# Liaison de canal activée pour LDAPS

ID METSYS : 37  
ID PingCastle : [A-DCLdapsChannelBinding](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)

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

****Description****

LDAPS (par opposition à LDAP) n'autorise pas de signature de message car cette protection est assurée par la couche TLS. Par conséquent, des paquets LDAP falsifiés peuvent être relayés dans un tunnel TLS, devenant ainsi du LDAPS sans aucune protection contre le relais.

Pour éviter cette attaque, une fonctionnalité appelée liaison de canal existe. Elle consiste à transmettre à la couche d'authentification une propriété du canal TLS (généralement un hachage du certificat du serveur) pour lier le canal externe (TLS) et le canal interne (LDAP). Cette protection est également appelée « protection étendue ».

****Recommandation****

Vous devez vous assurer que TOUS les clients LDAPS sont compatibles avec la liaison de canal. Toutes les versions de Windows prises en charge ont été mises à jour depuis mars 2020 pour prendre cela en compte, ainsi que la plupart des clients Unix.