Contrôleur de domaine Active Directory sous Windows Server 2025

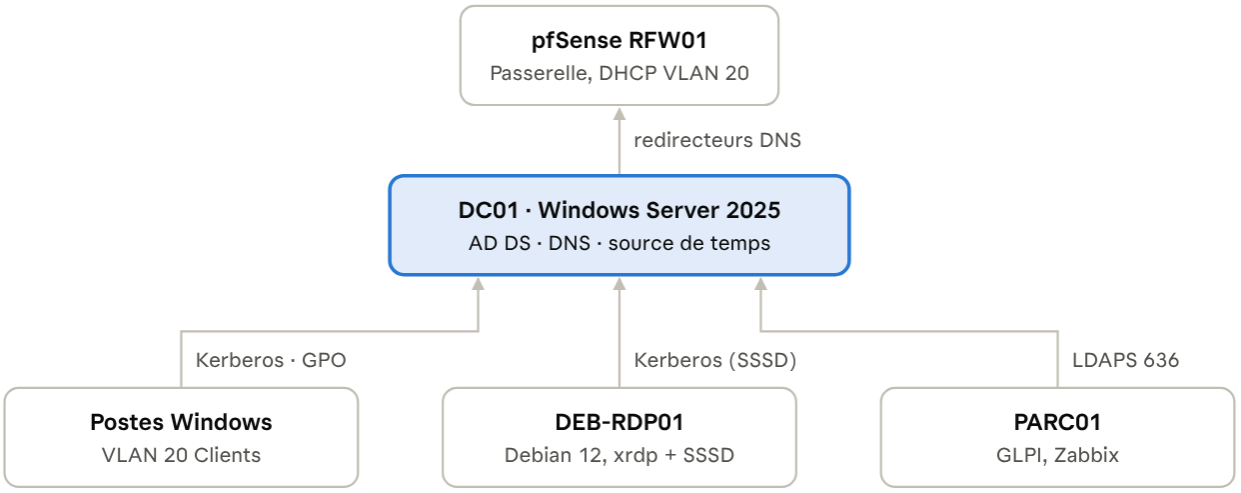
Nov 27, 2026 · @Serge Martins

Objectif et architecture

Ce guide installe le premier contrôleur de domaine **DC01** d'une nouvelle forêt `martinscie.lan` sous Windows Server 2025. DC01 porte aussi le DNS intégré à l'AD et sert de source de temps au domaine. Les serveurs Linux (xrdp, GLPI) et les postes Windows s'y authentifient ensuite.

Valeurs utilisées (à adapter) :

Élément	Valeur
Nom du serveur	`DC01`
Adresse IP	`192.168.10.10/24` (VLAN 10 Serveurs)
Passerelle	`192.168.10.254` (pfSense RFW01)
Domaine DNS / NetBIOS	`martinscie.lan` / `MARTINSCIE`
Niveau fonctionnel	Windows Server 2025 (forêt et domaine)
DNS redirecteurs	`1.1.1.1`, `9.9.9.9` (ou la passerelle)
Édition	Windows Server 2025 Standard, avec Expérience de bureau



Place de DC01 dans l'infrastructure martinscie.lan

Les postes Windows et les serveurs Linux s'authentifient en Kerberos auprès de DC01 ; les applications comme GLPI l'interrogent en LDAPS.

1. Prérequis

Un contrôleur de domaine doit avoir un nom définitif, une IP fixe et être à jour **avant** la promotion : le renommer après coup est délicat.

1.1 Machine virtuelle (lab) : 2 vCPU, 4 Go de RAM, disque de 60 Go, carte réseau dans le VLAN 10. Installer Windows Server 2025 Standard « Expérience de bureau », puis les outils d'intégration de l'hyperviseur.

1.2 Nom et adresse IP (PowerShell en administrateur) :

```
# Repérer le nom de la carte réseau
Get-NetAdapter

# IP fixe, passerelle, DNS temporaire = lui-même
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.10.10 -
PrefixLength 24 -DefaultGateway 192.168.10.254
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses
127.0.0.1

# Désactiver IPv6 n'est PAS recommandé sur un DC : le laisser actif

# Renommer puis redémarrer
Rename-Computer -NewName DC01 -Restart
```

1.3 Heure et mises à jour

- Fuseau horaire : `Set-TimeZone -Id "Romance Standard Time"` (Paris).
- Installer toutes les mises à jour cumulatives (Paramètres > Windows Update), redémarrer, recommencer jusqu'à ce qu'il n'y en ait plus.

1.4 Compte Administrateur local : définir un mot de passe fort. Il deviendra le compte `MARTINSCIE\Administrateur` du domaine.

2. Installation du rôle AD DS

Par l'interface : Gestionnaire de serveur > Gérer > Ajouter des rôles et fonctionnalités > Installation basée sur un rôle > DC01 > cocher **Services AD DS** (accepter l'ajout des outils de gestion) > Installer. Le DNS sera ajouté à l'étape suivante.

En PowerShell (équivalent) :

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
```

Le rôle est installé mais le serveur n'est pas encore contrôleur de domaine : un drapeau jaune apparaît dans le Gestionnaire de serveur.

3. Promotion en contrôleur de domaine

Par l'interface : drapeau jaune > **Promouvoir ce serveur en contrôleur de domaine**.

1. Configuration de déploiement : **Ajouter une nouvelle forêt**, domaine racine `martinscie.lan`.
2. Options : niveaux fonctionnels **Windows Server 2025** ; cocher Serveur DNS et Catalogue global ; saisir le mot de passe DSRM (mode de restauration des services d'annuaire) et le conserver dans un coffre.
3. Options DNS : ignorer l'avertissement sur la délégation (zone `.lan` locale).
4. Nom NetBIOS : `MARTINSCIE`.
5. Chemins : laisser `C:\Windows\NTDS` et `C:\Windows\SYSVOL`.
6. Vérification de la configuration requise : les avertissements sont normaux, aucune erreur ne doit apparaître. Installer : le serveur redémarre.

En PowerShell (équivalent) :

```
# Tester d'abord (ne modifie rien)
Test-ADDSForestInstallation -DomainName "martinscie.lan" -DomainNetbiosName
"MARTINSCIE" `
  -DomainMode 10 -ForestMode 10 -InstallDns

# Promotion : 10 = niveau fonctionnel Windows Server 2025
Install-ADDSForest -DomainName "martinscie.lan" -DomainNetbiosName
"MARTINSCIE" `
  -DomainMode 10 -ForestMode 10 -InstallDns `
  -DatabasePath "C:\Windows\NTDS" -LogPath "C:\Windows\NTDS" -SysvolPath
"C:\Windows\SYSVOL" `
  -SafeModeAdministratorPassword (Read-Host -AsSecureString "Mot de passe
DSRM") -Force
```

Après redémarrage, se connecter avec `MARTINSCIE\Administrateur`.

> Le niveau Windows Server 2025 n'accepte que des contrôleurs de domaine Windows Server 2025. Pour ajouter plus tard un DC plus ancien, choisir le niveau Windows Server 2016 (`-DomainMode WinThreshold -ForestMode WinThreshold`).

4. Configuration après la promotion

4.1 DNS : redirecteurs et zone inverse

```
# Résolution Internet via des redirecteurs
Set-DnsServerForwarder -IPAddress 1.1.1.1, 9.9.9.9

# Zone de recherche inversée pour les deux VLAN, répliquée dans l'AD
Add-DnsServerPrimaryZone -NetworkId "192.168.10.0/24" -ReplicationScope
Forest
Add-DnsServerPrimaryZone -NetworkId "192.168.20.0/24" -ReplicationScope
Forest

# Enregistrement PTR du DC
Add-DnsServerResourceRecordPtr -ZoneName "10.168.192.in-addr.arpa" -Name "10"
-PTRDomainName "dc01.martinscie.lan"
```

Sur pfSense, le DHCP du VLAN 20 doit distribuer `192.168.10.10` comme serveur DNS et `martinscie.lan` comme domaine.

4.2 Source de temps du domaine

DC01 détient le rôle émulateur PDC : il donne l'heure à tout le domaine (indispensable pour Kerberos).

```
w32tm /config /manualpeerlist:"0.fr.pool.ntp.org 1.fr.pool.ntp.org"
/syncfromflags:manual /reliable:yes /update
Restart-Service w32time
w32tm /query /status
```

4.3 Corbeille Active Directory (récupérer un objet supprimé par erreur) :

```
Enable-ADOptionalFeature "Recycle Bin Feature" -Scope
ForestOrConfigurationSet -Target "martinscie.lan" -Confirm:$false
```

4.4 Unités d'organisation, groupes et comptes

```
$base = "DC=martinscie,DC=lan"
New-ADOrganizationalUnit -Name "MARTINSCIE" -Path $base
"Utilisateurs","Groupes","Ordinateurs","Serveurs","Serveurs Linux" | ForEach-
Object {
  New-ADOrganizationalUnit -Name $_ -Path "OU=MARTINSCIE,$base"
}

New-ADGroup -Name "GG_RDP_Linux" -GroupScope Global -GroupCategory Security -
Path "OU=Groupes,OU=MARTINSCIE,$base"

New-ADUser -Name "Jean Dupont" -GivenName Jean -Surname Dupont -
SamAccountName jdupont `
  -UserPrincipalName jdupont@martinscie.lan -Path
"OU=Utilisateurs,OU=MARTINSCIE,$base" `
  -AccountPassword (Read-Host -AsSecureString "Mot de passe") -
ChangePasswordAtLogon $true -Enabled $true
Add-ADGroupMember -Identity GG_RDP_Linux -Members jdupont

# Les nouveaux ordinateurs joints arrivent dans l'OU Ordinateurs
redircmp "OU=Ordinateurs,OU=MARTINSCIE,$base"
```

4.5 Compte d'administration nominatif : créer un compte `adm-smartins` membre de « Admins du domaine » et l'utiliser au quotidien à la place du compte Administrateur intégré.

5. Vérifications et dépannage

```
Get-ADDomain | Select-Object DNSRoot, NetBIOSName, DomainMode, PDCEmulator
Get-ADForest | Select-Object ForestMode, SchemaMaster
dcdiag /v                      # santé complète du DC (tous les tests « réussi »)
dcdiag /test:dns               # DNS du domaine
repadmin /replsummary          # réplication (utile dès le 2e DC)
nltest /dsgetdc:martinscie.lan  # localisation du DC
Resolve-DnsName _ldap._tcp.dc._msdcs.martinscie.lan -Type SRV
Get-SmbShare SYSVOL, NETLOGON   # partages créés
w32tm /monitor
```

Symptôme	Cause probable	Correction
Promotion refusée : nom ou IP	IP dynamique ou nom changé après promotion	Fixer l'IP et le nom avant la promotion (§ 1.2)
`dcdiag` : erreurs DNS	DNS de la carte pointant vers un autre serveur	DNS préféré = `127.0.0.1` ou `192.168.10.10` uniquement
Les postes ne trouvent pas le domaine	DHCP distribuant un DNS public	DNS du DHCP = `192.168.10.10`
Erreurs Kerberos, écart d'heure	Source de temps non configurée	Reprendre § 4.2, `w32tm /resync`
Application (GLPI, NAS) refusée en LDAP 389	Signature LDAP exigée par défaut sur les nouvelles forêts 2025	Configurer l'application en LDAPS (636) avec un certificat sur le DC
Profil pare-feu « Public » après redémarrage	Problème connu de Windows Server 2025	Installer les dernières mises à jour cumulatives, puis redémarrer la carte réseau
Le DC redémarre en boucle après une mise à jour	Mise à jour d'avril 2026 (KB5082063)	Installer le correctif hors bande KB5091157

6. Sécurisation et récapitulatif

Windows Server 2025 durcit déjà plusieurs réglages par défaut (signature LDAP, Kerberos sans RC4, Credential Guard). Il reste à :

- [ ] Utiliser un compte nominatif pour l'administration et placer les administrateurs dans le groupe **Protected Users**.

- [ ] Déployer **Windows LAPS** pour les mots de passe des administrateurs locaux des postes : `Update-LapsADSchema` puis une GPO « LAPS ».
- [ ] Installer un certificat sur DC01 (AD CS ou autorité interne) pour proposer LDAPS aux applications.
- [ ] Sauvegarder l'état du système : `wbadmin start systemstatebackup -backupTarget:E:`.
- [ ] Ne jamais exposer DC01 sur Internet ; sur pfSense, n'autoriser vers DC01 que les ports AD nécessaires depuis le VLAN 20 (53, 88, 135, 389, 445, 464, 636, 3268, ports dynamiques RPC).
- [ ] Prévoir un second contrôleur de domaine (DC02) pour la tolérance de panne.

Récapitulatif PowerShell

```
# 1. Prérequis
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.10.10 -
PrefixLength 24 -DefaultGateway 192.168.10.254
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses
127.0.0.1
Set-TimeZone -Id "Romance Standard Time"
Rename-Computer -NewName DC01 -Restart

# 2. Rôle AD DS
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools

# 3. Nouvelle forêt (niveau Windows Server 2025)
Install-ADDSForest -DomainName "martinscie.lan" -DomainNetbiosName
"MARTINSCIE" `
  -DomainMode 10 -ForestMode 10 -InstallDns `
  -SafeModeAdministratorPassword (Read-Host -AsSecureString "Mot de passe
DSRM") -Force

# 4. Après redémarrage
Set-DnsServerForwarder -IPAddress 1.1.1.1, 9.9.9.9
Add-DnsServerPrimaryZone -NetworkId "192.168.10.0/24" -ReplicationScope
Forest
w32tm /config /manualpeerlist:"0.fr.pool.ntp.org" /syncfromflags:manual
/reliable:yes /update
Enable-ADOptionalFeature "Recycle Bin Feature" -Scope
ForestOrConfigurationSet -Target "martinscie.lan" -Confirm:$false

# 5. Contrôle
dcdiag /v
```