# Contrôleurs de domaine utilisant des pratiques régulières de changement de mot de passe

ID METSYS : 41  
ID PingCastle : [S-PwdLastSet-DC](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)  
ID ANSSI : [vuln1\_password\_change\_dc\_no\_change](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#password_change_dc_no_change)

Charge de travail : 0.5 jour  
Difficulté : 2 - Requière quelques connaissances sur l'infrastructure et l'anomalie qu'elle contient

****Description****

Par défaut, chaque ordinateur change automatiquement son mot de passe tous les 30 jours. C'est également le cas pour les contrôleurs de domaine. Le changement régulier de secrets tels que les mots de passe permet de s'assurer qu'ils ne sont pas utilisés dans des attaques par canaux secondaires. Par exemple, en utilisant « DCSync » pour exporter le hachage du mot de passe d'un contrôleur de domaine, puis en le réutilisant dans une attaque Silver pour créer des tickets Kerberos.

****Recommandation****

Certaines agences de sécurité signalent l'absence de changement de mot de passe comme un indicateur de compromission. Si ce n'est pas le cas, vérifiez les clés de registre suivantes :

* Doit être défini sur 0 ou inexistant : HKLM -> System -> CurrentControlSet -> Services -> Netlogon -> Parameters -> DisablePasswordChange
* Doit être défini sur 30 : HKLM -> System -> CurrentControlSet -> Services -> Netlogon -> Parameters -> MaximumPasswordAge