Mode Opératoire

Vérifier la santé de l'Active Directory avant intervention

Code :	MO-AD-005
Version :	1.1
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
1.1	15/04/2026	Nuance dépannage RPC 110/5722 (DFSR) confirmée *false-positive* ; ajout section "Voir aussi" (MO-AD-002, 006, 007, 008)

1 Objet

Ce mode opératoire décrit la procédure de vérification de santé du contrôleur de domaine Active Directory **avant toute intervention de maintenance** (sauvegarde, mise à jour, modification de la configuration, etc.). L'objectif est de s'assurer que l'annuaire fonctionne correctement et qu'aucune anomalie ne risque de compromettre l'opération planifiée.

La procédure couvre huit points de contrôle : réplication entre partitions, diagnostic général (`dcdiag`), état des écrivains VSS, rôles FSMO, services critiques, espace disque et sessions actives. L'ensemble prend entre 10 et 15 minutes et doit devenir un réflexe systématique avant chaque opération sensible sur le contrôleur de domaine.

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
Domaine	`bts.sio`
Durée estimée	10–15 minutes

3 Prérequis

Prérequis

- Accès WinRM ou RDP au contrôleur de domaine DC1 (`10.0.112.2`)
- Compte `Administrateur` du domaine (identifiants dans Vaultwarden, cf. MO-PLT-009)
- Connectivité réseau : câble RJ45 ou tunnel VPN WireGuard
- Script `bts` ou client WinRM (`pywinrm`) installé (cf. MO-AD-001)

4 Procédure

4.1 Se connecter au contrôleur de domaine

Étape 1 — Ouvrir une session WinRM vers DC1

Se connecter au contrôleur de domaine via le script `bts` :

```
bts winrm dc1
```

Le prompt `dc1>` apparaît. Toutes les commandes qui suivent sont à exécuter dans cette session. Les commandes PowerShell sont préfixées par `ps:` dans le shell `bts`.

Alternative RDP

Si l'accès WinRM n'est pas disponible, il est possible de se connecter en Bureau à distance (RDP) sur `10.0.112.2` et d'ouvrir une console PowerShell élevée. Les commandes restent identiques, sans le préfixe `ps:`.

4.2 Vérifier la réplication Active Directory

Étape 2 — Exécuter `repadmin /showrepl`

La première vérification porte sur la réplication des partitions de l'annuaire. Exécuter :

```
repadmin /showrepl
```

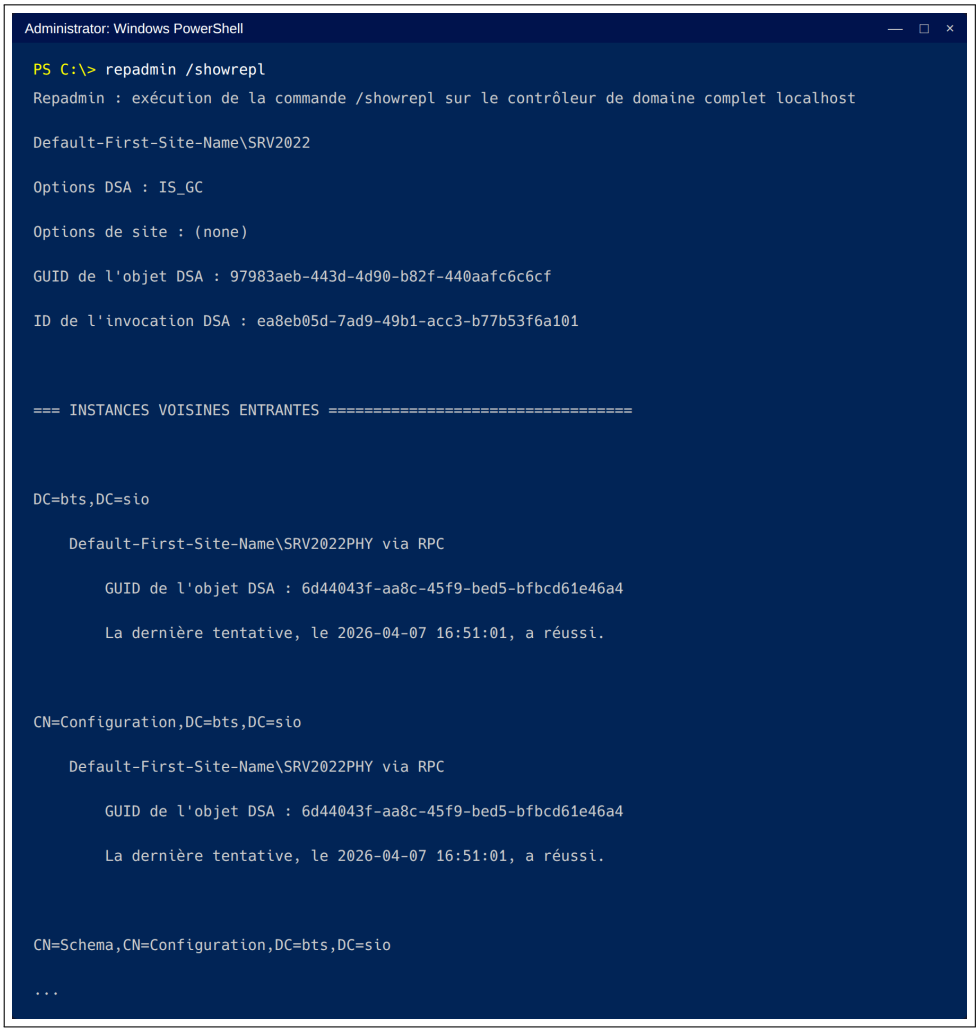

Figure 1 – Résultat de `repadmin /showrepl` — réplication réussie sur les 5 partitions

La commande affiche l'état de réplication pour chaque *naming context*. Les cinq partitions à contrôler sont :

- `DC=bts,DC=sio` — partition de domaine (comptes, groupes, GPO)
- `CN=Configuration,DC=bts,DC=sio` — topologie de réplication et sites
- `CN=Schema,CN=Configuration,DC=bts,DC=sio` — schéma de l'annuaire
- `DC=DomainDnsZones,DC=bts,DC=sio` — zones DNS du domaine
- `DC=ForestDnsZones,DC=bts,DC=sio` — zones DNS de la forêt

Pour chaque partition, le statut doit indiquer **succès** (*via RPC*). La date de dernière réplication permet de vérifier que la synchronisation est récente.

⚠ Échec de réplication

Si une ou plusieurs partitions affichent un échec de réplication, ne pas poursuivre l'intervention prévue. Vérifier la connectivité réseau entre les DCs, la résolution DNS et l'état du service NTDS. Consulter la section Dépannage en fin de document.

4.3 Diagnostiquer l'état général

Étape 3 — Exécuter `dcdiag /q`

L'outil `dcdiag` effectue une batterie de tests sur le contrôleur de domaine. L'option `/q` (quiet) n'affiche que les erreurs et avertissements, ce qui facilite la lecture :

```
dcdiag /q
```

Figure 2 – Sortie de `dcdiag /q` — trois avertissements non bloquants

En environnement réel, il est courant d'observer quelques avertissements. Voici les trois plus fréquents sur l'infrastructure BTS SIO et leur interprétation :

⚠ Erreurs critiques dcdiag

Si `dcdiag` signale des échecs sur les tests **NTDS**, **KCC** (*Knowledge Consistency Checker*) ou **NCSecDesc**, il s'agit d'erreurs critiques affectant directement le fonctionnement de l'annuaire. Dans ce cas, **ne pas procéder à l'intervention prévue** et diagnostiquer le problème en priorité.

4.4 Vérifier les écrivains VSS

Étape 4 — Lister les écrivains VSS

Le service VSS (*Volume Shadow Copy Service*) est indispensable pour les sauvegardes `System State`. Vérifier que tous les écrivains sont dans un état stable :

```
vssadmin list writers
```

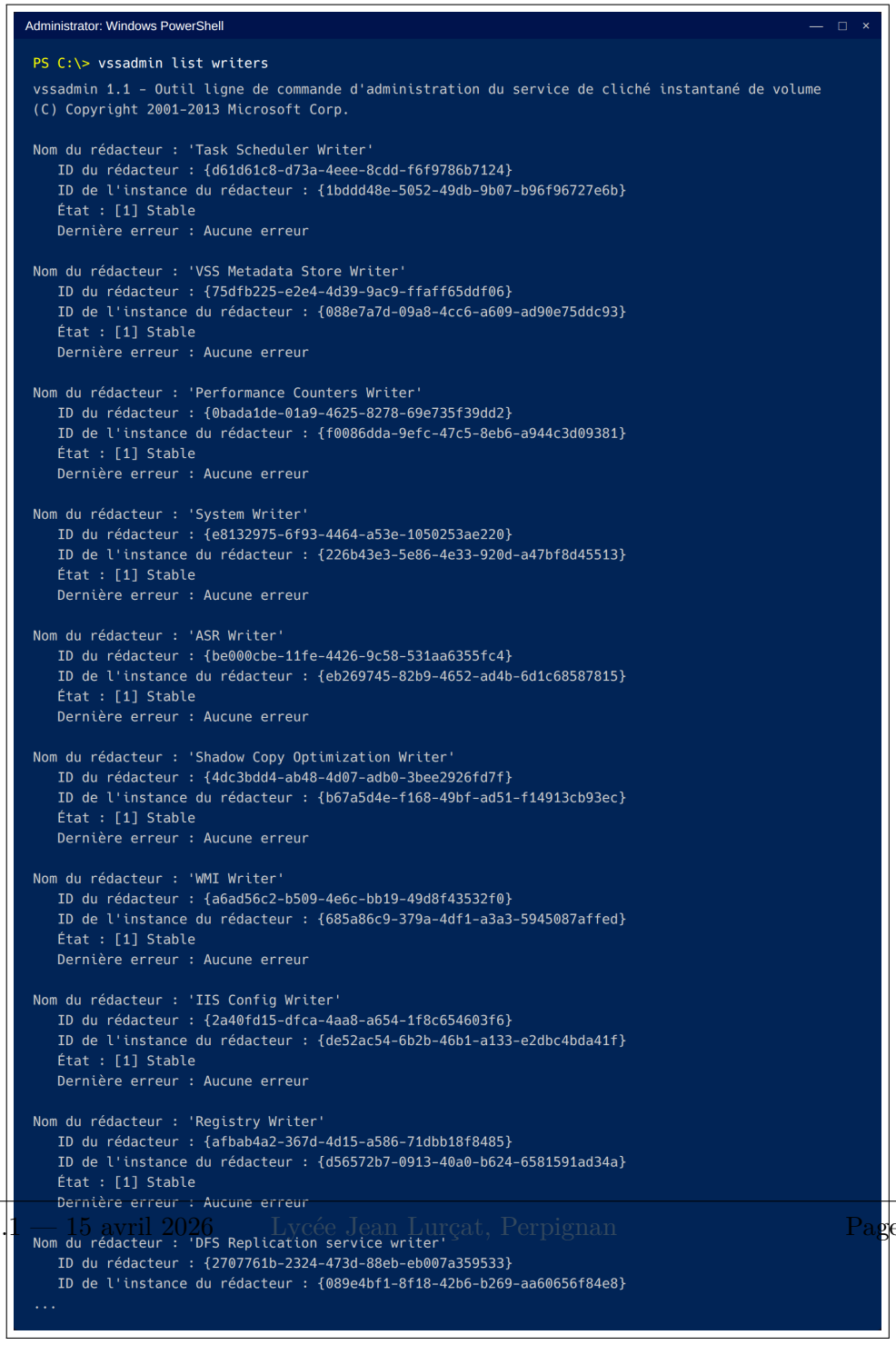

Figure 3 – État des 14 écrivains VSS — tous stables, aucune erreur

⚠ Écrivain NTDS instable

Si l'écrivain NTDS affiche un état différent de `Stable` ou une erreur, ne **jamais** lancer de sauvegarde `System State`. Redémarrer le service NTDS (`Restart-Service NTDS -Force`) et relancer la vérification. Si le problème persiste, consulter les journaux d'événements avant toute autre action.

4.5 Identifier le détenteur des rôles FSMO

Étape 5 — Interroger les rôles FSMO

Chaque forêt et chaque domaine Active Directory possèdent des rôles de *maître d'opérations* (FSMO, *Flexible Single Master Operations*). Cinq rôles existent au total. Pour les identifier :

```
netdom query fsmo
```

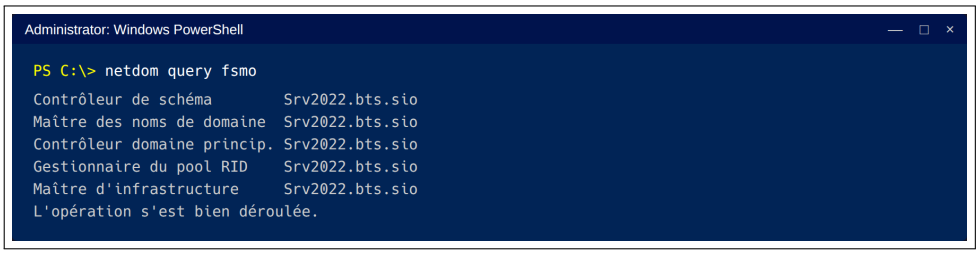

Figure 4 – Les 5 rôles FSMO attribués à Srv2022.bts.sio

Les cinq rôles et leur fonction :

Rôle FSMO	Fonction
Schema Master	Contrôle les modifications du schéma de l'annuaire (ajout d'attributs, classes)
Domain Naming Master	Gère l'ajout et la suppression de domaines dans la forêt
PDC Emulator	Référent pour l'authentification, la synchronisation horaire et les changements de mot de passe
RID Master	Distribue les pools d'identifiants relatifs (RID) pour la création d'objets
Infrastructure Master	Gère les références inter-domaines (SID et DN des objets étrangers)

SPOF : tous les rôles sur un seul DC

Sur l'infrastructure BTS SIO, les cinq rôles FSMO sont hébergés sur un unique contrôleur de domaine (Srv2022). Cette concentration est typique des petits domaines mono-site mais constitue un **point de défaillance unique** (*Single Point of Failure*). En cas de perte de ce DC, les opérations dépendant de ces rôles deviendraient impossibles. Ce point est identifié comme un risque dans l'audit de l'infrastructure.

4.6 Contrôler les services critiques

Étape 6 — Vérifier l'état des services AD

Six services sont essentiels au bon fonctionnement du contrôleur de domaine. Vérifier leur état en une seule commande :

```
Get-Service NTDS,DNS,DHCPServer,KDC,Netlogon,W32Time |
    Format-Table Name,Status,StartType
```

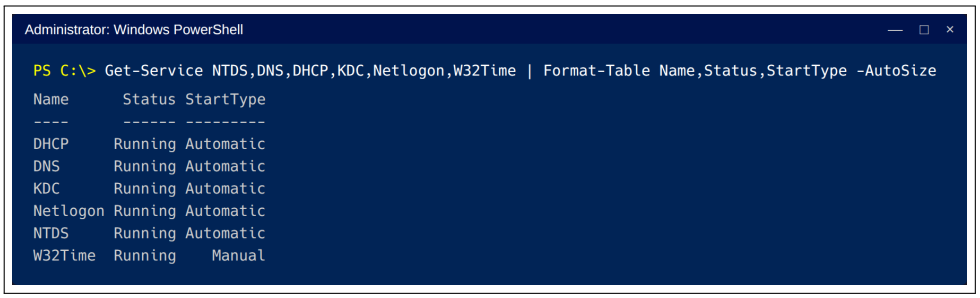

Figure 5 – Services critiques du DC — tous en état Running

Chaque service doit afficher le statut **Running** :

Service	Statut attendu	Rôle
NTDS	Running	Moteur de l'annuaire Active Directory
DNS	Running	Résolution de noms pour le domaine
DHCPServer	Running	Attribution des adresses IP (VLAN pédagogique)
KDC	Running	Centre de distribution de clés Kerberos
Netlogon	Running	Authentification NTLM et localisation du DC
W32Time	Running	Synchronisation horaire (critique pour Kerberos)

⚠ Service arrêté

Si l'un de ces services est à l'état `Stopped`, investiguer la cause avant de poursuivre. Un service NTDS ou KDC arrêté peut signaler un problème grave. Tenter un redémarrage :

```
Start-Service <NomDuService>
```

Si le service ne redémarre pas, consulter les journaux d'événements (`Get-EventLog -LogName System -Newest 20`).

4.7 Vérifier l'espace disque

Étape 7 — Contrôler l'espace disponible

Un espace disque insuffisant peut provoquer l'échec d'une sauvegarde ou, dans les cas extrêmes, le blocage de l'annuaire. Vérifier l'espace disponible :

```
Get-WmiObject Win32_LogicalDisk -Filter "DriveType=3" |
    Select DeviceID, @{N='Total(GB)';E={[math]::Round($_.Size/1GB,2)}},
    @{N='Free(GB)';E={[math]::Round($_.FreeSpace/1GB,2)}},
    @{N='Free%';E={[math]::Round($_.FreeSpace/$_.Size*100,1)}}
```

Figure 6 – Espace disque sur DC1 — 89,5 Go libres sur 126,3 Go (70 %)

Le seuil minimal recommandé est de **20 % d'espace libre**, en particulier avant une sauvegarde `System State` qui génère des snapshots VSS temporaires. Avec 70 % d'espace disponible, la situation est confortable sur DC1.

Surveillance proactive

Si l'espace libre descend en dessous de 20 %, envisager un nettoyage avant l'intervention : suppression des fichiers temporaires (`C:\Windows\Temp`), purge des anciens journaux d'événements et suppression des sauvegardes obsolètes.

4.8 Vérifier les sessions actives

Étape 8 — Lister les sessions utilisateurs

Avant une intervention qui pourrait nécessiter un redémarrage de service ou du serveur, vérifier si d'autres utilisateurs sont connectés :

```
query user
```

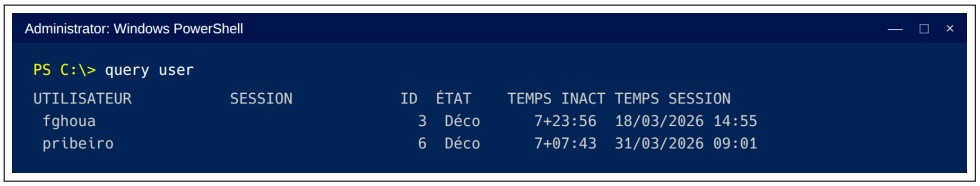

Figure 7 – Sessions utilisateurs sur DC1 — 2 sessions déconnectées

La commande affiche le nom d'utilisateur, le type de session, l'état (`Active` ou `Disc` pour déconnectée) et la durée d'inactivité.

— **Sessions déconnectées** (`Disc`) : sessions RDP fermées sans déconnexion propre. Elles consomment des ressources mais ne représentent pas un risque pour l'intervention. On peut les fermer avec `logoff <ID>` si nécessaire.

— **Sessions actives** (`Active`) : un utilisateur est actuellement connecté. Prévenir cette personne avant toute opération susceptible de perturber sa session.

5 Vérification

Vérification

Après avoir effectué les huit contrôles, valider la liste suivante avant de procéder à l'intervention prévue :

- ☐ Réplication OK sur les 5 partitions (`repadmin /showrepl`)
- ☐ `dcdiag /q` sans erreurs bloquantes (NTDS, KCC)
- ☐ VSS writers tous stables, en particulier l'écrivain NTDS
- ☐ Rôles FSMO identifiés et attribués au bon contrôleur
- ☐ Les 6 services critiques sont en état Running
- ☐ Espace disque suffisant (> 20 % libre)
- ☐ Sessions actives évaluées (aucun utilisateur ne sera impacté)

6 Dépannage

Problème	Solution
dcdiag Advertising en échec	Le DC n'est pas configuré comme source de temps fiable. Configurer la synchronisation NTP sur une source externe : `w32tm /config /manualpeerlist:"pool.ntp.org" /syncfromflags:manual /reliable:yes /update` puis `Restart-Service W32Time`.
Erreur RPC 110 ou 5722 (DFSR) dans dcdiag/repadmin	Le canal DFSR (port 5722) remonte une erreur RPC. Si `repadmin /replsummary` indique **0 échec de réplication** et que les partitions critiques (Schema, Configuration, DomainNC) sont à jour via les ports standards (135, 389, 636), cette erreur est une *fausse alerte* non bloquante. Elle reste à corriger à terme (DFSR gère SYSVOL), mais n'interdit pas une rotation de mot de passe ni une intervention AD courante. Confirmer l'état réel via `repadmin /showrepl` avant d'annuler une opération.
repadmin montre des échecs de réplication	Vérifier la connectivité réseau entre les DCs (`Test-NetConnection`). Contrôler la résolution DNS (`nslookup`). Si l'échec est ancien, vérifier que le *tombstone lifetime* n'est pas dépassé (60 ou 180 jours par défaut).
VSS writer en erreur	Identifier le writer concerné et redémarrer le service associé. Pour NTDS : `Restart-Service NTDS -Force`. Pour d'autres writers, consulter la correspondance service/writer dans la documentation Microsoft.
Service critique arrêté	Tenter `Start-Service <Nom>`. Si le service ne démarre pas, vérifier ses dépendances : `Get-Service <Nom> | Select -Expand DependentServices`. Consulter les 20 derniers événements système pour identifier la cause.
Espace disque critique (< 10 %)	Nettoyer les fichiers temporaires : `Remove-Item C:\Windows\Temp\* -Recurse -Force`. Purger les anciens journaux d'événements : `wevtutil cl Application`. Supprimer les sauvegardes `System State` obsolètes : `wbadmin delete systemstatebackup -keepVersions:12`.
Sessions déconnectées accumulées	Fermer les sessions orphelines : `logoff <ID_session>` où l'identifiant est visible dans la colonne `ID` de `query user`. Pour fermer toutes les sessions déconnectées d'un coup, utiliser un script PowerShell filtrant sur l'état `Disc`.

7 Voir aussi

— **MO-AD-002** — Rotation du compte `krbtgt` (utilise les pré-checks de ce MO)
— **MO-AD-006** — Backup *System State* (prérequis avant toute intervention sensible)
— **MO-AD-007** — Audit périodique des comptes et groupes AD
— **MO-AD-008** — Rotation périodique des mots de passe critiques