# Administrateurs hors des utilisateurs protégés

ID METSYS : 33  
ID PingCastle : [P-ProtectedUsers](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)  
ID PurplKnight : [Protected Users group not in use](https://www.purple-knight.com/fr/security-indicators/)  
ID ANSSI : [vuln3\_protected\_users](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#protected_users)

Charge de travail : 1 jour  
Difficulté : 2 - Requière quelques connaissances sur l'infrastructure et l'anomalie qu'elle contient

****Description****

Les membres de ce groupe qui s'authentifient auprès d'un contrôleur de domaine ne peuvent pas : s'authentifier avec le protocole NTLM, utiliser les types de chiffrement DES ou RC4 dans la pré-authentification Kerberos, être délégués (délégation non contrainte ou contrainte), et la durée de vie du ticket TGT est limitée à 4 heures.

****Recommandation****

Il faudrait ajouter dans ce groupe tous les comptes à fort privilèges afin de limiter les risques d’exploitation associés à ces comptes

NB : Sur Windows, les « groupes à privilèges » et les « groupes à forts privilèges » sont deux concepts différents en ce qui concerne la gestion des droits et des privilèges des utilisateurs :

• Groupes à privilèges (Privileged Groups) : Les groupes à privilèges sont des groupes de sécurité préconfigurés dans Windows qui sont associés à des privilèges ou des droits spécifiques. Ils sont utilisés pour déléguer certaines tâches administratives à des utilisateurs sans leur accorder un contrôle administratif complet sur le système. Les membres de ces groupes peuvent effectuer des actions spécifiques pour lesquelles les droits sont préalablement définis. Par exemple, le groupe « Administrateurs » a des privilèges étendus pour gérer le système, tandis que le groupe « Opérateurs de sauvegarde » a le droit de gérer les opérations de sauvegarde.

• Groupes à forts privilèges (High-Privilege Groups) : Les groupes à forts privilèges sont des groupes personnalisés créés pour octroyer des privilèges plus élevés à certains utilisateurs. Ces groupes sont généralement créés pour des besoins spécifiques, tels que l'accès à des ressources sensibles ou la gestion de certaines fonctions avancées du système. Les membres de ces groupes bénéficient de privilèges supplémentaires par rapport aux groupes à privilèges standard.

Cependant, ces groupes nécessitent une gestion et une surveillance plus étroites en raison de l'ampleur des droits accordés.