**Mode Opératoire**

# Création d'un compte utilisateur Active Directory

| | |
|---|---|
| **Code :** | MO-AD-012 |
| **Version :** | 1.1 |
| **Date :** | 26 juin 2026 |
| **Auteur :** | Cédric LEGRAND |
| **Classification :** | USAGE INTERNE — Équipe BTS SIO |

## Historique des révisions

| Version | Date | Modifications |
|---|---|---|
| 1.0 | 12/06/2026 | Création initiale |
| 1.1 | 26/06/2026 | Harmonisation de la présentation des étapes et des encadrés. |

# 1 Objet

Ce mode opératoire décrit la création d'un compte utilisateur dans le domaine Active Directory `bts.sio`. Au-delà du simple ajout d'un objet `user`, l'enjeu est de rattacher dès sa création le compte au bon contexte de sécurité : la bonne unité d'organisation, le bon groupe et, par voie de conséquence, la politique de mot de passe affinée (FGPP) attendue.

Trois profils sont traités, car ils n'obéissent pas aux mêmes exigences :

— le compte **standard**, qui couvre la grande majorité des cas : un enseignant ou un étudiant ;

— le compte **à privilèges** (administrateur durci), soumis à des contraintes renforcées et placé dans le groupe *Protected Users* ;

— le compte **temporaire** (examinateur externe), à durée de vie limitée et sans appartenance à un groupe métier.

Deux voies sont présentées pour chaque cas : l'interface graphique *Active Directory Users and Computers* (ADUC), adaptée à une création ponctuelle, et PowerShell, plus rigoureux et reproductible.

# 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) — Windows Server 2022 |
| **Domaine** | `bts.sio` (DC=bts,DC=sio) |
| **Outils** | Console ADUC (`dsa.msc`), PowerShell (module `ActiveDirectory` 1.0.1.0) |
| **Durée** | Environ 10 minutes par compte |

# 3 Concepts

## 3.1 Unités d'organisation cibles

Le placement d'un compte dans la bonne OU conditionne les GPO qui lui seront appliquées ainsi que la lisibilité de l'annuaire. Les OU utiles à la création de comptes utilisateurs sont les suivantes :

| Unité d'organisation | Usage |
|---|---|
| `OU=Profs` | Enseignants, comptes d'administration nominatifs, examinateurs temporaires |
| `OU=Sio1_2025` | Étudiants de première année (promotion 2025) |
| `OU=Sio2_2025` | Étudiants de deuxième année (promotion 2025) |
| `OU=Etudiants DU` | Étudiants du diplôme universitaire |
| `OU=Serveurs` | Objets serveurs (pas de compte utilisateur) |

## 3.2 Groupes et politiques de mot de passe affinées

Trois FGPP sont en place dans le domaine. Elles sont rattachées **par appartenance de groupe**, jamais par OU. Le tableau ci-dessous reprend les paramètres déployés (voir MO-AD-003) :

| FGPP | Groupe rattaché | Min. car. | Lockout | Expiration |
|---|---|---|---|---|
| FGPP-Admins | Admins du domaine | **16** | 5 | 90 j |
| FGPP-Staff | GGProfs | **12** | 10 | 180 j |
| FGPP-Etudiants | GGPromoSio1 / GGPromoSio2 | **10** | 10 | 365 j |
| *Default* | *Tous (baseline)* | *10* | *10* | *180 j* |

**La FGPP suit le groupe, pas l'OU**

**Une FGPP ne s'applique à un compte que si celui-ci est membre du groupe rattaché à la politique. Créer un enseignant dans `OU=Profs` sans l'ajouter à `GGProfs` le laisse soumis à la *Default Domain Policy* (10 caractères), et non à FGPP-Staff (12 caractères). L'oubli de l'ajout au groupe est donc une erreur silencieuse : le compte fonctionne, mais sa politique de mot de passe est plus faible que prévu. Le contrôle de l'étape 5.5 sert précisément à détecter ce cas.**

### 3.3 Convention de nommage

Les identifiants de connexion (`SamAccountName`) suivent la règle **initiale du prénom suivie du nom**, en minuscules et sans accent : Pauline Martin devient `pmartin`, Manuel Martinez devient `mmartinez`. L'UPN reprend ce même identifiant suffixé du domaine, soit `pmartin@bts.sio`. En cas d'homonymie sur l'initiale et le nom, on ajoute la deuxième lettre du prénom.

## 4 Prérequis

**Prérequis**

- **Droits : appartenance au groupe « Admins du domaine », ou délégation explicite sur l'OU cible**
- **Module PowerShell : `ActiveDirectory` importé (`Import-Module ActiveDirectory`)**
- **Accès au DC : console sur DC1 ou session WinRM ouverte vers DC1 (10.0.112.2)**
- **Mot de passe initial : choisi à l'avance et conforme à la FGPP cible (16 car. pour un compte admin, 12 pour un enseignant, 10 pour un étudiant)**
- **Identité : nom, prénom et rôle validés, afin de déterminer OU, groupe et durée de vie du compte**

**Saisie du mot de passe**

**Dans toute la procédure, le mot de passe initial est saisi de manière interactive via `Read-Host -AsSecureString` : il n'apparaît jamais en clair dans un script, dans l'historique de la console ou dans un journal. Ne jamais coder un mot de passe en dur dans un `.ps1`.**

## 5 Procédure

## 5.1 Méthode graphique (ADUC)

La console *Active Directory Users and Computers* convient à une création ponctuelle. La marche à suivre ci-dessous correspond à un compte enseignant standard ; les comptes à privilèges et temporaires réutilisent les mêmes écrans, en ajustant l'OU, les groupes et les options.

### 1 Ouvrir la console et l'OU cible

**Sur DC1, lancer `dsa.msc`. Déplier l'arborescence du domaine `bts.sio`, puis sélectionner l'OU de destination :**

**— bts.sio → Profs pour un enseignant ou un examinateur ;**

**— bts.sio → Sio1_2025 pour un étudiant de première année.**

**Clic droit sur l'OU, puis Nouveau → Utilisateur.**

### 2 Renseigner l'identité

**Dans l'assistant :**

1. ***Prénom*** **:** `Pauline` **—** ***Nom*** **:** `Martin`
2. ***Nom d'ouverture de session de l'utilisateur*** **:** `pmartin`**, et vérifier que le suffixe proposé est bien** `@bts.sio`
3. **Cliquer sur** Suivant

### 3 Définir le mot de passe et les options

**Écran suivant :**

1. **Saisir un** ***Mot de passe*** **conforme à la FGPP cible, puis le confirmer**
2. **Cocher « *L'utilisateur doit changer le mot de passe à la prochaine ouverture de session* »**
3. **Laisser décochées les cases « *Le mot de passe n'expire jamais* »**

et « *Le compte est désactivé* »

4. Cliquer sur **Suivant**, puis **Terminer**

#### 4 Rattacher le compte à son groupe

Le compte est créé mais isolé. Double-cliquer dessus, onglet Membre de, **Ajouter**, saisir `GGProfs`, valider. Sans cette étape, la FGPP-Staff ne s'appliquera pas (voir la note de la section 3).

**Préférer PowerShell pour la reproductibilité**

La voie graphique est commode pour un compte isolé, mais elle laisse place à l'oubli (case non cochée, groupe non ajouté). Pour une rentrée entière ou pour garantir un résultat identique, préférer les commandes PowerShell ci-dessous, qui rattachent OU et groupe en une seule séquence.

## 5.2 Compte standard en PowerShell

#### 5 Créer un enseignant (`pmartin`)

Le mot de passe est demandé de façon interactive, puis le compte est créé dans `OU=Profs` et ajouté à `GGProfs` :

```
$pwd = Read-Host "Mot de passe initial" -AsSecureString

New-ADUser -Name "Pauline MARTIN" `
    -GivenName "Pauline" -Surname "MARTIN" `
    -SamAccountName "pmartin" `
    -UserPrincipalName "pmartin@bts.sio" `
    -DisplayName "Pauline MARTIN" `
    -Path "OU=Profs,DC=bts,DC=sio" `
    -AccountPassword $pwd `
    -ChangePasswordAtLogon $true `
```

```
    -Enabled $true


Add-ADGroupMember -Identity "GGProfs" -Members "pmartin"
```

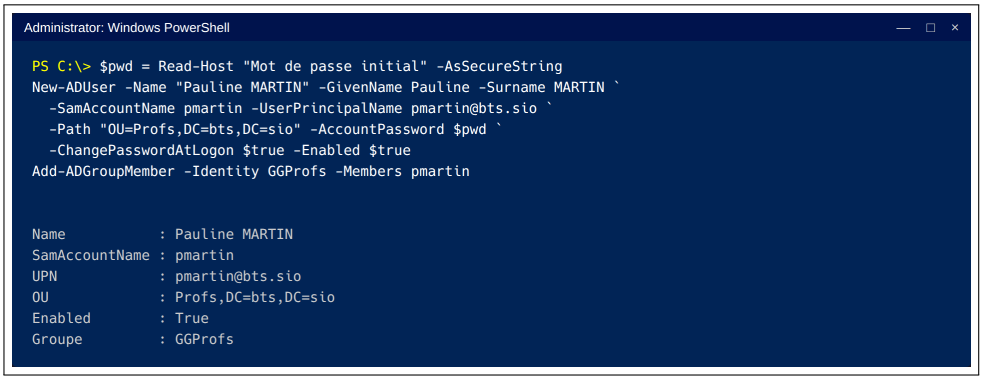


**Figure 1 :** Création du compte enseignant `pmartin` dans `OU=Profs` puis ajout au groupe `GGProfs`.

## 6 Variante étudiant (sdurand)

**Même logique, mais l'OU devient la promotion et le groupe `GGPromoSio1` :**

```
$pwd = Read-Host "Mot de passe initial" -AsSecureString

New-ADUser -Name "Sofiane DURAND" `
    -GivenName "Sofiane" -Surname "DURAND" `
    -SamAccountName "sdurand" `
    -UserPrincipalName "sdurand@bts.sio" `
    -DisplayName "Sofiane DURAND" `
    -Path "OU=Sio1_2025,DC=bts,DC=sio" `
    -AccountPassword $pwd `
    -ChangePasswordAtLogon $true `
    -Enabled $true

Add-ADGroupMember -Identity "GGPromoSio1" -Members "sdurand"
```

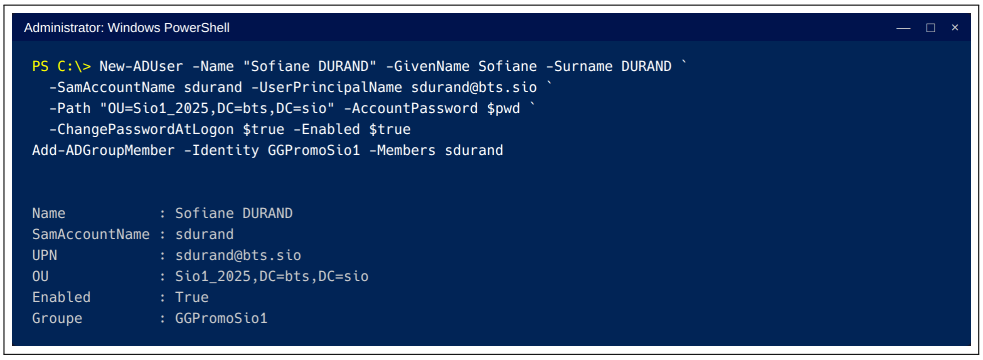


**Figure 2 :** Création du compte étudiant `sdurand` dans `OU=Sio1_2025` et rattachement à `GGPromoSio1`.

### Mot de passe initial communiqué de façon sûre

**Le couple `-ChangePasswordAtLogon $true` impose la redéfinition du mot de passe dès la première connexion. Le mot de passe initial reste donc transitoire ; il doit néanmoins être communiqué à l'utilisateur par un canal qui ne le divulgue pas à des tiers.**

## 5.3 Compte à privilèges (administrateur durci)

### 7 Créer un compte d'administration nominatif (`hpetit`)

**Le compte d'administration de Hugo Petit reçoit un mot de passe d'au moins 16 caractères (exigence FGPP-Admins), il est placé dans « Admins du domaine » et dans *Protected Users*, et il est marqué comme sensible et non délégable :**

```
$pwd = Read-Host "Mot de passe (>= 16 car.)" -AsSecureString

New-ADUser -Name "Hugo PETIT" `
    -GivenName "Hugo" -Surname "PETIT" `
```

```
    -SamAccountName "hpetit" `
    -UserPrincipalName "hpetit@bts.sio" `
    -DisplayName "Hugo PETIT (admin)" `
    -Path "OU=Profs,DC=bts,DC=sio" `
    -AccountPassword $pwd `
    -ChangePasswordAtLogon $true `
    -AccountNotDelegated $true `
    -Enabled $true

Add-ADGroupMember -Identity "Admins du domaine" -Members "hpetit"
Add-ADGroupMember -Identity "Protected Users"   -Members "hpetit"
```

**Le drapeau « sensible, ne peut pas être délégué » peut aussi être positionné après coup :**

```
Set-ADAccountControl -Identity "hpetit" -AccountNotDelegated $true
```


**Figure 3 :** Création du compte d'administration `hpetit` : ajout à « Admins du domaine » et à *Protected Users*, drapeau non délégable.

### Moindre privilège et modèle en tiers

**Un compte d'administration ne doit jamais servir aux usages quotidiens (messagerie, navigation). On applique le modèle en tiers de l'ANSSI : un administrateur dispose d'un compte nominatif standard pour son travail courant et d'un compte dédié, distinct, pour les tâches d'administration. L'appartenance à *Protected***

> ***Users*** **bloque NTLM et limite le TGT à 4 heures : avant l'ajout, vérifier les prérequis détaillés dans MO-AD-010 (poste joint au domaine, accès par nom DNS). Enfin, le drapeau « non délégable » empêche qu'un service tiers ne réutilise les identifiants du compte par délégation Kerberos.**

## 5.4 Compte temporaire (examinateur externe)

### 8 Créer un compte à durée limitée (`nfaure`)

**L'examinatrice Nadia Faure n'intervient que le temps d'une session d'examen. Le compte est créé dans `OU=Profs`, sans aucun groupe métier, avec une date d'expiration et un changement de mot de passe imposé à la première connexion :**

```
$pwd = Read-Host "Mot de passe initial" -AsSecureString

New-ADUser -Name "Nadia FAURE" `
    -GivenName "Nadia" -Surname "FAURE" `
    -SamAccountName "nfaure" `
    -UserPrincipalName "nfaure@bts.sio" `
    -DisplayName "Nadia FAURE (examen)" `
    -Path "OU=Profs,DC=bts,DC=sio" `
    -AccountPassword $pwd `
    -ChangePasswordAtLogon $true `
    -AccountExpirationDate "2026-06-19" `
    -Enabled $true
```

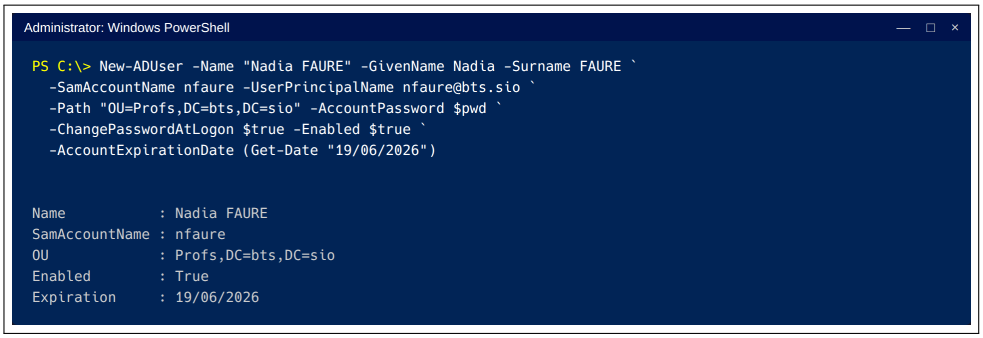


**Figure 4 :** Création du compte examinateur `nfaure` : aucun groupe, expiration datée au 19 juin 2026.

### Gabarit d'un compte examinateur

**Un compte temporaire respecte un gabarit constant : identifiant « initiale + nom », placement dans `OU=Profs` sans appartenance de groupe (donc Default Domain Policy), date d'expiration alignée sur la fin de la session, et changement de mot de passe au premier logon. À l'issue de l'examen, le compte est désactivé puis supprimé (voir la section Rollback). L'absence de groupe est ici volontaire : l'examinateur n'a pas à hériter des droits des enseignants permanents.**

## 5.5 Contrôle de la politique résultante

### 9 Vérifier la FGPP effectivement reçue par chaque compte

**La commande `Get-ADUserResultantPasswordPolicy` retourne la politique réellement appliquée à un compte, en tenant compte de ses appartenances de groupe :**

```
"pmartin","sdurand","hpetit","nfaure" | ForEach-Object {
    $p = Get-ADUserResultantPasswordPolicy -Identity $_
    [PSCustomObject]@{
        Compte = $_
        FGPP   = if ($p) { $p.Name } else { "(Default Domain Policy)" }
        MinLen = if ($p) { $p.MinPasswordLength } else { 10 }
```

```
    }
} | Format-Table -AutoSize
```

**Résultat attendu : `pmartin` reçoit FGPP-Staff (12), `sdurand` reçoit FGPP-Etudiants (10), `hpetit` reçoit FGPP-Admins (16). Pour `nfaure`, la commande ne retourne rien : c'est normal, le compte n'appartient à aucun groupe et relève donc de la Default Domain Policy.**

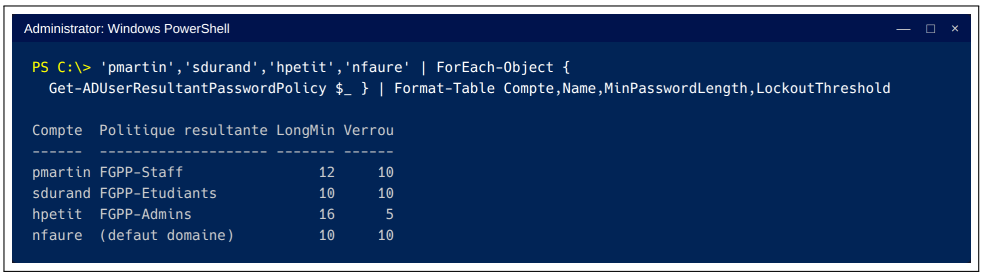


**Figure 5 :** Politique de mot de passe résultante pour les quatre comptes créés : chacun reçoit la FGPP attendue.

### Un retour vide n'est pas une erreur

**`Get-ADUserResultantPasswordPolicy` ne renvoyant rien signifie simplement « aucune FGPP, donc Default Domain Policy ». Pour un compte standard, c'est en revanche le signal d'un oubli d'ajout au groupe : dans ce cas, corriger l'appartenance puis relancer le contrôle.**

# 6 Vérification

**Vérification**

**Pour chaque compte créé, cocher les points suivants :**

- ☐ **Le compte existe : `Get-ADUser <sam>` retourne l'objet**
- ☐ **Il est dans la bonne OU (champ `DistinguishedName`)**
- ☐ **Il appartient au bon groupe : `Get-ADPrincipalGroupMembership <sam>`**
- ☐ **La FGPP reçue est celle attendue (étape 5.5)**
- ☐ **`ChangePasswordAtLogon` est à `True` (changement imposé au 1er logon)**
- ☐ **Pour un compte temporaire : `AccountExpirationDate` est correctement daté**
- ☐ **Pour un compte à privilèges : présence dans *Protected Users* et drapeau `AccountNotDelegated` à `True`**

**Commande de contrôle synthétique :**

```
Get-ADUser -Identity "pmartin" -Properties `
    DistinguishedName, MemberOf, AccountExpirationDate, `
    PasswordExpired, Enabled | Format-List
```

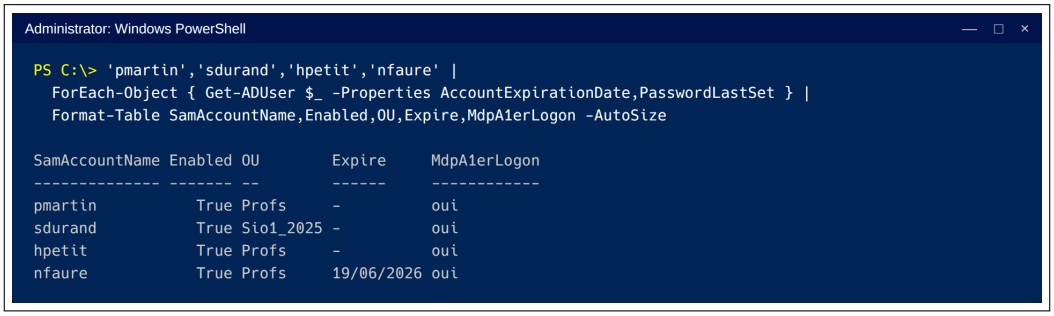


**Figure 6 :** Contrôle final d'un compte créé : OU, appartenances de groupe et options de mot de passe.

# 7 Rollback

10 **Désactiver avant de supprimer**

**La désactivation est réversible et constitue le premier réflexe (compte d'examen terminé, départ d'un agent) :**

```
Disable-ADAccount -Identity "nfaure"
```

11 **Retirer les appartenances sensibles**

**Pour un compte à privilèges, retirer d'abord des groupes critiques avant toute autre opération :**

```
Remove-ADGroupMember -Identity "Admins du domaine" `
    -Members "hpetit" -Confirm:$false
Remove-ADGroupMember -Identity "Protected Users" `
    -Members "hpetit" -Confirm:$false
```

12 **Supprimer le compte**

**Une fois la désactivation validée et les droits retirés, la suppression est définitive :**

```
Remove-ADUser -Identity "nfaure" -Confirm:$false
```

### Préférer la désactivation à la suppression immédiate

**Supprimer un compte détruit son SID : si un objet du même nom est recréé ensuite, il n'hérite pas des permissions de l'ancien. Pour un examinateur susceptible de revenir à la session suivante, la désactivation puis la réactivation à la prochaine échéance sont préférables.**

# 8 Dépannage

| Problème | Solution |
|---|---|
| « Le mot de passe ne satisfait pas aux exigences » | Le mot de passe est plus court que le minimum de la FGPP cible (16 car. pour un admin, 12 pour un enseignant). Reprendre la saisie avec un mot de passe conforme. La FGPP s'applique **dès** que le compte rejoint le groupe, y compris au moment de la création si l'ajout est simultané. |
| Le compte se verrouille très vite | Le seuil de verrouillage est bas pour les comptes à privilèges (5 tentatives en FGPP-Admins). Déverrouiller : `Unlock-ADAccount -Identity <sam>`, puis vérifier qu'aucun service ne rejoue un ancien mot de passe. |
| « Un compte portant ce nom existe déjà » | Le `SamAccountName` ou l'UPN est déjà pris (homonyme, compte non purgé). Contrôler : `Get-ADUser -Filter {SamAccountName -eq "<sam>"}`. Appliquer la règle d'homonymie (ajout d'une lettre du prénom) ou purger l'ancien objet. |
| `New-ADUser` : « accès refusé » | Le compte exécutant n'a pas les droits sur l'OU cible. Utiliser un compte « Admins du domaine » ou vérifier la délégation sur l'OU. |
| La commande échoue via WinRM (double-hop) | La création depuis une session WinRM peut échouer faute de TGT relayable (double-hop NTLM). Créer le compte directement **en local sur DC1**, ou recourir à `Resource-Based Delegation` / CredSSP. |

# 9 Voir aussi

— **MO-AD-003** : Politiques de mots de passe différenciées (FGPP) — définit les trois politiques reçues par les comptes
— **MO-AD-010** : Gestion du groupe Protected Users — prérequis avant d'y ajouter un compte à privilèges
— **MO-AD-007** : Audit périodique des comptes et groupes AD — contrôle des comptes périmés et des appartenances
— **MO-AD-011** : Jonction d'un poste au domaine Active Directory — préalable à l'ouverture de session d'un nouveau compte

# Références

— ANSSI — *Recommandations pour l'administration sécurisée des systèmes d'information reposant sur Active Directory* (modèle en tiers, comptes d'administration dédiés)
— ANSSI — *Administration sécurisée des systèmes d'information — Modèle en tiers* (2023)
— CIS — *Microsoft Windows Server 2022 Benchmark*, section comptes et groupes (2024)
— Microsoft — `New-ADUser` (documentation PowerShell, module ActiveDirectory)
— Audit BTS SIO — Constats et recommandations relatifs à la gestion du cycle de vie des comptes