# Relation de confiance sans filtre SID

ID METSYS : 1  
ID PingCastle : [T-SIDFiltering](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)  
ID PurplKnight : [Outbound forest trust with SID History enabled](https://www.purple-knight.com/fr/security-indicators/)  
ID ANSSI : [vuln1\_trusts\_forest\_sidhistory](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#trusts_forest_sidhistory)

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

****Description****

Le filtrage SID est un mécanisme utilisé pour bloquer les comptes présentant une propriété d'historique SID. L'historique SID est utilisé pour lier un compte existant à un autre compte et peut être utilisé pour propager une compromission via des relations d’approbation. Le filtrage SID pour une confiance de domaine à domaine est appelé quarantaine et est désactivé par défaut. Le filtrage SID pour une forêt est activé par défaut et le désactiver est appelé « activer l'historique SID ».

Une confiance sans filtrage SID signifie soit qu'une migration est en cours, soit que le domaine peut être compromis instantanément via la confiance. La solution consiste à terminer au plus vite la migration en cours et à activer la fonctionnalité de filtrage SID.

****Recommandation****

Si la confiance est une confiance de domaine, vous devriez utiliser « netdom /quarantine » et le définir sur « yes ». Si la confiance est une confiance de forêt, vous devriez utiliser « netdom /enablesidhistory » et le définir sur « no ». N'appliquez pas « /quarantine » à une confiance de forêt : vous romprez la transitivité de la confiance.