Protected Users : Le Groupe AD le Plus Sous-Utilisé en 2026

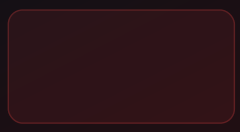
> Protected Users Active Directory : protections automatiques contre Kerberoasting, Pass-the-Hash, délégation. Qui ajouter, qui exclure, comment auditer.

Le groupe **Protected Users** est l'une des fonctionnalités de sécurité Active Directory les plus puissantes introduites avec Windows Server 2012 R2 — et paradoxalement l'une des moins déployées dans les organisations françaises en 2026. Pourtant, son utilisation correcte permet de neutraliser automatiquement plusieurs classes d'attaques qui figurent systématiquement dans les rapports de compromission : Pass-the-Hash, Kerberoasting, interception de credentials WDigest et délégation Kerberos non contrainte. Pour un RSSI ou un architecte sécurité Active Directory, comprendre le groupe Protected Users, c'est comprendre une ligne de défense dont le coût de déploiement est quasi nul mais dont l'impact sur la surface d'attaque Tier 0 est considérable. Ce guide expert détaille les protections automatiques activées, les comptes à inclure en priorité, ceux à ne jamais inclure sans test préalable, les interactions avec Kerberoasting, et les procédures d'audit et de dépannage adaptées aux environnements français soumis aux recommandations ANSSI et au cadre NIS 2. Il s'adresse aux équipes techniques qui gèrent des domaines Active Directory dans les secteurs finance, défense, santé et administration publique.

📋 EN BREF

ATTAQUES ACTIVE DIRECTORY

Protected Users Active Directory : Guide Complet 2026



Historique et prérequis techniques

Microsoft a introduit le groupe Protected Users dans Windows Server 2012 R2 comme réponse directe aux techniques d'attaque documentées par l'équipe du projet *Mimikatz* et popularisées lors des grandes compromissions de l'époque. Avant cette fonctionnalité, les comptes à hauts privilèges Active Directory étaient vulnérables à une série d'attaques basées sur la récupération de credentials en mémoire sur les contrôleurs de domaine ou les postes d'administration.

> ⚡ **Retour terrain**
>
> Dans mes missions de hardening Active Directory, le point le plus sous-estimé est la gestion du groupe 'Opérateurs de compte' et des délégations personnalisées créées au fil des années. Pour un groupe logistique de 1 500 utilisateurs, j'ai trouvé 312 ACL personnalisées dont 89 accordaient des permissions d'écriture sur des attributs sensibles (adminCount, memberOf sur groupes privilégiés) à des comptes d'utilisateurs standards. La dette technique en sécurité AD est souvent invisible jusqu'au premier audit sérieux.

Pour que les protections Protected Users soient pleinement opérationnelles, trois conditions doivent être réunies :

Forest Functional Level (FFL) Windows Server 2012 R2 minimum — sans ce niveau fonctionnel, le groupe existe mais les protections Kerberos côté KDC ne sont pas appliquées.

Au moins un contrôleur de domaine Windows Server 2012 R2 ou supérieur détenant le rôle PDC Emulator — c'est ce DC qui applique les politiques Protected Users lors de l'émission des tickets Kerberos.

Clients Windows 8.1 / Windows Server 2012 R2 ou supérieurs — les protections côté client (suppression du cache WDigest/CredSSP) ne s'appliquent que sur ces versions. Les vieux clients Windows 7 ou XP ne bénéficient pas des protections client, bien que les protections serveur/KDC restent actives.

Le groupe Protected Users est un groupe de sécurité global dans le conteneur `CN=Users,DC=domain,DC=local`. Il est créé automatiquement lors de la promotion du premier DC Windows Server 2012 R2 dans la forêt. Contrairement à un GPO ou à une politique de compte, les protections ne nécessitent aucune configuration supplémentaire : l'appartenance au groupe suffit à déclencher les mécanismes automatiques.

Protections automatiques : tableau de référence

L'appartenance au groupe Protected Users déclenche automatiquement les protections suivantes, sans aucune configuration GPO ni modification de stratégie :

Protection	Comportement sans Protected Users	Comportement avec Protected Users	Impact défensif
Authentification NTLM	Autorisée (LM, NTLMv1, NTLMv2)	**Bloquée complètement** — Kerberos uniquement	Neutralise Pass-the-Hash, NTLM relay, NTLMv1 downgrade
Cache WDigest	Credentials en clair possibles en mémoire LSASS (si WDigest activé)	**WDigest désactivé** pour ce compte sur tous clients 8.1+	Empêche la récupération de password en clair via Mimikatz
Cache CredSSP	Credentials peuvent être délégués/mis en cache via CredSSP	**Délégation CredSSP refusée**	Protège contre l'exfiltration de credentials via RDP/CredSSP
Durée de vie TGT	10 heures par défaut (configurable)	**Réduite à 4 heures** — non renouvellable	Limite la fenêtre d'utilisation d'un TGT volé (Pass-the-Ticket)
Algorithme de chiffrement Kerberos	RC4 (ARCFOUR) autorisé — utilisé par défaut dans certaines configs	**RC4 interdit** — AES-128 ou AES-256 uniquement	Neutralise le Kerberoasting RC4 et les attaques offline sur hashes
Délégation Kerberos	Délégation non contrainte ou contrainte possible	**Toute délégation Kerberos interdite**	Empêche l'usurpation de compte via delegation abuse (Unconstrained/RBCD)
Mise en cache des credentials	Hash NTLM stocké en local sur le poste (pour logon offline)	**Aucun cache de credentials locaux**	Pas de compromission possible via extraction du SAM ou LSASS offline

Ces sept protections s'appliquent **automatiquement et sans GPO** dès que le compte est membre du groupe. Elles opèrent à deux niveaux : le KDC (sur le PDC Emulator) pour les protections Kerberos, et le système client Windows 8.1+ pour les protections mémoire.

Qui ajouter dans Protected Users : comptes prioritaires

La stratégie optimale consiste à appliquer Protected Users à tout compte dont la compromission entraînerait une prise de contrôle complète du domaine (Tier 0) ou des systèmes critiques (Tier 1). Voici les catégories à prioriser :

Comptes Tier 0 — Priorité absolue

Domain Admins — Membres du groupe DA disposent des droits les plus étendus sur le domaine. Aucun compte DA ne devrait rester hors de Protected Users en 2026.

Enterprise Admins — Droits sur toute la forêt AD. Comptes rares mais critiques.

Schema Admins — Peuvent modifier le schéma AD. Doivent être dans Protected Users et désactivés quand non utilisés.

Administrateurs des contrôleurs de domaine — Tout compte avec des droits d'administration locaux sur un DC est de facto Tier 0.

Comptes Break Glass (Emergency Access) — Ces comptes d'urgence doivent être dans Protected Users ET être soumis à un monitoring d'utilisation strict. Leur inclusion empêche un attaquant de les compromettre via Pass-the-Hash même s'il accède au DC.

Comptes de service critiques — Priorité haute

Comptes de service d'annuaire LDAP — Comptes utilisés pour les requêtes LDAP/LDAPS depuis des applications métier, si et seulement si ces applications supportent Kerberos.

Comptes d'administration des systèmes de sauvegarde — Ces comptes accèdent à tout le SI et représentent une cible de choix pour les ransomwares.

Comptes PKI/CA — Les comptes d'administration de l'autorité de certification doivent être protégés au niveau Tier 0.

Comptes utilisateurs à hauts privilèges

Comptes d'administration dédiés (PAW — Privileged Access Workstations) — Comptes admin nommés utilisés uniquement depuis des postes d'administration sécurisés.

Comptes de délégation d'administration Tier 1 — Administrateurs de serveurs sans droits DC, mais dont la compromission permettrait un mouvement latéral significatif.

Qui NE PAS ajouter sans validation préalable

L'erreur la plus fréquente est d'ajouter des comptes de service dans Protected Users sans tester l'impact. Le résultat est systématique : l'application ou le service tombe immédiatement, souvent en production. Les catégories suivantes doivent être exclues ou validées très rigoureusement :

Comptes de service utilisant NTLM

Si une application s'authentifie en NTLM (très fréquent pour des applications legacy, des connecteurs RH, des middlewares anciens), l'ajout dans Protected Users bloque immédiatement toute authentification. La seule solution est de migrer l'application vers Kerberos — ce qui peut représenter un projet de plusieurs mois.

IIS Application Pool Identities

Les identités IIS Application Pool (`IIS APPPOOL\NomPool` ou des comptes de service AD associés) utilisent fréquemment NTLM pour l'authentification Windows intégrée. L'ajout dans Protected Users provoquera des erreurs HTTP 401 en cascade pour tous les utilisateurs de l'application.

Comptes SQL Server Service

Les comptes de service SQL Server peuvent utiliser NTLM pour les connexions Windows Authentication depuis des clients qui ne supportent pas le SPN Kerberos. Avant tout ajout, vérifier que les SPNs Kerberos sont correctement configurés (`setspn -L <compte>`) et tester sur un environnement de qualification.

Comptes avec délégation Kerberos contrainte (KCD)

Si un compte de service est configuré avec la délégation Kerberos contrainte (*Kerberos Constrained Delegation* ou *Resource-Based Constrained Delegation*), l'ajout dans Protected Users désactivera cette délégation. Les scénarios d'authentification en double-hop Kerberos cesseront de fonctionner. C'est particulièrement critique pour SharePoint, Exchange et les applications utilisant Kerberos CDP.

Comptes de service sMSA / gMSA

Les *Managed Service Accounts* (sMSA) et *Group Managed Service Accounts* (gMSA) ne peuvent pas être membres de Protected Users — cette restriction est documentée par Microsoft. En revanche, les gMSA bénéficient déjà de protections équivalentes sur les credentials (rotation automatique, pas de password connu).

Comptes utilisateurs sur clients Windows 7 / Windows Server 2008

Sur ces vieilles versions, les protections client (WDigest, CredSSP) ne s'appliquent pas. Les protections KDC s'appliquent, mais l'authentification peut échouer si le client tente une authentification NTLM en fallback.

Interaction avec Kerberoasting : une défense majeure

Le Kerberoasting est une technique d'attaque qui consiste à demander un ticket de service Kerberos (TGS) pour un compte de service Active Directory, puis à tenter de cracker le hash offline. L'efficacité de cette attaque dépend directement de l'algorithme de chiffrement utilisé pour le ticket : **RC4 (ARCFOUR) est crackable en quelques heures sur un GPU moderne, AES-256 résiste bien mieux**.

Pour les membres de Protected Users, le KDC refuse d'émettre des tickets Kerberos chiffrés en RC4. Tous les tickets sont forcés en AES-128 ou AES-256. Pour un attaquant qui tente le Kerberoasting contre un compte dans Protected Users :

Le TGS obtenu est chiffré en AES-256, non en RC4.

Le crack offline devient exponentiellement plus difficile (AES-256 vs RC4 : plusieurs ordres de grandeur de différence sur le temps de crack).

Si le mot de passe du compte est robuste (20+ caractères), le crack AES-256 devient statistiquement infaisable avec les ressources GPU actuellement disponibles.

Cette protection est particulièrement pertinente pour les comptes de service Tier 0 ou Tier 1 qui ont des SPNs enregistrés — comptes qui sont des cibles naturelles du Kerberoasting. En combinant Protected Users (force AES) et des mots de passe longs générés aléatoirement (ou gMSA qui le fait automatiquement), vous neutralisez pratiquement le Kerberoasting sur les comptes les plus sensibles.

Note importante : la protection anti-Kerberoasting de Protected Users ne s'applique que si le DC PDC Emulator est Windows Server 2012 R2+ et que le FFL est à 2012 R2+. Dans les forêts mixtes avec d'anciens DCs, la protection peut ne pas s'appliquer selon quel DC traite la demande TGS.

Impact sur les principales techniques d'attaque

Pass-the-Hash (PtH) — Neutralisé

Le Pass-the-Hash exploite le fait qu'NTLM accepte le hash du mot de passe directement comme preuve d'authentification, sans nécessiter le mot de passe en clair. Pour un compte dans Protected Users, NTLM est intégralement désactivé : même si un attaquant dispose du hash NTLM du compte (obtenu via Mimikatz, DCSync, ou dump du fichier NTDS.dit), il ne peut pas l'utiliser pour s'authentifier sur un service NTLM. La tentative échoue au niveau du protocole.

Pass-the-Ticket (PtT) — Impact réduit

Le Pass-the-Ticket consiste à voler un ticket Kerberos TGT en mémoire (via Mimikatz/Rubeus) et à le réutiliser. Protected Users réduit la durée de vie du TGT à 4 heures (non renouvellable). Un TGT volé perd sa validité après 4h maximum. Combiné avec une surveillance des événements d'authentification anormaux (ID 4768, 4769), la fenêtre d'exploitation est significativement réduite.

WDigest / Credentials en mémoire — Neutralisé

WDigest est un ancien protocole d'authentification qui stockait les credentials en clair en mémoire LSASS sur les systèmes Windows XP/Vista/7. Même si WDigest est officiellement désactivé depuis Windows 8.1/2012R2, des attaquants peuvent le réactiver via registre et attendre qu'un utilisateur se reconnecte. Pour les membres de Protected Users sur des clients Windows 8.1+, WDigest est désactivé de force et ne peut pas être réactivé pour ce compte.

Delegation Abuse (Unconstrained / RBCD) — Neutralisé

Les attaques basées sur la délégation Kerberos (unconstrained delegation, Resource-Based Constrained Delegation) permettent à un attaquant qui contrôle un compte avec délégation de se faire passer pour d'autres utilisateurs. Protected Users interdit toute forme de délégation pour ses

membres : même si un attaquant configure une délégation sur un autre compte pour cibler un compte Protected Users, ce dernier ne sera pas délégué.

Silver Ticket — Partiellement atténué

Un Silver Ticket est un faux ticket de service TGS forgé par un attaquant qui dispose du hash Kerberos d'un compte de service. Protected Users n'empêche pas directement la création de Silver Tickets (qui ne passent pas par le KDC), mais force l'utilisation d'AES-256, rendant la forge plus difficile si l'attaquant ne dispose que du hash RC4.

Audit : identifier les comptes à protéger et l'état actuel

Avant toute modification, un audit complet de l'état actuel du groupe Protected Users et des comptes à hauts privilèges est indispensable. Voici la méthodologie en quatre étapes :

Étape 1 : Lister les membres actuels de Protected Users

```
 # Voir tous les membres du groupe Protected Users
Get-ADGroupMember -Identity "Protected Users" -Recursive |
    Select Name, SamAccountName, ObjectClass | Sort Name
```

Étape 2 : Identifier les comptes Tier 0 non protégés

```
 # Identifier les comptes Domain Admins PAS dans Protected Users
$da = Get-ADGroupMember "Domain Admins" -Recursive
$pu = Get-ADGroupMember "Protected Users" -Recursive
$da | Where { $_.SamAccountName -notin $pu.SamAccountName } | Select Name, SamAccountName
```

Ce script produit la liste des comptes Domain Admins qui devraient être dans Protected Users mais ne l'ont pas encore été ajoutés. En environnement bien géré, cette liste devrait être vide ou limitée aux comptes de service légitimement exclus.

Étape 3 : Audit des comptes avec délégation dans Protected Users (incohérence)

```
 # Détecter les comptes Protected Users avec délégation configurée (configuration contradictoire)
$pu = Get-ADGroupMember "Protected Users" -Recursive
foreach ($member in $pu) {
    $user = Get-ADUser $member.SamAccountName -Properties TrustedForDelegation,
            TrustedToAuthForDelegation, msDS-AllowedToDelegateTo
    if ($user.TrustedForDelegation -or $user.TrustedToAuthForDelegation -or
        $user.'msDS-AllowedToDelegateTo') {
        Write-Warning "INCOHÉRENCE: $($user.SamAccountName) est dans Protected Users ET a une dél
    }
}
```

Étape 4 : Vérifier les protections actives pour un compte spécifique

```
 # Vérifier si un compte est dans Protected Users
Get-ADUser -Identity "admindc01" -Properties MemberOf |
    Select -Expand MemberOf | Where { $_ -like "*Protected Users*" }

# Ajouter un compte à Protected Users
Add-ADGroupMember -Identity "Protected Users" -Members "AdminTier0","SuperAdmin"
```

PowerShell : commandes essentielles de gestion

```
 # Voir tous les membres du groupe Protected Users
Get-ADGroupMember -Identity "Protected Users" -Recursive |
    Select Name, SamAccountName, ObjectClass | Sort Name

# Ajouter un compte à Protected Users
Add-ADGroupMember -Identity "Protected Users" -Members "AdminTier0","SuperAdmin"

# Vérifier les protections actives pour un compte
Get-ADUser -Identity "admindc01" -Properties MemberOf |
    Select -Expand MemberOf | Where { $_ -like "*Protected Users*" }

# Identifier les comptes Domain Admins PAS dans Protected Users
$da = Get-ADGroupMember "Domain Admins" -Recursive
$pu = Get-ADGroupMember "Protected Users" -Recursive
$da | Where { $_.SamAccountName -notin $pu.SamAccountName } | Select Name, SamAccountName

# Tester si NTLM est bien bloqué (depuis client)
Test-NetConnection -ComputerName "dc01" -Port 445
# L'authentification NTLM devrait échouer pour un membre de Protected Users

# Audit GPO : forcer les paramètres de Protected Users
Get-ADDefaultDomainPasswordPolicy | Select LockoutDuration, MaxPasswordAge

# Identifier les comptes de service avec SPN (cibles potentielles Kerberoasting)
Get-ADUser -Filter {ServicePrincipalName -ne "$null"} -Properties ServicePrincipalName,
    MemberOf | Where { ($_.MemberOf -join "") -notlike "*Protected Users*" } |
    Select SamAccountName, ServicePrincipalName

# Exporter la liste complète pour audit sécurité
Get-ADGroupMember "Protected Users" -Recursive |
    Get-ADUser -Properties PasswordLastSet, LastLogonDate, Enabled |
    Select SamAccountName, Enabled, PasswordLastSet, LastLogonDate |
    Export-Csv -Path "C:\Audit\ProtectedUsers-$(Get-Date -f yyyyMMdd).csv" -Encoding UTF8
```

Dépannage : que faire quand un service ou compte casse

L'ajout d'un compte dans Protected Users sans validation préalable est la première cause de coupures de service lors des projets de durcissement AD. Voici les scénarios les plus fréquents et leurs solutions :

Scénario 1 : Authentification NTLM échoue après ajout

Symptôme : L'utilisateur ne peut plus se connecter à certaines applications. Les logs montrent des erreurs NTLM 0xC000006D ou NTStatus ACCESS_DENIED.

Diagnostic : Vérifier si l'application utilise NTLM. Activer l'audit NTLM (`Security Settings > Local Policies > Security Options > Network Security: Restrict NTLM`) et capturer les événements ID 8001/8002/8004 dans les logs NTLM opérationnels.

Solution immédiate : Retirer le compte de Protected Users (`Remove-ADGroupMember -Identity "Protected Users" -Members "CompteProblematique"`). Puis planifier la migration de l'application vers Kerberos avant de ré-ajouter.

Scénario 2 : Kerberos échoue — "The encryption type requested is not supported"

Symptôme : Erreur Kerberos KDC_ERR_ETYPE_NOSUPP ou événement ID 4769 avec failure code 0x27.

Cause : Le serveur ou le client ne supporte pas AES-128/256, seulement RC4. Protected Users force AES et le client ou le service ne peut pas négocier.

Solution : Vérifier que les attributs `msDS-SupportedEncryptionTypes` du compte de service cible incluent AES (valeur 0x18 = AES-128 + AES-256). Mettre à jour avec : `Set-ADUser -Identity "SvcAccount" -KerberosEncryptionType AES128,AES256` .

Scénario 3 : Expiration TGT après 4h — sessions coupées

Symptôme : Des sessions longues (RDP, sessions applicatives) sont coupées toutes les 4 heures pour les membres de Protected Users.

Cause : La durée de vie du TGT est réduite à 4h non renouvelable. Les applications qui maintiennent des sessions longues sans re-authentification sont impactées.

Solution : Ce comportement est intentionnel. Configurer les applications pour re-s'authentifier toutes les 4h (recommandé) ou exclure les comptes d'administration interactive de Protected Users si les sessions longues sont opérationnellement nécessaires (déconseillé).

Scénario 4 : Logon offline impossible

Symptôme : Un administrateur en déplacement ne peut pas se connecter à son poste sans réseau.

Cause : Protected Users désactive le cache de credentials locaux. Aucun hash n'est stocké sur le poste pour l'authentification offline.

Solution : Les comptes d'administration devraient utiliser des PAW (Privileged Access Workstations) toujours connectées au réseau d'entreprise (via VPN obligatoire). L'authentification offline pour un compte Tier 0 est une mauvaise pratique indépendamment de Protected Users.

Comparaison et complémentarité avec d'autres mécanismes

Protected Users vs Authentication Silos

Les Authentication Policy Silos (introduits en même temps que Protected Users dans Windows Server 2012 R2) permettent d'aller encore plus loin : ils restreignent non seulement comment un compte s'authentifie, mais aussi depuis quels équipements. Un compte Tier 0 peut être configuré pour ne pouvoir s'authentifier que depuis les PAWs désignées. Protected Users et Authentication Silos sont complémentaires — Protected Users applique les restrictions d'authentification

automatiquement, les Silos ajoutent la restriction d'origine (quel poste peut faire l'authentification).

Fonctionnalité	Protected Users	Authentication Silos
Configuration requise	Aucune (appartenance au groupe)	Création de politique + assignation
Restriction de protocole	Oui (NTLM, WDigest, CredSSP)	Oui (via politique)
Restriction de poste source	Non	Oui — seuls les devices autorisés
Granularité	Binaire (dans/hors groupe)	Fine (par compte, par device)
Idéal pour	Déploiement rapide Tier 0	Architecture PAM complète

Protected Users vs LAPS

LAPS (Local Administrator Password Solution) gère les mots de passe des comptes administrateurs locaux des postes Windows. Protected Users protège les comptes de domaine. Ces deux mécanismes opèrent sur des périmètres différents et sont 100% complémentaires : LAPS empêche le mouvement latéral via les comptes locaux, Protected Users protège les comptes de domaine contre les attaques d'authentification. Dans un modèle de défense en profondeur, les deux doivent être déployés.

Protected Users vs Credential Guard

Credential Guard (disponible depuis Windows 10 Entreprise / Windows Server 2016) protège les credentials en mémoire LSASS en les isolant dans un environnement Hyper-V virtualisé (VBS — Virtualization Based Security). Comparaison :

Protected Users agit au niveau du protocole réseau (côté KDC et côté client) — il empêche certains protocoles d'être utilisés du tout.

Credential Guard agit au niveau de la mémoire — il protège les credentials même si Mimikatz tourne avec des droits SYSTEM, car les credentials sont dans un enclave VBS inaccessible depuis l'OS principal.

Les deux se complètent : Protected Users empêche NTLM à la source, Credential Guard protège les tickets Kerberos stockés en mémoire.

Recommandation de déploiement combiné

Couche de protection	Mécanisme	Priorité
Protocole d'authentification	Protected Users (Tier 0)	Immédiate
Restriction de poste source	Authentication Silos (PAW)	Court terme (1-3 mois)
Mots de passe locaux	LAPS v2 (Windows LAPS)	Immédiate
Mémoire LSASS	Credential Guard (VBS)	Court terme
Segmentation Tier	Tiering Model AD	Moyen terme (3-12 mois)

Checklist de déploiement et recommandations ANSSI

L'ANSSI, dans son guide "Recommandations de sécurité relatives à Active Directory" et dans les recommandations associées au *Tiering Model*, recommande explicitement l'utilisation du groupe Protected Users pour tous les comptes Tier 0. Pour les organisations soumises à NIS 2 (opérateurs de services essentiels, fournisseurs de services numériques), le durcissement AD incluant Protected Users fait partie des mesures techniques attendues dans la catégorie "gestion des accès à privilèges".

Pour les secteurs finance (DORA), défense (qualification SecNumCloud) et santé (HDS), les audits de conformité incluent désormais systématiquement la vérification de l'utilisation de Protected Users pour les comptes administrateurs de domaine.

À RETENIR

Checklist Protected Users — Déploiement sécurisé

☐ Vérifier le Forest Functional Level (2012 R2 minimum)

☐ Identifier le PDC Emulator et confirmer qu'il est Windows Server 2012 R2+

☐ Lister tous les comptes Tier 0 (DA, EA, Schema Admins, admins DC)

☐ Identifier les comptes de service avec SPN (risque Kerberoasting)

☐ Tester l'ajout sur un compte de test en environnement de validation

☐ Auditer les applications utilisant NTLM avant ajout des comptes de service

☐ Documenter les comptes exclus de Protected Users et la raison d'exclusion

☐ Ajouter les comptes DA en production — valider les authentifications

☐ Configurer le monitoring des événements 4768/4769/4770/4776 (Kerberos + NTLM)

☐ Planifier un audit trimestriel des membres du groupe Protected Users

☐ Combiner avec LAPS, Credential Guard et Authentication Silos

☐ Documenter dans le DPIA/registre de traitement si applicable (NIS 2)

FAQ — Questions fréquentes sur Protected Users

Quelles protections Protected Users active-t-il automatiquement ?

Le groupe Protected Users active automatiquement sept protections sans aucune configuration GPO supplémentaire : désactivation complète de NTLM (Kerberos uniquement), suppression du cache WDigest, interdiction de la délégation CredSSP, réduction du TGT Kerberos à 4 heures non renouvelables, interdiction du chiffrement RC4 (AES-128/256 uniquement), interdiction de toute délégation Kerberos (contrainte ou non), et suppression du cache local de credentials. Ces protections s'appliquent dès l'appartenance au groupe, à condition que le PDC Emulator soit Windows Server 2012 R2 ou supérieur.

Peut-on ajouter les comptes de service dans Protected Users ?

Oui, mais avec précaution et après validation en environnement de test. Les comptes de service peuvent être ajoutés dans Protected Users uniquement s'ils satisfont trois conditions : ils ne doivent pas utiliser NTLM pour l'authentification, ils ne doivent pas avoir de délégation

Kerberos configurée, et les applications associées doivent supporter AES-128/256 (pas RC4 uniquement). Les gMSA (Group Managed Service Accounts) ne peuvent pas être membres de Protected Users mais disposent de protections équivalentes sur les credentials. Les comptes IIS AppPool, SQL Service et tout compte avec délégation Kerberos contrainte sont généralement à exclure.

Protected Users désactive-t-il NTLM complètement ?

Protected Users désactive NTLM uniquement pour les membres du groupe — pas pour l'ensemble du domaine. Un compte dans Protected Users ne peut plus utiliser NTLM pour s'authentifier, quelle que soit la version NTLM (LM, NTLMv1, NTLMv2). La désactivation est totale et ne peut pas être outrepassée par une politique GPO. Elle s'applique même si le serveur cible accepte NTLM. Pour désactiver NTLM à l'échelle du domaine (recommandation ANSSI avancée), il faut utiliser des GPO "Restrict NTLM" en complément.

Quelle est la durée de vie du TGT Kerberos dans Protected Users ?

Pour les membres de Protected Users, la durée de vie du TGT Kerberos est systématiquement réduite à 4 heures, non renouvelable. Cette valeur est fixe et ne peut pas être modifiée via une politique de compte ou un GPO — elle est imposée par le KDC pour tous les membres du groupe. Après 4 heures, l'utilisateur ou le service doit obtenir un nouveau TGT en se réauthentifiant. Cette limitation impacte les sessions longues (RDP, sessions applicatives) qui doivent être configurées pour gérer ce renouvellement.

Comment récupérer l'accès si un compte Protected Users ne peut plus s'authentifier ?

La procédure de récupération est simple mais doit être réalisée avec un compte qui n'est pas dans Protected Users : exécuter `Remove-ADGroupMember -Identity "Protected Users" -Members "CompteBloqué"` avec un compte Domain Admin hors du groupe, ou utiliser les outils ADUC (Active Directory Users and Computers) pour retirer manuellement le compte du groupe. Le compte retrouvera immédiatement ses capacités d'authentification NTLM — le changement est quasi-instantané (quelques secondes à quelques minutes selon la réplication AD). Si l'accès au

domaine est totalement impossible, utiliser le compte Break Glass ou un compte d'administration locale sur un DC pour se connecter en mode DSRM (Directory Services Restore Mode) et modifier le groupe.

Références et documentation

Microsoft Learn — Sécurité Windows Server

ANSSI — Guide de sécurisation Active Directory

MITRE ATT&CK — Techniques Active Directory