# Comptes de service administrateurs de domaine

ID METSYS : 16  
ID PingCastle : [P-ServiceDomainAdmin](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)  
ID PurplKnight : [Privileged accounts with a password that never expires](https://www.purple-knight.com/fr/security-indicators/)  
ID ANSSI : [vuln1\_dont\_expire\_priv](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#dont_expire_priv)

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

****Description****

Les « comptes de service » peuvent représenter un risque de sécurité élevé car leur mot de passe est stocké en texte clair dans la base de données LSA, ce qui peut être facilement exploité à l'aide d'outils tels que « Mimikatz » ou « Cain&Abel ». De plus, leurs mots de passe ne changent pas et peuvent être utilisés dans des attaques de type « Kerberoast ».

****Recommandation****

Les comptes avec des mots de passe qui n'expirent jamais sont généralement des comptes de service. Pour atténuer le risque de sécurité, il est fortement recommandé de réduire les privilèges des « comptes de service », ce qui signifie qu'ils doivent être retirés du groupe « Administrateurs de domaine », tout en veillant à ce que le mot de passe de chaque « compte de service » soit composé d'au moins 20 caractères.