# Utilisateurs ou ordinateurs pouvant prendre le contrôle d'un objet clé du domaine en abusant des autorisations ciblées

ID METSYS : 30  
ID PingCastle : [P-ControlPathIndirectMany](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)

Charge de travail : 2 jours  
Difficulté : 1 - Requière quelques connaissances sur l'anomalie

****Description****

Des délégations en place dans l’AD accordent des permissions trop importantes.

****Recommandation****

Le groupe « Server operators » doit être vidé. Il possède des permissions trop élevées sur des objets critiques de l’annuaire (dont les contrôleurs de domaine). Si besoin, un groupe dédié doit être créé et des permissions accordées seulement sur les OU pertinentes.

Les permissions accordées au groupe Exchange Windows Permissions peuvent être retirées car Exchange n’est pas utilisé dans l’environnement Apicil.

Les chemins de contrôle doivent être analysés (avec PingCastle ou Bloodhound) afin de limiter au maximum le nombre de groupes/comptes pouvant prendre le contrôle d’objets critiques dans l’annuaire (comme les DC et les groupes/comptes à forts privilèges).

Parmi les recommandations :

* Utiliser des comptes d’administration dédiés pour l’AD, distincts des comptes d’administration pour les autres serveurs/systèmes.
* Stocker ces comptes privilégiés dans une OU où aucune délégation n’est présente (seuls les administrateurs du domaine doivent pouvoir créer/modifier ces comptes)