**Mode Opératoire**

# Jonction d'un poste de travail au domaine Active Directory

| | |
|---|---|
| **Code :** | MO-AD-011 |
| **Version :** | 1.0 |
| **Date :** | 7 mai 2026 |
| **Auteur :** | Cédric LEGRAND |
| **Classification :** | USAGE INTERNE — Équipe BTS SIO |

## Historique des révisions

| Version | Date | Modifications |
|---|---|---|
| 1.0 | 07/05/2026 | Création initiale — rédigé dans le cadre de la mise en conformité Protected Users (Sprint 3) |

## 1 Objet

Ce mode opératoire décrit la procédure de **jonction d'un poste de travail Windows au domaine Active Directory BTS.SIO**. La jonction au domaine est un prérequis pour l'authentification Kerberos, l'application des stratégies de groupe (GPO), et la compatibilité avec le groupe *Protected Users* (voir MO-AD-010).

Deux méthodes sont décrites : l'interface graphique Windows (recommandée pour un poste isolé) et PowerShell (adaptée à l'administration à distance ou en lot).

# 2 Champ d'application

| | |
|---|---|
| **Public concerné** | Administrateurs de l'infrastructure BTS SIO |
| **Systèmes ciblés** | Postes Windows 10/11 Pro ou Enterprise |
| **Domaine** | BTS.SIO — DCs : Srv2022 (10.0.112.2), Srv2022Phy (10.0.112.3) |
| **Outils** | Interface graphique Windows, PowerShell (`Add-Computer`) |
| **Durée** | 15 à 20 minutes (redémarrage inclus) |

# 3 Prérequis

**Prérequis**

- **Édition Windows** : Pro ou Enterprise. L'édition Home ne supporte pas la jonction à un domaine AD
- **Connectivité réseau** : le poste doit pouvoir atteindre le VLAN serveurs (10.0.112.0/24) : `ping 10.0.112.2` doit répondre
- **DNS** : le DNS primaire du poste doit pointer vers DC1 (10.0.112.2) ou DC2 (10.0.112.3), **pas** vers un DNS public
- **Compte autorisé** : un compte Domain Admin ou un compte ayant les droits de jonction (quota `ms-DS-MachineAccountQuota`)
- **Nom du poste** : maximum 15 caractères NetBIOS, sans caractères spéciaux
- **Horloge** : écart maximum de 5 minutes avec les DCs (contrainte Kerberos)

**Profil utilisateur**

La jonction au domaine crée un **nouveau profil** pour le compte domaine. Les données du profil local actuel (Bureau, Documents, favoris) ne sont **pas migrées** automatiquement vers le profil domaine. Sauvegarder les données de l'utilisateur avant la jonction si nécessaire.

# 4 Procédure

## 4.1 Vérifications préalables

### Étape 1 — Vérifier la configuration réseau

Ouvrir une invite de commandes en administrateur :

```
ipconfig /all
```

Vérifier que le **DNS primaire** pointe vers `10.0.112.2` ou `10.0.112.3`. Si ce n'est pas le cas, corriger :

```
netsh interface ip set dns "<NOM_INTERFACE>" static 10.0.112.2
netsh interface ip add dns "<NOM_INTERFACE>" 10.0.112.3 index=2
```

Remplacer `<NOM_INTERFACE>` par le nom de la carte réseau (ex. `Ethernet`, `Wi-Fi`).

### Étape 2 — Vérifier la résolution DNS

```
nslookup bts.sio
nslookup Srv2022.bts.sio
nslookup -type=SRV _ldap._tcp.bts.sio
```

Les trois requêtes doivent résoudre. Si `_ldap._tcp.bts.sio` ne répond pas, le DNS ne pointe pas vers un contrôleur de domaine : corriger l'étape précédente.

### Étape 3 — Vérifier la synchronisation horaire

```
w32tm /query /status
net time \\Srv2022.bts.sio
```

L'écart doit être inférieur à 5 minutes. Pour forcer la synchronisation :

```
w32tm /config /manualpeerlist:Srv2022.bts.sio /syncfromflags:manual
    /update
w32tm /resync
```

## 4.2 Méthode 1 — Interface graphique (recommandée)

**Étape 4 — Jonction via les paramètres Windows**

Deux chemins d'accès possibles :

**Chemin 1 (recommandé) :**

1. **Paramètres → Système → À propos**
2. Cliquer sur **Domaine ou groupe de travail** (section « Spécifications de l'appareil »)
3. Dans l'onglet « Nom de l'ordinateur », cliquer sur **Modifier**
4. Sélectionner *Domaine*, saisir `bts.sio`
5. Entrer les identifiants d'un compte Domain Admin (ex. `BTS\Administrateur`)
6. Choisir le type de compte : **Standard** (pas Administrateur, sauf justification)
7. Redémarrer le poste

**Chemin 2 (Windows 10/11 alternatif) :**

1. **Paramètres → Comptes → Accéder au professionnel ou scolaire**
2. **Se connecter** → **Joindre cet appareil à un domaine Active Directory local**
3. Saisir `bts.sio`, puis les identifiants Domain Admin

**Windows 11**

Sur Windows 11, le chemin 2 (« Accéder au professionnel ou scolaire ») propose parfois Azure AD au lieu d'AD on-premise. Le chemin 1 via « À propos » est plus fiable pour une jonction AD classique.

## 4.3 Méthode 2 — PowerShell

### Étape 5 — Jonction locale (depuis le poste)

En tant qu'administrateur local :

```
Add-Computer -DomainName "bts.sio" `
    -Credential (Get-Credential) `
    -OUPath "OU=Profs,DC=bts,DC=sio" `
    -Restart
```

**Paramètre OUPath**

Le paramètre `-OUPath` est optionnel. Si omis, le compte machine est créé dans `CN=Computers` par défaut. L'OU peut être modifiée après coup (voir étape de post-jonction).

### Étape 6 — Jonction à distance via WinRM

Si le poste est accessible en WinRM (administration à distance) :

```
$domainCred = Get-Credential   # Compte Domain Admin
$localCred  = Get-Credential   # Admin local du poste cible

Invoke-Command -ComputerName <IP_POSTE> `
    -Credential $localCred -ScriptBlock {
    Add-Computer -DomainName "bts.sio" `
        -Credential $using:domainCred `
        -OUPath "OU=Profs,DC=bts,DC=sio" `
        -Restart -Force
}
```

## 4.4 Vérifications post-jonction

### Étape 7 — Vérifier l'objet computer dans l'AD

Depuis un DC ou via WinRM :

```
Get-ADComputer -Filter {Name -eq "<NOM_PC>"} `
    -Properties Created, LastLogonDate,
    OperatingSystem, OperatingSystemVersion,
    DistinguishedName | Format-List
```

Le poste doit apparaître avec une date `Created` récente et l'`OperatingSystem` correct.

### Étape 8 — Vérifier l'application des GPO

Sur le poste, après redémarrage et ouverture de session avec un compte domaine :

```
gpresult /r /scope:computer
```

Vérifier que les GPO pertinentes apparaissent dans la section « Objets stratégie de groupe appliqués »(notamment « Securite - Restriction RDP » si le poste est dans l'OU des DCs).

### Étape 9 — Déplacer dans la bonne OU si nécessaire

Si le poste a été créé dans `CN=Computers` (OU par défaut) :

```
Move-ADObject `
    -Identity "CN=<NOM_PC>,CN=Computers,DC=bts,DC=sio" `
    -TargetPath "OU=Profs,DC=bts,DC=sio"
```

Puis sur le poste :

```
gpupdate /target:computer /force
```

### Étape 10 — Vérifier Kerberos

Sur le poste, après ouverture de session avec un compte domaine :

```
klist
```

La sortie doit afficher un TGT valide pour le realm `BTS.SIO` :

```
#0> Client: fghoua @ BTS.SIO
    Server: krbtgt/BTS.SIO @ BTS.SIO
    KerbTicket Encryption Type: AES-256
    Start Time: ...
    End Time:   ...
```

Si la liste est vide, faire un logoff/logon avec le compte domaine.

## 5 Vérification — Grille récapitulative

### ☑ Vérification

Cocher chaque point après la jonction :

- ☐ Le poste apparaît dans l'AD avec `LastLogonDate` récent
- ☐ `gpresult /r` montre les GPO appliquées
- ☐ `klist` affiche un TGT valide pour `BTS.SIO`
- ☐ La connexion RDP par hostname (`Srv2022.bts.sio`) fonctionne
- ☐ Le DNS résout `_kerberos._tcp.bts.sio`
- ☐ L'utilisateur peut être (ré)ajouté au groupe *Protected Users* si applicable (voir MO-AD-010)

# 6 Rollback

### Étape 11 — Quitter le domaine

```
Remove-Computer -UnjoinDomainCredential (Get-Credential) `
    -Restart -Force
```

Le profil domaine est conservé localement. Le compte machine dans l'AD peut être supprimé manuellement :

```
Remove-ADComputer -Identity "<NOM_PC>" -Confirm:$false
```

# 7 Dépannage

| Problème | Solution |
|---|---|
| « Le domaine bts.sio est introuvable » | Le DNS ne pointe pas vers les DCs. Configurer 10.0.112.2 en DNS primaire (étape 1). Vérifier la connectivité avec `ping 10.0.112.2`. |
| « Accès refusé »à la jonction | Le compte n'a pas les droits de jonction. Utiliser un Domain Admin. Si un compte délégué est utilisé, vérifier la valeur de `ms-DS-MachineAccountQuota` (défaut : 10 machines par utilisateur). |
| « L'horloge diffère trop du DC » | Kerberos refuse si l'écart dépasse 5 minutes. Synchroniser : `w32tm /resync` après avoir configuré le serveur NTP (étape 3). |
| GPO non appliquées après jonction | Vérifier l'OU du poste. Si le poste est dans `CN=Computers`, les GPO liées aux OUs spécifiques ne s'appliquent pas. Déplacer dans la bonne OU (étape 10). |
| Profil utilisateur vide | Normal : le profil domaine est distinct du profil local. Migrer les données manuellement (Bureau, Documents, favoris). |
| « Un compte portant ce nom existe déjà » | Un ancien objet computer avec le même nom existe dans l'AD. Le supprimer : `Remove-ADComputer -Identity "<NOM>"` puis retenter la jonction. |

# 8 Voir aussi

— **MO-AD-010** : Gestion du groupe Protected Users (prérequis : PC joint au domaine)
— **MO-AD-009** : Diagnostic d'un échec de connexion RDP
— **MO-AD-005** : Santé Active Directory
— **MO-PLT-001** : Création de comptes utilisateurs