Mode Opératoire

Audit périodique des comptes et groupes Active Directory

Code :	MO-AD-007
Version :	1.2
Date :	15 avril 2026
Auteur :	Cédric LEGRAND
Classification :	USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	13/04/2026	Création initiale — audit exécuté et validé sur bts.sio
1.1	14/04/2026	Renvoi vers MO-AD-008 pour le traitement des comptes compromis ; note audit 14/04 (5 comptes « toto » traités, 2 comptes compromis forcés au changement de MDP)
1.2	15/04/2026	Ajout § 4.6 *audit krbtgt* (seuils 90/180 j) ; ligne grille “Comptes critiques” ; renvoi MO-AD-002

1 Objet

Ce mode opératoire définit la procédure d'audit périodique des comptes et groupes Active Directory du domaine BTS SIO. L'objectif est de détecter et corriger les dérives de sécurité : comptes machines inactifs, comptes utilisateurs fantômes, appartenance abusive aux groupes privilégiés, attributs de sécurité manquants et indicateurs d'intégrité (`adminCount`).

Cette procédure doit être exécutée **une fois par mois** ou avant toute intervention majeure sur l'annuaire.

2 Champ d'application

Public concerné	Administrateurs de l'infrastructure BTS SIO
Domaine	Active Directory (bts.sio), DC1 (`10.0.112.2`)
Outil	PowerShell (module ActiveDirectory) via WinRM
Authentification	Compte Domain Admin (identifiants dans Vaultwarden)
Durée estimée	20–30 minutes (audit complet + corrections)
Fréquence	Mensuelle ou avant intervention critique

3 Prérequis

Prérequis

— Accès WinRM au contrôleur de domaine DC1 (`10.0.112.2:5985`)
— Compte membre du groupe *Admins du domaine*
— Module PowerShell `ActiveDirectory` (préinstallé sur les DCs)
— Se référer au MO-AD-001 pour la procédure de connexion WinRM

Protected Users et NTLM

Ne pas ajouter le compte utilisé pour WinRM au groupe *Protected Users* : ce groupe désactive l'authentification NTLM, ce qui bloque immédiatement l'accès WinRM. Configurer Kerberos WinRM au préalable si l'on souhaite utiliser Protected Users.

4 Procédure d'audit

4.1 Contrôler les groupes privilégiés

Étape 1 — Vérifier les membres de Domain Admins

Le groupe *Admins du domaine* doit contenir uniquement les comptes strictement nécessaires. Chaque membre doit avoir l'attribut `AccountNotDelegated` activé pour empêcher les attaques par délégation Kerberos.

```
# Lister les DA avec leur statut de delegation
Get-ADGroupMember "Admins du domaine" | ForEach-Object {
    $u = Get-ADUser $_.SamAccountName -Properties `
         AccountNotDelegated, Enabled, LastLogonDate
    [PSCustomObject]@{
        Compte       = $_.SamAccountName
        Actif        = $u.Enabled
        NonDelegable = $u.AccountNotDelegated
        DernierLogin = $u.LastLogonDate
    }
} | Format-Table -AutoSize
```

Résultat attendu (13/04/2026) :

```
Compte    Actif NonDelegable DernierLogin
------    ----- ------------ ------------
fghoua     True         True 30/03/2026
pribeiro   True         True 31/03/2026
mmartinez  True         True 01/04/2026
clegrand   True         True 30/03/2026
```

Actions correctives :

— Si `NonDelegable` est `False` : `Set-ADUser <compte> -AccountNotDelegated $true`

— Si un compte ne devrait pas être DA : le retirer du groupe après validation

Étape 2 — Vérifier que Schema Admins et Enterprise Admins sont vides

Ces deux groupes doivent être **vides** en fonctionnement normal. Ils ne sont utilisés que ponctuellement pour des modifications de schéma ou de forêt.

```
# Schema Admins (SID -518)
Get-ADGroupMember (Get-ADGroup -Filter `
    {SID -like "*-518"}) -ErrorAction SilentlyContinue

# Enterprise Admins (SID -519)
Get-ADGroupMember (Get-ADGroup -Filter `
    {SID -like "*-519"}) -ErrorAction SilentlyContinue
```

Résultat attendu : aucun membre dans les deux groupes.

Action corrective : si un compte ou un groupe est présent, le retirer immédiatement :

```
Remove-ADGroupMember -Identity (Get-ADGroup -Filter `
    {SID -like "*-518"}) -Members "<compte>" -Confirm:$false
```

Cas rencontré le 13/04/2026

Le groupe *Admins du domaine* était niché à l'intérieur de *Administrateurs du schéma*, donnant à tous les DA des privilèges de modification du schéma AD. Le compte `mmartinez` était membre de *Administrateurs de l'entreprise*. Les deux anomalies ont été corrigées.

4.2 Identifier les comptes machines inactifs

Étape 3 — Lister les machines inactives depuis plus de 90 jours

Les comptes machines qui ne se sont pas authentifiés depuis plus de 90 jours correspondent généralement à des postes décommissonnés, remplacés ou en panne.

```
$cutoff = (Get-Date).AddDays(-90)
Get-ADComputer -Filter {
    LastLogonDate -lt $cutoff -and Enabled -eq $true
} -Properties LastLogonDate, OperatingSystem |
    Select Name, LastLogonDate, OperatingSystem |
    Sort LastLogonDate | Format-Table -AutoSize
```

Résultat du 13/04/2026 : 3 machines encore actives (nov 2025 – jan 2026), 7 machines désactivées lors de cet audit.

Action corrective : désactiver les comptes identifiés (ne pas supprimer immédiatement, la corbeille AD est activée) :

```
Set-ADComputer -Identity "<nom>" -Enabled $false `
    -Description "Desactive <date> - audit periodique"
```

Corbeille AD

La corbeille Active Directory est activée sur le domaine bts.sio (depuis le 13/04/2026). Les objets désactivés puis supprimés restent récupérables pendant 180 jours via `Get-ADObject -IncludeDeletedObjects`.

4.3 Détecter les comptes utilisateurs fantômes

Étape 4 — Lister les comptes désactivés et les comptes jamais utilisés

```
# Comptes desactives
Get-ADUser -Filter {Enabled -eq $false} `
    -Properties LastLogonDate, Description |
    Select SamAccountName, Name, LastLogonDate,
           Description | Format-Table -AutoSize

# Comptes jamais connectes (mais actifs)
Get-ADUser -Filter {
    LastLogonDate -notlike "*" -and Enabled -eq $true
} -Properties whenCreated |
    Select SamAccountName, whenCreated |
    Format-Table -AutoSize
```

Interprétation :

— **Comptes désactivés** : vérifier que la désactivation est justifiée (ex. `krbtgt`, `Invité`, comptes de remédiation). Supprimer les comptes de test (ex. `toto`).

— **Comptes actifs jamais connectés** : peut indiquer des comptes étudiants créés récemment, ou des comptes oubliés. Vérifier avec les collègues avant suppression.

— **Comptes templates** : doivent être désactivés et avoir `PasswordNeverExpires = False`.

Étape 5 — Traiter les comptes détectés comme compromis

Lorsqu'un audit par *password spraying* (ou l'analyse des journaux d'authentification) identifie des comptes avec des mots de passe faibles ou connus, deux stratégies sont possibles selon le statut du compte :

— **Compte actif utilisé** : forcer le changement du mot de passe au prochain logon.

— **Compte inactif ou dont la formation est terminée** : désactiver le compte (conformité CIS Control 5.2).

```
# Forcer le changement de MDP au prochain logon
Set-ADUser -Identity "<compte>" `
    -PasswordNeverExpires $false
Set-ADUser -Identity "<compte>" `
    -ChangePasswordAtLogon $true

# Desactiver un compte inactif
Disable-ADAccount -Identity "<compte>"
```

⚠ PasswordNeverExpires bloque ChangePasswordAtLogon

Si un compte a l'attribut `PasswordNeverExpires = True`, la commande `Set-ADUser -ChangePasswordAtLogon $true` échoue avec le message « La modification du mot de passe du compte ne sera pas requise lors de la prochaine ouverture de session ». Désactiver `PasswordNeverExpires` **avant** de forcer le changement.

La procédure complète de rotation des mots de passe critiques (Administrateur, comptes de service, OPNsense, NAS) est documentée dans le **MO-AD-008 — Rotation périodique des mots de passe critiques**.

Audit 14/04/2026 — comptes « toto » et compromis

Lors de l'audit du 14 avril 2026, 5 comptes partageant le mot de passe `[MDP_FAIBLE_ROTATED]` ont été traités :

— **Actifs** : `clegrand` et `a.verrier` – forcés au changement MDP au prochain logon (`PasswordNeverExpires` retiré sur `a.verrier`).

— **Formation OPNsense 2026 terminée** : `jpv`, `aj`, `lg` – désactivés (derniers logons en décembre 2025).

Deux comptes compromis hors toto ont également été traités : `fog` (service FOG Project) et `eval` (compte d'évaluation dont le MDP était le nom du compte). Pour ces deux comptes, `PasswordNeverExpires` a dû être désactivé au préalable pour que `ChangePasswordAtLogon` soit effectif.

4.4 Nettoyer les adminCount orphelins

Étape 6 — Identifier les objets avec adminCount=1

L'attribut `adminCount` est positionné automatiquement par le processus *AdminSDHolder* sur les objets membres de groupes privilégiés. Lorsqu'un objet est retiré d'un groupe privilégié, l'attribut n'est **pas** nettoyé automatiquement : il faut le faire manuellement.

```
# Groupes avec adminCount orphelin
Get-ADGroup -Filter {adminCount -eq 1} `
    -Properties adminCount |
    Select Name, adminCount | Format-Table -AutoSize

# Utilisateurs avec adminCount orphelin
Get-ADUser -Filter {adminCount -eq 1} `
    -Properties adminCount |
    Select SamAccountName, adminCount |
    Format-Table -AutoSize
```

Interprétation :

— Les groupes système (*Administrateurs*, *Admins du domaine*, *Opérateurs de...*) ont légitimement `adminCount=1`.

— Un groupe fonctionnel (ex. `GGProfs`) avec `adminCount=1` est un résidu orphelin : le nettoyer.

— Un utilisateur qui n'est plus DA mais a toujours `adminCount=1` ne reçoit plus les ACL héritées normalement.

Action corrective :

```
# Nettoyer adminCount sur un groupe
Set-ADGroup -Identity "GGProfs" -Clear adminCount

# Nettoyer adminCount sur un utilisateur
Set-ADUser -Identity "<compte>" -Clear adminCount
```

4.5 Vérifier les GPO de sécurité

Étape 7 — Lister les GPO et contrôler leur état

```
Get-GPO -All | Select DisplayName, GpoStatus,
    CreationTime | Sort DisplayName |
    Format-Table -AutoSize
```

Vérifier que les GPO de sécurité suivantes sont présentes et actives :

GPO	Fonction
SEC - Disable LLMNR	Désactive le protocole LLMNR (anti-poisoning)
SEC - Audit Avancé	Audit des objets, privilèges, processus, groupes
SEC - Event Log Size	Journaux System/Application à 256 Mo
Securite - Audit PowerShell	Journalisation ScriptBlock

Résultat du 13/04/2026 : 18 GPO, dont 4 GPO de sécurité actives.

4.6 Auditer la rotation du compte `krbtgt`

Le compte `krbtgt` signe l'ensemble des tickets Kerberos émis par les KDCs du domaine. Une clé non rotatée depuis longtemps expose au risque *Golden Ticket* : un attaquant qui parvient à extraire le hash `krbtgt` peut forger des tickets arbitraires tant que la clé n'a pas été changée deux fois.

Étape 8 — Vérifier la date de dernière rotation

```
$k = Get-ADUser krbtgt -Properties PasswordLastSet, Created
$days = ((Get-Date) - $k.PasswordLastSet).Days

[PSCustomObject]@{
    Compte                  = $k.SamAccountName
    "Date derniere rotation" = $k.PasswordLastSet
    "Jours depuis rotation"  = $days
} | Format-Table -AutoSize

if ($days -gt 90)  { Write-Warning "krbtgt non rote depuis $days jours" }
if ($days -gt 180) { Write-Error   "ALERTE : krbtgt non rote depuis
    $days jours" }
```

Seuils retenus : avertissement à 90 jours, alerte à 180 jours (cible Microsoft / ANSSI). L'objectif est d'anticiper la rotation avant l'expiration de la fenêtre de sécurité, pas d'attendre le jour anniversaire.

Action corrective : si le seuil d'avertissement est franchi, planifier la rotation via **MO-AD-002 — Rotation du compte krbtgt** (double rotation espacée de 12 à 48 heures).

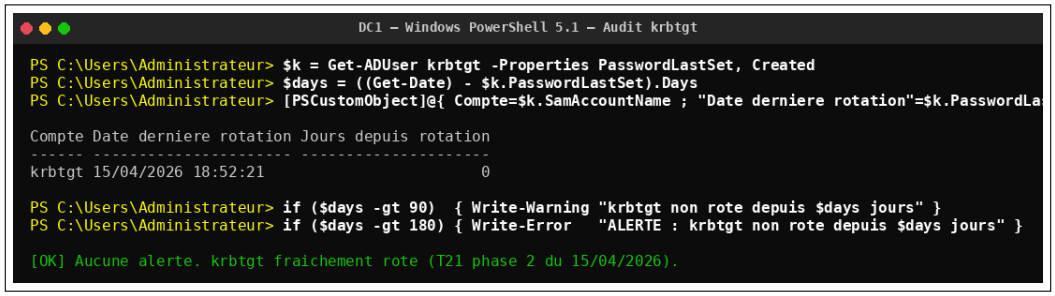

Figure 1 – Sortie de l'audit `krbtgt` après la double rotation du 14–15/04/2026

5 Vérification — Grille récapitulative

Vérification

Cocher chaque point lors de l'audit périodique :

Groupes privilégiés

☐ Domain Admins : nombre de membres justifié (cible : ≤ 5)

☐ Tous les DA ont `AccountNotDelegated = True`

☐ Schema Admins est **vide**

☐ Enterprise Admins est **vide**

Comptes machines

☐ Aucune machine active inactive depuis > 90 jours

☐ Les machines désactivées ont une description horodatée

Comptes utilisateurs

☐ Aucun compte de test actif (toto, test, admin2…)

☐ Les templates sont désactivés avec `PasswordNeverExpires = False`

☐ Les comptes jamais connectés sont justifiés

Comptes critiques

☐ `krbtgt` : `PasswordLastSet` dans les 90 derniers jours (sinon planifier MO-AD-002)

Indicateurs d'intégrité

☐ Aucun `adminCount` orphelin sur des groupes fonctionnels

☐ Les GPO de sécurité sont présentes et actives

6 Dépannage

Problème	Solution
WinRM 401 après ajout Protected Users	Le groupe désactive NTLM. Se connecter via Kerberos (`kinit Administrateur@BTS.SIO` puis `wmiexec.py -k`) pour retirer le compte du groupe.
`Get-ADGroupMember` échoue sur un groupe français	Les noms contenant des apostrophes ou accents posent problème. Utiliser le SID : `Get-ADGroup -Filter {SID -like "*-518"}` pour *Schema Admins*.
Un compte machine désactivé empêche un poste de se connecter	Réactiver le compte : `Set-ADComputer -Identity "<nom>" -Enabled $true`. La corbeille AD est active en cas de suppression accidentelle.
`adminCount` revient à 1 après nettoyage	L'objet est encore membre d'un groupe protégé par *AdminSDHolder*. Vérifier toutes les appartenances : `Get-ADUser <compte> -Properties MemberOf | Select -Expand MemberOf`.