# AES activé sur les relations de confiance

ID METSYS : 44  
ID PingCastle : [T-AlgsAES](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)

Charge de travail : 1 jour  
Difficulté : 3 - Requière des connaissances avancées sur l'anomalie

****Description****

Par défaut, RC4 est utilisé comme algorithme de signature des tickets Kerberos. Si AES est activé sur un domaine et que AES n'est pas activé sur une relation de confiance, les tickets AES ne pourront pas être utilisés sur la relation de confiance. Les tickets Kerberos envoyés à la relation de confiance échoueront ou le domaine de confiance basculera vers NTLM.

Les algorithmes de chiffrement autorisés pour une relation de confiance sont stockés dans un attribut nommé « msDS-SupportedEncryptionTypes ». Si cet attribut n'est pas défini (ou a une valeur de zéro), RC4 sera appliqué par défaut. Sinon, il définit l'algorithme à utiliser pour la signature Kerberos.

****Recommandation****

Attention : il y a une case à cocher dans les propriétés de la relation de confiance intitulée « L'autre domaine prend en charge le chiffrement AES Kerberos ». Si vous activez ce paramètre, AES sera activé mais RC4 sera également désactivé.

La méthode recommandée consiste à activer à la fois RC4 et AES en tant que transition. Cela peut être fait en exécutant la commande suivante :

ksetup /setenctypeattr mondomaine.com RC4-HMAC-MD5 AES128-CTS-HMAC-SHA1-96 AES256-CTS-HMAC-SHA1-96

Ainsi, l'attribut « msDS-SupportedEncryptionTypes » de la relation de confiance sera modifié pour prendre en charge à la fois RC4 et AES.