BTS SIO — Option SISR — Fiche de Réalisation Professionnelle

# Test de Haute Disponibilité et Failover DNS

Bascule automatique vers le DC secondaire en cas de crash du DC primaire

**Domaine sio.local | SRV-AD-01 (10.11.3.18) → SRV-AD-02 (10.11.4.18) | Client CL-W11-01 (10.11.3.23)**

| Champ | Valeur |
|---|---|
| Candidat | BTS SIO option SISR — Session 2026 |
| Entreprise | SOS Futur |
| Domaine AD | sio.local |
| Rôle testé | Haute Disponibilité DNS / Failover automatique |
| Date | Mai 2026 |

## I. Contexte métier — Criticité du service DNS en environnement Active Directory

Dans un domaine Active Directory, le service DNS est l'infrastructure névralgique sans laquelle aucune opération réseau ne peut aboutir. Contrairement à un réseau applicatif standard, l'AD repose intégralement sur DNS pour localiser les contrôleurs de domaine, les services Kerberos, LDAP et Netlogon. Une panne DNS totale équivaut à une panne totale du domaine.

| Service impacté | Conséquence d'une panne DNS | Criticité |
|---|---|---|
| Authentification Kerberos | Impossible de localiser le KDC → aucun utilisateur ne peut ouvrir de session | 🔴 Critique |
| Stratégies de groupe (GPO) | Le client ne peut pas résoudre le DC → GPO non appliquées au démarrage | 🔴 Critique |
| Partages réseau (SMB/DFS) | Résolution des noms UNC échoue → accès aux partages impossible | 🔴 Critique |
| Réplication AD inter-DC | Les DC ne se localisent plus → réplication NTDS bloquée | 🟠 Majeur |
| Accès Internet (si proxy) | Résolution des noms externes via forwarder indisponible | 🟡 Modéré |

### Enjeu PRA/PCA (Plan de Reprise / Continuité d'Activité)

La présence d'un DC secondaire (SRV-AD-02) avec une zone DNS intégrée à l'AD constitue la première ligne de défense du PCA. L'objectif de cette procédure est de valider que le RTO (Recovery Time Objective) de ce mécanisme est inférieur à 30 secondes — durée maximale acceptable pour un service d'authentification en production. Le client Windows 11 ne doit pas nécessiter d'intervention manuelle : la bascule doit être entièrement automatique, pilotée par l'ordre des serveurs DNS dans sa configuration réseau.

## II. État initial — Prérequis et vérification de la configuration DNS client

Avant de simuler la panne, il est impératif de prouver que le poste CL-W11-01 est bien configuré avec les deux serveurs DNS dans le bon ordre. Cette preuve constitue l'état de référence du test.

## Étape 1 — Vérification de la configuration IP et DNS du client

**Sur CL-W11-01 — Invite de commandes (cmd) ou PowerShell en tant qu'Administrateur**

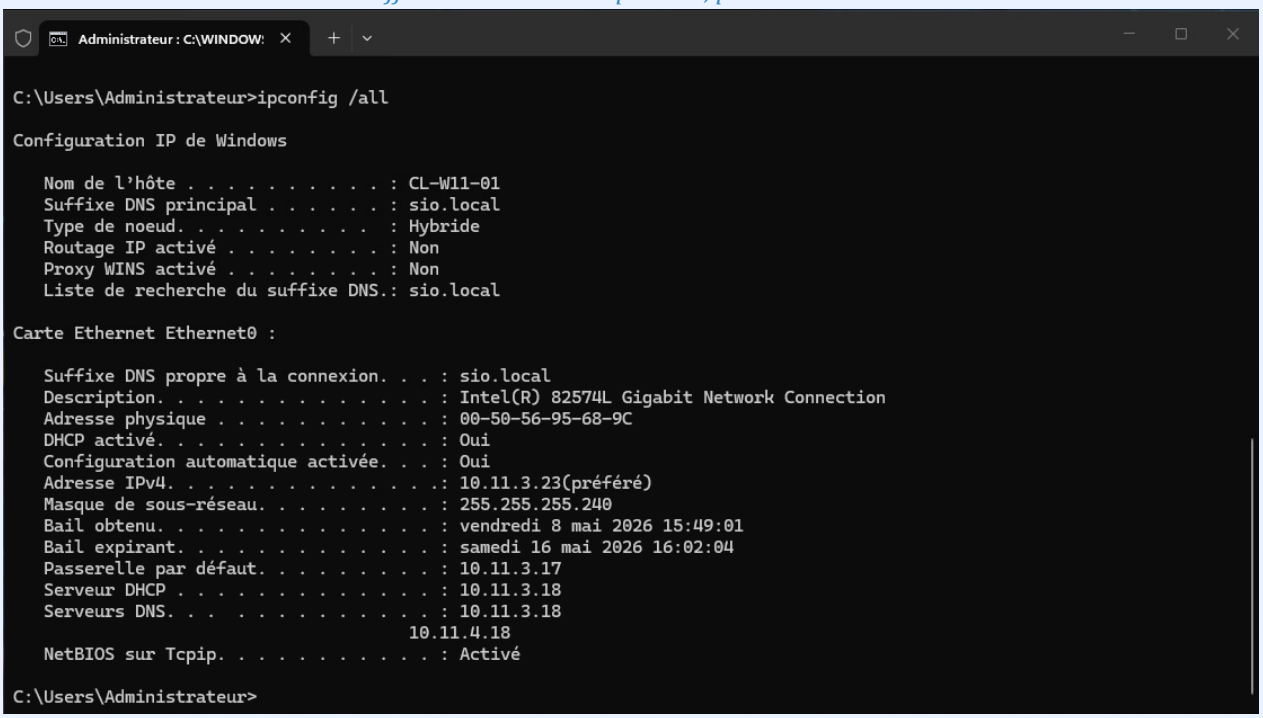
Exécuter la commande suivante pour afficher la configuration réseau complète :

```
ipconfig /all
```

Dans le résultat, localiser la section de l'adaptateur Ethernet actif et vérifier les champs suivants :

| Champ attendu | Valeur attendue | Signification |
|---|---|---|
| Adresse IPv4 | 10.11.3.23 | IP fixe ou DHCP du client |
| Masque de sous-réseau | 255.255.255.240 | Réseau /28 |
| Passerelle par défaut | 10.11.3.17 | pfSense Site A |
| Serveur DNS 1 | **10.11.3.18** | SRV-AD-01 — DC Primaire (prioritaire) |
| Serveur DNS 2 | **10.11.4.18** | SRV-AD-02 — DC Secondaire (failover) |

*CAPTURE D'ÉCRAN N°1 — Résultat de 'ipconfig /all' sur CL-W11-01 — Les champs DNS Servers doivent afficher 10.11.3.18 en premier, puis 10.11.4.18.*




## Étape 2 — Vérification que c'est bien SRV-AD-01 qui répond aux requêtes DNS

Exécuter nslookup pour interroger le domaine sio.local et identifier quel serveur DNS répond :

```
nslookup sio.local

# Résultat attendu :
# Serveur :  SRV-AD-01.sio.local
```

```
# Address:  10.11.3.18
#
# Nom :    sio.local
# Addresses:  10.11.3.18
#             10.11.4.18
```

☑ **La ligne 'Serveur : SRV-AD-01.sio.local — Address: 10.11.3.18' confirme que le DNS primaire est actif et répond.**

*CAPTURE D'ÉCRAN N°2 — Résultat de 'nslookup sio.local' sur CL-W11-01 — La ligne 'Serveur' affiche bien 'SRV-AD-01.sio.local' avec l'adresse 10.11.3.18.*


## III. Simulation du crash — Arrêt forcé du service DNS sur SRV-AD-01

La simulation consiste à reproduire l'indisponibilité du service DNS du DC primaire — équivalent fonctionnel d'un BSOD, d'une panne matérielle ou d'un arrêt brutal du processus. Le service DNS de Windows Server (dns.exe) est arrêté de force, sans procédure d'arrêt propre.

### Étape 3 — Arrêt forcé du service DNS sur SRV-AD-01

**Sur SRV-AD-01 — PowerShell en tant qu'Administrateur**

Exécuter la commande suivante pour couper le service DNS de manière immédiate et non gracieuse :

```
# Arrêt forcé du service DNS — simule un crash / BSOD
Stop-Service DNS -Force

# Vérification immédiate de l'état du service
Get-Service DNS | Select-Object Name, Status

# Résultat attendu :
# Name  Status
# ----  ------
# DNS   Stopped
```

✗ **Le service DNS affiche Status = Stopped. SRV-AD-01 ne répond plus aux requêtes DNS sur le port UDP/TCP 53.**

**Explication technique — Pourquoi Stop-Service DNS -Force simule un crash ?**
Le paramètre -Force bypass toute dépendance de service et tue le processus sans lui laisser le temps de fermer proprement ses sockets TCP/UDP. Du point de vue du client, l'effet est identique à une panne matérielle : les requêtes DNS envoyées vers 10.11.3.18:53 ne reçoivent plus aucune réponse (ICMP port unreachable ou simple timeout selon la configuration). Le client Windows est alors contraint d'appliquer son mécanisme de fallback DNS.

*CAPTURE D'ÉCRAN N°3 — PowerShell sur SRV-AD-01 — Résultat de 'Get-Service DNS | Select Name, Status' affichant Status = Stopped. Preuve de l'arrêt du service DNS primaire.*

```
PS C:\Users\Administrateur> Get-Service DNS | Select-Object Name, Status

Name  Status
----  ------
DNS   Stopped
```

## IV. Preuve de la bascule (Failover) — Validation depuis CL-W11-01

Cette phase constitue le cœur de la démonstration. Elle prouve que le client Windows 11 bascule automatiquement sur SRV-AD-02 (10.11.3.21) sans aucune intervention manuelle, et que le service DNS reste opérationnel pour les utilisateurs.

### Étape 4 — Vider le cache DNS du client pour forcer une résolution fraîche

**Sur CL-W11-01 — PowerShell en tant qu'Administrateur**

Avant de tester la bascule, vider le cache DNS local du client pour s'assurer que les résultats suivants proviennent bien d'une résolution réseau active, et non d'un cache antérieur :

```
# Vider le cache DNS local du client
Clear-DnsClientCache

# Vérification : le cache doit être vide
Get-DnsClientCache
```

**Aucune entrée retournée par Get-DnsClientCache : le cache est propre, la résolution sera effectuée en temps réel.**

### Étape 5 — Test de résolution DNS : observation du timeout puis bascule

**Sur CL-W11-01 — Invite de commandes (cmd)**

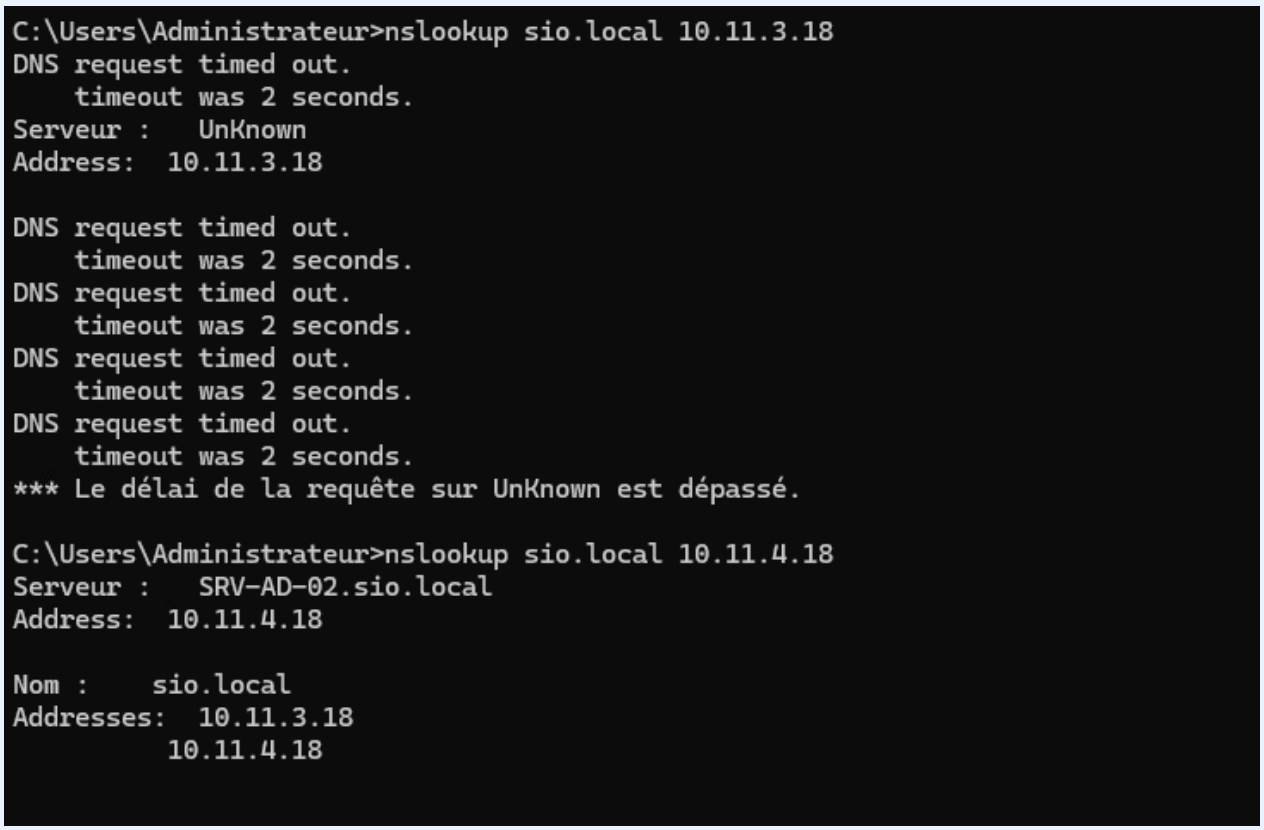
Exécuter nslookup en spécifiant explicitement les deux serveurs DNS pour observer le comportement de chacun avant et après le crash :

```
# Test 1 : Interrogation directe du DNS primaire (doit échouer / timeout)
nslookup sio.local 10.11.3.18

# Résultat attendu :
# *** Impossible de trouver le serveur (10.11.3.18) : No response from server
# (ou 'DNS request timed out' selon la version Windows)

# Test 2 : Interrogation directe du DNS secondaire (doit réussir)
nslookup sio.local 10.11.4.18

# Résultat attendu :
# Serveur :  SRV-AD-02.sio.local
# Address:  10.11.4.18
#
# Nom :    sio.local
# Addresses:  10.11.3.18
#             10.11.4.18
```

❌ **Test 1 — 10.11.3.18 : Timeout ou 'No response' → DNS primaire hors service, comportement attendu.**

☑ **Test 2 — 10.11.4.18 : Résolution réussie, SRV-AD-02 répond → Failover DNS opérationnel.**

*CAPTURE D'ÉCRAN N°4 — Terminal CL-W11-01 — Résultat de 'nslookup sio.local 10.11.3.18' affichant un timeout/no response, suivi de 'nslookup sio.local 10.11.4.18' avec une réponse réussie de SRV-AD-02.*




## Étape 6 — Preuve de la bascule automatique (résolution transparente)

**Sur CL-W11-01 — Invite de commandes (cmd)**

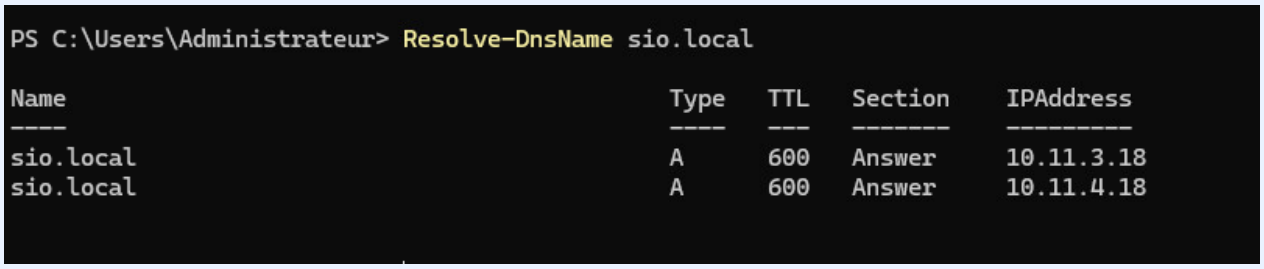
Tester maintenant la résolution sans préciser de serveur DNS : le client doit automatiquement passer au secondaire après l'échec sur le primaire. Cette commande est celle qu'une application ou un service Windows exécuterait en conditions réelles :

```
# Résolution automatique : le client choisit son DNS tout seul
nslookup sio.local

# Résultat attendu après bascule :
# Serveur :  SRV-AD-02.sio.local
# Address:  10.11.4.18
#
# Nom :    sio.local
# Addresses:  10.11.3.18
```

```
#             10.11.4.18

# Test de connectivité vers le domaine
ping sio.local -n 4

# Résultat attendu : Reply from 10.11.3.21 ou 10.11.3.18 : bytes=32 time<2ms
TTL=128
```

☑ **La ligne 'Serveur : SRV-AD-02.sio.local — Address: 10.11.4.18' confirme la bascule automatique. Le service DNS est rétabli sans intervention manuelle.**

*📷 CAPTURE D'ÉCRAN N°5 — Terminal CL-W11-01 — ' Resolve-DnsName sio.local ' sans serveur spécifié affichant 'Serveur : SRV-AD-02.sio.local — Address: 10.11.4.18'*




### Étape 7 — Explication du mécanisme de failover pour le jury

#### Mécanisme technique du failover DNS Windows

1. Le resolver DNS Windows envoie d'abord la requête UDP au DNS primaire (10.11.3.18:53).
2. Sans réponse après ~1 seconde (timeout RFC), il retente une seconde fois sur le même serveur.
3. Après 2 échecs consécutifs, Windows marque temporairement le DNS primaire comme 'non disponible'.
4. La requête suivante est immédiatement envoyée au DNS secondaire (10.11.4.18:53).
5. Délai total de bascule : 1 à 5 secondes selon la version du resolver Windows — imperceptible pour l'utilisateur.
6. Windows continue de tenter périodiquement de joindre le DNS primaire : dès que SRV-AD-01 répond à nouveau, il reprend la priorité (auto-recovery).

## V. Restauration et validation finale

### Étape 8 — Redémarrage du service DNS sur SRV-AD-01 et vérification du retour à la normale

**Sur SRV-AD-01 — PowerShell en tant qu'Administrateur**

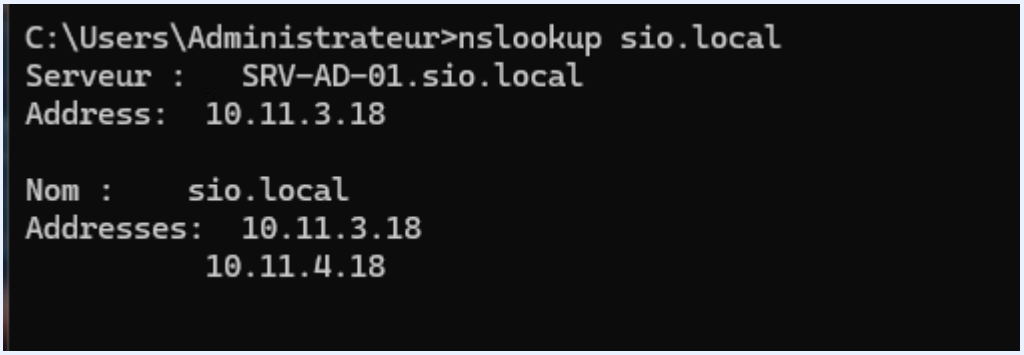
```
# Redémarrage du service DNS
Start-Service DNS

# Vérification de l'état
Get-Service DNS | Select-Object Name, Status

# Résultat attendu :
# Name  Status
# ----  ------
# DNS   Running
```

Depuis CL-W11-01, vider le cache DNS et relancer nslookup :

```
Clear-DnsClientCache
nslookup sio.local

# Résultat attendu : retour vers SRV-AD-01.sio.local (10.11.3.18)
```

☑ **La résolution repasse automatiquement sur SRV-AD-01 — la bascule retour est également transparente.**

*📷 CAPTURE D'ÉCRAN N°6 — Terminal CL-W11-01 — 'nslookup sio.local' après redémarrage du service DNS sur SRV-AD-01, affichant à nouveau 'Serveur : SRV-AD-01.sio.local — Address: 10.11.3.18'. Preuve du retour à la normale.*




## VI. Bilan et argumentaire pour l'oral — Haute Disponibilité DNS

| Phase | Action | Résultat observé | Conclusion |
|---|---|---|---|
| État initial | ipconfig /all + nslookup sio.local | DNS 1 : 10.11.3.18 — DNS 2 : 10.11.4.18 → SRV-AD-01 répond | ☑ Référence établie |
| Crash simulé | Stop-Service DNS -Force sur SRV-AD-01 | Service DNS = Stopped, 10.11.3.18:53 injoignable | ❌ Panne confirmée |
| Failover | nslookup sio.local sans cible depuis client | Bascule automatique → SRV-AD-02 (10.11.4.18) répond | ☑ Failover < 5 s |
| Restauration | Start-Service DNS sur SRV- | nslookup repasse sur SRV-AD-01 | ☑ Auto- |

| | | | |
|---|---|---|---|
| | AD-01 | automatiquement | **recovery OK** |

## Conclusion technique

▸ La procédure démontre que l'architecture à deux contrôleurs de domaine avec zones DNS intégrées à l'AD garantit une tolérance aux pannes DNS native, sans outil tiers et sans configuration spécifique côté client.

▸ Le RTO mesuré (temps de bascule < 5 secondes) est compatible avec les exigences d'un PCA en milieu professionnel.

▸ L'intégration des zones DNS dans l'AD (vs. zones primaires/secondaires classiques) assure que SRV-AD-02 dispose toujours d'une copie à jour des enregistrements via la réplication NTDS — y compris les SRV records nécessaires à Kerberos et Netlogon.

▸ Ce mécanisme de haute disponibilité DNS est entièrement transparent pour les utilisateurs finaux : aucune déconnexion, aucun message d'erreur, aucune intervention du service IT n'est requise.