Backup et Recovery Active Directory 2026 : Guide Complet Windows Server 2025

Stratégie complète de backup et recovery Active Directory 2026 : règle 3-2-1-1, WSB, NTDSUTIL, Azure Backup, scripts PowerShell et conformité NIS 2 DORA.

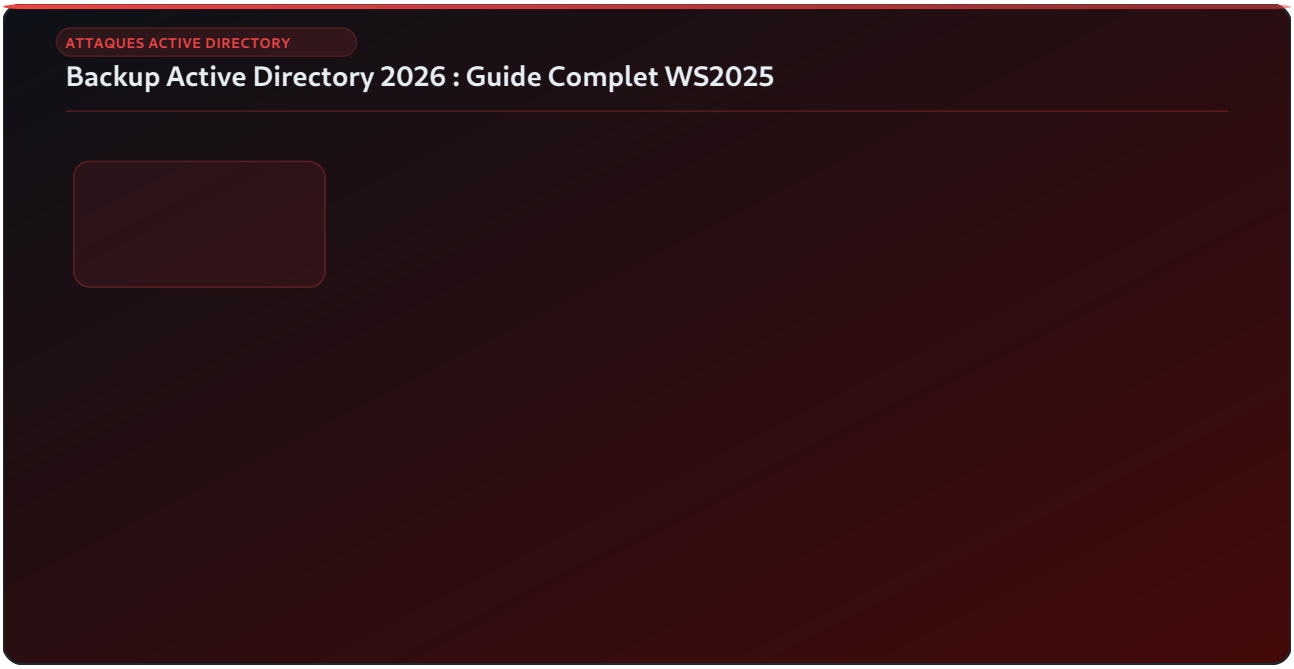
📋 EN BREF

En bref

- Active Directory est le SPOF numéro un des infrastructures Windows : une panne ou une attaque ransomware sans backup valide peut immobiliser toute l'entreprise pendant des jours.
- La règle 3-2-1-1 (3 copies, 2 médias différents, 1 hors-site, 1 immuable offline) est le standard minimum pour protéger les contrôleurs de domaine en 2026.
- Windows Server Backup (WSB) couvre le System State natif ; NTDSUTIL fournit des snapshots VSS cohérents sans interruption de service.
- La Corbeille AD (Active Directory Recycle Bin) permet de récupérer des objets supprimés en quelques secondes, mais doit être activée *avant* l'incident.
- NIS 2 (article 21§2.c) et DORA (article 12) imposent des exigences documentées de RTO/RPO et de test régulier des procédures de recovery pour les entités françaises.

La sécurité d'Active Directory est au cœur des préoccupations des RSSI et des équipes IT en France depuis l'explosion des attaques ransomware ciblant spécifiquement les contrôleurs de domaine. À Paris comme dans l'ensemble du territoire, les incidents de type BlackCat, LockBit ou Royal ont mis en évidence une réalité brutale : sans une stratégie de backup et de recovery

Active Directory rigoureuse, l'entreprise est paralysée en quelques heures. Les attaquants savent pertinemment que compromettre les DC revient à prendre en otage l'intégralité du système d'information. Face à cette menace, la résilience opérationnelle passe obligatoirement par la maîtrise des procédures de sauvegarde — System State, SYSVOL, snapshots NTDS, sauvegarde Azure — et par la capacité à restaurer un domaine complet dans des délais contractuels. En 2026, Windows Server 2025 apporte des améliorations notables en matière de snapshot cohérent et d'intégration cloud, tandis que les réglementations NIS 2 et DORA durcissent les obligations de continuité pour les opérateurs d'importance vitale et les établissements financiers. Ce guide complet, destiné aux administrateurs système et aux équipes sécurité de niveau avancé, couvre l'ensemble du cycle de vie backup/recovery AD : planification, outils natifs et tiers, automatisation PowerShell, restauration authoritative et non-authoritative, forest recovery, et conformité réglementaire.



Stratégie de Backup AD : Règle 3-2-1-1 pour les Contrôleurs de Domaine

Pourquoi Active Directory est le SPOF numéro un

Active Directory centralise l'authentification, l'autorisation et la gestion des stratégies de groupe pour l'ensemble des ressources Windows d'une organisation. Un contrôleur de domaine unique qui tombe — qu'il s'agisse d'une corruption matérielle, d'un ransomware, ou d'une suppression accidentelle d'objets critiques — entraîne immédiatement l'impossibilité pour les utilisateurs de se connecter, pour les applications de valider les tickets Kerberos, et pour les services automatisés d'accéder aux ressources réseau. Dans les architectures sans redondance DC, l'impact est total et immédiat. Même avec plusieurs DC, la réplication Active Directory peut propager une corruption en quelques minutes via le mécanisme USN (Update Sequence Number), transformant un problème localisé en désastre multi-sites.

Les ransomwares modernes ciblent systématiquement les DC : chiffrement de NTDS.dit, suppression des shadow copies VSS via `vssadmin delete shadows`, et sabotage des agents de sauvegarde. Sans backup hors ligne et immuable, la restauration est impossible. Les entreprises françaises qui ont subi des incidents majeurs (CHU, collectivités, PME industrielles) confirment que le délai de recovery sans backup valide dépasse systématiquement les 72 heures, avec un coût moyen estimé entre 500 000 € et 2 M€ selon l'ANSSI.

La règle 3-2-1-1 appliquée à Active Directory

La règle 3-2-1-1, évolution de la règle 3-2-1 classique, est devenue le standard de facto pour les environnements critiques :

3 copies : la production (le DC en service) + 2 sauvegardes distinctes

2 médias différents : par exemple, un NAS local + un stockage cloud ou bande magnétique

1 copie hors-site : Azure Backup, autre datacenter, bande en coffre physique

1 copie immuable offline : Write-Once-Read-Many (WORM), Azure Immutable Blob Storage, bande hors réseau — inaccessible aux ransomwares

Pour Active Directory spécifiquement, la copie immuable est critique : les attaquants désactivent en priorité tous les mécanismes de sauvegarde accessibles depuis le réseau. Un backup Azure

avec verrouillage légal (*Litigation Hold*) ou une copie sur bande LTO déconnectée du réseau constituent les derniers recours lors d'une attaque totale.

RTO et RPO pour Active Directory

Les objectifs de temps de reprise (RTO — Recovery Time Objective) et de point de reprise (RPO — Recovery Point Objective) doivent être définis contractuellement avant tout incident :

Scénario	RPO recommandé	RTO cible	Impact si non atteint
Panne DC unique (redondance existante)	24h (dernier backup)	2-4h (rebuild depuis backup)	Dégradation des performances, pas d'indisponibilité totale
Corruption NTDS.dit multi-DC	24h	4-8h	Authentification impossible sur le domaine
Suppression d'OU / objets critiques	15 min (snapshot VSS)	30 min (Recycle Bin) / 2h (restore authoritative)	Perte d'accès pour utilisateurs/ services concernés
Ransomware Forest-wide	24-48h	8-24h (procédure forest recovery)	Arrêt total de l'entreprise

Windows Server Backup (WSB) — Sauvegarde Native des DC

Le System State : ce qui doit absolument être sauvegardé

Windows Server Backup, inclus gratuitement dans Windows Server, permet de capturer le **System State** d'un contrôleur de domaine. Ce composant est fondamental : il inclut l'intégralité des éléments nécessaires à une restauration complète du DC.

⚡ **Retour terrain**

Dans mes missions de hardening Active Directory, le point le plus sous-estimé est la gestion du groupe 'Opérateurs de compte' et des délégations personnalisées créées au fil des années. Pour un groupe logistique de 1 500 utilisateurs, j'ai trouvé 312 ACL personnalisées dont 89 accordaient des permissions d'écriture sur des attributs sensibles (adminCount, memberOf sur groupes privilégiés) à des comptes d'utilisateurs standards. La dette technique en sécurité AD est souvent invisible jusqu'au premier audit sérieux.

Le System State d'un contrôleur de domaine comprend :

NTDS.dit : la base de données Active Directory (comptes, groupes, stratégies, attributs)

SYSVOL : les scripts de connexion et les templates de stratégies de groupe (GPO)

Registre système : HKLM\SYSTEM, HKLM\SOFTWARE et autres ruches critiques

Boot files : MBR, BCD, fichiers de démarrage Windows

Certificate Services (si PKI installée) : base de l'autorité de certification

COM+ Class Registration Database

La sauvegarde System State seule (sans BMR — Bare Metal Recovery) ne permet pas de restaurer le DC sur un nouveau matériel, mais suffit pour une restauration sur un OS Windows Server existant ou dans DSRM.

Commande de base WSB

```
 # Sauvegarde System State vers un partage réseau
wbadmin start systemstatebackup -backuptarget:\\BACKUPSRV\DC_Backups -quiet

# Sauvegarde System State vers un disque local
wbadmin start systemstatebackup -backuptarget:D: -quiet

# Lister les versions disponibles
wbadmin get versions -backuptarget:\\BACKUPSRV\DC_Backups
```

Event IDs à surveiller pour les sauvegardes WSB :

`Event ID 1` (Microsoft-Windows-Backup) : démarrage d'une opération de sauvegarde

`Event ID 517` (Microsoft-Windows-Backup) : sauvegarde complétée avec succès

`Event ID 518` (Microsoft-Windows-Backup) : échec de la sauvegarde — alerte critique

`Event ID 325` (NTDS General) : la base NTDS a été restaurée avec succès

`Event ID 326` (NTDS General) : NTDS a détecté une incohérence lors du démarrage

La surveillance de ces Event IDs est détaillée dans notre guide sur les événements Windows à surveiller sur un contrôleur de domaine.

Script PowerShell complet de sauvegarde automatisée

```
 #Requires -RunAsAdministrator
<#
.SYNOPSIS
    Sauvegarde automatisée System State des contrôleurs de domaine
    avec rotation, vérification d'intégrité et alertes email.
.NOTES
    Planification recommandée : tâche planifiée quotidienne à 02:00
    Exécuter avec un compte de service disposant des droits Backup Operator
#>

param(
    [string]$BackupTarget = "\\BACKUPSRV\DC_Backups",
    [int]$RetentionDays = 30,
    [string]$SmtpServer = "smtp.entreprise.fr",
    [string]$AlertEmail = "soc@entreprise.fr",
    [string]$FromEmail = "backup-dc@entreprise.fr"
)

$DCName = $env:COMPUTERNAME
$LogFile = "C:\Logs\DC_Backup_$(Get-Date -Format 'yyyyMMdd_HHmmss').log"
$StartTime = Get-Date

function Write-Log {
    param([string]$Message, [string]$Level = "INFO")
    $Entry = "[$(Get-Date -Format 'yyyy-MM-dd HH:mm:ss')] [$Level] $Message"
    Add-Content -Path $LogFile -Value $Entry
    Write-Host $Entry
}

function Send-Alert {
    param([string]$Subject, [string]$Body)
    try {
        Send-MailMessage -SmtpServer $SmtpServer -From $FromEmail `
            -To $AlertEmail -Subject "[$DCName] $Subject" -Body $Body -Encoding UTF8
        Write-Log "Alerte email envoyée : $Subject"
    } catch {
        Write-Log "Échec envoi email : $_" "ERROR"
    }
}

# Créer le répertoire de logs si nécessaire
if (-not (Test-Path "C:\Logs")) { New-Item -ItemType Directory -Path "C:\Logs" | Out-Null }
```

```
Write-Log "=== Démarrage sauvegarde System State DC : $DCName ==="
Write-Log "Cible : $BackupTarget"

# Vérifier la connectivité vers le partage de sauvegarde
if (-not (Test-Path $BackupTarget)) {
    Write-Log "Partage de sauvegarde inaccessible : $BackupTarget" "ERROR"
    Send-Alert "ECHEC Backup - Partage inaccessible" "Le partage $BackupTarget est inaccessible d
    exit 1
}

# Lancer la sauvegarde System State
Write-Log "Lancement wbadmin start systemstatebackup..."
$WBOutput = & wbadmin start systemstatebackup -backuptarget:$BackupTarget -quiet 2>&1
$ExitCode = $LASTEXITCODE

$WBOutput | ForEach-Object { Write-Log $_ }

if ($ExitCode -ne 0) {
    Write-Log "Échec de la sauvegarde (code $ExitCode)" "ERROR"
    Send-Alert "ECHEC Backup System State" `
        "La sauvegarde System State a échoué sur $DCName.`nCode de sortie : $ExitCode`nSortie : $
    exit $ExitCode
}

Write-Log "Sauvegarde terminée avec succès (code $ExitCode)"

# Récupérer et logger la version de backup créée
$Versions = & wbadmin get versions -backuptarget:$BackupTarget 2>&1
Write-Log "Versions disponibles après sauvegarde :"
$Versions | ForEach-Object { Write-Log $_ }

# Rotation : supprimer les backups plus anciens que $RetentionDays jours
Write-Log "Rotation des backups (rétention : $RetentionDays jours)..."
$CutoffDate = (Get-Date).AddDays(-$RetentionDays)

# Récupérer toutes les versions et identifier celles à supprimer
$AllVersions = & wbadmin get versions -backuptarget:$BackupTarget 2>&1
$VersionDates = @()
foreach ($Line in $AllVersions) {
    if ($Line -match "Backup time:\s+(.+)") {
        $DateStr = $Matches[1].Trim()
        try {
            $BackupDate = [datetime]::Parse($DateStr)
            $VersionDates += $BackupDate
```

```
        } catch { Write-Log "Impossible de parser la date : $DateStr" "WARN" }
    }
}

$ToDelete = $VersionDates | Where-Object { $_ -lt $CutoffDate }
foreach ($OldDate in $ToDelete) {
    $DateFormatted = $OldDate.ToString("MM/dd/yyyy-HH:mm")
    Write-Log "Suppression du backup du $OldDate..."
    & wbadmin delete systemstatebackup -backuptarget:$BackupTarget `
        -version:$DateFormatted -keepVersions:1 -quiet 2>&1 | ForEach-Object { Write-Log $_ }
}

# Calculer la durée totale
$Duration = (Get-Date) - $StartTime
Write-Log "=== Sauvegarde réussie en $([int]$Duration.TotalMinutes) minutes ==="

# Email de confirmation quotidien (optionnel — commenter si trop verbeux)
# Send-Alert "Backup System State OK" "Sauvegarde réussie sur $DCName en $([int]$Duration.TotalMi

exit 0
```

Pour planifier ce script comme tâche journalière :

```
 # Créer la tâche planifiée (exécuter en tant qu'administrateur)
$Action = New-ScheduledTaskAction -Execute "PowerShell.exe" `
    -Argument "-NonInteractive -ExecutionPolicy Bypass -File C:\Scripts\Backup-DC-SystemState.ps1
$Trigger = New-ScheduledTaskTrigger -Daily -At "02:00AM"
$Principal = New-ScheduledTaskPrincipal -UserId "SYSTEM" -LogonType ServiceAccount -RunLevel High
$Settings = New-ScheduledTaskSettingsSet -ExecutionTimeLimit (New-TimeSpan -Hours 4) -RestartCoun

Register-ScheduledTask -TaskName "DC-SystemState-Backup" -Action $Action `
    -Trigger $Trigger -Principal $Principal -Settings $Settings -Force
```

NTDSUTIL Snapshot et Sauvegarde VSS

Snapshots VSS avec NTDSUTIL : la sauvegarde sans interruption

Contrairement à WSB qui nécessite l'utilisation du Volume Shadow Copy Service de façon globale, NTDSUTIL permet de créer directement des snapshots cohérents de la base NTDS sans arrêter le contrôleur de domaine ni le service AD DS. C'est la méthode privilégiée pour des sauvegardes fréquentes (toutes les heures par exemple) sans impact sur la production. Notre guide complet NTDSUTIL détaille toutes les commandes disponibles.

```
 :: Créer un snapshot de la base AD
ntdsutil "snapshot" "activate instance ntds" "create" "quit" "quit"

:: Lister les snapshots disponibles
ntdsutil "snapshot" "activate instance ntds" "list all" "quit" "quit"

:: Monter un snapshot pour inspection ou extraction
:: (remplacer {GUID} par le GUID affiché par "list all")
ntdsutil "snapshot" "activate instance ntds" "mount {GUID}" "quit" "quit"

:: Démonter le snapshot
ntdsutil "snapshot" "activate instance ntds" "unmount {GUID}" "quit" "quit"

:: Supprimer le snapshot
ntdsutil "snapshot" "activate instance ntds" "delete {GUID}" "quit" "quit"
```

Montage et inspection d'un snapshot NTDS

Une fois monté, le snapshot expose une copie cohérente de NTDS.dit accessible en lecture seule. Il est possible d'utiliser `dsamain.exe` pour démarrer un annuaire AD en lecture seule depuis ce snapshot et y connecter des outils comme ADUC ou PowerShell :

```
 :: Monter le snapshot (exemple : monte en C:\$SNAP_xxx\)
ntdsutil "snapshot" "activate instance ntds" "mount {GUID}" "quit" "quit"

:: Démarrer un DC LDAP de lecture seule sur port 33389 depuis le snapshot
dsamain.exe -dbpath "C:\$SNAP_xxx\Windows\NTDS\ntds.dit" -ldapport 33389

:: Dans une autre session PowerShell, requêter ce DC temporaire :
Get-ADUser -Filter * -Server "localhost:33389" | Select-Object Name, Enabled
```

Différences entre Snapshot VSS et Backup System State

Critère	Snapshot VSS (ntdsutil)	Backup System State (WSB)
Impact sur le DC	Aucun (lecture seule instantanée)	Charge I/O pendant la sauvegarde
Fréquence possible	Toutes les heures	Quotidienne (durée 30-90 min)
Contenu sauvegardé	NTDS.dit uniquement	NTDS.dit + SYSVOL + Registre + BCD
Restauration authoritative	Via IFM + ntdsutil	Via DSRM + wbadmin restore
Stockage	Sur le volume local (VSS)	Distant ou local
Protection ransomware	Faible (accessible depuis le DC)	Bonne si destination hors réseau

Microsoft Azure Backup pour Active Directory

MARS Agent : sauvegarde cloud des DC

Microsoft Azure Recovery Services (MARS) Agent est le composant qui permet de sauvegarder des contrôleurs de domaine on-premises directement dans un coffre Azure Recovery Services. C'est aujourd'hui la solution recommandée pour satisfaire à l'exigence de copie hors-site immuable de la règle 3-2-1-1.

Installation et configuration de base :

```
 # Télécharger et installer le MARS Agent (depuis le portail Azure ou via script)
# Enregistrement du DC auprès du vault Recovery Services
# (exécuté après installation du MARS Agent)

$VaultCredentialPath = "C:\Temp\VaultCredentials.vaultcredentials"
# Fichier téléchargé depuis le portail Azure > Recovery Services vault > +Backup

# Enregistrement interactif (ou via API REST pour automatisation)
Start-Process -FilePath "MARSAgentInstaller.exe" -ArgumentList "/q /nu" -Wait

# Après installation, configurer via la console MARS :
# Manage Backup > Register Server > Import Vault Credential
```

Configuration de la politique de rétention Azure

Dans le portail Azure Recovery Services, définir une **Backup Policy** adaptée aux DC :

Fréquence : quotidienne (System State), idéalement à 02h00 hors heures de travail

Rétention quotidienne : 30 jours minimum

Rétention hebdomadaire : 12 semaines (recommandé par Microsoft pour AD)

Rétention mensuelle : 6 mois (pour conformité NIS 2)

Rétention annuelle : 1 an (pour conformité DORA secteur financier)

Immutability : activer le verrouillage "Soft Delete" + "Immutable vault" pour prévenir la suppression par ransomware/insider

Avantages d'Azure Backup pour les DC

Immutabilité : une fois le vault verrouillé, même un compte administrateur Azure compromis ne peut pas supprimer les données avant expiration de la rétention

Géo-redondance : avec GRS (Geo-Redundant Storage), les données sont répliquées dans une région Azure secondaire automatiquement

Coût prévisible : facturation au Go sauvegardé (System State ≈ 5-15 Go par DC selon la taille de l'annuaire)

Encryption at rest : chiffrement AES-256 avec clé gérée par Microsoft ou CMK (Customer Managed Key) via Azure Key Vault

Intégration Azure Monitor : alertes natives sur les échecs de backup

---

Sauvegarde de SYSVOL : DFS-R vs FRS

Pourquoi SYSVOL mérite une attention particulière

SYSVOL est le répertoire partagé sur chaque DC qui contient les scripts de connexion (`Netlogon`) et les fichiers ADMX/ADML des modèles de stratégies de groupe. Sa corruption ou sa perte sans backup entraîne l'application incorrecte ou l'impossibilité de déployer des GPO, ce qui affecte la configuration de sécurité de tous les postes et serveurs du domaine. Notre article sur la sécurisation des RODC sous Windows Server 2025 aborde le rôle de SYSVOL dans les environnements distribués.

DFS-R (mécanisme recommandé depuis Windows Server 2012)

Depuis la migration de FRS (File Replication Service, obsolète) vers DFS-R (Distributed File System Replication), la réplication SYSVOL est plus robuste et plus facile à réparer. Pour vérifier le mécanisme actif :

```
 # Vérifier si SYSVOL utilise DFS-R ou FRS
Get-ADDomain | Select-Object -ExpandProperty SYSVOLReady
dfsrmig /getglobalstate
# État 3 = "Eliminated" = DFS-R pleinement actif, FRS désactivé
```

Sauvegarde SYSVOL avec Robocopy (en complément de WSB) :

```
 # Sauvegarde complète du SYSVOL avec préservation des ACL et attributs
$SysvolPath = "C:\Windows\SYSVOL"
$BackupPath = "\\BACKUPSRV\SYSVOL_Backup\$(Get-Date -Format 'yyyyMMdd')"

robocopy $SysvolPath $BackupPath /E /COPYALL /MIR /R:3 /W:10 /LOG:"C:\Logs\SYSVOL_Backup.log"
```

Restauration SYSVOL : procédure D4/D2

Lorsque SYSVOL est désynchronisé entre DC ou corrompu, la procédure de restauration DFS-R utilise les marqueurs D4 (authoritative — la source fait autorité) et D2 (non-authoritative — le DC récupère depuis ses pairs) :

```
 # Sur le DC qui sera la source authoritative (D4) :
# Modifier la clé de registre DFS-R
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\DFSR\Parameters\SysVols\Seeding S
    -Name "msDFSR-Options" -Value 1 -Type DWord
# Valeur 1 = D4 (authoritative primary)

# Redémarrer le service DFS-R
Restart-Service DFSR

# Sur tous les autres DC (D2, non-authoritative) :
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\DFSR\Parameters\SysVols\Seeding S
    -Name "msDFSR-Options" -Value 0 -Type DWord
Restart-Service DFSR
```

Restauration Non-Authoritative d'un DC (Rebuild)

Quand utiliser la restauration non-authoritative

La restauration non-authoritative est utilisée quand un DC unique est perdu (panne matérielle, VM supprimée, corruption OS) mais que d'autres DC du domaine sont sains et disponibles.

Après restauration, le DC se met à jour automatiquement via la réplication AD pour rattraper les changements survenus depuis le dernier backup.

Procédure complète de restauration non-authoritative

```
 ## ÉTAPE 1 : Démarrer en DSRM (Directory Services Restore Mode)
# Au démarrage : F8 > "Directory Services Restore Mode"
# Ou via bcdedit pour le prochain redémarrage :
bcdedit /set safeboot dsrepair

## ÉTAPE 2 : Restaurer le System State depuis la sauvegarde WSB
# Lister les versions disponibles
wbadmin get versions -backuptarget:\\BACKUPSRV\DC_Backups

# Restaurer (remplacer VERSION par la date/heure affichée)
wbadmin start systemstaterecovery -version:"MM/DD/YYYY-HH:MM" `
    -backuptarget:\\BACKUPSRV\DC_Backups -authsysvol -quiet

## ÉTAPE 3 : Retirer le mode DSRM et redémarrer normalement
bcdedit /deletevalue safeboot
Restart-Computer

## ÉTAPE 4 : Vérifications post-restauration
# Vérifier la réplication AD
repadmin /replsummary
repadmin /showrepl

# Vérifier le service Netlogon et l'état de SYSVOL
Get-Service Netlogon | Select-Object Status
Test-Path "\\$env:COMPUTERNAME\SYSVOL"

# Vérifier les rôles FSMO
netdom query fsmo

# Forcer la réplication depuis tous les DC
repadmin /syncall /AdeP
```

Checklist de validation post-restauration DC

Service `NTDS` démarré et en état Running

Service `Netlogon` démarré — partage SYSVOL accessible

Réplication AD verte sur tous les partenaires (`repadmin /replsummary`)

Tickets Kerberos fonctionnels : `klist purge && klist get host/dc01.domaine.local`

GPO appliquées correctement sur un poste de test : `gpresult /r`

DNS résolu depuis le DC restauré : `nslookup domaine.local`

Event IDs 325 (NTDS restauré OK) présent dans les logs

Aucun Event ID 326 (incohérence NTDS) sans résolution documentée

---

Restauration Authoritative — Récupérer des Objets AD Supprimés

Active Directory Recycle Bin : la première ligne de défense

La Corbeille Active Directory (Recycle Bin), disponible depuis le niveau fonctionnel Windows Server 2008 R2, permet de restaurer des objets supprimés (utilisateurs, groupes, OU, ordinateurs) avec la totalité de leurs attributs, y compris les memberships de groupe. C'est la méthode la plus rapide et la moins risquée pour récupérer des suppressions accidentelles.

```
 # Vérifier si la Recycle Bin est activée
Get-ADOptionalFeature -Filter {Name -like "Recycle Bin*"} | Select-Object Name, EnabledScopes

# Activer la Recycle Bin (opération irréversible, nécessite Forest Functional Level 2008 R2+)
Enable-ADOptionalFeature "Recycle Bin Feature" `
    -Scope ForestOrConfigurationSet `
    -Target (Get-ADForest).Name -Confirm:$false

# Lister les objets supprimés (dans la Corbeille)
Get-ADObject -Filter {isDeleted -eq $true} -IncludeDeletedObjects `
    -Properties * | Select-Object Name, ObjectClass, WhenChanged | Sort-Object WhenChanged -Desce

# Restaurer un utilisateur supprimé (par son DistinguishedName de suppression)
$DeletedUser = Get-ADObject -Filter {DisplayName -eq "Jean Dupont" -and isDeleted -eq $true} `
    -IncludeDeletedObjects
Restore-ADObject -Identity $DeletedUser

# Restaurer une OU entière avec tous ses objets enfants
Get-ADObject -Filter {isDeleted -eq $true -and DistinguishedName -like "*OU=Services*"} `
    -IncludeDeletedObjects | Sort-Object DistinguishedName | Restore-ADObject
```

Restauration authoritative via NTDSUTIL

Quand la Recycle Bin n'est pas activée ou quand l'objet a été supprimé il y a plus de 180 jours (durée de vie par défaut des tombstone objects), la restauration authoritative via NTDSUTIL est nécessaire. Cette procédure restaure des objets depuis un backup System State et les marque comme "faisant autorité" pour qu'ils soient répliqués vers tous les DC, écrasant les versions supprimées.

```
 :: En mode DSRM après restauration System State non-authoritative :

:: Lancer ntdsutil pour restauration authoritative
ntdsutil

:: Dans ntdsutil :
authoritative restore
restore subtree "OU=Finance,DC=contoso,DC=com"
:: Pour un seul objet :
restore object "CN=Jean Dupont,OU=Finance,DC=contoso,DC=com"
quit
quit

:: Redémarrer normalement (sans DSRM)
bcdedit /deletevalue safeboot
shutdown /r /t 0
```

Important : la restauration authoritative d'une OU entière restaure tous les objets qu'elle contenait au moment du backup, y compris les comptes créés et supprimés légitimement entre le backup et la suppression. Procéder avec précaution et documenter chaque restauration.

Scénario IFM (Install From Media) quand la Recycle Bin est inactive

Si la Recycle Bin n'était pas activée et que le backup date de plus de 180 jours, il faut utiliser IFM : créer un media d'installation depuis un snapshot NTDS, extraire les données avec `dsamain`, puis réimporter manuellement via PowerShell AD. Cette procédure avancée est documentée dans notre article sur NTDSUTIL et la gestion avancée d'Active Directory.

Forest Recovery — Scénario de Catastrophe Totale

Quand la procédure Forest Recovery s'applique

La récupération de forêt AD (Forest Recovery) est le scénario le plus grave : tous les DC sont compromis, la réplication propage la corruption, ou un ransomware a chiffré l'intégralité de

l'infrastructure AD. Dans ce cas, la restauration normale DC par DC n'est pas suffisante — il faut reconstruire la forêt depuis zéro en suivant la procédure Microsoft Forest Recovery, qui impose un ordre précis pour éviter la réintroduction de la corruption par la réplication. Notre article dédié sur la forest recovery après un ransomware couvre ce scénario en détail.

Ordre des opérations Forest Recovery

Isolation réseau immédiate : couper tous les DC du réseau pour stopper la propagation. Couper également les liens de réplication inter-sites.

Identifier le DC racine de forêt (le DC qui porte le rôle Schema Master dans le domaine racine de la forêt)

Restaurer le DC racine en DSRM depuis le backup System State le plus récent non-compromis

Nettoyer les métadonnées des autres DC via `ntdsutil metadata cleanup`

Restaurer les DC des domaines enfants un par un, en commençant par les PDC Emulator de chaque domaine

Réinitialiser tous les mots de passe des comptes de service, comptes krbtgt (2 fois avec délai de 10 heures), comptes administrateurs

Réactiver les liens de réplication progressivement et surveiller la convergence

Vérification finale : tous les rôles FSMO, réplication verte, services applicatifs

```
 # Réinitialiser le compte krbtgt (à faire 2 fois avec 10h d'intervalle)
# CRITIQUE : ce compte signe tous les tickets Kerberos de la forêt
$KrbtgtAccount = Get-ADUser -Identity krbtgt
$NewPassword = ConvertTo-SecureString -AsPlainText (New-Guid).ToString() -Force
Set-ADAccountPassword -Identity $KrbtgtAccount -NewPassword $NewPassword -Reset

# Forcer la réplication du changement krbtgt sur tous les DC
repadmin /syncall /AdeP

# Attendre 10 heures (durée de vie maximale des tickets Kerberos),
# puis répéter la réinitialisation krbtgt une seconde fois
```

Test et Validation des Sauvegardes AD

Environnement de test isolé

Tester les procédures de backup/recovery dans l'environnement de production est risqué et potentiellement perturbateur. La bonne pratique consiste à maintenir un environnement de test isolé : un VLAN dédié sans routage vers la production, avec au minimum un DC Windows Server 2025 et une station Windows 11. Les sauvegardes sont importées dans cet environnement pour validation complète. La sécurisation des DC via Credential Guard sur Windows Server 2025 s'applique également à l'environnement de test pour des conditions réalistes.

Script PowerShell de validation automatique des backups

```
 #Requires -RunAsAdministrator
<#
.SYNOPSIS
    Validation automatique de l'intégrité des sauvegardes DC.
    Vérifie l'existence, l'âge et la taille minimale des backups.
    À exécuter quotidiennement après la sauvegarde.
#>

param(
    [string]$BackupTarget = "\\BACKUPSRV\DC_Backups",
    [int]$MaxAgeHours = 26,          # Alerte si backup > 26h (tolérance +2h)
    [long]$MinSizeGB = 2,            # Taille minimale attendue en Go
    [string]$AlertEmail = "soc@entreprise.fr",
    [string]$SmtpServer = "smtp.entreprise.fr"
)

$Errors = @()
$Report = @()

function Add-Issue { param([string]$Msg) $script:Errors += $Msg; $script:Report += "[FAIL] $Msg"
function Add-OK    { param([string]$Msg) $script:Report += "[OK]   $Msg" }

# 1. Vérifier que le partage de backup est accessible
if (-not (Test-Path $BackupTarget)) {
    Add-Issue "Partage de backup inaccessible : $BackupTarget"
} else {
    Add-OK "Partage de backup accessible : $BackupTarget"

    # 2. Lister les versions de backup disponibles
    $VersionsOutput = & wbadmin get versions -backuptarget:$BackupTarget 2>&1
    $VersionLines = $VersionsOutput | Where-Object { $_ -match "Backup time:" }

    if ($VersionLines.Count -eq 0) {
        Add-Issue "Aucun backup trouvé dans $BackupTarget"
    } else {
        Add-OK "$($VersionLines.Count) version(s) de backup trouvée(s)"

        # 3. Vérifier l'âge du backup le plus récent
        $LatestLine = $VersionLines | Select-Object -Last 1
        if ($LatestLine -match "Backup time:\s+(.+)") {
            $LatestDate = [datetime]::Parse($Matches[1].Trim())
            $AgeHours = [math]::Round(((Get-Date) - $LatestDate).TotalHours, 1)
```

```
            if ($AgeHours -gt $MaxAgeHours) {
                Add-Issue "Dernier backup trop ancien : $AgeHours heures (max : $MaxAgeHours h)"
            } else {
                Add-OK "Dernier backup récent : $AgeHours heures ($('{0:dd/MM/yyyy HH:mm}' -f $La
            }
        }
    }

    # 4. Vérifier la taille du répertoire de backup
    $BackupSize = (Get-ChildItem $BackupTarget -Recurse -ErrorAction SilentlyContinue |
                   Measure-Object -Property Length -Sum).Sum
    $BackupSizeGB = [math]::Round($BackupSize / 1GB, 2)

    if ($BackupSizeGB -lt $MinSizeGB) {
        Add-Issue "Taille backup suspecte : $BackupSizeGB Go (minimum attendu : $MinSizeGB Go)"
    } else {
        Add-OK "Taille backup cohérente : $BackupSizeGB Go"
    }
}

# 5. Vérifier les Event IDs backup récents dans les 24h
$Since = (Get-Date).AddHours(-24)
$BackupEvents = Get-WinEvent -FilterHashtable @{
    LogName = 'Microsoft-Windows-Backup'
    StartTime = $Since
    Id = @(517, 518)
} -ErrorAction SilentlyContinue

$SuccessCount = ($BackupEvents | Where-Object { $_.Id -eq 517 }).Count
$FailureCount = ($BackupEvents | Where-Object { $_.Id -eq 518 }).Count

if ($FailureCount -gt 0) { Add-Issue "$FailureCount échec(s) de backup dans les 24h (Event ID 518
elseif ($SuccessCount -gt 0) { Add-OK "$SuccessCount sauvegarde(s) réussie(s) dans les 24h (Event
else { Add-Issue "Aucun Event ID 517/518 trouvé dans les 24h — backup peut-être non exécuté" }

# Rapport final
$ReportText = $Report -join "`n"
Write-Host $ReportText

if ($Errors.Count -gt 0) {
    $Body = "RAPPORT DE VALIDATION BACKUP DC - $($env:COMPUTERNAME)`n`nANOMALIES DÉTECTÉES :`n$($
    Send-MailMessage -SmtpServer $SmtpServer -From "backup-dc@entreprise.fr" `
        -To $AlertEmail -Subject "[ALERTE] Backup DC - $($Errors.Count) anomalie(s) sur $($env:CO
        -Body $Body -Encoding UTF8
```

```
    exit 1
}

Write-Host "`nValidation OK - aucune anomalie détectée"
exit 0
```

Fréquence et planning des tests

Type de test	Fréquence recommandée	Durée estimée	Périmètre
Validation automatique (script)	Quotidienne	5 min	Existence, âge, taille backup
Test restauration objet AD (Recycle Bin)	Mensuelle	30 min	Création/suppression/restauration user test
Test restauration DC complet (lab)	Trimestrielle	4-8h	Restauration System State en environnement isolé
Test Forest Recovery complet	Annuelle	1-2 jours	Simulation ransomware, reconstruction forêt

Conformité NIS 2 et DORA : Exigences Backup AD en France

NIS 2 Article 21§2.c : plan de continuité

La directive NIS 2 (Network and Information Security Directive 2), transposée en droit français en 2024 et applicable aux entités essentielles et importantes, impose à l'article 21§2.c des "**plans de continuité des activités, tels que la gestion des sauvegardes et la reprise des activités**". Pour les organisations dont Active Directory est critique (soit la quasi-totalité des entreprises de plus de 50 personnes), cela signifie concrètement :

Politique de sauvegarde AD documentée avec RTO/RPO définis et approuvés par la direction

Procédures de restauration formalisées et à jour (au moins annuellement)

Preuves de test des procédures de recovery (compte-rendu de test, date, résultat)

Gestion des risques documentée incluant la perte du DC comme scénario

Notification ANSSI dans les 24h en cas d'incident significatif affectant AD

DORA Article 12 : ICT Backup pour le secteur financier

Le règlement DORA (Digital Operational Resilience Act), applicable depuis janvier 2025 aux établissements financiers européens, impose à l'article 12 des exigences encore plus précises sur les sauvegardes ICT :

Sauvegardes "**sécurisées et redondantes**" stockées dans un emplacement physique distinct

Tests de restauration "**au moins annuels**" — mais les superviseurs français (ACPR) recommandent semestriels

RTO définis contractuellement pour les fonctions critiques (paiement, trading, etc.)

Traçabilité complète : chaque opération de backup/restore doit être journalisée et archivée 5 ans

Rapport de résilience opérationnelle annuel incluant les résultats des tests de recovery

Documentation et preuves d'audit

Pour un audit NIS 2 ou DORA, préparer les éléments suivants :

```
 INVENTAIRE DE PREUVES AUDIT BACKUP AD
=====================================
1. Politique de sauvegarde signée (PBA – Policy Backup Active Directory)
   - Version actuelle + historique des révisions
   - RTO/RPO définis et approuvés

2. Logs de sauvegarde (12 derniers mois minimum)
   - Logs WSB : C:\Windows\Logs\WindowsServerBackup\
   - Event ID 517/518 exportés depuis l'Observateur d'événements
   - Logs Azure Backup depuis le portail Recovery Services

3. Compte-rendus de tests de restauration
   - Date du test, DC testé, durée, résultat, observations
   - Signature du responsable technique et du RSSI

4. Inventaire des sauvegardes actives
   - Localisation physique et cloud de chaque backup
   - Politique de rétention et date d'expiration
   - Mécanisme d'immutabilité en place

5. Plan de Forest Recovery documenté
   - Procédure pas à pas, rôles et responsabilités
   - Contacts d'astreinte, coordonnées Microsoft Support
```

Questions fréquentes sur le backup Active Directory

Quelle est la différence entre une sauvegarde System State et une sauvegarde BMR (Bare Metal Recovery) pour un DC ?

La sauvegarde System State inclut uniquement les composants système critiques (NTDS.dit, SYSVOL, Registre, BCD) et permet de restaurer les rôles AD DS sur un OS Windows Server déjà installé ou en mode DSRM. La sauvegarde BMR (Bare Metal Recovery), en plus du System State, inclut l'intégralité des volumes système et permet de restaurer le serveur sur un matériel vide ou différent sans réinstallation préalable. Pour les DC virtuels sur Hyper-V ou VMware, le

snapshot VM peut remplacer le BMR mais ne remplace pas le backup System State pour les restaurations d'objets AD.

Peut-on utiliser un snapshot VMware ou Hyper-V comme seule sauvegarde d'un contrôleur de domaine ?

Non — les snapshots hyperviseur ne sont pas un remplacement valide des sauvegardes System State. Les snapshots VM ne sont pas cohérents avec l'état de la base NTDS en fonctionnement (risque de journal de transaction NTDS incohérent), ne permettent pas la restauration authoritative d'objets AD supprimés, et sont stockés sur le même espace de stockage que la VM (vulnérables au même ransomware). Ils peuvent être utilisés *en complément* comme mécanisme de recovery rapide sur la même infrastructure, mais le backup System State vers un stockage distant reste obligatoire.

Quelle est la durée de rétention minimale recommandée pour les sauvegardes AD ?

Microsoft recommande une rétention minimale de 60 jours pour les sauvegardes Active Directory, car certains incidents (corruption lente, suppression d'objets non détectée immédiatement) peuvent ne pas être détectés avant plusieurs semaines. Pour la conformité NIS 2, une rétention de 6 mois est recommandée. Pour DORA, 1 an avec archivage des logs pendant 5 ans. La durée de vie par défaut des objets tombstone (180 jours) est également un repère : un backup de moins de 180 jours permet toujours une restauration authoritative sans IFM.

Comment vérifier que mon backup AD est vraiment utilisable avant un incident ?

La vérification complète implique : (1) exécuter le script de validation automatique quotidiennement pour confirmer l'existence et l'âge du backup ; (2) mensuellemen, tester la restauration d'un utilisateur de test supprimé via la Recycle Bin ou wbadmin dans l'environnement de lab ; (3) trimestriellement, réaliser une restauration complète du System State sur un DC de test isolé et vérifier la réplication, les GPO, les tickets Kerberos. Sans test réel en environnement isolé, aucun backup ne peut être considéré comme fiable.

Que faire si la Corbeille Active Directory n'est pas activée et qu'une OU critique a été supprimée ?

Sans Recycle Bin, les objets supprimés deviennent des "tombstone objects" qui ne conservent que quelques attributs (objectGUID, sAMAccountName) pendant 180 jours. La procédure est : (1) démarrer en DSRM le DC le plus récemment sauvegardé ; (2) restaurer le System State (restauration non-authoritative) ; (3) utiliser ntdsutil en mode authoritative restore pour marquer l'OU et ses objets comme authoritative ; (4) redémarrer et laisser la réplication propager les objets restaurés vers tous les DC. Cette procédure est perturbatrice — elle peut écraser des changements légitimes survenus entre le backup et la suppression. Activer la Recycle Bin immédiatement après résolution de l'incident.

À RETENIR

À retenir

Règle 3-2-1-1 obligatoire : 3 copies, 2 médias, 1 hors-site, 1 immuable offline — sans copie immuable offline, une attaque ransomware peut détruire toutes vos sauvegardes accessibles depuis le réseau.

System State = minimum absolu : chaque DC doit avoir une sauvegarde quotidienne du System State (NTDS.dit + SYSVOL + Registre) via WSB ou Azure Backup, avec alertes sur les Event IDs 517 et 518.

Active Directory Recycle Bin à activer maintenant : cette fonctionnalité gratuite, disponible depuis WS 2008 R2, permet de récupérer des objets supprimés en moins de 5 minutes — ne pas l'activer est une faute technique inexcusable.

Tester trimestriellement : un backup non testé est un backup dont vous ne connaissez pas la valeur. La restauration réelle dans un environnement isolé est la seule façon de valider que vos procédures fonctionnent avant un vrai incident.

NIS 2 et DORA exigent des preuves : documenter chaque sauvegarde, chaque test, chaque procédure de recovery avec signature et archivage — les auditeurs de l'ANSSI et de l'ACPR demandent ces preuves lors des contrôles.

Références et documentation

Microsoft Learn — Sécurité Windows Server

ANSSI — Guide de sécurisation Active Directory

MITRE ATT&CK — Techniques Active Directory