Microsoft LDAP defaults 2020

“LDAP channel binding and LDAP signing provide ways to increase the security of network communications between an Active Directory Domain Services (AD DS) or an Active Directory Lightweight Directory Services (AD LDS) and its clients. There is a vulnerability in the default configuration for Lightweight Directory Access Protocol (LDAP) channel binding and LDAP signing and may expose Active directory domain controllers to elevation of privilege vulnerabilities. “ – Microsoft

Beginning in March 2020, Microsoft has enabled LDAP channel binding and LDAP signing support by default in these products:

- Windows Server 2008 SP2
- Windows 7 SP1
- Windows Server 2008 R2 SP1
- Windows Server 2012
- Windows 8.1
- Windows Server 2012 R2
- Windows 10 1507
- Windows Server 2016
- Windows 10 1607
- Windows 10 1703
- Windows 10 1709
- Windows 10 1803
- Windows 10 1809
- Windows Server 2019
- Windows 10 1903
- Windows 10 1909

This change impacts LDAP communication between the TrueNAS server and the Domain Controllers in the Active Directory domain. This can cause interruptions or connection loss between TrueNAS and the Active Directory. Specifically, any Windows system from the above list that installs the March 2020 update can see this default behavior:

- Channel binding information must be provided from the Windows client to the server.
- Domain Controllers require signing
- Servers and clients require signing

For more details about this change to Windows, please see Microsoft’s article about LDAP Channel Binding and LDAP Signing Requirements.

This Microsoft change to the default behavior has been addressed in the FreeNAS/TrueNAS 11.2-U8 and newer releases. The methods of communicating with the Domain Controller now use strong authentication. The strong authentication methods are either SSL-encrypted transport or signed *sasl_gssapi bind* (Kerberos).

It is strongly recommended to update all TrueNAS (and FreeNAS) systems that use LDAP and/or Active Directory to 11.2-U8, 11.3, or newer TrueNAS versions. This prevents the new Windows security defaults from disrupting your Active Directory connectivity.