# Comptes non protégés avec l'option « adminCount=1 »

ID METSYS : 48  
ID PurplKnight : [Unprotected accounts with adminCount=1](https://www.purple-knight.com/fr/security-indicators/)

Charge de travail : 0.5 jour  
Difficulté : 1 - Requière quelques connaissances sur l'anomalie

****Description****

Le scénario le plus courant pour ce comportement est lorsque qu'un utilisateur est déplacé d'un groupe privilégié vers un groupe non privilégié et que sa variable « adminCount » n'est pas réinitialisée. Bien que cela soit inoffensif, cela peut poser des problèmes pour les contrôles de sécurité qui surveillent les utilisateurs privilégiés et réduit l'hygiène globale de l'environnement. Dans de rares cas, cela peut également être une preuve qu'un attaquant a tenté de masquer ses traces en supprimant un utilisateur qu'il a utilisé pour compromettre le système.

****Recommandation****

Supprimez l'attribut « adminCount = 1 » de ces utilisateurs. Enquêtez sur les utilisateurs inconnus avec cette caractéristique.