# Politique d’audit sur les contrôleurs de domaine ne récoltant pas d’évènements clés

ID METSYS : 36  
ID PingCastle : [A-AuditDC](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)

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

****Description****

Pour détecter et atténuer une attaque, il est nécessaire de collecter le bon ensemble d'événements. La stratégie d'audit est un compromis entre collecter trop d'événements et en collecter trop peu.

****Recommandation****

Identifier les paramètres d'audit à appliquer et les corriger. Sachez qu'il existe deux endroits pour les paramètres d'audit. Pour une configuration d'audit « Simple » : dans Configuration de l'ordinateur -> Stratégies -> Paramètres Windows -> Paramètres de sécurité -> Stratégies locales -> Stratégies d'audit Pour une configuration d'audit « Avancée » : dans Configuration de l'ordinateur -> Stratégies -> Paramètres Windows -> Paramètres de sécurité -> Configuration avancée de la stratégie d'audit Assurez-vous également que la stratégie d'audit GPO est appliquée à tous les contrôleurs de domaine, car l'objet sous-jacent peut se trouver dans une unité d'organisation où la GPO n'est pas appliquée.