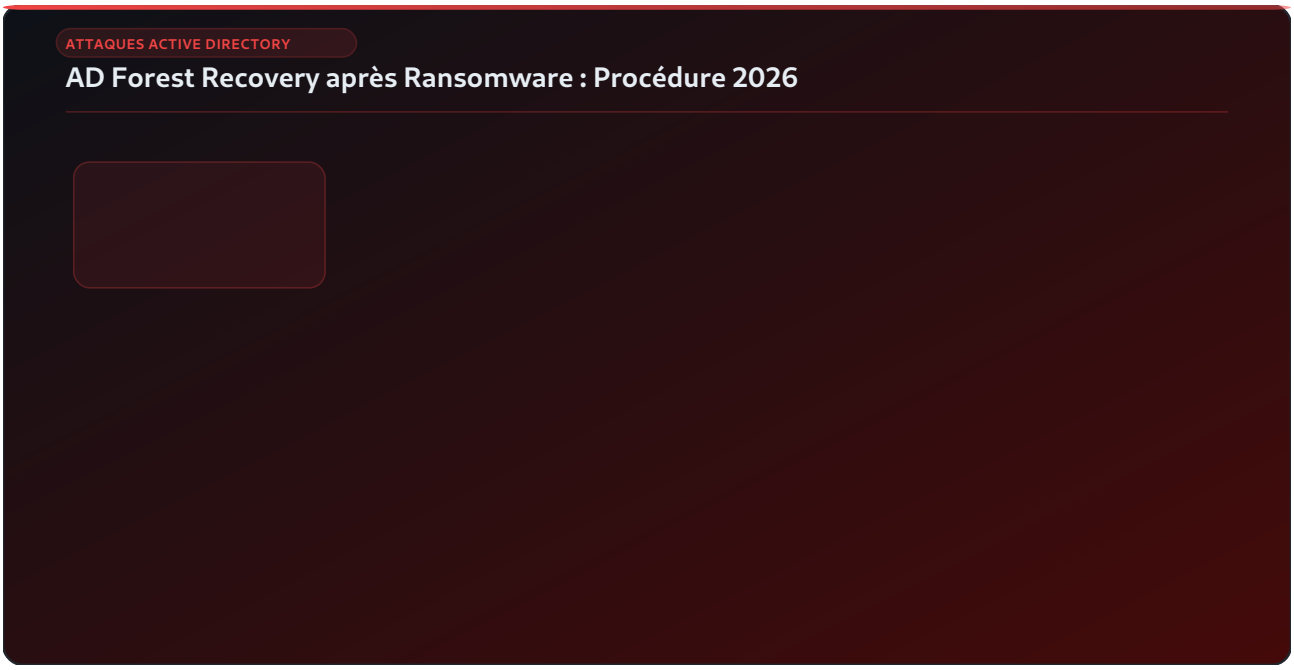
Active Directory Forest Recovery après Ransomware : Guide Complet

> Restaurez Active Directory après un ransomware : procédure forest recovery complète, isoler les DC, NTDSUTIL, reconstruction du domaine. Guide ANSSI 2026.

Quand un ransomware frappe les contrôleurs de domaine, la survie de l'entreprise dépend d'une décision prise dans les premières heures : restaurer partiellement ou déclencher un forest recovery complet. Les groupes Conti, LockBit et BlackBasta ont fait de l'Active Directory leur cible prioritaire depuis 2022 : compromettre le PDC Emulator, puis déployer le ransomware via GPO à l'ensemble du parc en moins de quatre heures. Le forest recovery n'est pas une simple restauration de sauvegarde. C'est une procédure chirurgicale documentée par Microsoft, qui exige un ordre strict, la neutralisation de toutes les réplications entre DC compromis, la seizure des rôles FSMO, la rotation obligatoire du compte KRBTGT, et la re-validation de chaque trust inter-domaines. Sans ce protocole, un DC encore infecté peut re-compromettre l'ensemble du domaine en quelques minutes après le redémarrage. Ce guide détaille chaque phase, les commandes NTDSUTIL critiques, les pièges à éviter, et fournit une timeline réaliste selon la taille de votre annuaire. Il s'appuie sur les recommandations ANSSI (PA-060), les retours d'expérience de réponse à incident en secteur santé et industrie en France, et la procédure officielle Microsoft Active Directory Forest Recovery.



La première décision conditionne toutes les suivantes. Elle doit être prise sur la base d'une analyse technique rigoureuse, pas sous la pression émotionnelle de l'incident.

Critères pour un forest recovery complet

Le forest recovery complet est obligatoire dans les cas suivants : tous les DC sont potentiellement compromis ou chiffrés ; l'heure de compromission initiale est inconnue ou antérieure à la dernière sauvegarde ; des artefacts de mouvement latéral (Golden Ticket, DCSync) ont été détectés dans les logs ; les sauvegardes AD ont elles-mêmes été chiffrées ou supprimées ; la confiance dans l'intégrité de NTDS.dit ne peut pas être établie.

Critères pour une restauration partielle

La restauration partielle est envisageable si : au moins un DC n'a pas été touché par le ransomware (isolé physiquement ou en VLAN séparé) ; ce DC possède des sauvegardes System

State récentes (moins de 24h avant l'incident) ; l'heure de compromission est connue et postérieure à la dernière sauvegarde ; aucun indicateur de compromission de compte Tier0 n'a été détecté avant l'heure de compromission.

RTO/RPO selon le scénario

Forest recovery complet : RTO de 8 à 48 heures selon la taille, RPO = dernière sauvegarde AD valide. Restauration partielle : RTO de 2 à 8 heures, RPO potentiellement meilleur si un DC survivant est récent. Dans les deux cas, le RPO ne peut pas être inférieur à l'heure de compromission : toute donnée créée après l'intrusion initiale est suspecte.

Phase 0 — Isolation immédiate sans éteindre les DC

L'erreur la plus fréquente en réponse à incident est d'éteindre immédiatement les serveurs compromis. Cette réaction instinctive détruit les preuves en mémoire (credentials, processus actifs, connexions réseau) et peut aggraver la situation si le ransomware dispose d'un mécanisme de failsafe déclenché à l'arrêt.

> ⚡ **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.

Procédure d'isolation réseau sans extinction

Déconnectez physiquement les câbles réseau des DC compromis ou désactivez leurs ports switch en VLAN isolation. Conservez l'alimentation électrique. Si des DC sont virtualisés sous VMware ou Hyper-V, suspendez la VM (suspend/pause, pas shutdown) : cela préserve la mémoire vive pour l'analyse forensique ultérieure.

Sur les DC survivants potentiellement non touchés, désactivez immédiatement la réplication AD entrante pour éviter de recevoir des objets modifiés par l'attaquant :

```
 # Sur chaque DC potentiellement sain — désactiver réplication entrante
repadmin /options DCsurvivant01 +DISABLE_INBOUND_REPL

# Vérifier l'état de réplication avant isolation
repadmin /showrepl

# Vérifier les DC et leur état (identifie lesquels répondent encore)
nltest /dclist:votre-domaine.local
```

Snapshots VSS et sauvegardes d'urgence

Avant toute intervention, déclenchez des snapshots VSS de tous les volumes des DC encore accessibles, ainsi qu'une sauvegarde Veeam ou Windows Server Backup en mode System State si l'infrastructure de sauvegarde n'est pas compromise. Ces snapshots constituent votre filet de sécurité si la restauration doit être annulée.

```
 # Sauvegarde System State d'un DC survivant (Windows Server Backup)
wbadmin start systemstatebackup -backuptarget:\\NAS-BACKUP\AD-Emergency -quiet

# Vérification du System State sauvegardé
wbadmin get versions -backuptarget:\\NAS-BACKUP\AD-Emergency
```

Documentez l'heure exacte de chaque action : ce journal sera utilisé pour l'analyse forensique et le rapport d'incident.

Phase 1 — Évaluation des dommages AD

L'évaluation doit répondre à trois questions avant de choisir la procédure de restauration : quels DC sont compromis ? Les sauvegardes AD sont-elles intactes et exploitables ? NTDS.dit est-il lisible sur les DC survivants ?

Identification des DC compromis

```
 # Lister tous les DC du domaine
Get-ADDomainController -Filter * | Select-Object Name, Site, IPv4Address, OperationMasterRoles, I

# Vérifier la connectivité de chaque DC
foreach ($dc in (Get-ADDomainController -Filter *).HostName) {
    $ping = Test-Connection -ComputerName $dc -Count 1 -Quiet
    Write-Host "$dc : $(if($ping){'ACCESSIBLE'}else{'INACCESSIBLE'})"
}

# Vérifier les événements ransomware (chiffrement de masse)
Get-EventLog -LogName System -ComputerName DCsurvivant01 -EntryType Error,Warning -Newest 100 |
    Where-Object {$_.Source -match "VSS|Backup|Shadow"}
```

Vérification de l'intégrité de NTDS.dit

```
 # Sur un DC survivant — vérifier l'intégrité de la base AD
ntdsutil "activate instance ntds" "files" "integrity" quit quit

# Vérifier la taille cohérente de NTDS.dit (alerte si < 10 MB ou > 50% variation)
Get-Item "C:\Windows\NTDS\ntds.dit" | Select-Object Length, LastWriteTime
```

Validation des sauvegardes AD

Identifiez la dernière sauvegarde AD valide antérieure à l'heure de compromission. Vérifiez que le System State backup inclut bien SYSVOL, NTDS.dit, les clés de registre AD, et les certificats.

Un backup System State sans SYSVOL ne permet pas de restaurer le DC en contrôleur de domaine opérationnel.

Phase 2 — Forest Recovery Complet (procédure Microsoft)

La procédure de forest recovery complète est documentée par Microsoft dans *AD DS Design Guide — Forest Recovery*. Elle exige un ordre strict pour éviter les conflits de réplication et les objets zombies.

Ordre de restauration : PDC Emulator en premier

Le PDC Emulator du domaine racine de la forêt doit être restauré en premier. C'est lui qui sera la source d'autorité pour tous les autres DC. Restaurez-le depuis la sauvegarde System State sur un serveur physiquement isolé du réseau de production.

```
 # Restauration du System State (exécuté depuis Windows Recovery Environment)
wbadmin start systemstaterecovery -version:<VERSION> -backuptarget:\\NAS-BACKUP\AD-Emergency -qui

# Après restauration, démarrer en DSRM (Directory Services Restore Mode)
# Modifier le registre pour forcer DSRM au prochain boot
bcdedit /set safeboot dsrepair

# Après restauration NTDS, retirer le flag DSRM
bcdedit /deletevalue safeboot
```

Nettoyage metadata des DC morts

Après restauration du PDC Emulator, supprimez les objets de tous les DC qui ne seront pas restaurés (DC compromis définitivement abandonnés). Cette étape évite les objets orphelins et les erreurs de réplication.

```
# NTDSUTIL — metadata cleanup d'un DC mort
ntdsutil "metadata cleanup" "connections" "connect to server DCsurvivant01" quit "select operatio

# Vérification : le DC mort ne doit plus apparaître
Get-ADDomainController -Filter * | Select-Object Name
repadmin /showrepl
```

Seizure des rôles FSMO

Si le DC portant les rôles FSMO est compromis et ne peut pas être restauré proprement, saisissez (seizure) les rôles sur le DC survivant restauré. La seizure est une opération forcée, à distinguer du transfer qui est gracieux. Elle ne doit être utilisée que si le DC d'origine est définitivement perdu.

```
# Seizure FSMO après perte PDC
Move-ADDirectoryServerOperationMasterRole -Identity "DCsurvivant01" -OperationMasterRole PDCEmula

# Vérification des rôles FSMO
netdom query fsmo
```

Réparation DNS et SYSVOL

Après restauration des DC, le service DNS et SYSVOL doivent être vérifiés et éventuellement réparés. Des DC mal restaurés peuvent avoir des enregistrements DNS obsolètes ou un SYSVOL désynchronisé.

```
# Forcer la synchronisation SYSVOL (sur le PDC restauré)
net stop netlogon && net start netlogon

# Vérifier la santé DNS
dcdiag /test:dns /v

# Vérifier la réplication AD globale
repadmin /replsummary
repadmin /showrepl * /csv > replication-report.csv
```

Phase 3 — Restauration Partielle (DC survivant mais compromis)

Quand un ou plusieurs DC ont survécu et sont intègres mais que les autres sont compromis, la restauration partielle consiste à promouvoir de nouveaux DC depuis les DC sains, transférer les FSMO, puis démissionner et nettoyer les DC compromis.

Promotion d'un nouveau DC depuis le DC sain

```
 # Sur le nouveau serveur membre propre — promotion en DC supplémentaire
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
Import-Module ADDSDeployment

Install-ADDSDomainController `
    -DomainName "votre-domaine.local" `
    -SiteName "Default-First-Site-Name" `
    -InstallDns:$true `
    -CreateDnsDelegation:$false `
    -NoRebootOnCompletion:$false `
    -Force:$true
```

Transfert gracieux des FSMO

```
 # Transfert FSMO (gracieux — depuis l'ancien DC encore accessible)
Move-ADDirectoryServerOperationMasterRole -Identity "NouveauDC01" `
    -OperationMasterRole PDCEmulator,RIDMaster,InfrastructureMaster,DomainNamingMaster,SchemaMast

# Vérification
netdom query fsmo
```

Démission et nettoyage des DC compromis

```
 # Sur le DC compromis (si accessible) — démission propre
Uninstall-ADDSDomainController -LocalAdministratorPassword (ConvertTo-SecureString "TempP@ss2026!

# Si inaccessible — nettoyage metadata depuis un DC sain
ntdsutil "metadata cleanup" "connections" "connect to server NouveauDC01" quit "select operation
```

NTDSUTIL — Commandes clés pour le forest recovery

NTDSUTIL est l'outil d'administration en ligne de commande de la base de données Active Directory. Sa maîtrise est indispensable pour toute opération de forest recovery.

Référentiel des commandes critiques

```
 # 1. Snapshot de NTDS.dit (copie cohérente à chaud)
ntdsutil "activate instance ntds" "snapshot" "create" quit quit

# 2. Installation From Media (IFM) — créer une source pour promotion DC sans réseau
ntdsutil "activate instance ntds" "ifm" "create full C:\IFM" quit quit

# 3. Metadata cleanup — supprimer un DC mort de l'annuaire
ntdsutil "metadata cleanup" "connections" "connect to server <DC_SAIN>" quit "select operation ta

# 4. Authoritative restore — forcer la restauration d'un sous-arbre OU
ntdsutil "authoritative restore" "restore subtree ou=utilisateurs,dc=domaine,dc=local" quit quit

# 5. Vérification intégrité base
ntdsutil "activate instance ntds" "files" "integrity" quit quit

# 6. Compaction de la base (maintenance post-recovery)
# Exécuté en mode DSRM uniquement
ntdsutil "activate instance ntds" "files" "compact to C:\NTDScompact" quit quit
```

Rotation obligatoire des secrets post-ransomware

Après tout incident de compromission AD, la rotation des secrets Tier0 est non négociable. Un attaquant ayant eu accès à un DC dispose potentiellement du hash NTLM de tous les comptes, du ticket Kerberos KRBTGT, et des secrets des comptes de service. Sans rotation complète, le risque de re-compromission par Golden Ticket reste entier, même après forest recovery.

Rotation KRBTGT obligatoire x2

Le compte KRBTGT est la clé de voûte de Kerberos. Un attaquant ayant volé son hash peut forger des Golden Tickets valides pour 10 ans. La rotation doit être effectuée **deux fois**, avec un délai minimum égal à la durée de vie maximale des tickets Kerberos (par défaut 10 heures) entre les deux rotations.

```
 # Rotation KRBTGT x2 (obligatoire post-compromission)
$currentPwd = (Get-ADUser krbtgt -Properties PasswordLastSet).PasswordLastSet
Write-Host "KRBTGT dernière rotation : $currentPwd"

# Rotation 1
Set-ADAccountPassword -Identity krbtgt -Reset -NewPassword (ConvertTo-SecureString -AsPlainText (
Write-Host "Rotation 1 effectuée à $(Get-Date) — attendre réplication AD (15-30 min minimum)"

# ATTENDRE : vérifier réplication avant rotation 2
repadmin /syncall /AdeP

# Rotation 2 (après réplication confirmée et délai Kerberos)
Set-ADAccountPassword -Identity krbtgt -Reset -NewPassword (ConvertTo-SecureString -AsPlainText (
Write-Host "Rotation 2 effectuée à $(Get-Date)"

# Vérification
(Get-ADUser krbtgt -Properties PasswordLastSet).PasswordLastSet
```

Rotation des comptes admin Tier0

```
 # Lister tous les membres du groupe Domain Admins et Enterprise Admins
$tier0Groups = @("Domain Admins","Enterprise Admins","Schema Admins","Administrators")
foreach ($g in $tier0Groups) {
    $members = Get-ADGroupMember -Identity $g -Recursive | Select-Object SamAccountName,Name
    Write-Host "=== $g ==="
    $members | ForEach-Object { Write-Host $_.SamAccountName }
}

# Forcer la rotation de mot de passe pour tous les comptes Tier0
Get-ADGroupMember "Domain Admins" -Recursive | ForEach-Object {
    Set-ADUser $_ -ChangePasswordAtLogon $true
    Write-Host "Rotation forcée : $($_.SamAccountName)"
}

# Révoquer toutes les sessions Kerberos actives (nécessite redémarrage des services ou reboot)
klist purge
```

Reconstruction de la confiance et validation post-recovery

Après le forest recovery, plusieurs éléments doivent être re-validés avant de remettre l'annuaire en production.

Re-validation des trusts inter-domaines

```
 # Vérifier tous les trusts existants
Get-ADTrust -Filter * | Select-Object Name, TrustType, TrustDirection, TrustAttributes

# Tester la connectivité des trusts
netdom verify <TRUST_DOMAIN> /domain:votre-domaine.local /ud:admin /pd:*

# Réinitialiser le trust si nécessaire
netdom trust <TRUST_DOMAIN> /domain:votre-domaine.local /reset /ud:admin /pd:*
```

Re-création des comptes de service

Tous les comptes de service (SQL Server, IIS, applications métier) dont le mot de passe était connu d'un administrateur compromis doivent être recréés ou avoir leur mot de passe changé. Profitez de cette opportunité pour migrer vers des Managed Service Accounts (gMSA) qui gèrent automatiquement la rotation.

```
 # Créer un gMSA pour remplacer un compte de service classique
New-ADServiceAccount -Name "svc-sqlprod" -DNSHostName "sqlprod.domaine.local" `
    -PrincipalsAllowedToRetrieveManagedPassword "SQL-Servers-Group" `
    -ManagedPasswordIntervalInDays 30

# Installer le gMSA sur le serveur cible
Install-ADServiceAccount -Identity "svc-sqlprod"
Test-ADServiceAccount -Identity "svc-sqlprod"
```

Audit post-incident obligatoire

Avant remise en production, un audit complet des permissions AD doit être effectué. Consultez notre guide sur le modèle de tiering AD et la segmentation des privilèges et notre article sur la sécurisation complète d'Active Directory.

```
 # DCDiag complet sur tous les DC restaurés
dcdiag /test:replications /test:fsmo /test:dns /test:netlogons /v

# Vérification santé globale AD
Get-ADForest | Select-Object Name, ForestMode, GlobalCatalogs, Sites
Get-ADDomain | Select-Object Name, DomainMode, PDCEmulator, RIDMaster, InfrastructureMaster

# Netlogon events (vérification authentifications)
Get-EventLog -LogName System -Source NETLOGON -Newest 50
```

Timeline réaliste du forest recovery

La durée d'un forest recovery dépend directement de la taille de l'annuaire Active Directory, de la qualité des sauvegardes disponibles, et du nombre de DC à restaurer. Ces estimations sont basées sur des retours terrain et s'entendent hors temps de préparation (isolation, forensique) :

Taille AD	Objets	DC	RTO estimé	Points de risque
Très petite	~100	2	2-3 heures	Disponibilité sauvegardes
Petite	1 000	3-4	4-6 heures	DNS, trusts
Moyenne	10 000	5-10	8-12 heures	Réplication SYSVOL, GPO
Grande	50 000	10-20	16-24 heures	Sites multiples, trusts complexes
Très grande	100 000+	20+	24-48 heures	Multi-forêts, fédération IdP

Ces délais supposent des sauvegardes System State récentes et fonctionnelles. Sans sauvegarde exploitable, la reconstruction from scratch multiplie le RTO par 3 à 5. La protection de NTDS.dit est un prérequis absolu — consultez notre article sur la protection de NTDS.dit contre l'extraction.

Cas terrain France — Retours d'expérience ransomware

Secteur santé — CHU régional (2024)

Un CHU régional a subi une attaque BlackBasta qui a chiffré 4 des 5 DC du domaine principal. Le DC survivant — un DC secondaire en VLAN isolé dédié aux sauvegardes — avait une réplication désactivée en dehors des heures de nuit. Le forest recovery a pu s'appuyer sur ce DC et des sauvegardes System State de J-1. RTO effectif : 14 heures pour le domaine principal, 48 heures pour la remise en production complète de 1 200 postes. Leçon clé : l'existence d'un DC hors-ligne ou en isolation réseau stricte a été déterminante. La rotation KRBTGT et de 47 comptes de service a pris 3 heures supplémentaires.

Secteur industrie — Équipementier automobile (2025)

Attaque LockBit 3.0 ciblant le domaine racine d'une forêt multi-domaines. Les DC du domaine racine ont été chiffrés mais deux DC des domaines enfants ont survécu. Le choix a été fait de reconstruire uniquement le domaine racine et de re-établir les trusts. RTO : 22 heures. La difficulté principale a été la re-création des trusts entre le domaine racine reconstruit et les domaines enfants survivants, ainsi que la re-synchronisation de 3 applications SSO qui s'appuyaient sur des comptes de service du domaine racine.

Prévention : sauvegardes AD dédiées et test annuel

La meilleure réponse à un forest recovery est de ne jamais avoir à l'exécuter en urgence. Trois mesures préventives sont critiques : des sauvegardes System State quotidiennes sur au moins un DC par site, conservées hors ligne ou en air gap ; un DC en lecture seule (RODC) en isolation réseau partielle, non exposé aux GPO de déploiement ; et un **test annuel de forest recovery** documenté, exécuté en environnement de test. Le guide de durcissement Windows Server 2025 détaille les pré-requis de sécurité à mettre en place avant qu'un incident se produise. Pour la rotation KRBTGT en conditions normales, consultez notre guide sur la rotation sécurisée du compte KRBTGT par script PowerShell.

Checklist forest recovery en 4 phases

Une stratégie de backup rigoureuse est le prérequis absolu à tout forest recovery. Notre guide Backup et Recovery Active Directory 2026 couvre Windows Server Backup, NTDSUTIL snapshots, Azure Backup et les procédures de restauration authoritative.

À RETENIR

Phase 0 — Isolation (J+0, 0-2h)

Déconnecter les câbles réseau des DC compromis (pas d'extinction)

Suspendre les VM compromises (preserve RAM)

Désactiver la réplication entrante sur les DC potentiellement sains

Déclencher snapshots VSS / Veeam d'urgence

Documenter heure d'isolation et état de chaque DC

Alerter RSSI, DG, CERT interne, éventuellement ANSSI (OIV)

Phase 1 — Évaluation (J+0, 2-4h)

Identifier DC compromis vs survivants

Vérifier intégrité NTDS.dit sur DC survivants

Localiser et valider les sauvegardes System State

Déterminer heure de compromission initiale

Décider : forest recovery complet ou restauration partielle

Phase 2 — Recovery (J+0 à J+2)

Restaurer PDC Emulator en premier (environnement isolé)

Metadata cleanup de tous les DC abandonnés

Seizure ou transfer des rôles FSMO

Vérifier DNS et SYSVOL

Restaurer/promouvoir DC supplémentaires dans l'ordre

Re-établir les trusts inter-domaines

Phase 3 — Hardening post-recovery (J+1 à J+3)

Rotation KRBTGT x2 (avec délai réplication entre les deux)

Rotation de tous les comptes admin Tier0

Re-création / rotation comptes de service (migration gMSA)

DCDiag complet sur tous les DC

Audit des permissions AD et GPO

Test authentification applicatif complet

Rapport d'incident et plan de remédiation

FAQ — Active Directory Forest Recovery après Ransomware

Faut-il reconstruire tout le domaine après un ransomware ?

Pas nécessairement. La décision dépend du nombre de DC compromis et de l'existence de DC sains avec des sauvegardes récentes. Si au moins un DC est intègre et dispose d'une sauvegarde System State valide antérieure à la compromission, une restauration partielle est possible et plus rapide. Le forest recovery complet est obligatoire si tous les DC sont compromis ou si les sauvegardes sont elles-mêmes chiffrées.

Dans quel ordre restaurer les contrôleurs de domaine ?

La procédure Microsoft impose un ordre strict : 1) PDC Emulator du domaine racine de la forêt en premier, en environnement isolé ; 2) nettoyage metadata des DC abandonnés ; 3) seizure des rôles FSMO si nécessaire ; 4) DC Global Catalog supplémentaires du domaine racine ; 5) DC des domaines enfants dans l'ordre hiérarchique. Ne jamais restaurer un DC dans le réseau de production avant que le PDC Emulator soit opérationnel et que la réplication soit contrôlée.

Combien de temps prend un forest recovery complet ?

Pour un Active Directory de taille moyenne (10 000 objets, 5 à 10 DC), comptez 8 à 12 heures pour le domaine principal, et 48 heures pour la remise en production complète incluant la rotation des secrets, la re-validation des applications et les tests d'authentification. Pour les grandes infrastructures (100 000 objets, multi-domaines), le RTO peut dépasser 48 heures. La disponibilité et la fraîcheur des sauvegardes System State est le facteur le plus déterminant.

Pourquoi faut-il changer le mot de passe KRBTGT deux fois ?

Le compte KRBTGT conserve ses deux derniers mots de passe pour permettre la validation des tickets Kerberos en cours de validité pendant la rotation. Lors de la première rotation, l'ancien mot de passe reste valide pour les tickets existants. Ce n'est qu'après la seconde rotation que l'ancien hash est définitivement invalidé. Un attaquant ayant volé le hash initial peut forger des Golden Tickets valides jusqu'à ce que les deux rotations soient effectuées. Le délai entre les deux rotations doit être supérieur à la durée de vie maximale des tickets TGT (10 heures par défaut).

Comment préserver les preuves forensiques avant la restauration ?

Avant toute intervention, preservez la mémoire vive (RAM dump avec WinPmem ou Magnet RAM Capture), les journaux d'événements Windows exportés en EVTX, les logs Sysmon, les logs firewall et proxy, et une image disque des volumes système. Suspendez (ne pas éteindre) les VM compromises pour conserver la RAM. Ces éléments seront nécessaires pour l'analyse forensique, le rapport à l'ANSSI, et éventuellement les procédures judiciaires. La restauration peut attendre 2 à 4 heures pour permettre une collection forensique minimale.

Références et documentation

Microsoft Learn — Sécurité Windows Server

ANSSI — Guide de sécurisation Active Directory

MITRE ATT&CK — Techniques Active Directory

