NTDSUTIL : Guide Complet pour l'Administration Active Directory 2026

NTDSUTIL : maîtrisez toutes les commandes, snapshots VSS, metadata cleanup, rôles FSMO et détection des attaques T1003.003 sur Active Directory.

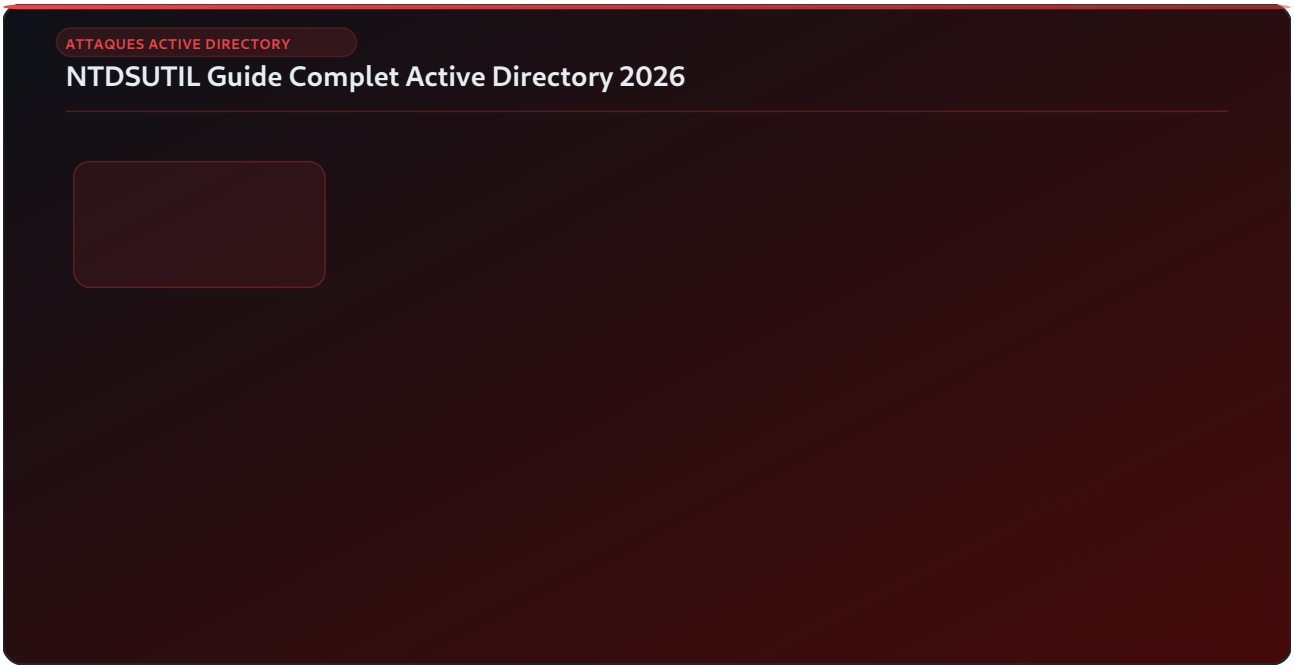
📋 EN BREF

En bref

- NTDSUTIL est l'outil d'administration natif Windows pour gérer la base de données Active Directory (NTDS.dit), les rôles FSMO et les instantanés VSS.
- Il permet la sauvegarde et restauration offline de l'annuaire, le nettoyage des métadonnées de contrôleurs de domaine orphelins et le transfert/saisie des rôles FSMO.
- La commande `ifm create` est largement exploitée par les attaquants pour extraire les hachages de mots de passe (T1003.003 MITRE ATT&CK) — son usage doit être audité en permanence.
- Les Event IDs 325, 326, 327 permettent de tracer chaque opération NTDS ; une règle Sigma et une supervision Wazuh suffisent à détecter les usages anormaux.
- La conformité NIS 2 impose aux entités françaises importantes et essentielles de journaliser, surveiller et contrôler l'accès à cet outil hautement sensible.

Dans les grandes organisations françaises, Paris et les métropoles régionales concentrent des environnements Active Directory parfois vieux de vingt ans, bâtis autour de milliers d'objets, de domaines imbriqués et d'une dette technique considérable. Les RSSI et administrateurs système

qui en ont la charge font face à des opérations de maintenance délicates : retirer un contrôleur de domaine défaillant sans casser la réplication, transférer les rôles FSMO avant une migration vers Windows Server 2025, ou restaurer l'annuaire après un ransomware. Dans tous ces scénarios, NTDSUTIL est l'outil natif incontournable — fourni par Microsoft, présent sur chaque contrôleur de domaine depuis Windows 2000, et pourtant redouté car sa maîtrise est insuffisamment documentée en français. Ce guide exhaustif couvre l'intégralité des commandes NTDSUTIL, leur contexte d'usage légitime, leur détournement possible par des attaquants, et les mesures de détection alignées sur la directive NIS 2 et le référentiel MITRE ATT&CK. Que vous prépariez un plan de reprise d'activité, un audit de sécurité Active Directory ou simplement une migration planifiée, vous trouverez ici chaque procédure, chaque exemple interactif et chaque signal de détection dont vous avez besoin.



NTDSUTIL (*NT Directory Services Utility*) est un outil en ligne de commande intégré à Windows Server depuis la version 2000. Il s'appuie directement sur la bibliothèque **NTDS.dit** — la base de données Extensible Storage Engine (ESE) qui stocke l'intégralité de l'annuaire Active

Directory : comptes utilisateurs, groupes, politiques de groupe, hachages de mots de passe (NTLM et LM), tickets Kerberos et relations d'approbation inter-domaines.

Microsoft le positionne comme un outil de *dernier recours* pour les opérations que l'interface graphique Active Directory ne peut pas accomplir : nettoyage de métadonnées après une panne matérielle grave, maintenance offline de la base NTDS, transfert forcé de rôles FSMO. Cette nature même — accès direct à l'annuaire, hors réplication, hors journalisation standard — en fait aussi l'outil de prédilection des équipes Red Team et des groupes APT lors d'attaques sur l'identité.

Historique et évolution

Introduit avec Windows 2000 Server, NTDSUTIL a peu changé visuellement, mais son périmètre de commandes s'est étendu à chaque version de Windows Server. Windows Server 2008 R2 a ajouté la gestion des instantanés VSS (*snapshot*). Windows Server 2012 a introduit le sous-menu **IFM** (*Install From Media*) pour le déploiement de nouveaux DC sans répliquer l'intégralité de l'annuaire sur le réseau. Windows Server 2019 et 2022 ont consolidé la gestion des *Lightweight Directory Services* (AD LDS). La version fournie avec Windows Server 2025 est compatible avec les groupes de sécurité basés sur le chiffrement post-quantique expérimental, mais le noyau de l'outil reste identique.

Place dans l'écosystème Active Directory

NTDSUTIL interagit avec quatre composants critiques :

NTDS.dit — la base ESE de l'annuaire, typiquement dans `C:\Windows\NTDS\`

Volume Shadow Copy Service (VSS) — pour créer des instantanés cohérents sans arrêter AD

FRS / DFSR — la réplication des stratégies de groupe (SYSVOL), dont il peut forcer la resynchronisation

RID Master, PDC Emulator, Infrastructure Master, Schema Master, Domain Naming Master — les cinq rôles FSMO qu'il peut transférer ou saisir

Cas d'usage légitimes vs usage attaquant

Contexte	Usage légitime	Détournement attaquant
Sauvegarde	Snapshot VSS + copie NTDS.dit pour PRA	Extraction NTDS.dit offline → Secretsdump, Mimikatz
Metadata cleanup	Suppression d'un DC orphelin après panne	Rarement détourné, mais masque parfois une suppression délibérée
FSMO transfer/ seize	Migration planifiée, DR	Seize non autorisé pour prendre le contrôle du domaine
IFM create	Déploiement d'un nouveau DC sans réplication réseau	Exfiltration discrète de l'annuaire complet (T1003.003)
Set DSRM password	Remise à zéro du mot de passe DSRM oublié	Persistance via DSRM pour accès offline ultérieur

Commandes NTDSUTIL Essentielles — Référence Complète

NTDSUTIL fonctionne en mode interactif : chaque sous-menu expose ses propres commandes, accessibles par saisie partielle (autocomplétion). Le tableau ci-dessous recense toutes les commandes principales, leur syntaxe, leur contexte d'usage et leur niveau de risque sécurité.

⚡ **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.

Commande / Sous-menu	Description	Contexte d'usage	Risque sécurité
`activate instance ntds`	Sélectionne l'instance AD DS active (nécessaire avant toute opération sur la base)	Pré-requis systématique	Faible
`files` → `integrity`	Vérifie l'intégrité de la base NTDS.dit (lecture seule, mode offline)	Diagnostic après crash	Faible
`files` → `recover`	Rejoue le journal ESE pour récupérer une base incohérente	Après arrêt brutal du DC	Moyen (modifications irréversibles)
`files` → `compact to <path>`	Compacte la base NTDS.dit (défragmentation offline)	Maintenance semestrielle, réduction de taille	Moyen
`files` → `move DB to <path>`	Déplace physiquement NTDS.dit vers un autre volume	Migration de stockage	Moyen
`files` → `move logs to <path>`	Déplace les journaux de transaction ESE	Migration de stockage	Faible
`metadata cleanup`	Supprime les références à un DC qui n'existe plus dans l'annuaire	DC orphelin après panne matérielle	Élevé (modifications AD permanentes)
`roles` → `connections` → `connect to server <DC>`	Établit une connexion LDAP vers un DC cible pour les opérations FSMO	Pré-requis transfer/ seize	Faible
`roles` → `transfer PDC`	Transfère gracieusement le rôle PDC Emulator au DC connecté	Migration planifiée, maintenance	Élevé (impact domaine entier)
`roles` → `seize PDC`	Saisie forcée du rôle PDC (DC source inaccessible)	DR, panne critique	Critique
`roles` → `transfer RID master`	Transfère le rôle RID Master (attribution des SID)	Migration	Élevé
`roles` → `transfer schema master`	Transfère le rôle Schema Master (modifications du schéma AD)	Avant extension de schéma (Exchange, Lync)	Critique
`roles` → `transfer domain naming master`	Transfère le rôle Domain Naming Master	Avant ajout/ suppression de domaine	Élevé
`roles` → `transfer infrastructure master`	Transfère le rôle Infrastructure Master	Migration, restructuration AD	Élevé
`snapshot` → `create`			

Commande / Sous-menu	Description	Contexte d'usage	Risque sécurité
	Crée un instantané VSS de la base NTDS (à chaud, sans arrêter AD)	Sauvegarde, forensique, IFM	Élevé (copie complète de l'annuaire)
`snapshot` → `mount <GUID>`	Monte l'instantané sous un chemin accessible pour copie	Extraction de la base pour analyse offline	Critique
`snapshot` → `unmount <GUID>`	Démonte l'instantané	Nettoyage post-opération	Faible
`snapshot` → `delete <GUID>`	Supprime définitivement l'instantané	Nettoyage	Faible
`ifm` → `create full <path>`	Crée un média d'installation IFM complet (NTDS.dit + SYSVOL)	Déploiement nouveau DC	Critique (exfiltration possible)
`ifm` → `create rodc <path>`	Crée un IFM pour RODC (Read-Only DC, sans secrets de comptes sensibles)	Déploiement RODC site distant	Élevé
`security account management` → `connect to server`	Connexion pour réinitialiser le mot de passe DSRM	Récupération accès DSRM oublié	Critique (persistance possible)
`domain management`	Gestion des partitions de l'annuaire et des serveurs de catalogue global	Restructuration multi-domaine	Élevé
`ldap policies`	Affiche et modifie les politiques LDAP (timeouts, taille max des résultats)	Optimisation performance, hardening	Moyen
`popups %on|off%`	Active/désactive les confirmations interactives (pour scripting)	Automatisation	Faible
`quit` / `q`	Quitte le sous-menu courant ou NTDSUTIL	Navigation	Sans objet

Sauvegarde et Restauration de la Base NTDS.dit

La sauvegarde de NTDS.dit via NTDSUTIL repose sur le **Volume Shadow Copy Service (VSS)**, qui permet de créer une copie cohérente de la base pendant que le service Active

Directory Domain Services est en cours d'exécution. Cette approche est préférable à un arrêt du service AD, qui perturberait l'authentification de toute l'infrastructure.

Procédure complète de snapshot NTDS

Exemple de session interactive annotée (à exécuter sur le DC cible, en tant qu'administrateur du domaine) :

```
 C:\> ntdsutil
ntdsutil: snapshot
snapshot: activate instance ntds
Active instance set to "ntds".
snapshot: create
Creating snapshot...
Snapshot set {a3f1c2d4-5e6f-7890-abcd-ef1234567890} generated successfully.

snapshot: list all
1: 2026-06-05 08:42:17 {a3f1c2d4-5e6f-7890-abcd-ef1234567890}

snapshot: mount {a3f1c2d4-5e6f-7890-abcd-ef1234567890}
Snapshot {a3f1c2d4-5e6f-7890-abcd-ef1234567890} mounted as C:\$SNAP_202606050842_VOLUMEC$\

snapshot: quit
ntdsutil: quit

:: Copie de NTDS.dit et de la ruche SYSTEM (nécessaire pour déchiffrer les hachages)
C:\> copy "C:\$SNAP_202606050842_VOLUMEC$\Windows\NTDS\ntds.dit" D:\Backup\ntds.dit
C:\> reg save HKLM\SYSTEM D:\Backup\SYSTEM

:: Démontage de l'instantané
C:\> ntdsutil snapshot "unmount {a3f1c2d4-5e6f-7890-abcd-ef1234567890}" quit quit
C:\> ntdsutil snapshot "delete {a3f1c2d4-5e6f-7890-abcd-ef1234567890}" quit quit
```

Pourquoi la ruche SYSTEM est-elle indispensable ? La base NTDS.dit est chiffrée avec une clé dérivée de la *Boot Key* (ou SYSKEY), stockée dans la ruche SYSTEM du registre. Sans cette ruche, un attaquant — ou un administrateur en mode restauration — ne peut pas déchiffrer les hachages. C'est pourquoi toute politique de sauvegarde sérieuse doit protéger ces deux fichiers avec le même niveau de rigueur.

Script PowerShell : sauvegarde automatisée et vérification santé NTDS

```
 # Backup-NTDS.ps1 — Sauvegarde NTDS.dit via snapshot VSS
# Nécessite : droits Domain Admin, Windows Server 2012+
# Usage : .\Backup-NTDS.ps1 -Destination D:\ADBackup

param(
    [Parameter(Mandatory=$true)]
    [string]$Destination,
    [int]$RetentionDays = 30
)

$ErrorActionPreference = "Stop"
$LogFile = "$Destination\backup-$(Get-Date -Format 'yyyyMMdd-HHmm').log"

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

# Vérification des prérequis
Write-Log "Démarrage de la sauvegarde NTDS"
if (-not (Test-Path $Destination)) {
    New-Item -ItemType Directory -Path $Destination | Out-Null
    Write-Log "Répertoire de sauvegarde créé : $Destination"
}

# Test de connectivité au service NTDS
$ntdsService = Get-Service -Name "NTDS" -ErrorAction SilentlyContinue
if ($ntdsService.Status -ne "Running") {
    Write-Log "Service NTDS non démarré — sauvegarde impossible en mode online" "ERROR"
    exit 1
}

# Vérification intégrité avant sauvegarde (mode DISM)
Write-Log "Vérification de l'intégrité de la base NTDS..."
$ntdsDitPath = (Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters")."DSA D
if (-not (Test-Path $ntdsDitPath)) {
    Write-Log "NTDS.dit introuvable à : $ntdsDitPath" "ERROR"
    exit 1
}
Write-Log "NTDS.dit localisé : $ntdsDitPath ($(
    [math]::Round((Get-Item $ntdsDitPath).Length / 1MB, 1)
) Mo)"
```

```
# Création du snapshot VSS via NTDSUTIL
Write-Log "Création du snapshot VSS..."
$ntdsutilScript = @"
snapshot
activate instance ntds
create
list all
quit
quit
"@
$snapshotOutput = $ntdsutilScript | ntdsutil 2>&1 | Out-String
$guid = [regex]::Match($snapshotOutput, '\{[0-9A-Fa-f\-]{36}\}').Value

if (-not $guid) {
    Write-Log "Impossible d'extraire le GUID du snapshot" "ERROR"
    Write-Log $snapshotOutput "DEBUG"
    exit 1
}
Write-Log "Snapshot créé : $guid"

# Montage et copie
$mountOutput = "snapshot`nactivate instance ntds`nmount $guid`nquit`nquit`n" | ntdsutil 2>&1 | Out
$mountPath = [regex]::Match($mountOutput, 'C:\\\$SNAP_[^\s]+').Value

if (-not $mountPath) {
    Write-Log "Montage du snapshot échoué" "ERROR"
    exit 1
}

$backupFolder = "$Destination\$(Get-Date -Format 'yyyyMMdd-HHmmss')"
New-Item -ItemType Directory -Path $backupFolder | Out-Null

Copy-Item "$mountPath\Windows\NTDS\ntds.dit" "$backupFolder\ntds.dit"
reg save HKLM\SYSTEM "$backupFolder\SYSTEM" /y | Out-Null
Write-Log "Fichiers copiés dans $backupFolder"

# Démontage et suppression du snapshot
"snapshot`nactivate instance ntds`nunmount $guid`ndelete $guid`nquit`nquit`n" | ntdsutil 2>&1 | Ou
Write-Log "Snapshot démonté et supprimé"

# Nettoyage des sauvegardes anciennes
Get-ChildItem -Path $Destination -Directory |
    Where-Object { $_.CreationTime -lt (Get-Date).AddDays(-$RetentionDays) } |
    ForEach-Object {
        Remove-Item $_.FullName -Recurse -Force
        Write-Log "Ancienne sauvegarde supprimée : $($_.Name)"
```

```
    }

# Calcul du hash SHA256 pour vérification d'intégrité
$hash = (Get-FileHash "$backupFolder\ntds.dit" -Algorithm SHA256).Hash
Set-Content -Path "$backupFolder\ntds.dit.sha256" -Value $hash
Write-Log "Hash SHA256 NTDS.dit : $hash"
Write-Log "Sauvegarde terminée avec succès"
```

Metadata Cleanup — Supprimer un DC Orphelin

Lorsqu'un contrôleur de domaine est physiquement détruit (incendie, panne matérielle irréparable, suppression accidentelle d'une VM) sans avoir été proprement démis de ses fonctions, ses entrées persistent dans l'annuaire Active Directory. Ces *métadonnées orphelines* provoquent des erreurs de réplication, des timeouts d'authentification et des alertes DCDIAG incessantes. La procédure **metadata cleanup** de NTDSUTIL supprime chirurgicalement ces références.

Pour aller plus loin sur la surveillance des événements de réplication, consultez notre guide sur la surveillance des événements Windows sur les contrôleurs de domaine.

Quand utiliser metadata cleanup ?

DC irrécupérable après panne matérielle grave (sans possibilité de redémarrer le service AD)

VM supprimée par erreur sans démission préalable

DC victime d'un ransomware — voir notre article sur la récupération de forêt Active Directory après ransomware

Démantèlement d'un site distant avec DC local

Procédure metadata cleanup complète

```
 C:\> ntdsutil
ntdsutil: metadata cleanup
metadata cleanup: connections
server connections: connect to server DC-PARIS-01     :: DC survivant et sain
Binding to DC-PARIS-01 ...
Connected to DC-PARIS-01 using credentials of locally logged on user.
server connections: quit

metadata cleanup: select operation target
select operation target: list domains
Found 1 domain(s)
0 - DC=corp,DC=example,DC=fr
select operation target: select domain 0
No current site
Domain - DC=corp,DC=example,DC=fr

select operation target: list sites
Found 3 site(s)
0 - CN=Default-First-Site-Name,CN=Sites,...
1 - CN=SITE-BORDEAUX,CN=Sites,...
2 - CN=SITE-LYON,CN=Sites,...
select operation target: select site 1             :: Site du DC orphelin

select operation target: list servers in site
Found 2 server(s)
0 - CN=DC-BORDEAUX-01,CN=Servers,...
1 - CN=DC-BORDEAUX-02,CN=Servers,...
select operation target: select server 0           :: DC orphelin à nettoyer

select operation target: quit

metadata cleanup: remove selected server
Transferring / Seizing FSMO roles held by server...
Removing server DC-BORDEAUX-01 from site SITE-BORDEAUX...
DC-BORDEAUX-01 has been successfully removed from Active Directory.

metadata cleanup: quit
ntdsutil: quit
```

Après l'opération, vérifiez avec `repadmin /showrepl` et `dcdiag /test:replications` que les erreurs liées au DC supprimé ont disparu. Supprimez également manuellement l'objet DNS du DC orphelin dans la console DNS.

Alternative : GUI Active Directory Sites and Services

Depuis Windows Server 2012 R2, il est possible d'effectuer un metadata cleanup directement depuis la console Active Directory Sites and Services : clic droit sur l'objet Serveur orphelin → *Delete*. Windows effectue automatiquement le cleanup des métadonnées. Cette méthode est moins risquée pour les administrateurs peu familiers avec NTDSUTIL, mais ne fonctionne que si le DC orphelin n'est plus joignable.

Transfert et Saisie des Rôles FSMO

Les cinq rôles FSMO (*Flexible Single Master Operation*) sont des fonctions critiques du domaine et de la forêt Active Directory, hébergées chacune sur un seul DC à la fois. Lors d'une migration vers Windows Server 2025 ou d'un plan de reprise d'activité, leur gestion via NTDSUTIL est souvent indispensable.

Différence entre Transfer et Seize

Opération	Condition	DC source requis ?	Risque
Transfer	DC source fonctionnel, réplication opérationnelle	Oui — handshake gracieux	Faible
Seize	DC source inaccessible (panne, DR)	Non — prise de contrôle forcée	Élevé — ne jamais remettre en ligne l'ancien DC après seize

Procédure de transfert (PDC Emulator)

```
 C:\> ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server DC-PARIS-02     :: DC cible (receveur du rôle)
Connected to DC-PARIS-02 ...
server connections: quit

fsmo maintenance: transfer PDC
Server "DC-PARIS-02" knows about 5 roles
Schema - CN=NTDS Settings,CN=DC-PARIS-01,...
Domain Naming Master - CN=NTDS Settings,CN=DC-PARIS-01,...
PDC - CN=NTDS Settings,CN=DC-PARIS-01,...
RID - CN=NTDS Settings,CN=DC-PARIS-01,...
Infrastructure - CN=NTDS Settings,CN=DC-PARIS-01,...
Transferring PDC role to server "DC-PARIS-02"
Transferred PDC role to server "DC-PARIS-02"
fsmo maintenance: quit
ntdsutil: quit
```

Procédure de saisie (Seize RID Master en DR)

```
 ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server DC-BACKUP-01
server connections: quit
fsmo maintenance: seize RID master
Attempting safe transfer of RID FSMO before seizure.
FSMO transfer was NOT successful - aborting seizure.
Would you like to attempt a force seizure? (yes/no) yes
Seizing RID master role...
Successfully seized RID master role.
fsmo maintenance: quit
ntdsutil: quit
```

Vérification post-opération

```
 C:\> netdom query fsmo
Schema master          DC-PARIS-01.corp.example.fr
Domain naming master   DC-PARIS-01.corp.example.fr
PDC                    DC-PARIS-02.corp.example.fr   <-- Transféré
RID pool manager       DC-BACKUP-01.corp.example.fr  <-- Saisi
Infrastructure master  DC-PARIS-01.corp.example.fr
The command completed successfully.
```

Consultez également notre guide sur les Authentication Silos Windows Server 2025 pour sécuriser les comptes liés aux rôles FSMO après toute opération de transfert.

NTDSUTIL et la Sécurité : Risques et Détection

Du point de vue d'un attaquant, NTDSUTIL est un outil rêvé : il est signé par Microsoft (*Living off the Land Binary*, ou LoLBin), présent nativement sur chaque contrôleur de domaine, et permet d'extraire l'intégralité des secrets d'authentification du domaine sans déclencher les antivirus traditionnels.

Technique T1003.003 : OS Credential Dumping — NTDS

Le chemin d'attaque le plus courant :

L'attaquant compromet un compte Domain Admin (ou délégation excessive)

Il exécute `ntdsutil ifm create full C:\Temp\IFM` sur le DC

Il exfiltre le dossier `C:\Temp\IFM\Active Directory\ntds.dit` et la ruche SYSTEM

Offline (sur sa propre machine), il utilise `impacket-secretsdump` ou Mimikatz pour extraire tous les hachages NTLM

Il réalise des attaques Pass-the-Hash ou craque les mots de passe offline

Cette technique a été utilisée par les groupes APT28 (Fancy Bear), Lazarus, et de nombreux opérateurs de ransomware comme LockBit avant sa disruption.

Event IDs critiques liés à NTDSUTIL

Event ID	Source	Description	Criticité
325	NTDS (ActiveDirectory_DomainService)	La base de données a été créée (backup/ IFM)	Critique
326	NTDS	La base de données a été restaurée depuis une sauvegarde	Critique
327	NTDS	La base de données a été détachée (snapshot démonté)	Élevé
1000	NTDS General	Démarrage du service Active Directory Domain Services	Moyen
1168	NTDS Internal	Erreur interne NTDS (corruption potentielle)	Élevé
2087	DNS Client	Échec de résolution DNS d'un DC — peut indiquer un DC orphelin	Moyen
4662	Security	Opération effectuée sur un objet AD (réplication incluant les secrets)	Critique (si réplication non autorisée)
7036	System (SCM)	Changement d'état du service NTDS	Moyen

Règle Sigma pour détecter NTDSUTIL IFM (exfiltration)

```
 title: NTDSUTIL IFM — Création de Média d'Installation Suspect
id: f2e3a4b5-6c7d-8e9f-0a1b-2c3d4e5f6a7b
status: stable
description: Détecte l'exécution de ntdsutil avec le paramètre IFM (Install From Media),
  technique utilisée pour extraire NTDS.dit et exfiltrer les hachages Active Directory.
  Correspond à MITRE ATT&CK T1003.003.
author: Ayinedjimi Consultants — Équipe SOC
date: 2026-06-05
references:
  - https://attack.mitre.org/techniques/T1003/003/
  - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-ds-ntdsutil
tags:
  - attack.credential_access
  - attack.t1003.003
  - attack.defense_evasion
logsource:
  category: process_creation
  product: windows
detection:
  selection_main:
    Image|endswith: '\ntdsutil.exe'
  selection_ifm:
    CommandLine|contains:
      - 'ifm'
      - 'install from media'
      - 'create full'
      - 'create rodc'
  condition: selection_main and selection_ifm
falsepositives:
  - Déploiement légitime d'un nouveau contrôleur de domaine (IFM autorisé)
  - Opérations de sauvegarde documentées et planifiées
level: high
fields:
  - User
  - CommandLine
  - ParentImage
  - ParentCommandLine
  - ComputerName
```

Détection avec Wazuh

Pour les équipes SOC françaises utilisant Wazuh comme SIEM open-source, ajoutez cette règle dans `/var/ossec/etc/rules/local_rules.xml` :

```
<group name="windows,active_directory,credential_access,">

  <rule id="100500" level="14">
    <if_group>windows</if_group>
    <field name="win.eventdata.image" type="pcre2">(?i)ntdsutil\.exe</field>
    <field name="win.eventdata.commandLine" type="pcre2">(?i)(ifm|install\s+from\s+media|create\s-
    <description>NTDSUTIL IFM détecté — risque d'exfiltration NTDS.dit (T1003.003)</description>
    <options>no_full_log</options>
    <group>credential_access,pci_dss_10.2.7,gdpr_IV_35.7.d,hipaa_164.312.b,nist_800_53_AU.14,tsc_C
  </rule>

  <rule id="100501" level="12">
    <if_group>windows</if_group>
    <field name="win.system.eventID">^325$</field>
    <field name="win.system.channel">Directory Service</field>
    <description>Event 325 NTDS — Création/sauvegarde base AD (snapshot ou IFM)</description>
    <group>credential_access,</group>
  </rule>

  <rule id="100502" level="12">
    <if_group>windows</if_group>
    <field name="win.system.eventID">^326$</field>
    <field name="win.system.channel">Directory Service</field>
    <description>Event 326 NTDS — Restauration base AD (impact domaine entier possible)</descripti
    <group>impact,</group>
  </rule>

</group>
```

Pour une stratégie de surveillance complète, consultez notre guide sur l'audit des groupes privilégiés Active Directory — la détection NTDSUTIL s'inscrit dans une démarche plus large de contrôle des accès à privilèges.

Install From Media (IFM) : Déploiement Sécurisé de DC

La fonctionnalité IFM permet de déployer un nouveau contrôleur de domaine en utilisant une copie locale de l'annuaire, sans avoir à répliquer plusieurs gigaoctets via le réseau WAN. C'est particulièrement utile pour les agences ou filiales françaises avec une connexion réseau limitée.

Création du média IFM

```
 :: Sur le DC source (doit être sain et répliqué)
C:\> ntdsutil
ntdsutil: ifm
ifm: create full C:\IFM-Media

Snapshot set {b7c8d9e0-1f2a-3b4c-5d6e-7f8a9b0c1d2e} generated successfully.
Snapshot mounted as C:\$SNAP_202606050900_VOLUMEC$\

Initializing NTDS...
Copying registry files...
Copying NTDS.dit...
Creating IFM media at C:\IFM-Media

IFM media created successfully in C:\IFM-Media

ifm: quit
ntdsutil: quit
```

Le dossier `C:\IFM-Media` contient :

`Active Directory\ntds.dit` — la base de l'annuaire

`registry\SYSTEM` — la ruche SYSTEM (boot key)

`SYSVOL\` — les stratégies de groupe et scripts de connexion

Sécurisation du média IFM

Le média IFM contient **l'intégralité des secrets du domaine**. Les bonnes pratiques de sécurisation sont impératives :

Chiffrement en transit : Transférez le média uniquement via un canal chiffré (BitLocker To Go sur clé USB, partage SMB chiffré, VPN dédié)

Délai minimal : Le média IFM ne doit pas rester accessible plus de 24h — définissez une procédure de destruction sécurisée dès la promotion du nouveau DC terminée

Traçabilité : Journalisez l'opération (qui, quand, quel DC source, quel DC cible) dans votre SIEM

IFM RODC préféré : Si le nouveau DC est un RODC (Read-Only), utilisez `ifm create rodc` — la base générée ne contient pas les hachages des comptes sensibles exclus de la réplication RODC. Voir notre guide sur les RODC sécurisés sous Windows Server 2025

Destruction sécurisée : `cipher /w:C:\IFM-Media` pour écraser les données avant suppression sur les volumes non-SSD

```
 # PowerShell : vérification et destruction sécurisée du média IFM
$ifmPath = "C:\IFM-Media"

# Vérification que le nouveau DC est bien promu avant destruction
$dcCheck = Get-ADDomainController -Filter * | Where-Object { $_.Name -eq "DC-NOUVEAU-01" }
if ($dcCheck) {
    Write-Host "[OK] DC-NOUVEAU-01 promu — destruction du média IFM en cours..."
    # Écrasement sécurisé (fichiers non-SSD)
    cipher /w:$ifmPath
    Remove-Item -Path $ifmPath -Recurse -Force
    Write-Host "[OK] Média IFM détruit"
} else {
    Write-Warning "DC-NOUVEAU-01 non trouvé — vérifiez la promotion avant de détruire le média"
}
```

Meilleures Pratiques et Conformité NIS 2

La directive NIS 2, transposée en droit français depuis octobre 2024, impose aux entités essentielles et importantes (OIV, opérateurs de services essentiels, administrations de l'État, grandes entreprises françaises) de démontrer leur capacité à détecter, contenir et analyser les incidents affectant leurs services d'identité. Active Directory étant le cœur névralgique de l'authentification, NTDSUTIL doit faire l'objet d'une politique d'usage stricte.

Contrôle d'accès

Principe du moindre privilège : Seuls les administrateurs de domaine (groupe *Domain Admins*) et les opérateurs de sauvegarde (*Backup Operators*) doivent être autorisés à exécuter NTDSUTIL. Utilisez les Authentication Silos pour restreindre ces comptes aux DC uniquement.

Stations d'administration dédiées (PAW) : Les opérations NTDSUTIL ne doivent être lancées que depuis des *Privileged Access Workstations* — jamais depuis un poste utilisateur.

MFA sur les comptes administrateurs : Bien que NTDSUTIL ne supporte pas directement le MFA, l'accès aux DC doit passer par une solution PAM (CyberArk, Delinea, HashiCorp Vault) avec session enregistrée.

Journalisation et supervision

Activez la stratégie d'audit **Object Access** et **Detailed Directory Service Replication** via GPO sur tous les DC

Centralisez les logs des Event IDs 325, 326, 327, 4662 dans votre SIEM avec rétention de 12 mois minimum (exigence NIS 2)

Configurez des alertes en temps réel sur l'Event 325 et sur l'exécution de `ntdsutil.exe` depuis un processus parent inhabituel

Audits trimestriels recommandés

```
 # Script PowerShell : audit des opérations NTDS des 90 derniers jours
$startDate = (Get-Date).AddDays(-90)
$eventIDs = @(325, 326, 327)

Get-WinEvent -ComputerName (Get-ADDomainController -Filter *).Name -FilterHashtable @{
    LogName = 'Directory Service'
    Id = $eventIDs
    StartTime = $startDate
} | Select-Object TimeCreated, Id, MachineName, Message |
    Sort-Object TimeCreated -Descending |
    Export-Csv -Path "C:\Audit\NTDS-Audit-$(Get-Date -Format 'yyyyMMdd').csv" -NoTypeInformation

Write-Host "Rapport généré dans C:\Audit\"
```

Checklist conformité NIS 2 pour NTDSUTIL

Politique d'usage documentée et approuvée par le RSSI

Liste blanche des comptes autorisés à exécuter NTDSUTIL

Journalisation centralisée des Event IDs 325/326/327 avec rétention 12 mois

Alerte SIEM sur tout IFM non planifié

Audit trimestriel des opérations NTDS exporté et signé

Procédure de destruction sécurisée des médias IFM documentée

Test de restauration NTDS.dit annuel intégré au PRA/PCA

Questions fréquentes sur NTDSUTIL

Faut-il arrêter Active Directory pour exécuter NTDSUTIL ?

Non, pour la plupart des opérations. La création de snapshots VSS (`ntdsutil snapshot create`) et la génération d'un média IFM (`ntdsutil ifm create`) s'effectuent sans interruption du service

AD. En revanche, les opérations sur les fichiers en mode offline (`files integrity` , `files compact`) nécessitent de démarrer le DC en *DSRM* (Directory Services Restore Mode), ce qui interrompt l'authentification sur ce DC pendant toute l'opération.

Quelle est la différence entre IFM complet et IFM RODC ?

L'IFM complet (`create full`) inclut la totalité de NTDS.dit avec tous les hachages de mots de passe — c'est le plus sensible. L'IFM RODC (`create rodc`) génère une base épurée des secrets des comptes qui n'ont pas été répliqués sur le RODC (comptes membres du groupe *Denied RODC Password Replication Group*). Pour les déploiements en zone peu sécurisée (agence, succursale, cloud public), privilégiez toujours l'IFM RODC.

Comment savoir si NTDSUTIL a été utilisé sur mes DC récemment ?

Interrogez le journal *Directory Service* sur tous vos DC pour les Event IDs 325, 326 et 327. En PowerShell : `Get-WinEvent -FilterHashtable @{LogName='Directory Service'; Id=325,326,327} | Select TimeCreated, MachineName, Message` . Complétez avec une recherche dans les logs de sécurité sur l'exécution du processus `ntdsutil.exe` (Event ID 4688 si l'audit de création de processus est activé).

Le seize FSMO est-il réversible ?

Non, pas directement. Une fois un rôle FSMO saisi (*seize*), l'ancien DC porteur de ce rôle **ne doit jamais être remis en ligne** dans le domaine — cela créerait un conflit de rôles aux conséquences imprévisibles (réplication inconsistante, corruption potentielle de la base). Si l'ancien DC doit revenir en production, il faut d'abord le rétrograder (*dcpromo /forceremoval*) avant de le rejoindre au domaine en tant que simple membre.

NTDSUTIL peut-il réparer une base NTDS.dit corrompue ?

NTDSUTIL offre deux niveaux de réparation : `files recover` rejoue les journaux de transaction ESE pour corriger une incohérence légère (arrêt brutal), et `files integrity` détecte les

corruptions mais ne les corrige pas. Pour une corruption profonde, Microsoft recommande de restaurer depuis la dernière sauvegarde saine. L'outil `esentutl` (Engine Utility for ESE) offre des options de réparation plus avancées mais avec un risque de perte de données.

À RETENIR

À retenir

NTDSUTIL est un outil à double tranchant : indispensable pour l'administration AD, il est aussi l'un des vecteurs d'exfiltration de credentials les plus discrets (LoLBin signé Microsoft, T1003.003).

La commande `ifm create full` est la plus dangereuse : elle produit une copie complète de l'annuaire incluant tous les hachages. Elle doit déclencher une alerte SIEM immédiate si elle n'est pas planifiée et documentée.

Les Event IDs 325, 326 et 327 sont vos meilleurs alliés pour détecter toute opération NTDS non autorisée — ils doivent être collectés sur tous les DC et analysés en temps réel.

Ne jamais remettre en ligne un DC après un seize FSMO — cette erreur peut corrompre irrémédiablement la base Active Directory et provoquer une panne d'authentification majeure.

La conformité NIS 2 exige une politique d'usage formalisée pour NTDSUTIL, une journalisation centralisée de 12 mois et des audits trimestriels — documentez chaque opération avec les éléments *qui*, *quand*, *pourquoi*.

Références et documentation

Microsoft Learn — Sécurité Windows Server

ANSSI — Guide de sécurisation Active Directory

MITRE ATT&CK — Techniques Active Directory

