How-To Library

Informatica

How to Connect to a Microsoft SQL Server Database that Uses Kerberos Authentication in Informatica 10.x

Abstract

You can connect to a Microsoft SQL Server database with Kerberos authentication from PowerCenter. This article describes how you can configure a connection to a Microsoft SQL Server database that uses Kerberos authentication in Informatica 10.x.

Supported Versions

- PowerCenter 10.0.0 - 10.1.1

Table of Contents

Overview

Kerberos is a network authentication protocol that uses tickets to authenticate access to services and nodes in a network. You can use Kerberos to provide mutual authentication between the machine where the PowerCenter Integration Service runs and the Microsoft SQL Server database.

Kerberos uses a Key Distribution Center (KDC) to validate the identities of users and services and to grant tickets to authenticated user and service accounts. In the Kerberos protocol, users and services are known as principals. The KDC has a database of principals and their associated secret keys that are used as proof of identity. Kerberos authentication is built on symmetric-key cryptography.

You can use Kerberos authentication when you connect to relational databases, like Microsoft SQL Server. You can configure Kerberos authentication for a connection to Microsoft SQL Server on the machine where you install the PowerCenter Integration Service. Compared to regular user name and password authentication, Kerberos authentication is more secure because the passwords are not stored locally or sent over the network.

To configure Kerberos authentication for a connection to Microsoft SQL Server, perform the following tasks:

1. Update the system configuration files.
2. Verify and test the Microsoft SQL Server connection from the machine where the PowerCenter Integration Service runs to the Microsoft SQL Server database.
3. Restart the Informatica Services with the Kerberos user.

4. Create the Microsoft SQL Server connection in PowerCenter with Kerberos authentication and run the mapping.

Prerequisites

Before you configure the machine where the PowerCenter Integration Service runs for Kerberos authentication to Microsoft SQL Server database, perform the following tasks:

1. Ensure that the Microsoft SQL Server database and the machine where the PowerCenter Integration Service runs are on the same Kerberos network. Verify that the Kerberos implementation of the network is based on Microsoft Active Directory.
2. Verify with your database administrator that the Microsoft SQL Server database uses Kerberos authentication.
3. Work with your system administrator to verify that the Microsoft SQL Server database user is a valid user in the Microsoft Active Directory domain.
4. Install the SQL Server Native Client 2012 (SNAC) on the machine where the PowerCenter Integration Service runs.
5. Install MIT Kerberos v5 client libraries on the machine where the PowerCenter Integration Service runs.

Step 1. Update the System Configuration Files

Configure the services and hosts file on the machine where the PowerCenter Integration Service runs.

1. Work with your system administrator to get the krb5.conf file, which is the Kerberos configuration file.

   The following example shows the content of the Kerberos configuration file named krb5.conf with the required properties:

```
[libdefaults]
default_realm = AFNIKRB.AFNIDEV.COM
forwardable = true
default_tkt_enctypes = rc4-hmac
udp_preference_limit = 1

[realms]
AFNIKRB.AFNIDEV.COM = {
    admin_server = SMPLKERDC01.AFNIKRB.AFNIDEV.COM
    kdc = SMPLKERDC01.AFNIKRB.AFNIDEV.COM:88
 }

[domain_realm]
afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
.afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
```

2. To configure the Informatica domain to run with Kerberos authentication, perform one of the following steps:

   - Copy the krb5.conf configuration file to the following Informatica directory:
     `<INFA_HOME>/services/shared/security`

     If the domain has multiple nodes, copy the krb5.conf file to the same directory on all the nodes in the domain.
   - Set the KRB5_CONFIG environment variable to store the complete path and file name of the Kerberos configuration file, krb5.conf.
     For example, set the environment variable as follows:

     `KRB5_CONFIG=<INFA_HOME>/services/shared/security/krb5.conf`

     You must set the KRB5_CONFIG environment variable on each machine that runs the PowerCenter Integration Service.

For more information about the Kerberos configuration file, see the Kerberos network authentication documentation.

3. Work with your system administrator to edit the hosts file on the machine where the PowerCenter Integration Service runs based on the sample syntax:

   ```
   <IP address of the machine where the Microsoft SQL Server database runs> <fully qualified domain name of the machine where the Microsoft SQL Server database runs> <alias of machine where the Microsoft SQL Server database runs>
   ```

   ```
   <IP address of the machine where the Microsoft Active Directory Key Distribution Center runs> <fully qualified domain name of the machine where the Microsoft Active Directory KDC runs> <alias of machine where the Microsoft Active Directory KDC runs>
   ```

   For example, the system admin can enter the first line of the syntax as follows:

   ```
   10.65.143.123 myMSSQLdb.afnikrb.afnidev.com myMSSQLdb
   ```

   The system admin can enter the second line of the syntax as follows:

   ```
   10.65.143.111 SMPLKERDC01.AFNIKRB.AFNIDEV.COM myKDC
   ```

   On UNIX machines, the hosts file is present in the following path:

   ```
   /etc/hosts
   ```

   On Windows machines, the hosts file is present in the following path:

   ```
   C:\Windows\System32\drivers\etc
   ```

4. Work with your system administrator to ensure that the etc/services file contains the entry for Kerberos service.

   On UNIX machines, the services file is present in the following path:

   ```
   /etc/services
   ```

   On Windows machines, the hosts file is present in the following path:

   ```
   C:\Windows\System32\drivers\etc
   ```

   For example, the etc/services file contains the Kerberos service entries as follows:

   ```
   kerberos  88/tcp  krb5 kerberos-sec  #Kerberos
   kerberos  88/udp  krb5 kerberos-sec  #Kerberos
   ```

   where kerberos is the service name. 88/tcp or 88/udp is port/protocol. Kerberos service can run on either the tcp or udp protocol.

5. In the command prompt, enter the kdstry command for cleaning up the credential cache:

   ```
   kdstry
   ```

6. Initialize the Kerberos ticket for the Active Directory user who is also a valid user in the Microsoft SQL Server database with the following command:

   ```
   kinit <AD_user>
   ```

7. Enter the klist command to view all the entries present in the credential cache.

   This displays the default principal, the ticket cache, and the ticket validity details.

Alternatively, if the Microsoft SQL Server database uses SSL encryption, install the server SSL certificate using the Microsoft Management Console (MMC). For more information, see step 1 in the following Informatica How-to Library article: How to Configure a Secure Connection to Microsoft SQL Server.

Step 2. Verify the Connection to the Microsoft SQL Server Database

Verify and test the connection to the Microsoft SQL Server database on the machine where the PowerCenter Integration Service runs.

1. To verify the connection to the Microsoft SQL Server database:
   - Install the SQL Server Management Studio (SSMS) on the machine where the PowerCenter Integration Service runs.
   - Install the SQLCMD command line utility to connect to the Microsoft SQL Server database.
2. To test connection to the Microsoft SQL Server Kerberos instance:
   - If you have installed SSMS, you can then attempt to connect to the Microsoft SQL Server Kerberos instance from the SSMS.
   - If you have installed the SQLCMD command line utility, verify the connectivity to Microsoft SQL Server kerberized instance with the following command: `C:\> SQLCMD -S <server_name>`

Step 3. Restart the Informatica Services with the Kerberos User

Ensure that you start the Informatica Services with the same Kerberos user, who is a valid user in the Microsoft SQL Server Kerberos database.

1. Click **Start** > **Run** and enter `services.msc`.
2. Click **OK**.
3. Select **Informatica <version>**.
4. Right-click and select **Properties**.
5. In the Informatica Properties dialog box, navigate to the **Log On** tab and select **This account**.
6. Enter the Kerberos user credentials.
7. Click **Apply**.
8. Click **OK**.
9. Select **Start the service**.

   The Informatica Services start on Windows.
10. Start the PowerCenter Integration Service again that runs on the Windows machine.

Step 4. Configure a Microsoft SQL Server Data Source

The Microsoft SQL Server native connection uses DataDirect SQL Server ODBC driver. You can configure the Microsoft SQL Server data source in different ways based on whether the PowerCenter Integration Service runs on Windows or UNIX.

Configure a Microsoft SQL Server Data Source for Windows

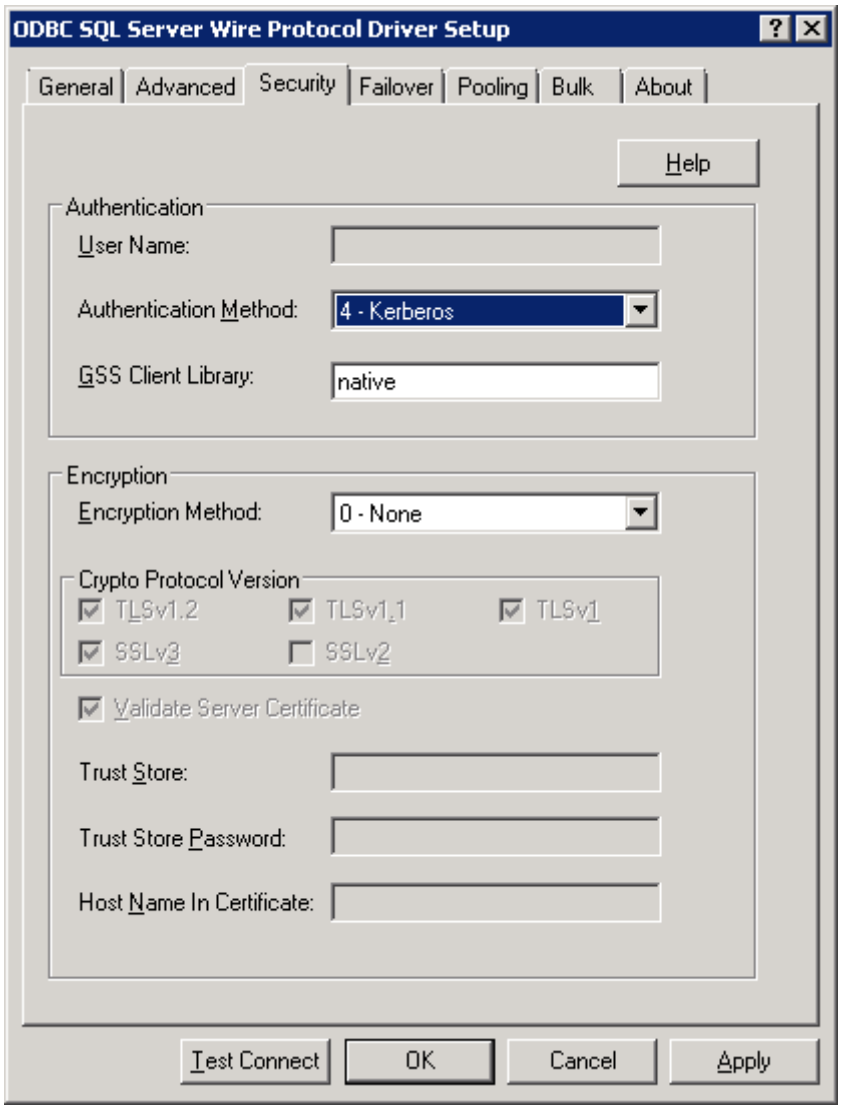
1. Open the Microsoft ODBC Administrator.
2. Go to the system DSN tab.
3. Click **Add**.
4. Select **DataDirect 7.1 New SQL Server Wire Protocol**.
5. Click **Finish**.

6. Enter the data source name.
7. Enter the host name.

   A host name is the machine where you installed the Microsoft SQL Server database.
8. Enter the port number.

   Default is 1433.
9. Enter the Microsoft SQL Server database name.
10. On the security tab of DSN, set the following secure database parameters:

Property	Description
Authentication Method	Authentication method to access Microsoft SQL Server. Specify the authentication method to select 4- Kerberos.
GSS Client Library	An API for programs to access security services. Select native.



Configure a Microsoft SQL Server Data Source on UNIX

1. Set the environment variable ODBCINI to point it to the odbc.ini file path.

   By default, the odbc.ini path is in the following location: `<INFA_HOME>\ODBC7.1\odbc.ini`.
2. Open the odbc.ini file.
3. Under the ODBC Data Sources section of the odbc.ini file, add a data source name with a description.

   For example, you can enter the following data source details in the odbc.ini file:

   ```
   [ODBC Data Sources]
       DSN_SQLSERVER_KERB=SQL Server with Kerberos Authentication
   ```
4. Enter the following properties for the new data source entry in the odbc.ini file:

Property	Description
Driver	Required. Absolute path to the Data Direct New SQL Server ODBC driver. By default, the driver is located at `<INFA_HOME>/ODBC7.1/lib/DWsqls27.so`
Description	Optional. Describes the connection information.
HostName	Required. Name of the machine where you installed the Microsoft SQL Server database.
PortNumber	Required. Port where the Microsoft SQL Server database server listens. Default is 1433.
Database	Required. Name of the Microsoft SQL Server database.
Authentication Method	Required. Authentication method to access Microsoft SQL Server. To enable Kerberos authentication, specify the authentication method as 4.
GSSClient	Required. Location of the Informatica Kerberos libraries.
Domain	Required. Domain administrating both Microsoft SQL Server and the machine that runs the Integration Service.

Sample data source entry:

```
[DSN_SQLSERVER_KERB]
Driver=<Informatica installation directory>/ODBC7.1/lib/DWsqls27.so
Description=SQL Server Connection with Kerberos Authentication
HostName=<hostname of the machine where SQL Server is installed>
PortNumber=<port no>
Database=<database name>
AuthenticationMethod=4
GSSClient=<Informatica installation directory>/server/bin/libgssapi_krb5.so.2
Domain=<The domain administrating both SQL Server and the machine that runs the
Integration Service>
```

Step 5. Test a Microsoft SQL Server Connection to Microsoft SQL Server

You can test the Microsoft SQL Server connection in different ways depending on whether the PowerCenter Integration Service runs on Windows or UNIX.

Test a Microsoft SQL Server Connection to Microsoft SQL Server on Windows

1. On Windows, open Microsoft ODBC Administrator.

2. Select the DSN that you created in "Configure a Microsoft SQL Server Data Source for Windows" on page 5.
3. Click **Configure**.
4. Click **Test Connect**.
5. Enter the valid database user name and password.
6. Click **OK**.

Test a Microsoft SQL Server Connection to Microsoft SQL Server on UNIX

To test connection on UNIX, use the Informatica Global Customer Support toolssgodbc present under the debugtools folder of the Informatica installation directory. Ensure that you have configured the ODBCINI environment variable to use the ssgodbc command.

1. From the command prompt, navigate to the location of the ssgodbc file path.

   The ssgodbc file is in the following directory:

   `<INFA_HOME>/tools/debugtools/ssgodbc/<linux or unix version>`

   For example, you can find the ssgodbc command for Linux 64 bit in the following path: `<INFA_HOME>/tools/debugtools/ssgodbc/linux64/ssgodbc.linux64`
2. Run the ssgodbc command.

   For example, enter the following ssgodbc command:

   ```
   ssgodbc.linux64 -d DSN_SQLSERVER_SSL -u sqluser -p sqlpass123 -v
   ```

   In the example, -d refers to the data source name, -u refers to the database user name, -p refers to the database password, and -v refers to the verbose output.

If the test connection is successful, the command prompt displays the database version and other details. You can close the ssgodbc command manually by pressing CTRL + C.

If the test connection fails, you can review the related error message and edit the connection.

Step 6. Configure a Microsoft SQL Server Connection to Use Kerberos Authentication from the PowerCenter Workflow Manager

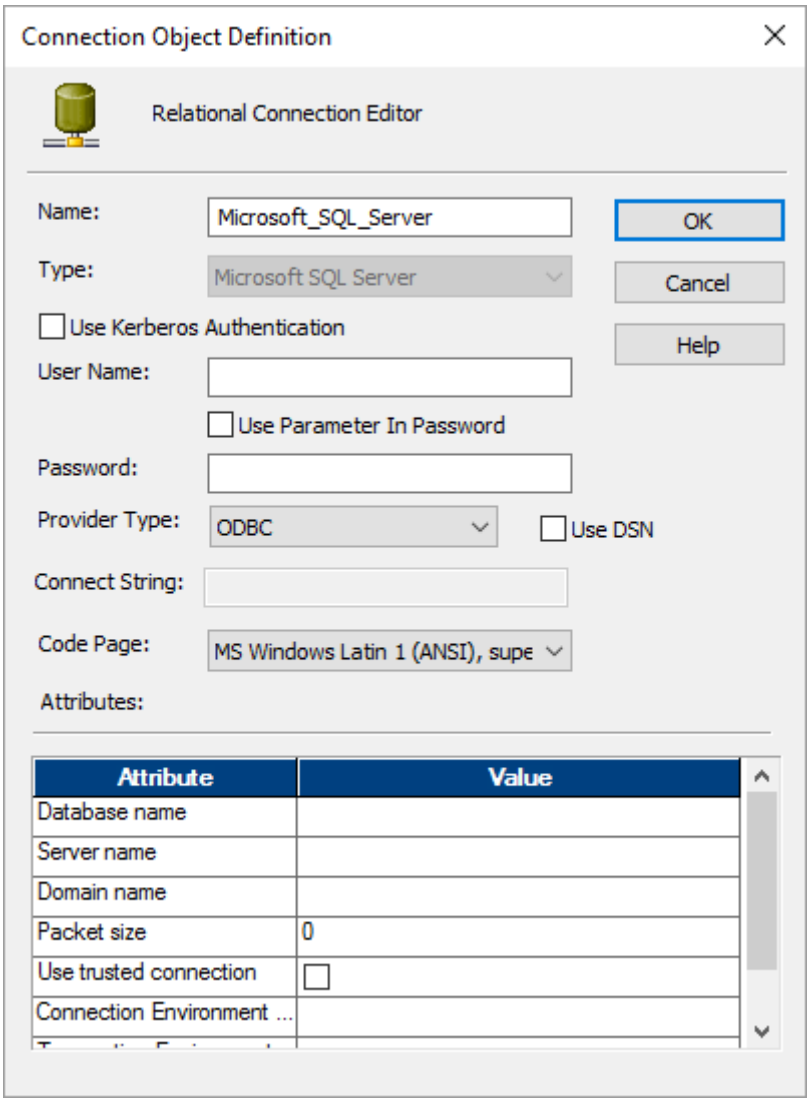
You can select the option to use Kerberos authentication while configuring the Microsoft SQL Server connection from the Workflow Manager.

1. Open the Workflow Manager and log in to the PowerCenter repository.
2. Click **Connections** > **Relational**.

   The **Relational Connection Browser** dialog box appears.
3. Click **New**.

   The **Select Subtype** dialog box appears.
4. To create a connection to a Microsoft SQL Server database, select **MSSQL** from the **Select Subtype** list.
5. Click **OK**.

The **Connection Object Definition** dialog box appears.



6. Select the **Use Kerberos Authentication** option.

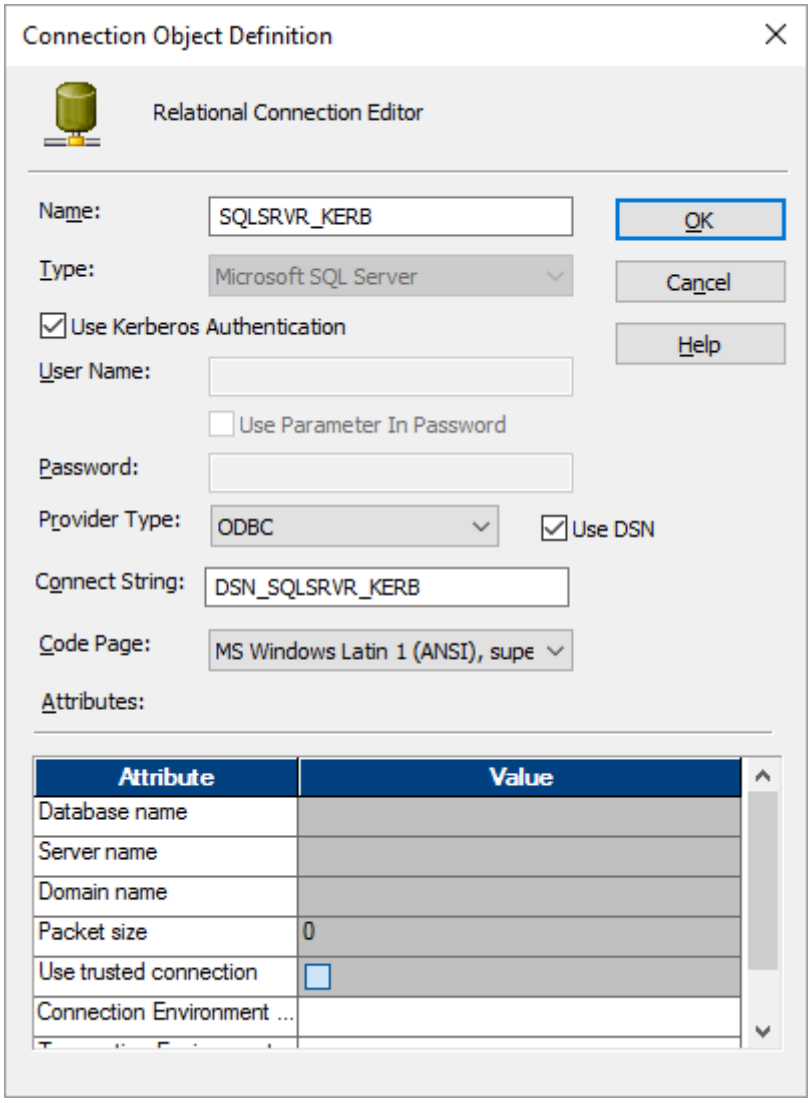
   The **Use Kerberos Authentication** option indicates that the database to connect to runs on a network that uses Kerberos authentication. By selecting this option, you cannot set the user name and password in the connection object. The connection uses the credentials of the user account that runs the session that connect to the database. The user account must have a user principal on the Kerberos network where the database runs.

7. You can create a Microsoft SQL Server connection either by using the DSN or without using the DSN.

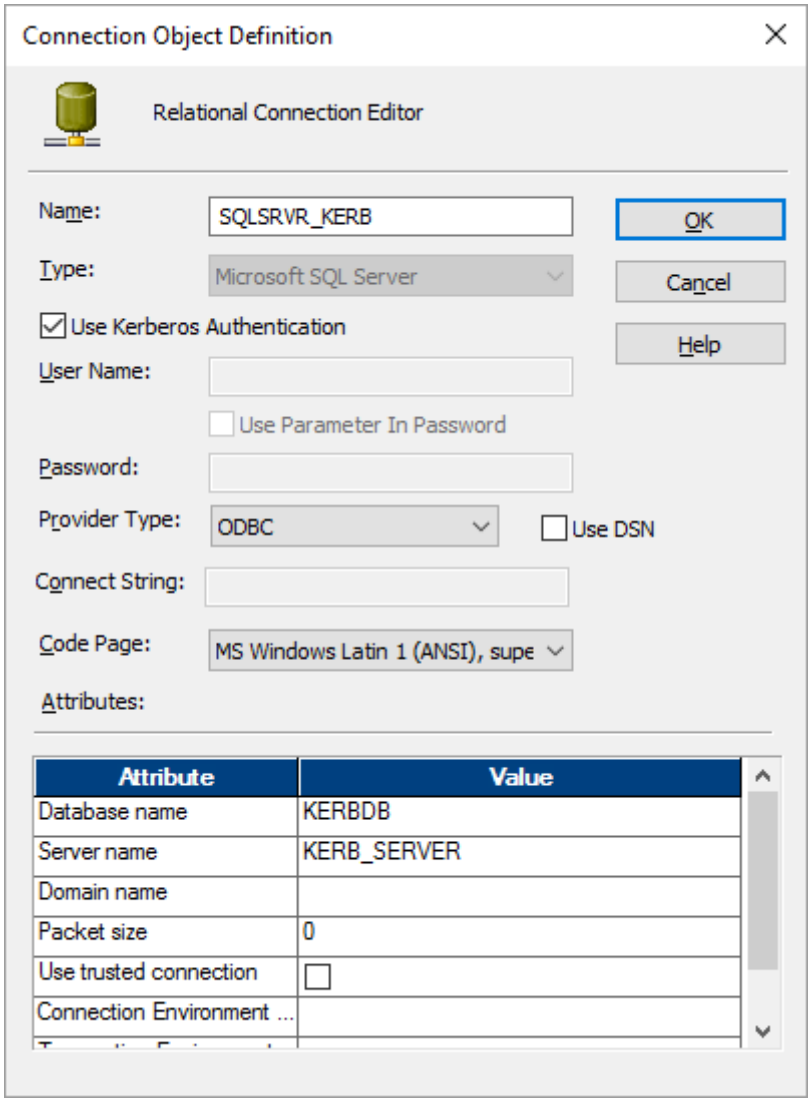
   You can create a connection by using the DSN if you want to specify ODBC driver properties such as AuthenticationMethod and GSSClient. To configure SSL, you must use the DSN option.

   If you do not enable the Use DSN option, you must specify the database name in the connection properties. You can create a connection without using the DSN if you do not want to specify any ODBC driver property.

- If you configure DSN on Windows, enter the **Connect String** attribute. Ensure that the connect string is the data source name that you configure.



- If you do not configure DSN on Windows, enter the **Database name** attribute. Ensure that the server name is the fully qualified domain name of the machine where the Microsoft SQL Server database runs.



- If you configure DSN on Linux, set ODBCINI environment variable to point to the odbc.ini file. Set the following properties for the specified data source:

```
AuthenticationMethod=4
GSSClient= <Informatica installation directory>/server
/bin/libgssapi_krb5.so.2
Domain=<The domain administrating both SQL server and
Informatica server>
```

- If you do not configure DSN on Linux, set ODBCINST environment variable to point to the odbcinst.ini file. Add **GSSClient** property to point to the Informatica Kerberos libraries. Add the following entry under the DataDirect 7.1 SQL Server Wire Protocol section:

```
GSSClient= <Informatica installation directory>/server/bin/libgssapi_krb5.so.2
```

8. Click **OK**.

   The database connection appears in the **Relational Connection Browser** list.

Select the Microsoft SQL Server connection to run the mapping with Kerberos authentication from the Workflow Manager.

Authors

Gurumoorthy N

Sujitha Alexander