Repadmin : diagnostiquer et réparer la réplication Active Directory

Repadmin est l'outil de diagnostic de référence pour la réplication Active Directory. Une réplication défaillante entre contrôleurs de domaine peut entraîner des incohérences d'annuaire, des authentifications Kerberos échouées et des verrouillages de comptes inexpliqués. Ce guide couvre les commandes essentielles, le dépannage des erreurs les plus fréquentes (1722, 8452, 1396), les lingering objects, le USN rollback et les scripts PowerShell de monitoring préventif.

Maîtriser **repadmin pour diagnostiquer la réplication Active Directory** (repadmin réplication active directory) est une compétence incontournable pour tout administrateur AD. La réplication entre contrôleurs de domaine (DC) est le mécanisme qui synchronise les objets — utilisateurs, groupes, stratégies GPO, mots de passe — entre tous les DC de la forêt. Quand elle flanche, les symptômes sont variés et souvent trompeurs : un utilisateur dont le mot de passe ne fonctionne que sur certains postes, un compte verrouillé sans raison apparente, des stratégies GPO qui ne s'appliquent pas sur un site distant. Sur des incidents que j'ai analysés, ces symptômes pointaient systématiquement vers une réplication AD défaillante — parfois bloquée depuis plusieurs semaines sans que personne ne s'en soit aperçu, parce que les utilisateurs du site distant avaient contourné le problème en changeant leur mot de passe depuis leur site. Repadmin, intégré depuis Windows Server 2008, permet de diagnostiquer l'état de la réplication en quelques commandes, d'identifier les DC problématiques et, dans la plupart des cas, de réparer sans intervention physique ni redémarrage de service.

À RETENIR

À retenir

repadmin /replsummary : vue d'ensemble rapide de la santé de réplication — première commande à lancer lors de tout diagnostic, elle affiche les erreurs et les retards par DC en quelques secondes.

Erreur 1722 (RPC Server Unavailable) : problème réseau ou de connectivité RPC entre DC — vérifier pare-feu, résolution DNS et service RPC avant tout autre diagnostic.

Erreur 8452 / Lingering Objects : le DC source ne connaît plus l'objet demandé — souvent lié à des objets résiduels apparus quand un DC a été hors ligne plus de 180 jours (Tombstone Lifetime).

USN Rollback : situation critique causée par la restauration d'un snapshot VM sans précaution — le DC affecté doit être retiré du domaine et réjoignant proprement pour éviter la corruption d'annuaire.

Monitoring préventif : un script PowerShell planifié qui vérifie quotidiennement `repadmin /replsummary` et alerte sur les erreurs détecte les problèmes avant qu'ils deviennent des incidents critiques.

Comprendre la réplication Active Directory avant de diagnostiquer

La réplication AD fonctionne sur un modèle **multi-maître** : chaque DC peut recevoir des modifications et les répliquer vers les autres. Les modifications sont identifiées par des *USN (Update Sequence Numbers)* — des compteurs qui s'incrémentent à chaque modification sur un

DC. Pour savoir si une modification a déjà été répliquée, chaque DC maintient un *UTD Vector (Up-To-Date Vector)* qui liste les USN maximum reçus depuis chaque partenaire.

La réplication est organisée par **sites AD** — des groupes logiques de DC connectés par des liens rapides. La réplication intra-site (au sein d'un même site) est déclenchée presque immédiatement après une modification (notification en 15 secondes). La réplication inter-sites suit les **site links** configurés — fréquence minimum 15 minutes, 180 minutes par défaut. C'est cette asymétrie qui explique pourquoi un problème de réplication sur un site distant peut passer inaperçu pendant des heures ou des jours.

Les commandes repadmin essentielles pour le diagnostic

Voici le kit de diagnostic minimal. À exécuter sur un DC avec les droits Administrateur de domaine ou Administrateur entreprise :

```
 # 1. Vue d'ensemble rapide — commencer ici
repadmin /replsummary

# 2. Détail de l'état de réplication par DC et par partition
repadmin /showrepl

# 3. Forcer la réplication depuis tous les partenaires vers un DC cible
# /A=tous partenaires, /d=afficher les DN, /e=intersite, /P=push (du DC courant)
repadmin /syncall DC-CIBLE /AdeP

# 4. Voir les USN / UTD Vector d'un DC (détecter USN Rollback)
repadmin /showvector /latency DC01.domaine.local "dc=domaine,dc=local"

# 5. Voir les objets en attente de réplication (backlog)
repadmin /showchanges DC01.domaine.local "dc=domaine,dc=local"

# 6. Forcer la réplication sur tout le domaine + diagnostic dcdiag
repadmin /syncall /Adeq
dcdiag /test:Replications /v
```

Diagnostiquer et résoudre l'erreur 1722 : RPC Server Unavailable

L'erreur **1722 "The RPC server is unavailable"** est la plus fréquente dans les environnements multi-sites. Elle signifie qu'un DC ne peut pas joindre un autre DC via RPC pour répliquer. Les causes et solutions par ordre de probabilité :

Cause probable	Diagnostic	Solution
Pare-feu bloquant les ports RPC	`portqry -n DC_CIBLE -e 135`	Ouvrir TCP 135 + 49152-65535 entre DC
Service RPC arrêté sur le DC cible	`sc query rpcss` sur le DC cible	`net start rpcss`
Résolution DNS défaillante	`nslookup DC_CIBLE` depuis DC source	Corriger les enregistrements DNS A et SRV
Canal sécurisé Netlogon cassé	`nltest /sc_verify:domaine.local`	`nltest /sc_reset:domaine.local`
DC source hors ligne / inaccessible	`ping DC_SOURCE` + `tracert`	Vérifier connectivité réseau et état du DC

```
 # Diagnostic complet erreur 1722
# Étape 1 : Résolution DNS du DC problématique
nslookup DC-PROBLEMATIQUE.domaine.local
Resolve-DnsName DC-PROBLEMATIQUE.domaine.local -Type A

# Étape 2 : Test de connectivité RPC
Test-NetConnection -ComputerName DC-PROBLEMATIQUE.domaine.local -Port 135

# Étape 3 : Vérifier et réparer le canal sécurisé Netlogon
nltest /sc_query:domaine.local
nltest /sc_verify:domaine.local
# Si cassé :
nltest /sc_reset:domaine.local

# Étape 4 : Vérifier les enregistrements DNS SRV du DC (enregistrés par Netlogon)
nslookup -type=SRV _ldap._tcp.dc._msdcs.domaine.local
nslookup -type=SRV _kerberos._tcp.dc._msdcs.domaine.local

# Étape 5 : Forcer la réenregistrement DNS par Netlogon
nltest /dnsregonly
ipconfig /registerdns
```

Résoudre l'erreur 8452 et nettoyer les objets résiduels (lingering objects)

L'erreur **8452 "The naming context or directory partition does not exist on the domain controller"** est plus sérieuse. Elle indique que le DC source ne connaît plus l'objet demandé par le DC destination. La cause la plus fréquente : des *lingering objects* — objets résiduels apparus quand un DC est resté hors ligne plus longtemps que la **Tombstone Lifetime** (durée de vie des objets supprimés, 180 jours par défaut).

À son retour, ce DC contient des objets qui ont été supprimés sur les autres DC pendant son absence. Ces objets "fantômes" persistent indéfiniment sur le DC mal synchronisé et perturbent la réplication globale. La solution est leur suppression avec `repadmin /removelingeringobjects`.

```
 # Identifier les lingering objects — mode simulation d'abord
# DC-REFERENCE = DC sain, DC-PROBLEMATIQUE = DC avec objets résiduels
repadmin /removelingeringobjects DC-PROBLEMATIQUE.domaine.local `
    DC-REFERENCE.domaine.local "dc=domaine,dc=local" /advisory_mode
# /advisory_mode = liste les objets sans les supprimer

# Vérifier les résultats dans le journal des événements (Event ID 1946)
Get-WinEvent -LogName "Directory Service" |
    Where-Object { $_.Id -eq 1946 } |
    Select-Object TimeCreated, Message | Format-List

# Si des objets résiduels sont confirmés, procéder à la suppression
repadmin /removelingeringobjects DC-PROBLEMATIQUE.domaine.local `
    DC-REFERENCE.domaine.local "dc=domaine,dc=local"

# Répéter pour la partition Configuration (contient les sites, services, schéma partiel)
repadmin /removelingeringobjects DC-PROBLEMATIQUE.domaine.local `
    DC-REFERENCE.domaine.local "cn=configuration,dc=domaine,dc=local"

# Forcer la réplication après nettoyage
repadmin /syncall DC-PROBLEMATIQUE.domaine.local /AdeP
```

Qu'est-ce qu'un USN Rollback et pourquoi est-ce si dangereux ?

Le *USN Rollback* est la situation la plus critique en réplication AD. Il se produit quand un DC est restauré depuis un snapshot VMware, Hyper-V ou autre — sans utiliser les mécanismes de restauration AD dédiés (Authoritative Restore via ntdsutil, ou restauration System State sur un DC en mode DSRM).

Le DC restauré reprend des USN anciens, mais les autres DC ont mémorisé des USN plus élevés pour ce DC. Résultat : ils pensent avoir déjà reçu toutes les modifications jusqu'au dernier USN connu — et n'en demandent plus. La réplication s'arrête silencieusement pour ce DC. Les modifications faites sur ce DC après la restauration ne se propagent jamais aux autres. L'annuaire se désynchronise progressivement jusqu'à divergence complète.

Signe révélateur : `repadmin /showrepl` indique que les partenaires ont "mis en quarantaine" (quarantined) le DC. L'Event ID **2095** dans le log Directory Service sur le DC affecté confirme le diagnostic.

Attention critique : Un DC victime d'un USN Rollback confirmé doit être retiré du domaine proprement et réjoignant comme nouveau DC. Tenter de forcer la réplication sans résoudre le rollback corrompra l'annuaire. La seule exception documentée : intervention avec ntdsutil en mode autoritative restore depuis une sauvegarde System State récente et validée — une opération réservée aux experts AD.

```
 # Identifier un USN Rollback — chercher l'Event ID 2095 dans Directory Service
Get-WinEvent -LogName "Directory Service" |
    Where-Object { $_.Id -eq 2095 } |
    Select-Object TimeCreated, Message | Format-List

# Vérifier si un DC est en quarantaine dans les résultats repadmin
$replOutput = repadmin /showrepl 2>&1
$replOutput | Select-String "quarantined|QUARANTINE" -Context 5

# Si USN Rollback confirmé — procédure de retrait du DC affecté
# Étape 1 : Vérifier que ce DC ne détient pas de rôles FSMO
netdom query fsmo

# Étape 2 : Transférer les rôles FSMO si nécessaire vers un DC sain
# (via ntdsutil ou Move-ADDirectoryServerOperationMasterRole)
Move-ADDirectoryServerOperationMasterRole -Identity "DC-SAIN" `
    -OperationMasterRole PDCEmulator, RIDMaster, InfrastructureMaster

# Étape 3 : Rétrograder le DC affecté proprement
Uninstall-ADDSDomainController -DemoteOperationMasterRole `
    -RemoveApplicationPartitions -Force

# Étape 4 : Le réinstaller comme nouveau DC depuis un DC source sain
Install-ADDSDomainController -DomainName "domaine.local" `
    -InstallationMediaPath "C:\IFM" -Credential (Get-Credential)
```

Résoudre l'erreur 1396 : problème d'authentification inter-DC

L'erreur **1396 "Logon Failure: The target account name is incorrect"** apparaît souvent après une migration de DC, un changement de nom de domaine, ou une mauvaise synchronisation des enregistrements SPN. Elle indique que les DC ne parviennent pas à s'authentifier mutuellement pour la réplication.

```
 # Vérifier les SPNs du DC problématique
setspn -L DC-PROBLEMATIQUE

# Rechercher les SPNs dupliqués dans tout le domaine
setspn -X -F
# Des doublons = cause directe de l'erreur 1396

# Supprimer un SPN dupliqué
setspn -D "ldap/DC-PROBLEMATIQUE.domaine.local" DC-INCORRECT

# Réinitialiser le compte machine du DC (dernier recours)
# A exécuter depuis un autre DC sain
Reset-ComputerMachinePassword -Server DC-SAIN.domaine.local -Credential (Get-Credential)

# Forcer la mise à jour des enregistrements Kerberos
klist purge
gpupdate /force
```

Script de monitoring préventif de la réplication AD

Détecter les problèmes de réplication avant qu'ils deviennent des incidents critiques — c'est l'objectif du monitoring préventif. Un script planifié quotidiennement sur un DC de référence couvre ce besoin à coût quasi nul.

```
 # Script de monitoring réplication AD — à planifier en tâche quotidienne (Task Scheduler)
# Envoie une alerte email si des erreurs de réplication sont détectées

param(
    [string]$SmtpServer = "smtp.domaine.local",
    [string]$AlertEmail  = "admin-ad@domaine.local",
    [string]$FromEmail   = "monitoring-ad@domaine.local",
    [int]$MaxRetries     = 3  # Alerter si plus de N échecs consécutifs
)

$timestamp = Get-Date -Format "yyyy-MM-dd HH:mm"
$errors = [System.Collections.ArrayList]::new()

# Récupérer les DC du domaine
$dcs = Get-ADDomainController -Filter * | Select-Object -ExpandProperty HostName

foreach ($dc in $dcs) {
    # Tester l'accessibilité réseau
    if (-not (Test-Connection -ComputerName $dc -Count 1 -Quiet)) {
        [void]$errors.Add("[CRITIQUE] DC inaccessible : $dc")
        continue
    }

    # Récupérer les erreurs de réplication pour ce DC
    try {
        $replInfo = repadmin /showrepl $dc /csv 2>&1
        $replRows = $replInfo | ConvertFrom-Csv

        foreach ($row in $replRows) {
            if ($row.'Number of Failures' -as [int] -gt $MaxRetries) {
                [void]$errors.Add("[ERREUR] DC=$dc | Source=$($row.'Source DC') | Echecs=$($row.'
            }
        }
    } catch {
        [void]$errors.Add("[AVERTISSEMENT] Impossible de récupérer les infos de réplication pour
    }
}

# Vérifier l'état SYSVOL via DFS-R
foreach ($dc in $dcs) {
    try {
        $backlog = Get-DfsrBacklog -DestinationComputerName $dc `
            -SourceComputerName $dcs[0] -GroupName "Domain System Volume" `
```

```
            -FolderName "SYSVOL Share" -ErrorAction Stop
        if ($backlog.BacklogFileCount -gt 100) {
            [void]$errors.Add("[AVERTISSEMENT] Backlog SYSVOL élevé sur $dc : $($backlog.BacklogF
        }
    } catch { }
}

# Envoyer une alerte si des erreurs sont trouvées
if ($errors.Count -gt 0) {
    $body  = "=== ALERTE REPLICATION ACTIVE DIRECTORY — $timestamp ===`n`n"
    $body += "Domaine : $((Get-ADDomain).DNSRoot)`n"
    $body += "DC analysés : $($dcs.Count)`n`n"
    $body += ($errors -join "`n")
    $body += "`n`n=== Actions recommandées ===`n"
    $body += "1. Exécuter : repadmin /replsummary`n"
    $body += "2. Identifier le DC source de l'erreur`n"
    $body += "3. Consulter le journal 'Directory Service' sur le DC affecté`n"

    Send-MailMessage -To $AlertEmail -From $FromEmail `
        -Subject "[ALERTE AD] Réplication — $($errors.Count) problème(s) détecté(s) — $timestamp"
        -Body $body -SmtpServer $SmtpServer
    Write-Warning "Alerte envoyée : $($errors.Count) problème(s) de réplication"
} else {
    Write-Host "[$timestamp] Réplication AD : OK — aucune erreur détectée" -ForegroundColor Green
}
```

Ce script peut être planifié avec Task Scheduler pour exécution quotidienne à 7h00, avant l'arrivée des utilisateurs. Le combiner avec notre guide de sécurisation Active Directory 2025 et notre article sur les outils d'audit Active Directory permet de couvrir l'ensemble de la supervision AD.

Repadmin et la sécurité : l'attaque DCSync

La réplication AD n'est pas seulement un sujet d'administration — c'est aussi un vecteur d'attaque. L'attaque **DCSync**, disponible dans Mimikatz via la commande `lsadump::dcsync`, imite le comportement d'un DC légitime pour demander la réplication des hashes de mots de

passe. L'attaquant n'a pas besoin d'accès physique au DC — il lui suffit de détenir les droits *Replicating Directory Changes* et *Replicating Directory Changes All* sur l'objet domaine.

Ces droits sont détenus par défaut par les Domain Admins, Enterprise Admins et les DC. Si un compte utilisateur ou de service les possède, c'est une anomalie à investiguer immédiatement. La détection passe par l'Event ID **4662** dans le journal Security des DC, filtré sur l'accès `Control Access Right: Replicating Directory Changes` depuis un objet qui n'est pas un DC.

Notre article sur les 10 attaques Active Directory les plus critiques couvre DCSync en détail, avec les règles de détection SIEM. Pour un test de votre exposition à cette attaque, notre service de pentest Active Directory inclut systématiquement le test DCSync dans sa méthodologie. Pour les entreprises soumises à NIS 2, la supervision de la réplication AD est une mesure de surveillance des systèmes d'information au sens de l'article 21 de la directive NIS 2.

Repadmin et la topologie inter-sites : diagnostiquer les liens défaillants

Dans les environnements multi-sites, les erreurs de réplication inter-sites ont souvent une cause réseau — lien WAN saturé, routeur intermédiaire qui bloque les ports RPC, MTU mal configurée sur les tunnels VPN. Avant de diagnostiquer les DC eux-mêmes, vérifier la couche réseau est indispensable.

Chaque lien inter-sites est représenté par un objet **Site Link** dans AD. Le KCC (Knowledge Consistency Checker) — service qui s'exécute sur chaque DC — calcule automatiquement la topologie de réplication optimale et crée les objets **Connection Objects** entre DC partenaires. Quand un site devient inaccessible pendant plusieurs cycles, le KCC peut recalculer la topologie pour contourner le site défaillant — ce qui peut masquer le problème pendant un temps.

```
 # Analyser la topologie de réplication inter-sites
# Lister tous les site links et leur configuration
Get-ADReplicationSiteLink -Filter * | Select-Object Name, SitesIncluded, Cost, ReplicationFrequen

# Afficher les connexions de réplication actives sur un DC
Get-ADReplicationConnection -Filter * | Select-Object Name, ReplicateFromDirectoryServer, AutoGen

# Vérifier si le KCC a détecté des problèmes de topologie
repadmin /istg
# ISTG = Inter-Site Topology Generator — le DC responsable du calcul de topologie

# Forcer le KCC à recalculer la topologie sur tous les DC du domaine
repadmin /kcc
# Sur un DC spécifique
repadmin /kcc DC01.domaine.local

# Afficher les connexions de réplication qui seraient calculées par le KCC
repadmin /showism
```

Diagnostic avancé : analyser les métadonnées de réplication d'un objet

Quand une modification spécifique ne se réplique pas — par exemple, le mot de passe d'un utilisateur qui fonctionne sur certains DC mais pas d'autres — il est possible de tracer la réplication d'un objet précis grâce aux métadonnées de réplication AD. Chaque attribut d'un objet AD porte des informations sur sa dernière modification (DC source, date, USN) qui permettent de détecter des divergences entre DC.

```
 # Afficher les métadonnées de réplication d'un objet AD spécifique
# Utile pour diagnostiquer une modification qui ne se réplique pas
$user = "CN=Utilisateur Test,CN=Users,DC=domaine,DC=local"
repadmin /showobjmeta DC01.domaine.local "$user"

# Comparer les métadonnées du même objet sur deux DC différents
$dc1Meta = repadmin /showobjmeta DC01.domaine.local "$user" 2>&1
$dc2Meta = repadmin /showobjmeta DC02.domaine.local "$user" 2>&1

# Afficher côte à côte pour comparaison
Write-Host "=== DC01 ===" ; $dc1Meta
Write-Host "=== DC02 ===" ; $dc2Meta

# Via PowerShell Active Directory module
Get-ADObject -Identity $user -Properties * -Server DC01.domaine.local |
    Select-Object DistinguishedName, WhenChanged, WhenCreated, ObjectGUID

# Vérifier la réplication de l'attribut pwdLastSet spécifiquement
Get-ADUser -Identity "utilisateurtest" -Server DC01.domaine.local `
    -Properties pwdLastSet | Select-Object SamAccountName, pwdLastSet
Get-ADUser -Identity "utilisateurtest" -Server DC02.domaine.local `
    -Properties pwdLastSet | Select-Object SamAccountName, pwdLastSet
```

Prévenir les problèmes de réplication dans les environnements virtualisés

La virtualisation est aujourd'hui la norme pour les DC — VMware vSphere, Microsoft Hyper-V, Nutanix. Mais la virtualisation introduit des risques spécifiques pour la réplication AD que les administrateurs méconnaissent parfois.

Le risque principal : **la restauration de snapshot**. Restaurer un snapshot d'un DC virtuel sans précaution déclenche un USN Rollback. Les hyperviseurs modernes ont intégré des protections pour limiter ce risque :

VMware vSphere 5.5+ : détection automatique du USN Rollback via la génération VM-ID stockée dans le fichier de configuration VMX. Windows Server 2012+ la lit au démarrage et invalide automatiquement le contexte de réplication si nécessaire.

Hyper-V : les DC sur Hyper-V avec Windows Server 2012+ bénéficient de la même protection via le VM-ID Hyper-V.

Best practice VMware : ne jamais restaurer un snapshot de DC sans le mettre en mode DSRM (Directory Services Restore Mode) d'abord. Préférer les sauvegardes System State via Windows Server Backup ou un outil compatible VSS-aware.

Pour les VM qui migrent entre hyperviseurs (P2V ou V2V), toujours retirer le DC de l'AD avant la migration et le réinstaller depuis zéro après. La documentation Microsoft sur ce point est explicite : détecter et récupérer d'un USN Rollback (Microsoft Learn).

Les recommandations de l'ANSSI sur la sécurisation des systèmes d'information incluent la gestion correcte des sauvegardes et restaurations de DC comme point de contrôle de sécurité. Notre article sur le hub de sécurité Active Directory centralise les ressources sur la protection des environnements AD. Pour un audit complet de votre infrastructure AD, notre service de pentest Active Directory inclut une revue des pratiques de sauvegarde et restauration des DC.

Questions fréquentes sur repadmin et la réplication AD

Combien de temps faut-il pour que la réplication se propage sur tout le domaine ?

En intra-site (même site AD), la réplication est déclenchée dans les 15 secondes après une modification et se propage à tous les DC du site en général en moins de 1 minute pour un domaine de taille standard. En inter-sites, le délai dépend de la fréquence configurée sur les Site Links — 180 minutes par défaut, souvent réduit à 15 minutes dans les configurations modernes. Pour une propagation urgente, `repadmin /syncall /Adeq` force la réplication immédiate sur tous les partenaires inter-sites.

Repadmin /replsummary affiche "Consecutive failures" — que faire en premier ?

Notez le code d'erreur affiché (1722, 8452, 1396, etc.) et le nom du DC source et destination en échec. Consultez la section correspondante de ce guide. Si le nombre de failures dépasse 5 et que

le dernier succès remonte à plus de 24 heures, traitez-le comme un incident prioritaire : la divergence d'annuaire s'aggrave à chaque cycle manqué. Exécutez en parallèle `repadmin /showrepl DC-AFFECTE` et consultez le journal "Directory Service" sur ce DC.

Peut-on utiliser repadmin sur des environnements Azure AD DS ?

Non. Azure Active Directory Domain Services (Azure AD DS) est un service managé — Microsoft gère les contrôleurs de domaine et la réplication en interne. Vous n'avez pas accès aux DC eux-mêmes et ne pouvez pas exécuter repadmin. Le diagnostic des problèmes passe par les journaux Azure AD DS dans le portail Azure et le support Microsoft pour les problèmes internes. Repadmin est spécifique aux environnements AD on-premise et hybrides.

La commande repadmin /syncall a-t-elle des effets secondaires ?

Oui : elle déclenche une synchronisation active simultanée sur tous les partenaires de réplication. Sur un domaine avec de nombreux DC ou des liaisons WAN lentes, cela peut générer un pic de trafic réseau significatif. Sur un domaine standard (moins de 20 DC, liens à 100 Mbps+), l'impact est négligeable. Évitez d'exécuter cette commande en heures de pointe sur des liaisons WAN limitées à moins de 10 Mbps.

Comment vérifier que la réplication SYSVOL fonctionne indépendamment d'AD DS ?

La réplication SYSVOL (GPO, scripts de démarrage) utilise **DFS-R** depuis Windows Server 2012. Pour diagnostiquer SYSVOL : `dfsrdiag replicationstate /member:DC-CIBLE` et `Get-DfsrBacklog -DestinationComputerName DC-CIBLE`. Des problèmes SYSVOL se manifestent souvent par des GPO qui ne s'appliquent pas sur certains sites, même si la réplication AD des objets GPO (dans la partition domaine) est fonctionnelle. Vérifier également dans `\\domaine.local\SYSVOL\domaine.local\Policies` que les dossiers GPO sont présents sur tous les DC. Notre article sur la sécurisation GPO Active Directory couvre la supervision des stratégies de groupe en détail.