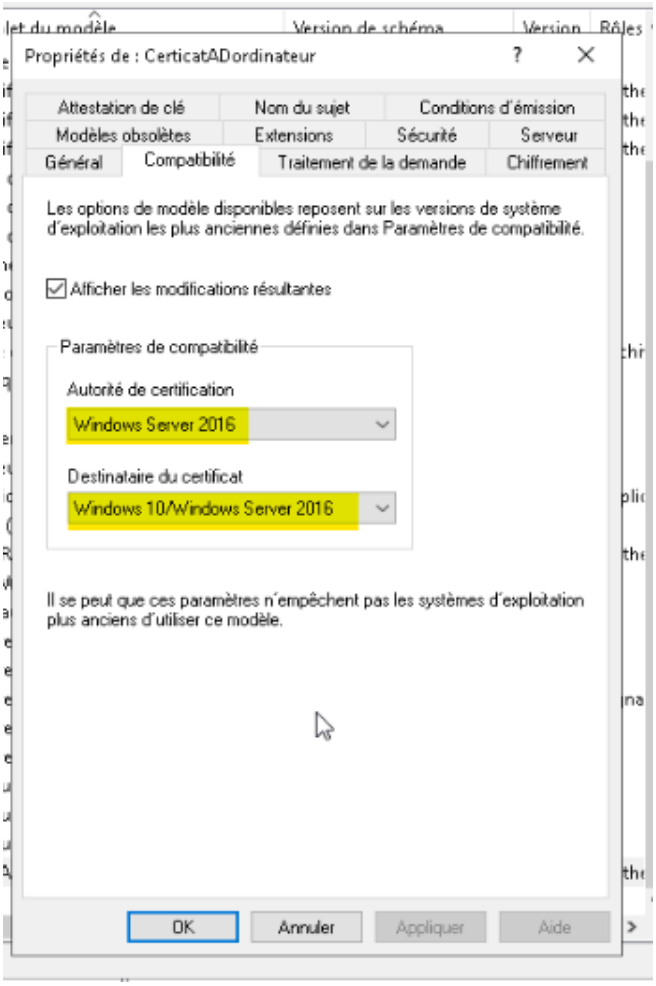


Éditeur GPO — GPO CertificatAutomatiqueAD : auto-enrôlement ordinateur et utilisateur activés

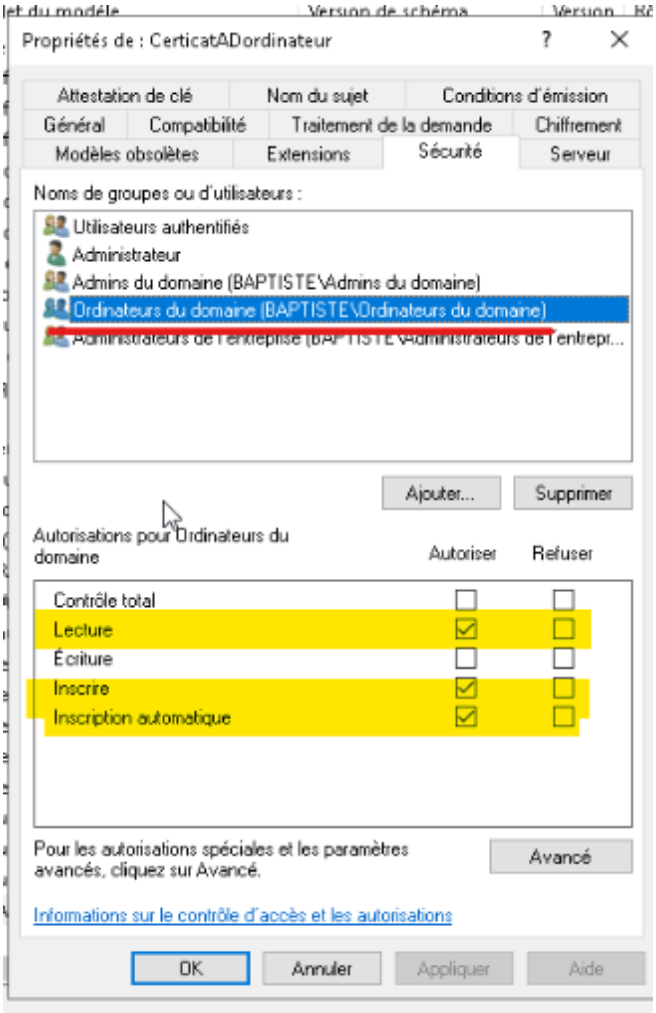
ÉTAPE 18 Dupliquer et configurer le modèle de certificat Ordinateur



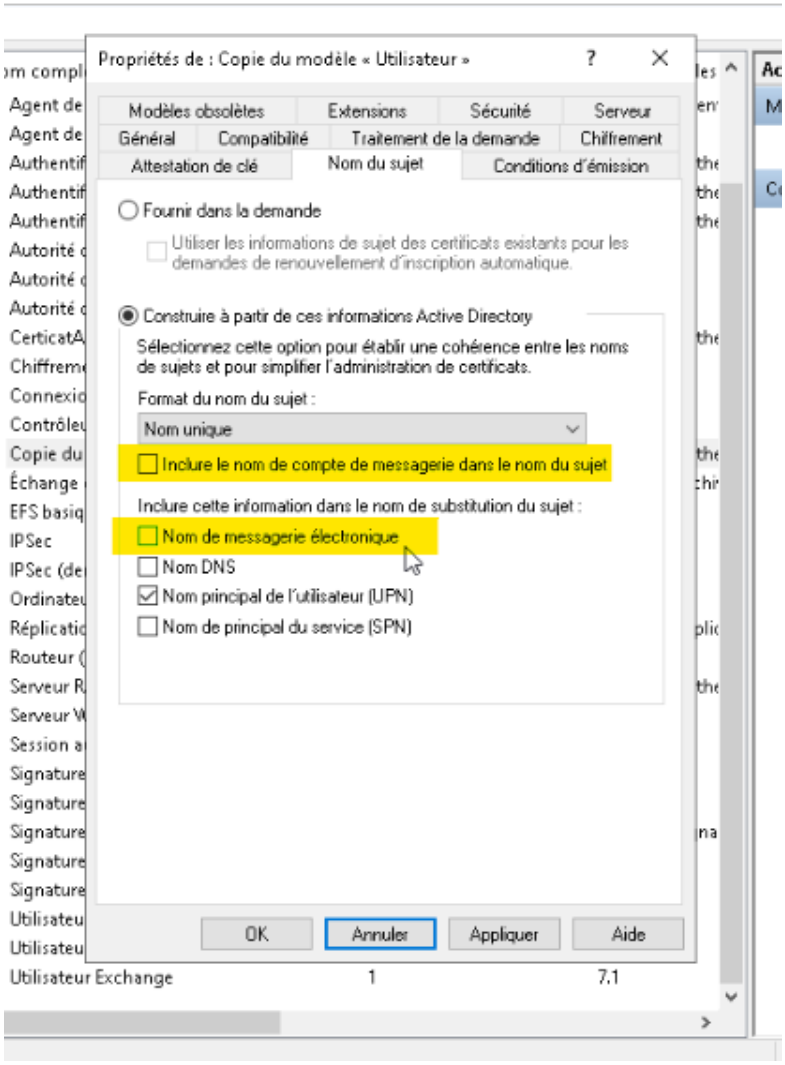
Console des modèles de certificat — Dupliquer le modèle 'Ordinateur'



Compatibilité : AC = Windows Server 2016, Destinataire = Windows 10/Server 2016

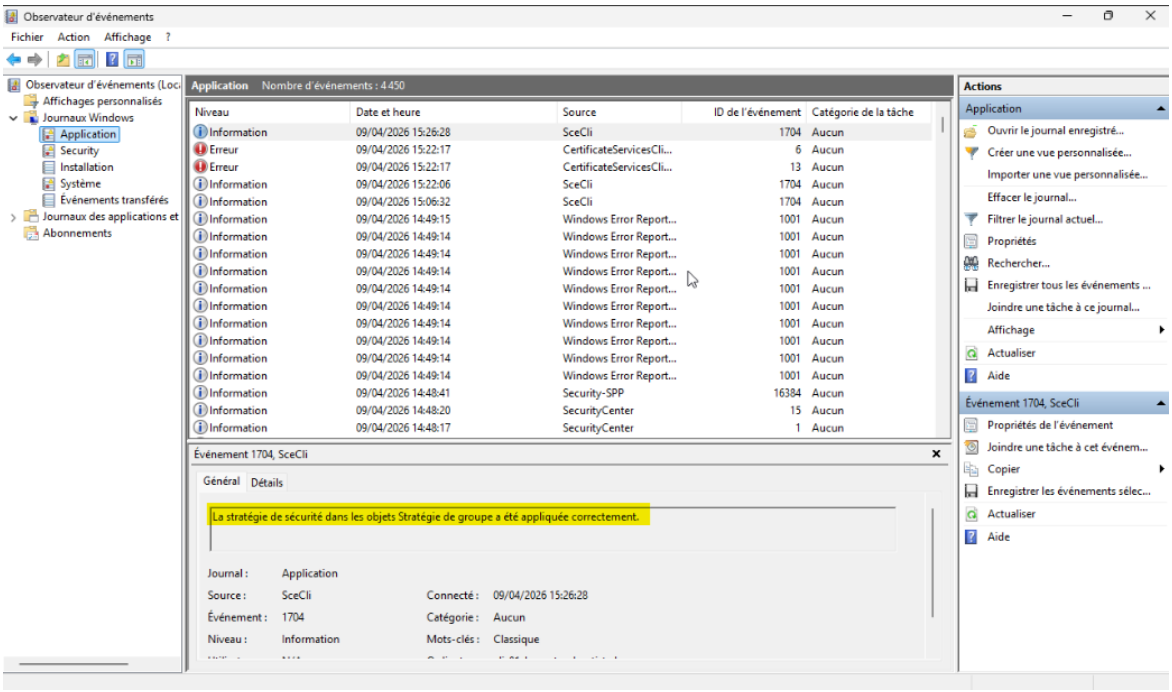


Sécurité : Ordinateurs du domaine → Lecture + Inscrire + Inscription automatique

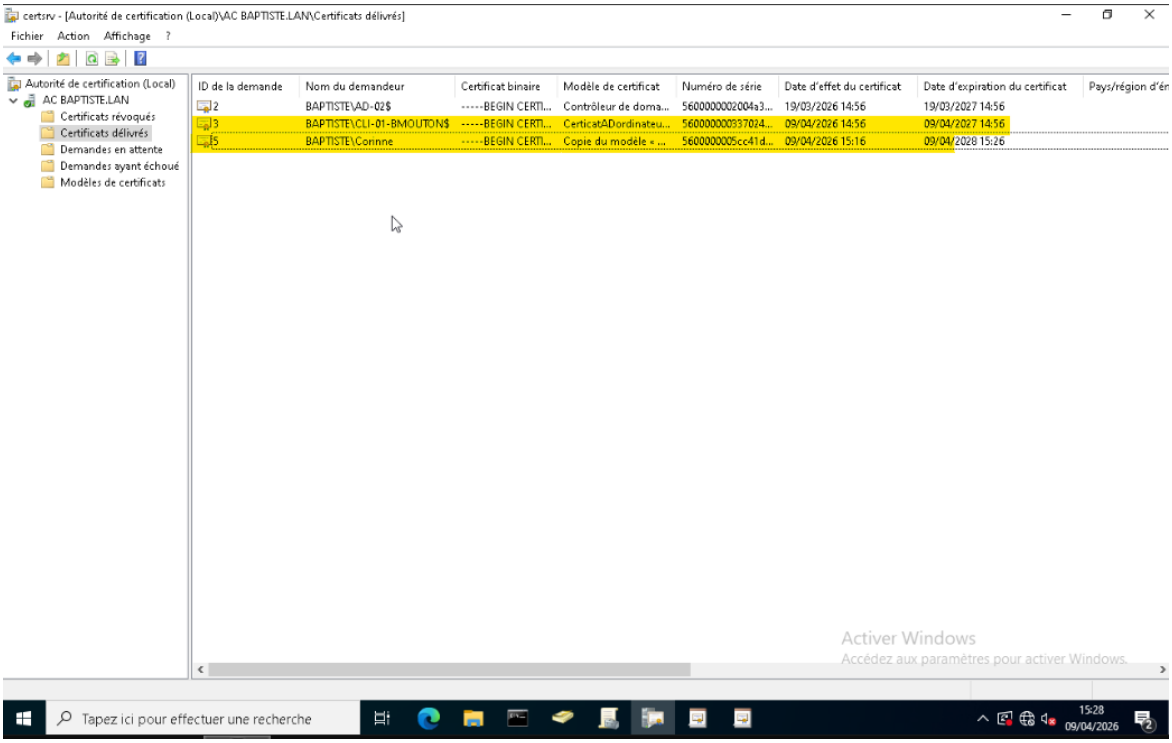


Nom du sujet : Construire à partir de l'AD, Format = Nom unique, UPN coché

ÉTAPE 19 Vérifier les certificats émis



Observateur d'événements — Événement 1704 SceCli : stratégie de sécurité appliquée



certsrv — Certificats délivrés : contrôleur de domaine, CerticatADordinateur, Corinne

⚙ POWERSHELL

```
# Vérifier les certificats émis depuis l'AC
certutil -view -out 'RequestID,CommonName,NotAfter' CSV

# Forcer l'enrôlement du certificat sur le client
certutil -pulse

# Voir les certificats sur le client
```

```
certmgr.msc
```

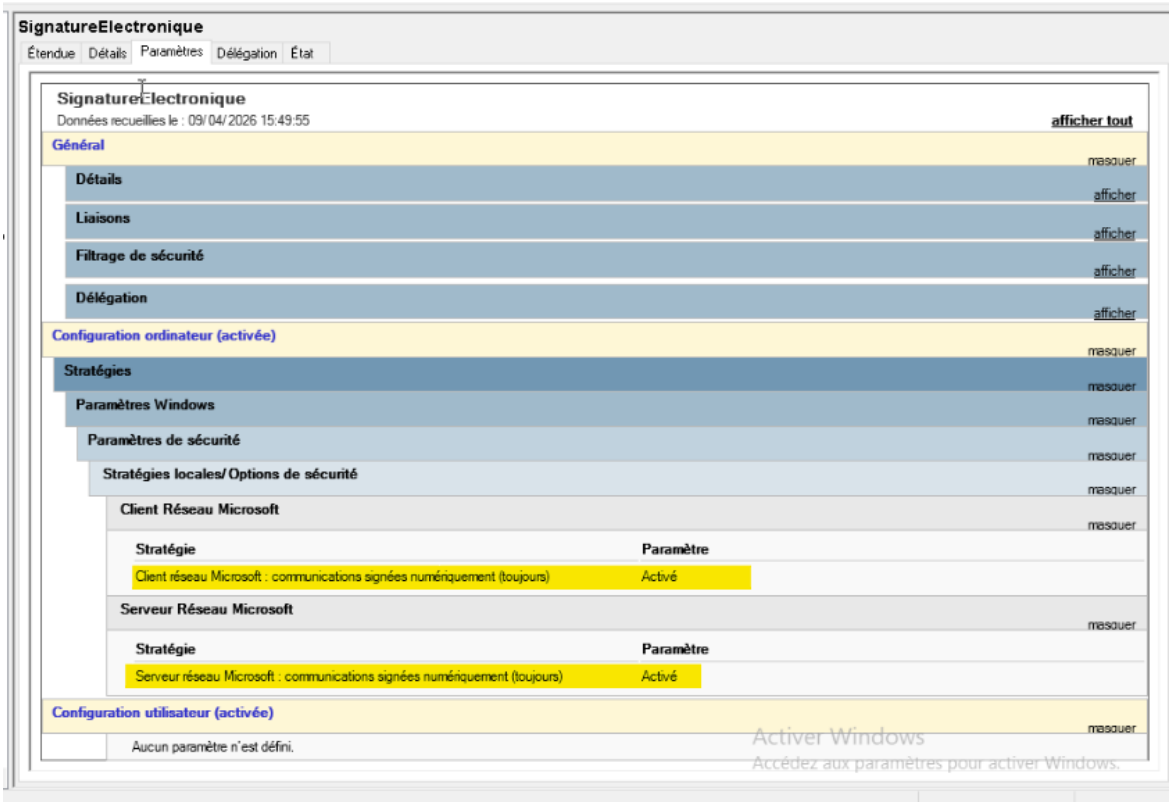
09 GPO — Signature SMB (Sécurité réseau)

La GPO SignatureElectronique force la signature numérique des communications SMB, protégeant contre les attaques de type man-in-the-middle sur les partages réseau.

ÉTAPE 20 Configurer la GPO de signature SMB

Dans l'éditeur GPO, naviguer vers :

- Configuration ordinateur → Stratégies → Paramètres Windows → Paramètres de sécurité → Stratégies locales → Options de sécurité



GPO SignatureElectronique — Client et Serveur réseau Microsoft : communications signées numériquement (toujours) = Activé

Paramètre SMB	Valeur
Client réseau Microsoft : communications signées numériquement (toujours)	Activé
Serveur réseau Microsoft : communications signées numériquement (toujours)	Activé

⚠ La signature SMB obligatoire peut casser la compatibilité avec d'anciens partages réseau (NAS, imprimantes anciennes). Tester en environnement de test avant déploiement en production.

Debugging — GPO

Problème	Cause probable	Solution
La GPO ne s'applique pas	Client dans mauvaise OU	Déplacer l'objet dans OU=DSI puis gpupdate /force
gpresult ne montre pas la GPO	GPO non liée ou état désactivé	Vérifier le lien dans GPMC et l'état 'Appliqué'
Paramètre Win 11 absent	ADMX Windows 11 manquants	Copier les ADMX Win 11 dans C:\Windows\PolicyDefinitions\
Barre des tâches revient au redémarrage	Préférence registre non persistante	Utiliser la méthode Préférences Registre (Étape 14)
Erreur auto-enrôlement certificat	Modèle non publié dans l'AC	Dans certsrv → Modèles de certificats → Nouveau → Publier le modèle
Événement ID 13 dans les logs	AC inaccessible depuis le client	Vérifier que le port TCP 135 et les ports RPC sont ouverts
SMB signature casse les partages	Serveur distant ne supporte pas SMB signing	Désactiver temporairement 'toujours' → mettre 'si le serveur l'accepte'

Récapitulatif — Checklist

Ordre d'exécution et vérifications

#	Étape	Commande de vérification	Résultat attendu
1	IP statique 10.2.0.201 configurée	ipconfig /all	IP = 10.2.0.201, DNS = 10.2.0.201
2	Serveur renommé AD-1	hostname	AD-1
3	Rôle AD DS installé	Get-WindowsFeature AD-Domain-Services	Installed = True
4	Promotion contrôleur de domaine qscarpa.lan	Get-ADDomain	Name = qscarpa
5	DNS opérationnel	dcdiag /test:dns	Aucune erreur
6	Structure OU créée	Get-ADOrganizationalUnit -Filter *	OUs SOCIETE/DSI/DJ/DT présentes
7	Groupe gr-DSI créé	Get-ADGroup gr-DSI	Groupe trouvé
8	Utilisateurs qscarpa et ADMIN créés	Get-ADUser -Filter *	Les deux comptes présents et activés
9	Membres dans gr-DSI	Get-ADGroupMember gr-DSI	qscarpa et ADMIN listés
10	GPO barre des tâches créée et liée	gpresult /r (sur client)	GPO-MasquerBarreDesTaches appliquée
11	AD CS installé	Get-WindowsFeature AD-Certificate	Installed = True
12	GPO auto-enrôlement certificats	certmgr.msc (sur client)	Certificat Ordinateur présent
13	GPO signature SMB active	gpresult /r	SignatureElectronique appliquée

⚠ Ordre impératif : IP statique → Renommage → AD DS → Promotion → OU → Groupes → Utilisateurs → GPO. Ne jamais configurer les GPO avant que l'AD et les OU soient en place.