InterSystems Official
David Reche · Mar 2, 2020

Aviso: LDAP Active Directory Connections

Desde marzo de 2020, Microsoft planea lanzar una serie de actualizaciones de seguridad que harán que los servidores Active Directory (AD) de Windows rechacen vínculos de canales no cifrados. Para más detalles de los cambios en Active Directory, pueden consultar el aviso de seguridad de Microsoft: ADV190023.

Las instancias de todos los productos de InterSystems que utilizan LDAP con los servidores Windows AD para el acceso de usuarios, pueden verse afectadas si no están configuradas correctamente para usar TLS/SSL. No solo las instancias ejecutándose en los servidores de Windows pueden verse afectadas. El riesgo potencial existe tanto para instancias que realizan la autenticación LDAP directamente como a través del mecanismo de Autenticación Delegada.

En base a las pruebas de InterSystems usando servidores AD actualizados con las políticas de seguridad estándar, se recomienda configurar todas las conexiones LDAP AD para utilizar TLS/SSL antes de aplicar los pertinentes parches de Microsoft a los servidores AD. Consulten la nota al final de este aviso para obtener ayuda en la configuración.

Además, antes de actualizar cualquier servidor AD, se debe instalar el parche CVE-2017-8563 de Microsoft en todos los servidores Windows que conectan con estos servidores AD. Si no, los servidores AD rechazarán las conexiones desde los servidores de Windows, incluso si usan TLS/SSL.

Para cualquier pregunta relacionada con este aviso, contacten por favor con el Centro de Soporte Internacional.

Nota sobre configuración:

- Si estas usando configuraciones LDAP, selecciona el checkbox de **Use TLS/SSL encryption for LDAP sessions**, tal y como se describe en el capitulo "Using LDAP " de la *Security Administration Guide*.
- Si usas la clase **%SYS.LDAP**, invoca el método **StartTLSs()**, tal y como se describe en la documentación *Class Reference Documentation*. Los métodos **Init()** y **SetOption()** son también relevantes.

Tanto las Configuraciones LDAP como la clase **%SYS.LDAP** deben disponer de todos los certificados necesarios para validar el servidor de AD utilizado en la negociación TLS, incluyendo el Certificado raiz de la Autoridad de Certificación y cualquier certificado intermedio. Contacta con tu administrador de Windows Active Directory para obtener una copia the los certificados requeridos. Instala los mismos según:

- Para clientes Windows, en el almacén de certificados local del computador Windows local
- Para clientes no-Windows, en un fichero accesible por la instancia en formato PEM. Si exportas el certificado desde Windows utilizando el Certificate Export Wizard, el formato correcto es el denominado "Base-64 encoded X.509".

para más información acerca de localización de certificados, mira el capitulo "Using LDAP" de la *Security Administration Guide*

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