InterSystems Official
Pete Greskoff · Feb 27, 2020

February 27, 2020 – Advisory: LDAP Active Directory Connections

Starting in March 2020, Microsoft plans to release a series of security updates that will cause Windows Active Directory (AD) servers to reject unencrypted simple binds. For more details on the changes to Active Directory, see Microsoft ' s Security Advisory ADV190023.

Instances of all InterSystems products using LDAP with Windows AD servers for user login can be impacted if they are not already properly configured to use TLS/SSL. The impact is not limited to instances running on Windows versions. The potential impact exists whether instances perform LDAP authentication directly or via the Delegated Authentication mechanism.

Based on InterSystems testing using updated AD servers with the default security policies, it is recommended that you configure all LDAP AD connections to use TLS/SSL prior to applying the relevant Microsoft patches to your AD servers. See the note at the end of this advisory for guidance on configuration.

Additionally, prior to updating any AD servers, you must install Microsoft patch CVE-2017-8563 on all Windows servers that connect to these AD servers. Otherwise, the AD servers will reject connections from the Windows servers, even if they use TLS/SSL.

If you have any questions regarding this advisory, please contact the Worldwide Response Center .

Note on configuration:

- If you are using LDAP configurations, select the **Use TLS/SSL encryption for LDAP sessions** checkbox, as described in the "Using LDAP" chapter of the *Security Administration Guide*.
- If you are using the **%SYS.LDAP** class, call the **StartTLS()** method, as described in the *Class Reference Documentation*. The **Init()** and **SetOption()** methods are also relevant.

Both LDAP configurations and the **%SYS.LDAP** class must have all certificate(s) necessary to validate the AD server ' s certificate used in the TLS handshake, including the Certificate Authority root certificate and any intermediate certificates. Contact your Windows Active Directory administrator to obtain a copy of the required certificate(s). Install these as appropriate:

- For Windows clients, in the Windows local computer certificate store
- For non-Windows clients, in a file accessible by the instance in PEM format. If exporting the certificate from Windows using the Certificate Export Wizard, this format will be called "Base-64 encoded X.509".

For more information on certificate locations, see the "Using LDAP" chapter of the *Security Administration Guide*

#Alerts #Caché #Ensemble #HealthShare #InterSystems IRIS #InterSystems IRIS for Health #InterSystems Official

Source URL:https://community.intersystems.com/post/february-27-2020-%E2%80%93-advisory-ldap-active-directory-connections