**Mode Opératoire**

# Gestion du groupe Protected Users

| | |
|---|---|
| **Code :** | MO-AD-010 |
| **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 suite à incident RDP causé par l'incompatibilité Protected Users + NLA sur poste non joint (Sprint 3) |

# 1 Objet

Ce mode opératoire décrit la gestion du groupe de sécurité Active Directory **Protected Users**, introduit avec Windows Server 2012 R2. Ce groupe applique des restrictions d'authentification renforcées aux comptes sensibles (Domain Admins, comptes de service critiques) en désactivant les protocoles d'authentification obsolètes.

Le document couvre les restrictions techniques imposées, les prérequis avant ajout d'un membre, les procédures d'ajout et de retrait, ainsi que la matrice de compatibilité avec les protocoles d'accès distant.

**Recommandation ANSSI**

L'ANSSI recommande de placer tous les comptes à privilèges dans le groupe *Protected Users* (guide AD, R68). Cette mesure fait partie du durcissement de l'infrastructure réalisé dans le cadre du Sprint 3.

# 2 Champ d'application

| | |
|---|---|
| **Public concerné** | Administrateurs de l'infrastructure BTS SIO |
| **Systèmes ciblés** | DC1 (Srv2022, 10.0.112.2), DC2 (Srv2022Phy, 10.0.112.3) |
| **Niveau fonctionnel** | Windows Server 2012 R2 ou supérieur |
| **Outils** | PowerShell (WinRM HTTPS 5986), module ActiveDirectory |
| **Durée** | 10 minutes par opération |

# 3 Fonctionnement du groupe Protected Users

Le groupe *Protected Users* impose des restrictions à deux niveaux : côté contrôleur de domaine (KDC) et côté poste client.

## 3.1 Restrictions appliquées par le KDC

| Restriction | Effet |
|---|---|
| NTLM interdit | Le DC refuse toute authentification NTLM pour les membres du groupe |
| DES et RC4 interdits | Seul AES est accepté pour la pré-authentification Kerberos |
| Délégation Kerberos interdite | Ni contrainte ni non contrainte : le TGT ne peut pas être transmis |
| TGT limité à 4 heures | Durée non configurable, non renouvelable au-delà |

## 3.2 Restrictions appliquées sur le poste client

Ces restrictions s'appliquent lorsque le membre se connecte sur un poste Windows 8.1+ ou Server 2012 R2+ :

— **CredSSP désactivé** : pas de mise en cache des credentials en clair

— **Windows Digest désactivé** : pas de hash WDigest en mémoire (protection contre Mimikatz)

— **Pas de profil hors connexion** : le profil n'est pas créé localement au premier logon si le DC est injoignable

**⚠ Incompatibilité NLA + poste non joint**

La combinaison *Protected Users* + NLA (Network Level Authentication) provoque un échec RDP systématique si le poste client **n'est pas joint au domaine**.

Mécanisme : NLA utilise CredSSP pour la pré-authentification. Lorsque Kerberos n'est pas disponible (poste non joint au domaine, ou connexion par adresse IP), CredSSP tombe en NTLM. Or *Protected Users* bloque NTLM au niveau du KDC : le DC retourne `STATUS_ACCOUNT_RESTRICTION` (`0xC000006E`).

Le message affiché par le client RDP est trompeur : « *Une restriction de compte d'utilisateur (ex. une restriction temporelle) vous empêche de vous connecter* ».

# 4 Matrice de compatibilité

| Protocole | PC joint | PC non joint | Commentaire |
|---|---|---|---|
| RDP + NLA (hostname) | ✓ | × | Kerberos requis |
| RDP + NLA (IP) | × | × | Kerberos nécessite un hostname DNS |
| RDP sans NLA | ✓ | ✓ | Non recommandé (sécurité réduite) |
| WinRM HTTPS | ✓ | × | Transport Kerberos requis |
| LDAP / LDAPS | ✓ | ✓ | Le *simple bind* LDAP n'est pas affecté par Protected Users |
| PowerShell Remoting | ✓ | × | Même transport que WinRM |

**Remote Credential Guard**

Pour les comptes *Protected Users* accédant aux serveurs depuis des postes non joints, la solution recommandée est **Remote Credential Guard** :

— **GPO serveur** : *Computer Configuration* → *Administrative Templates* → *System* → *Credentials Delegation* → *Restrict delegation of credentials to remote servers*

— **Client** : lancer `mstsc /remoteGuard /v:Srv2022.bts.sio`

Remote Credential Guard utilise Kerberos sans délégation de credentials : compatible avec *Protected Users*.

# 5 Prérequis avant ajout

**Prérequis**

Avant d'ajouter un utilisateur au groupe *Protected Users*, vérifier **tous** les points suivants :

- Le poste de travail de l'utilisateur est **joint au domaine** BTS.SIO (voir MO-AD-011)
- Le DNS du poste pointe vers DC1 (10.0.112.2) et/ou DC2 (10.0.112.3)
- L'utilisateur se connecte aux serveurs par **hostname** (`Srv2022.bts.sio`), jamais par adresse IP
- Un **backup SystemState** récent existe (voir MO-AD-006)
- L'utilisateur n'utilise **aucun service** reposant exclusivement sur NTLM ou CredSSP
- Tester une connexion RDP par hostname **avant** l'ajout pour confirmer que Kerberos fonctionne

# 6 Procédure d'ajout

### Étape 1 — Vérifier les prérequis du poste

```
# Verifier que le PC est dans l'AD
Get-ADComputer -Filter {Name -eq "<NOM_PC>"} `
    -Properties LastLogonDate, OperatingSystem | Format-List

# Verifier la resolution DNS depuis le poste (via WinRM)
Resolve-DnsName Srv2022.bts.sio -DnsOnly

# Verifier les SRV Kerberos
Resolve-DnsName _kerberos._tcp.bts.sio -Type SRV
```

Si le poste n'est pas trouvé dans l'AD : **ne pas continuer**. Joindre d'abord le poste au domaine (voir MO-AD-011).

### Étape 2 — Ajouter l'utilisateur au groupe

```
# Ajout
Add-ADGroupMember -Identity "Protected Users" -Members "<login>"

# Verification immediate
Get-ADGroupMember -Identity "Protected Users" |
    Select Name, SamAccountName | Format-Table -AutoSize
```

### Étape 3 — Forcer la réplication inter-DCs

```
repadmin /syncall /AdeP
```

### Étape 4 — Validation post-ajout

Demander à l'utilisateur de tester immédiatement une connexion RDP au DC par hostname :

```
mstsc /v:Srv2022.bts.sio
```

Si la connexion réussit, l'ajout est validé. Si elle échoue, retirer immédiatement l'utilisateur (section suivante) et diagnostiquer via MO-AD-009.

# 7 Procédure de retrait (urgence)

### Étape 5 — Retirer l'utilisateur du groupe

```
Remove-ADGroupMember -Identity "Protected Users" `
    -Members "<login>" -Confirm:$false

# Verification
Get-ADGroupMember -Identity "Protected Users" |
    Select Name, SamAccountName | Format-Table -AutoSize
```

### Prise d'effet

Le retrait est effectif **immédiatement** pour les nouvelles authentifications. Les TGT Kerberos déjà émis restent valides jusqu'à leur expiration (maximum 4 heures). L'utilisateur n'a pas besoin de redémarrer son poste.

### Étape 6 — Documenter le retrait

Noter la raison du retrait et planifier la remise en conformité :

— Cause : poste non joint au domaine, incompatibilité logicielle, urgence opérationnelle

— Plan : joindre le poste au domaine (MO-AD-011), puis remettre dans *Protected Users*

— Délai : ne pas laisser un compte Domain Admin hors de *Protected Users* plus d'une semaine

# 8 État actuel du groupe (référence)

Au 7 mai 2026, le groupe *Protected Users* du domaine BTS.SIO contient :

| Nom | Login | Rôle |
|---|---|---|
| Cédric LEGRAND | clegrand | Administrateur infrastructure |
| Manuel Martinez | mmartinez | Tuteur, administrateur |
| Paul Jorge-Ribeiro | pribeiro | Domain Admin |

**Compte retiré**

Le compte `fghoua` (Fatima Ghoua, Domain Admin) a été retiré le 7 mai 2026 en raison d'un poste non joint au domaine empêchant l'authentification Kerberos. À remettre dans le groupe après jonction du poste (voir MO-AD-011).

# 9 Vérification

**Vérification**

Après ajout ou retrait, valider les points suivants :

- ☐ La liste des membres est identique sur DC1 et DC2 (`repadmin /syncall` si nécessaire)
- ☐ Si ajout : l'utilisateur peut se connecter en RDP par hostname
- ☐ Si ajout : l'event log Security ne montre pas de 4625 pour le compte
- ☐ Si retrait : l'utilisateur peut se connecter en RDP par IP ou depuis un poste non joint
- ☐ Vaultwarden : noter le changement dans les notes de l'item concerné

# 10 Rollback

Les opérations sur le groupe *Protected Users* sont entièrement réversibles :

| **Action effectuée** | **Retour arrière** |
|---|---|
| Ajout d'un membre | `Remove-ADGroupMember -Identity "Protected Users" -Members "<login>"` |
| Retrait d'un membre | `Add-ADGroupMember -Identity "Protected Users" -Members "<login>"` |

# 11 Dépannage

| **Problème** | **Solution** |
|---|---|
| RDP échoue après ajout | Vérifier : (1) le PC est joint au domaine, (2) la connexion utilise le hostname (pas l'IP), (3) le DNS résout `Srv2022.bts.sio`. Voir MO-AD-009 pour le diagnostic complet. |
| TGT expire après 4 heures | Comportement attendu de *Protected Users*. Le TGT est renouvelé automatiquement à la prochaine authentification. L'utilisateur peut ressentir un délai ponctuel. |
| WinRM échoue après ajout | Utiliser le transport Kerberos au lieu de NTLM. Depuis un poste joint au domaine : `Enter-PSSession -ComputerName Srv2022.bts.sio`. |
| L'utilisateur ne voit pas le changement | Faire un logoff/logon pour renouveler le TGT. Les restrictions *Protected Users* s'appliquent au prochain ticket Kerberos, pas rétroactivement. |
| Erreur « restriction temporelle » | C'est le message générique pour `0xC000006E`. Voir l'arbre de décision dans MO-AD-009. |

# 12 Voir aussi

— **MO-AD-001** : Administration distante des contrôleurs de domaine
— **MO-AD-009** : Diagnostic d'un échec de connexion RDP
— **MO-AD-011** : Jonction d'un poste au domaine Active Directory
— **MO-AD-003** : Politiques FGPP (Fine-Grained Password Policies)