¿Cómo verificar si la conexión de su cliente ODBC/JDBC al CIS se cifra?

Contenido

Introducción

¿Este documento describe cómo verificar si la conexión de su ODBC/Java cliente de la conectividad de la base de datos (JDBC) al servidor de información de Cisco (CIS) está cifrada?

¿Cómo verificar si la conexión de su cliente ODBC/JDBC al CIS se cifra?

Si usted ha optado fijar su DSN o JDBC URL con un modo de encripción para su herramienta del cliente, usted puede verificar fácilmente la conexión encriptada.

A la hora del modo de encripción, la conexión utiliza el puerto SSL ODBC/JDBC (puerto bajo +3 HTTP) y agrega +2 al puerto del módulo de escucha del valor por defecto ODBC/JDBC (base +1).

No hay necesidad de especificar el puerto SSL (base+3) usted mismo en el DSN o el URL.

Verifique el uso del puerto SSL:

1. Inhabilite temporalmente el modo del texto claro esa habilitación de los controles del puerto UNencrypted (puerto bajo +1).

    a. En la interfaz de usuario de la configuración del estudio (UI), navegue a esta trayectoria: **Driveres de cliente > comunicaciones > texto claro del server> habilitado** (en el reinicio del servidor)

    b. Cambie esto a “falso” y recomience el servidor para que tome el efecto.

2. Conecte con el CIS con una conexión UNencrypted. Debe ahora fallar puesto que el módulo de escucha NON-SSL está inactivo ahora.

3. Conecte con el CIS con su conexión encriptada y si es acertado, después usted está conectado sobre el puerto SSL (puerto bajo +3).