# Principaux non par défaut avec des droits de « DC Sync » sur le domaine

ID METSYS : 8  
ID PurplKnight : [Non-default principals with DC Sync rights on the domain](https://www.purple-knight.com/fr/security-indicators/)  
ID ANSSI : [vuln1\_permissions\_naming\_context](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#permissions_naming_context)

Charge de travail : 2 jours  
Difficulté : 3 - Requière des connaissances avancées sur l'anomalie

****Description****

« DCSync » est une attaque permettant d'accéder aux informations d'identification via cette méthode. Si un attaquant obtient ces privilèges, il est facile de récupérer du matériel d'identification à l'aide d'outils tels que « Mimikatz », pour n'importe quel utilisateur d'un domaine.

****Recommandation****

Assurez-vous qu'il n'y a pas de permissions de réplication inutiles et enquêtez sur les permissions suspectes. Dans certaines situations (par exemple, le regroupement Microsoft PAM), un groupe vide peut apparaître dans les résultats - cela est normal, mais gardez à l'esprit qu'il s'agit d'un groupe très privilégié.