Mode Opératoire

Sauvegarder l'Active Directory (Backup SystemState)

Code :	MO-AD-006
Version :	1.3
Date :	15 avril 2026
Auteur :	Cédric LEGRAND
Classification :	USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	07/04/2026	Création initiale — première sauvegarde DC1 via VHD
1.1	09/04/2026	Copie directe DC1→NAS via NTLM, automatisation (tâche planifiée), résolution SMB
1.2	14/04/2026	Externalisation des credentials NAS dans `nas.cred` (ACL *SYSTEM+Administrators*), procédure de mise à jour lors d'une rotation MDP NAS
1.3	15/04/2026	Renvois explicites vers MO-AD-002 (rollback krbtgt via DSRM) et MO-AD-008 § 5.5 (mise à jour `nas.cred` après rotation NAS)

1 Objet

Ce mode opératoire décrit la procédure complète de sauvegarde de l'Active Directory du contrôleur de domaine principal (DC1) via un backup **SystemState**, et le transfert de cette sauvegarde vers un stockage externe. Le backup SystemState inclut l'ensemble des composants critiques du contrôleur de domaine :

— Base de données Active Directory (`ntds.dit`)
— Répertoire SYSVOL (stratégies de groupe, scripts d'ouverture de session)
— Registre Windows
— Fichiers de démarrage et partition EFI
— Données des services de certificats
— Base d'enregistrement COM+

⚠ Contexte critique

L'infrastructure BTS SIO ne disposait d'**aucune sauvegarde** de l'Active Directory depuis juin 2022, soit **1 371 jours** sans backup au moment de la rédaction de ce document. Cette procédure a été exécutée pour la première fois le 7 avril 2026.

2 Champ d'application

Public concerné	Enseignants de l'équipe BTS SIO, administrateurs de l'infrastructure pédagogique
Système	DC1 — Srv2022 (`10.0.112.2`), Windows Server 2022
Cible de sauvegarde	NAS Scotty (`10.0.112.5`) ou tout support de stockage réseau/local
Durée estimée	1 heure (backup ∼45 min + copie ∼15 min)
Taille typique	10–15 Go

3 Prérequis

Prérequis

— Fonctionnalité **Windows Server Backup** installée sur DC1
— Accès WinRM ou RDP au contrôleur de domaine
— Compte **Administrateur du domaine**
— Connectivité réseau vers le stockage cible (NAS, partage SMB)
— Pré-checks AD effectués (cf. **MO-AD-005** — Santé de l'Active Directory)
— Espace libre suffisant : ∼20 Go sur `C:` et ∼15 Go sur la cible

Vérifier la santé de l'AD avant toute sauvegarde

Ne **jamais** lancer un backup sans avoir préalablement vérifié la santé de l'Active Directory (MO-AD-005). Sauvegarder un annuaire corrompu ne ferait que pérenniser les problèmes.

4 Procédure

4.1 Vérifier l'installation de Windows Server Backup

Étape 1 — Contrôler la présence de Windows Server Backup

Se connecter à DC1 via WinRM ou RDP, puis exécuter :

```
Get-WindowsFeature Windows-Server-Backup
```

La colonne `Install State` doit indiquer `Installed`. Si la fonctionnalité n'est pas installée, exécuter :

```
Install-WindowsFeature -Name Windows-Server-Backup
```

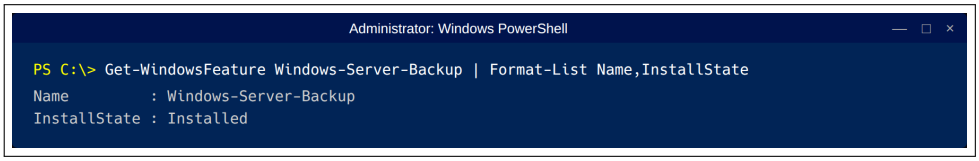

Figure 1 – Vérification de l'installation de Windows Server Backup

Pas de redémarrage

L'installation de Windows Server Backup ne nécessite **aucun redémarrage** du serveur. La fonctionnalité est immédiatement disponible après installation.

4.2 Méthode A — Backup via VHD local (recommandé)

DC1 ne dispose que d'un seul volume (`C:`). Or, `wbadmin` refuse de sauvegarder le SystemState sur le volume source : le volume cible doit être différent du volume sauvegardé. La solution retenue consiste à créer un **disque virtuel VHD** qui se comporte comme un volume séparé, tout en étant physiquement stocké sur `C:`.

Étape 2 — Créer le disque virtuel (VHD)

Ouvrir une invite de commandes élevée ou une session PowerShell, puis lancer `diskpart` :

```
diskpart
```

Dans la console diskpart, exécuter les commandes suivantes pour créer et attacher le VHD :

```
create vdisk file="C:\Backups-AD\backup.vhdx" maximum=20480
   type=expandable
select vdisk file="C:\Backups-AD\backup.vhdx"
attach vdisk
```

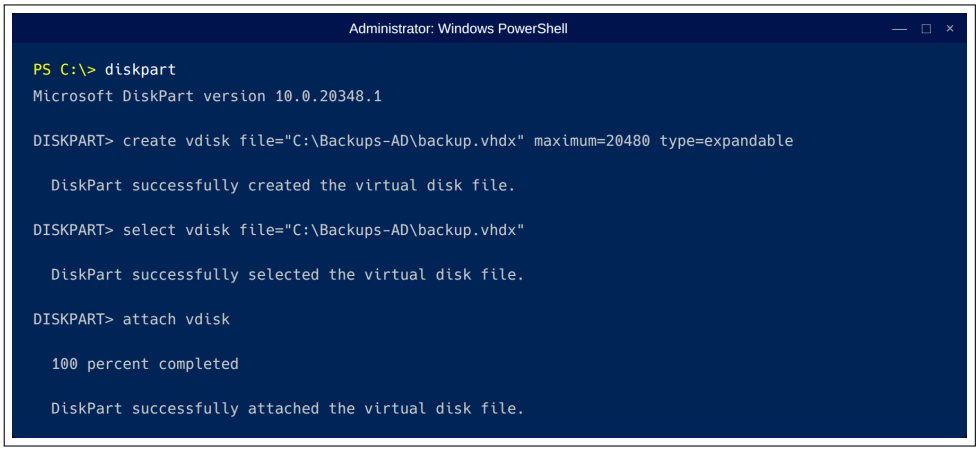

Figure 2 – Création et attachement du disque virtuel VHD

Le disque virtuel est désormais attaché au système comme un disque physique supplémentaire. Il reste à l'initialiser et le formater.

Étape 3 — Initialiser et formater le VHD

Toujours dans diskpart, sélectionner le nouveau disque (généralement Disk 1), le convertir en GPT, créer une partition et la formater en NTFS :

```
select disk 1
convert gpt
create partition primary
format fs=ntfs label="AD-Backup" quick
assign letter=D
```

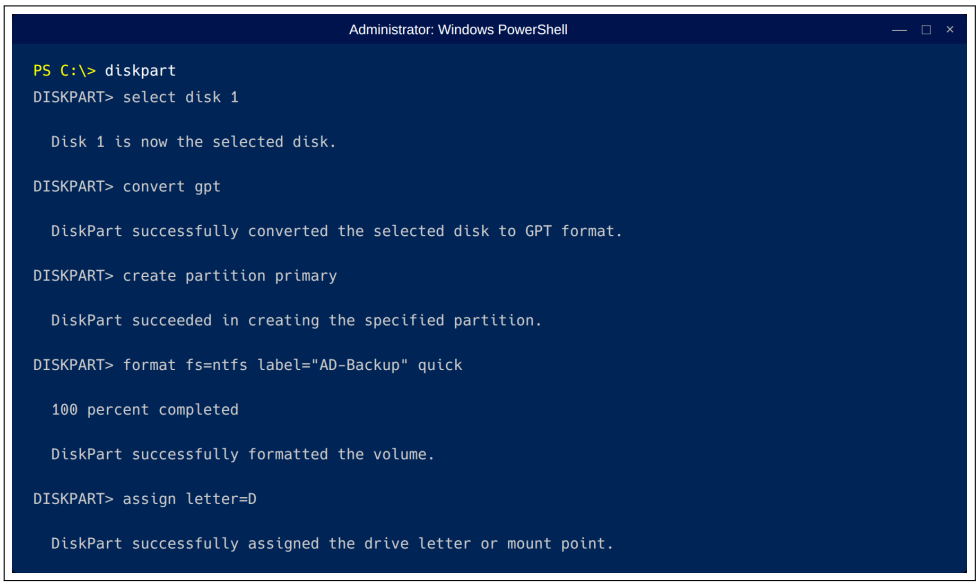

Figure 3 – Initialisation GPT, création de partition et formatage NTFS

Le volume `D:` est maintenant disponible comme cible de sauvegarde. Quitter diskpart :

```
exit
```

Disque dynamique (expandable)

Le paramètre `type=expandable` crée un VHD à taille dynamique : le fichier `.vhdx` n'occupe sur disque que l'espace réellement utilisé par les données, et non la taille maximale déclarée (20 Go). Avant le backup, le fichier ne pèse que quelques Mo.

Étape 4 — Lancer le backup SystemState

Exécuter la commande `wbadmin` pour démarrer la sauvegarde SystemState vers le volume `D:` :

```
wbadmin start systemstatebackup -backupTarget:D: -quiet
```

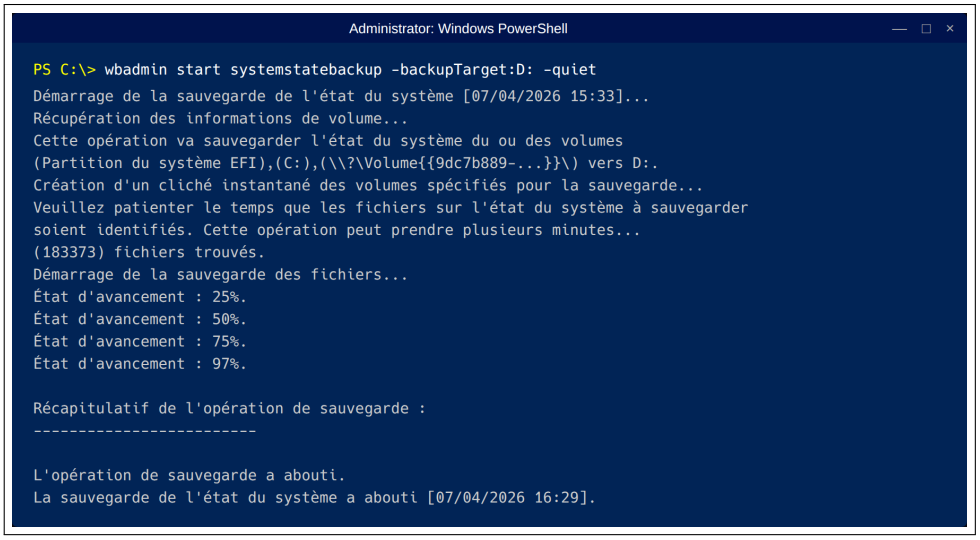

Figure 4 – Exécution du backup SystemState — session complète

Le processus se déroule en plusieurs phases successives :

1. **Identification des volumes** : wbadmin détermine les volumes à inclure dans le SystemState
2. **Création du snapshot VSS** : un *Volume Shadow Copy* est créé pour garantir la cohérence des données
3. **Énumération des fichiers** : inventaire complet des fichiers à sauvegarder (183 373 fichiers lors de la première exécution)
4. **Copie des données** : transfert des fichiers vers le volume cible
5. **Vérification** : contrôle d'intégrité de la sauvegarde

La durée totale est d'environ **45 à 60 minutes** pour la première exécution. Les sauvegardes ultérieures seront plus rapides grâce au mécanisme incrémentiel.

Opération non perturbante

Le backup SystemState est une opération de **lecture**. Il n'interrompt aucun service, ne nécessite aucun redémarrage et ne provoque aucune coupure. Les utilisateurs continuent de travailler normalement pendant la sauvegarde. Le snapshot VSS assure la cohérence des données même si des modifications sont en cours.

Étape 5 — Vérifier le backup

Une fois la sauvegarde terminée, vérifier qu'elle est bien enregistrée :

```
wbadmin get versions
```

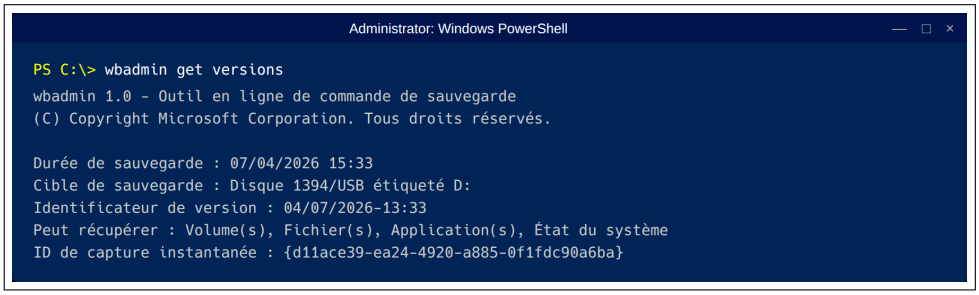

Figure 5 – Versions de sauvegarde disponibles sur DC1

La sortie affiche les informations suivantes :

Champ	Description
`Backup time`	Date et heure de la sauvegarde
`Backup target`	Volume cible utilisé (`D:`)
`Version identifier`	Identifiant unique de la version (nécessaire pour la restauration)
`Can recover`	Types de données récupérables (Application, System State, etc.)

Vérifier que le champ `Can recover` mentionne bien **System State** parmi les éléments récupérables.

Étape 6 — Démonter le VHD

Après vérification du backup, démonter proprement le disque virtuel pour libérer le verrouillage sur le fichier `.vhdx` :

```
diskpart
select vdisk file="C:\Backups-AD\backup.vhdx"
detach vdisk
exit
```

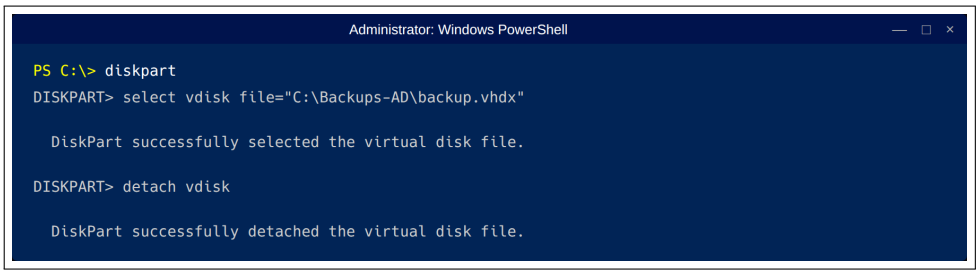

Figure 6 – Détachement du disque virtuel après sauvegarde

Le volume `D:` disparaît du système. Le fichier `C:\Backups-AD\backup.vhdx` contient désormais la totalité de la sauvegarde et peut être copié vers un stockage externe.

4.3 Copier le backup vers le NAS

Le NAS Scotty (QNAP QTS 4.2.6) ne supporte pas l'authentification Kerberos, qui est le mécanisme utilisé par défaut lorsqu'un poste membre du domaine accède à un partage SMB. Le symptôme observé était une erreur 58 lors de toute tentative de connexion depuis DC1. La solution : forcer l'authentification NTLM en spécifiant explicitement les credentials avec `net use /user:`.

Étape 7 — Monter le partage NAS avec authentification NTLM

Depuis une session PowerShell élevée sur DC1, monter le partage du NAS en forçant les credentials locaux :

```
net use X: "\\10.0.112.5\Partage NAS" /user:admin MOT_DE_PASSE
```

Cette commande contourne la négociation Kerberos en fournissant directement un couple login/mot de passe que le NAS peut vérifier en NTLM. Le lecteur `X:` est désormais accessible.

⚠ Credentials en clair

Le mot de passe apparaît en clair dans la commande interactive. Dans le script automatisé (section 4.5), les credentials NAS sont **externalisés** dans le fichier `C:\Backups-AD\nas.cred` dont la procédure de gestion (création, ACL, rotation) est décrite en section 4.6.

Étape 8 — Copier le VHD vers le NAS

Transférer le fichier `backup.vhdx` vers le partage monté :

```
Copy-Item -Path "C:\Backups-AD\backup.vhdx" -Destination "X:\" -Force
```

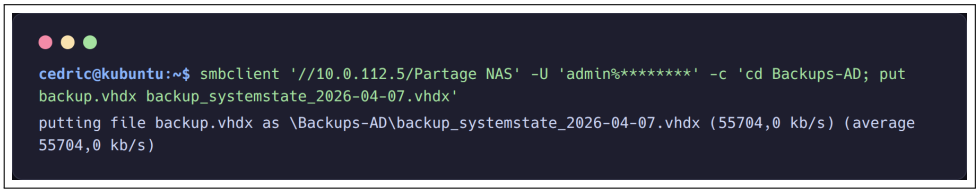

Figure 7 – Copie du VHD vers le NAS via NTLM

Durée du transfert

Le fichier VHD pèse environ 12–13 Go. Sur le réseau local Gigabit, le transfert prend entre 10 et 15 minutes.

Étape 9 — Démonter le partage et vérifier

Après la copie, supprimer le mappage réseau :

```
net use X: /delete
```

Vérifier la présence et la taille du fichier copié :

```
net use X: "\\10.0.112.5\Partage NAS" /user:admin MOT_DE_PASSE
Get-ChildItem X:\backup.vhdx | Select-Object Name, Length, LastWriteTime
net use X: /delete
```

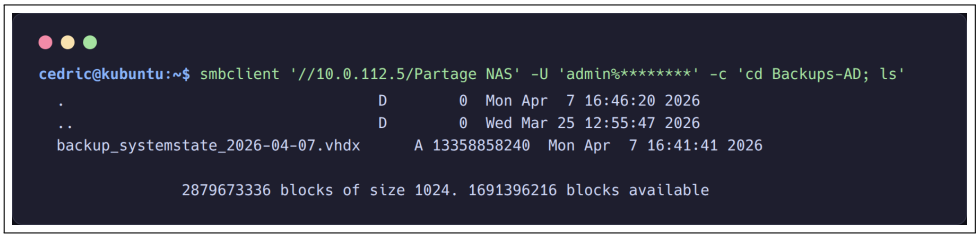

Figure 8 – Vérification de la présence du backup sur le NAS

La taille du fichier sur le NAS doit correspondre à celle du fichier source. Lors de la première sauvegarde du 7 avril 2026, la taille était de **13 358 858 240 octets** (12,44 Go).

Méthode alternative

Si la copie directe depuis DC1 n'était plus possible (changement de firmware NAS, modification de politique réseau…), la méthode par relais Linux décrite en section 4.4 reste fonctionnelle.

4.4 Méthode alternative — Copie via relais Linux

Historique

Cette méthode a été utilisée pour le premier backup du 7 avril 2026, avant la résolution du problème d'accès SMB entre DC1 et le NAS. Elle reste disponible comme solution de repli si la copie directe via NTLM (section 4.3) n'était plus utilisable.

Le principe consiste à utiliser un poste Linux comme relais de transfert, en récupérant le VHD depuis DC1 par `smbclient`, puis en le déposant sur le NAS :

1. Récupérer le VHD depuis DC1 :

```
smbclient //10.0.112.2/C$ -U 'BTS\Administrateur%MOT_DE_PASSE'
smb: \> cd Backups-AD
smb: \> get backup.vhdx
```

2. Déposer le VHD sur le NAS Scotty :

```
smbclient "//10.0.112.5/Partage NAS" -U 'admin%MOT_DE_PASSE'
smb: \> put backup.vhdx
```

Durée totale

Chaque étape de transfert prend 10 à 15 minutes sur le réseau Gigabit (12–13 Go), soit environ 25 minutes au total contre 15 minutes pour la méthode directe.

4.5 Planification automatisée

Un script PowerShell déployé dans `C:\Backups-AD\` orchestre l'ensemble du processus de sauvegarde de manière autonome. Une tâche planifiée Windows l'exécute chaque dimanche à 3h00.

Étape 10 — Script de backup automatisé

Le script `C:\Backups-AD\backup_auto.ps1` effectue les opérations suivantes dans l'ordre :

1. **Vérification des prérequis** : espace disque suffisant sur `C:`, présence de Windows Server Backup
2. **Montage du VHD** : attachement du disque virtuel `backup.vhdx` et assignation du volume `D:`
3. **Backup SystemState** : exécution de `wbadmin start systemstatebackup -backupTarget:D: -quiet`
4. **Démontage du VHD** : détachement propre du disque virtuel
5. **Copie vers le NAS** : montage NTLM du partage (`net use /user:admin`), `Copy-Item` du VHD, démontage
6. **Rotation** : conservation des 3 dernières copies sur le NAS, suppression des plus anciennes

Chaque étape est tracée dans le fichier de log `C:\Backups-AD\backup_auto.log`.

Étape 11 — Créer la tâche planifiée

Enregistrer la tâche via PowerShell avec les paramètres suivants :

```
$action  = New-ScheduledTaskAction `
    -Execute "powershell.exe" `
    -Argument "-NoProfile -ExecutionPolicy Bypass -File
    C:\Backups-AD\backup_auto.ps1"

$trigger = New-ScheduledTaskTrigger -Weekly -DaysOfWeek Sunday -At 03:00

$settings = New-ScheduledTaskSettingsSet `
    -ExecutionTimeLimit (New-TimeSpan -Hours 4) `
    -StartWhenAvailable

Register-ScheduledTask `
    -TaskName "Backup AD SystemState" `
    -Action $action `
    -Trigger $trigger `
    -Settings $settings `
    -User "SYSTEM" `
    -RunLevel Highest `
    -Description "Backup hebdomadaire AD SystemState + copie NAS"
```

Étape 12 — Vérifier la tâche planifiée

Contrôler l'enregistrement et le dernier résultat d'exécution :

```
Get-ScheduledTask -TaskName "Backup AD SystemState" | Format-List
    TaskName, State
Get-ScheduledTaskInfo -TaskName "Backup AD SystemState" | Format-List
    LastRunTime, LastTaskResult, NextRunTime
```

Un `LastTaskResult` de `0` indique une exécution réussie. Toute autre valeur nécessite la consultation du log `backup_auto.log`.

⚠ Limitation de la sauvegarde sur VHD local

La copie locale du VHD (sur `C:`) ne protège **pas** contre une défaillance du disque physique. La copie vers le NAS assure une première externalisation, mais reste dans le même local technique. Une sauvegarde hors site devrait être envisagée à terme.

4.6 Gestion du fichier credentials NAS (`nas.cred`)

Le script automatisé de la section 4.5 lit les credentials du NAS depuis le fichier `C:\Backups-AD\nas.cred` au lieu de les coder en dur. Cette séparation permet la rotation du mot de passe du NAS sans modification du script lui-même, et limite l'exposition du secret dans les sauvegardes du système.

Format du fichier

Le fichier contient une seule ligne au format `login|motdepasse`, sans saut de ligne final :

```
admin|<MOT_DE_PASSE>
```

Le script T43 (`backup_auto.ps1`) le parse ainsi :

```
$cred = (Get-Content "C:\Backups-AD\nas.cred" -Raw).Trim()
$user, $pwd = $cred -split '\|', 2
```

Création initiale du fichier (avec ACL restrictive)

Étape 13 — Créer `nas.cred` et restreindre les permissions

Depuis une session PowerShell élevée sur DC1 :

```
$credPath = 'C:\Backups-AD\nas.cred'
$cred     = 'admin|<MOT_DE_PASSE>'
Set-Content -Path $credPath -Value $cred -NoNewline -Force

# Desactiver l'heritage et retirer toutes les ACE existantes
$acl = Get-Acl $credPath
$acl.SetAccessRuleProtection($true, $false)
$acl.Access | ForEach-Object { $acl.RemoveAccessRule($_) | Out-Null }

# Autoriser uniquement SYSTEM et Administrators
$rules = @(
    New-Object System.Security.AccessControl.FileSystemAccessRule(
        'NT AUTHORITY\SYSTEM', 'FullControl', 'Allow'),
    New-Object System.Security.AccessControl.FileSystemAccessRule(
        'BUILTIN\Administrators', 'FullControl', 'Allow')
)
foreach ($r in $rules) { $acl.AddAccessRule($r) }
Set-Acl -Path $credPath -AclObject $acl

# Verification
(Get-Acl $credPath).Access |
    Format-Table IdentityReference, FileSystemRights, AccessControlType
```

⚠ Importance de l'ACL

Sans cette ACL restrictive, tout utilisateur authentifié pourrait lire le fichier (héritage par défaut depuis `C:\`). La tâche planifiée exécute le script en tant que `SYSTEM`, qui doit être conservé dans la liste. Le groupe *Administrators* permet aux administrateurs locaux de mettre à jour le fichier sans élévation supplémentaire.

Mise à jour lors d'une rotation du MDP du NAS

Après chaque rotation du mot de passe du compte `admin` du NAS (cf. MO-AD-008), le fichier doit être actualisé avec le nouveau secret. La procédure préserve l'ACL existante (le `Set-Content` sur un fichier existant ne réinitialise pas les permissions) :

Étape 14 — Réécrire `nas.cred` avec le nouveau MDP

```
$credPath = 'C:\Backups-AD\nas.cred'
$nouveau  = 'admin|<NOUVEAU_MOT_DE_PASSE>'
Set-Content -Path $credPath -Value $nouveau -NoNewline -Force

# Verifier que l'ACL est toujours restreinte (defense en profondeur)
(Get-Acl $credPath).Access |
    Format-Table IdentityReference, FileSystemRights
```

Étape 15 — Tester la copie vers le NAS après rotation

Avant d'attendre la prochaine exécution planifiée (dimanche 3h00), valider que la connexion au NAS fonctionne avec le nouveau MDP :

```
$cred = (Get-Content 'C:\Backups-AD\nas.cred' -Raw).Trim()
$user, $pwd = $cred -split '\|', 2
net use Y: "\\10.0.112.5\Partage NAS" /user:$user $pwd
Get-ChildItem Y:\ | Select-Object -First 5
net use Y: /delete
```

Une listing réussi (sans erreur 58) confirme que la rotation est opérationnelle. En cas d'échec, vérifier le contenu du fichier (encodage UTF-8, absence de saut de ligne final).

Historique

Cette section a été ajoutée en version 1.2 (14/04/2026), après la rotation du mot de passe du NAS dans le cadre du Sprint 2 (T19). Avant cette version, le mot de passe était en dur dans le script PowerShell : cette pratique est désormais déconseillée et a été corrigée rétroactivement.

5 Vérification

Vérification

Après avoir effectué l'ensemble de la procédure, vérifier les points suivants :

- ☐ Windows Server Backup est installé (`Get-WindowsFeature Windows-Server-Backup`)
- ☐ Le VHD est créé et monté en `D:` (ou autre lettre disponible)
- ☐ `wbadmin get versions` affiche au moins une sauvegarde récente
- ☐ Le champ `Can recover` mentionne **System State**
- ☐ Le VHD a été copié sur le NAS (taille identique au fichier source)
- ☐ Le VHD a été démonté proprement après la copie
- ☐ La tâche planifiée « Backup AD SystemState » est enregistrée et active
- ☐ Espace suffisant restant sur `C:` et sur la cible de stockage
- ☐ Le fichier `C:\Backups-AD\nas.cred` existe et a une ACL restreinte (*SYSTEM* et *Administrators* uniquement)
- ☐ La connexion au partage NAS réussit avec le couple `user|password` courant (test `net use`)

6 Dépannage

Problème	Solution
wbadmin refuse `C:` comme cible	Le volume cible ne peut pas être inclus dans la sauvegarde. Utiliser la méthode VHD décrite dans ce document (section 4.2) pour créer un volume distinct sur le même disque physique.
« Le volume est inclus dans la sauvegarde »	Même cause : la cible et la source se trouvent sur le même volume. Le VHD monté en `D:` résout ce problème car Windows le considère comme un volume indépendant.
Erreur VSS writer	Vérifier l'état des writers VSS : `vssadmin list writers`. Si un writer est en état d'échec, redémarrer le service *Volume Shadow Copy* : `Restart-Service VSS`. Relancer le backup.
Erreur 58 lors de la copie vers le NAS	Le NAS QNAP QTS 4.2.6 ne supporte pas Kerberos. Utiliser des credentials NTLM explicites : `net use X: "\\10.0.112.5\Partage NAS" /user:admin MOT_DE_PASSE`. Voir la procédure détaillée en section 4.3.
La tâche planifiée ne s'exécute pas	Vérifier l'état : `Get-ScheduledTask -TaskName "Backup AD SystemState"`. Consulter le log `C:\Backups-AD\backup_auto.log` pour le détail des erreurs. Vérifier que le compte SYSTEM dispose des privilèges suffisants et que le script est accessible.
`NT_STATUS_DISK_FULL` pendant la copie	Espace insuffisant sur la destination. Vérifier l'espace libre sur le NAS ou sur le poste relais. Le VHD complet pèse environ 12–15 Go.
Le VHD ne se démonte pas	Un processus utilise encore le volume `D:`. Fermer l'Explorateur de fichiers, arrêter tout processus accédant au volume, puis relancer `detach vdisk` dans diskpart.
Backup très long (> 2h)	La première exécution est la plus longue en raison de l'énumération complète des fichiers. Les exécutions suivantes bénéficient du mécanisme incrémentiel. Vérifier également la charge CPU et disque du serveur pendant le backup.

7 Voir aussi

— **MO-AD-002** — Rotation du compte `krbtgt` (le backup *System State* décrit ici est le seul vecteur de rollback en cas d'échec critique de la rotation `krbtgt`, via une restauration authoritative en mode DSRM)
— **MO-AD-005** — Vérification de la santé AD (prérequis avant tout backup)
— **MO-AD-007** — Audit périodique (contrôle que le dernier backup date de moins de 7 jours)
— **MO-AD-008** § 5.5 — Mise à jour du fichier `nas.cred` après rotation du mot de passe NAS (cas typique : la rotation casse silencieusement la tâche planifiée décrite ici si `nas.cred` n'est pas synchronisé)

Références

— Microsoft — *Wbadmin start systemstatebackup* (documentation Windows Server 2022)
— Microsoft — *Back Up and Recover Active Directory Domain Services* (TechNet)
— ANSSI — *Recommandations de sécurité relatives à Active Directory*, R47–R49 (2023)
— ANSSI — *Guide d'hygiène informatique*, mesure 36 (2017)
— Audit BTS SIO — Constat F-AD-010 / Recommandation R-023